ExtremeCloud™ IQ Site Engine v26.11.10 User Guide:

Comprehensive Configuration, Management, and Advanced Network Features

11/2026
26.11.10
PN: 9041348-00 Rev AA
Subject to Change Without Notice



Abstract

This user guide provides detailed instructions for deploying, configuring, and managing ExtremeCloud IQ Site Engine version 26.11.10. The guide covers essential topics such as access requirements, licensing, device management, network monitoring, and policy enforcement. This user guide includes step-by-step procedures for configuring network devices, integrating Access Control, managing ExtremeAnalytics, and utilizing Fabric Connect. The document also outlines the use of various tools, reports, and dashboards to optimize network performance and security. Additionally, this document highlights advanced features like ZTP+ (Zero Touch Provisioning), VLAN management, and fabric services configuration. This user guide is intended for IT professionals with advanced knowledge in network administration and security.

Copyright © 2026 Extreme Networks, Inc. All Rights Reserved.

Legal Notices

Extreme Networks, Inc., on behalf of or through its wholly-owned subsidiary, Enterasys Networks, Inc., reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:
www.extremenetworks.com/company/legal/trademarks/

Contact

If you require assistance, contact Extreme Networks using one of the following methods.

- **Global Technical Assistance Center (GTAC) for Immediate Support**
  - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or 1-603-952-5000. For the Extreme Networks support phone number in your country, visit: www.extremenetworks.com/support/contact
  - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- **GTAC Knowledge** — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- **The Hub** — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- **Support Portal** — Manage cases, downloads, service contracts, product licensing, and training and certifications.

Extreme Networks® Software License Agreement

This Extreme Networks Software License Agreement is an agreement ("Agreement") between You, the end user, and Extreme Networks, Inc. ("Extreme"), on behalf of itself and its Affiliates (as hereinafter defined and including its wholly owned subsidiary, Enterasys Networks, Inc. as well as its other subsidiaries). This Agreement sets forth Your rights and obligations with respect to the Licensed Software and Licensed Materials. BY INSTALLING THE LICENSE KEY FOR THE SOFTWARE ("License Key"), COPYING, OR OTHERWISE USING THE LICENSED SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE LICENSE KEY TO EXTREME OR YOUR DEALER, IF ANY, OR DO NOT USE THE LICENSED SOFTWARE AND CONTACT EXTREME OR YOUR DEALER WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A REFUND. IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT EXTREME, Attn: LegalTeam@extremenetworks.com.

1. DEFINITIONS. "Affiliates" means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. "Server Application" shall refer to the License Key for software installed on one or more of Your servers. "Client Application" shall refer to the application to access the Server Application. "Licensed Materials" shall collectively refer to the licensed software (including the Server Application and Client Application), Firmware, media embodying the software, and the documentation. "Concurrent User" shall refer to any of Your individual employees who You provide access to the Server Application at any one time. "Firmware" refers to any software program or code imbedded in chips or other media. "Licensed Software" refers to the Software and Firmware collectively.
2. TERM. This Agreement is effective from the date on which You install the License Key, use the Licensed Software, or a Concurrent User accesses the Server Application. You may terminate the Agreement at any time by destroying the Licensed Materials, together with all copies, modifications and merged portions in any form. The Agreement and Your license to use the Licensed Materials will also terminate if You fail to comply with any term of condition herein.
3. GRANT OF SOFTWARE LICENSE. Extreme will grant You a non-transferable, non-exclusive license to use the machine-readable form of the Licensed Software and the accompanying documentation if You agree to the terms and conditions of this Agreement. You may install and use the Licensed Software as permitted by the license type purchased as described below in License Types. The license type purchased is specified on the invoice issued to You by Extreme or Your dealer, if any. YOU MAY NOT USE, COPY, OR MODIFY THE LICENSED MATERIALS, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT.

4. LICENSE TYPES.
    - *Single User, Single Computer*. Under the terms of the Single User, Single Computer license, the license granted to You by Extreme when You install the License Key authorizes You to use the Licensed Software on any one, single computer only, or any replacement for that computer, for internal use only. A separate license, under a separate Software License Agreement, is required for any other computer on which You or another individual or employee intend to use the Licensed Software. A separate license under a separate Software License Agreement is also required if You wish to use a Client license (as described below).
    - *Client*. Under the terms of the Client license, the license granted to You by Extreme will authorize You to install the License Key for the Licensed Software on your server and allow the specific number of Concurrent Users shown on the relevant invoice issued to You for each Concurrent User that You order from Extreme or Your dealer, if any, to access the Server Application. A separate license is required for each additional Concurrent User.
5. AUDIT RIGHTS. You agree that Extreme may audit Your use of the Licensed Materials for compliance with these terms and Your License Type at any time, upon reasonable notice. In the event that such audit reveals any use of the Licensed Materials by You other than in full compliance with the license granted and the terms of this Agreement, You shall reimburse Extreme for all reasonable expenses related to such audit in addition to any other liabilities You may incur as a result of such non-compliance, including but not limited to additional fees for Concurrent Users over and above those specifically granted to You. From time to time, the Licensed Software will upload information about the Licensed Software and the associated devices to Extreme. This is to verify the Licensed Software is being used with a valid license. By using the Licensed Software, you consent to the transmission of this information. Under no circumstances, however, would Extreme employ any such measure to interfere with your normal and permitted operation of the Products, even in the event of a contractual dispute.
6. RESTRICTION AGAINST COPYING OR MODIFYING LICENSED MATERIALS. Except as expressly permitted in this Agreement, You may not copy or otherwise reproduce the Licensed Materials. In no event does the limited copying or reproduction permitted under this Agreement include the right to decompile, disassemble, electronically transfer, or reverse engineer the Licensed Software, or to translate the Licensed Software into another computer language.

    The media embodying the Licensed Software may be copied by You, in whole or in part, into printed or machine readable form, in sufficient numbers only for backup or archival purposes, or to replace a worn or defective copy. However, You agree not to have more than two (2) copies of the Licensed Software in whole or in part, including the original media, in your possession for said purposes without Extreme's prior written consent, and in no event shall You operate more copies of the Licensed Software than the specific licenses granted to You. You may not copy or reproduce the documentation. You agree to maintain appropriate records of the location of the original media and all copies of the Licensed Software, in whole or in part, made by You. You may modify the machine-readable form of the Licensed Software for (1) your own internal use or (2) to merge the Licensed Software into other program material to form a modular work for your own use, provided that such work remains modular, but on termination of this Agreement, You are required to completely remove the Licensed Software from any such modular work. Any portion of the Licensed Software included in any such modular work shall be used only on a single computer for internal purposes and shall remain subject to all the terms and conditions of this Agreement. You agree to include any copyright or other proprietary notice set forth on the label of the media embodying the Licensed Software on any copy of the Licensed Software in any form, in whole or in part, or on any modification of the Licensed Software or any such modular work containing the Licensed Software or any part thereof.

7. TITLE AND PROPRIETARY RIGHTS

   a. The Licensed Materials are copyrighted works and are the sole and exclusive property of Extreme, any company or a division thereof which Extreme controls or is controlled by, or which may result from the merger or consolidation with Extreme (its "Affiliates"), and/or their suppliers. This Agreement conveys a limited right to operate the Licensed Materials and shall not be construed to convey title to the Licensed Materials to You. There are no implied rights. You shall not sell, lease, transfer, sublicense, dispose of, or otherwise make available the Licensed Materials or any portion thereof, to any other party.

   b. You further acknowledge that in the event of a breach of this Agreement, Extreme shall suffer severe and irreparable damages for which monetary compensation alone will be inadequate. You therefore agree that in the event of a breach of this Agreement, Extreme shall be entitled to monetary damages and its reasonable attorney's fees and costs in enforcing this Agreement, as well as injunctive relief to restrain such breach, in addition to any other remedies available to Extreme.

8. PROTECTION AND SECURITY. In the performance of this Agreement or in contemplation thereof, You and your employees and agents may have access to private or confidential information owned or controlled by Extreme relating to the Licensed Materials supplied hereunder including, but not limited to, product specifications and schematics, and such information may contain proprietary details and disclosures. All information and data so acquired by You or your employees or agents under this Agreement or in contemplation hereof shall be and shall remain Extreme's exclusive property, and You shall use your best efforts (which in any event shall not be less than the efforts You take to ensure the confidentiality of your own proprietary and other confidential information) to keep, and have your employees and agents keep, any and all such information and data confidential, and shall not copy, publish, or disclose it to others, without Extreme's prior written approval, and shall return such information and data to Extreme at its request. Nothing herein shall limit your use or dissemination of information not actually derived from Extreme or of information which has been or subsequently is made public by Extreme, or a third party having authority to do so.

   You agree not to deliver or otherwise make available the Licensed Materials or any part thereof, including without limitation the object or source code (if provided) of the Licensed Software, to any party other than Extreme or its employees, except for purposes specifically related to your use of the Licensed Software on a single computer as expressly provided in this Agreement, without the prior written consent of Extreme. You agree to use your best efforts and take all reasonable steps to safeguard the Licensed Materials to ensure that no unauthorized personnel shall have access thereto and that no unauthorized copy, publication, disclosure, or distribution, in whole or in part, in any form shall be made, and You agree to notify Extreme of any unauthorized use thereof. You acknowledge that the Licensed Materials contain valuable confidential information and trade secrets, and that unauthorized use, copying and/or disclosure thereof are harmful to Extreme or its Affiliates and/or its/their software suppliers.

9. MAINTENANCE AND UPDATES. Updates and certain maintenance and support services, if any, shall be provided to You pursuant to the terms of an Extreme Service and Maintenance Agreement, if Extreme and You enter into such an agreement. Except as specifically set forth in such agreement, Extreme shall not be under any obligation to provide Software Updates, modifications, or enhancements, or Software maintenance and support services to You.

10. DEFAULT AND TERMINATION. In the event that You shall fail to keep, observe, or perform any obligation under this Agreement, including a failure to pay any sums due to Extreme, or in the event that you become insolvent or seek protection, voluntarily or involuntarily, under any bankruptcy law, Extreme may, in addition to any other remedies it may have under law, terminate the License and any other agreements between Extreme and You.

a. Immediately after any termination of the Agreement or if You have for any reason discontinued use of Software, You shall return to Extreme the original and any copies of the Licensed Materials and remove the Licensed Software from any modular works made pursuant to Section 3, and certify in writing that through your best efforts and to the best of your knowledge the original and all copies of the terminated or discontinued Licensed Materials have been returned to Extreme.

b. Sections 1, 7, 8, 10, 11, 12, 13, 14 and 15 shall survive termination of this Agreement for any reason.

11. EXPORT REQUIREMENTS. You are advised that the Software is of United States origin and subject to United States Export Administration Regulations; diversion contrary to United States law and regulation is prohibited. You agree not to directly or indirectly export, import or transmit the Software to any country, end user or for any Use that is prohibited by applicable United States regulation or statute (including but not limited to those countries embargoed from time to time by the United States government); or contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or Use.

12. UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The Licensed Materials (i) were developed solely at private expense; (ii) contain "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Extreme and/or its suppliers. For Department of Defense units, the Licensed Materials are considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth herein.

13. LIMITED WARRANTY AND LIMITATION OF LIABILITY. The only warranty that Extreme makes to You in connection with this license of the Licensed Materials is that if the media on which the Licensed Software is recorded is defective, it will be replaced without charge, if Extreme in good faith determines that the media and proof of payment of the license fee are returned to Extreme or the dealer from whom it was obtained within ninety (90) days of the date of payment of the license fee.

    NEITHER EXTREME NOR ITS AFFILIATES MAKE ANY OTHER WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, WITH RESPECT TO THE LICENSED MATERIALS, WHICH ARE LICENSED "AS IS". THE LIMITED WARRANTY AND REMEDY PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE EXPRESSLY DISCLAIMED, AND STATEMENTS OR REPRESENTATIONS MADE BY ANY OTHER PERSON OR FIRM ARE VOID. ONLY TO THE EXTENT SUCH EXCLUSION OF ANY IMPLIED WARRANTY IS NOT PERMITTED BY LAW, THE DURATION OF SUCH IMPLIED WARRANTY IS LIMITED TO THE DURATION OF THE LIMITED WARRANTY SET FORTH ABOVE. YOU ASSUME ALL RISK AS TO THE QUALITY, FUNCTION AND PERFORMANCE OF THE LICENSED MATERIALS. IN NO EVENT WILL EXTREME OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR SPECIAL, DIRECT, INDIRECT, RELIANCE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF DATA OR PROFITS OR FOR INABILITY TO USE THE LICENSED MATERIALS, TO ANY PARTY EVEN IF EXTREME OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL EXTREME OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU OR ANY OTHER PARTY EXCEED THE LICENSE FEE YOU PAID FOR THE LICENSED MATERIALS.

    Some states do not allow limitations on how long an implied warranty lasts and some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation and exclusion may not apply to You. This limited warranty gives You specific legal rights, and You may also have other rights which vary from state to state.

14. JURISDICTION. The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws and in the State and Federal courts of the State of California, without regard to its rules with respect to choice of law. You waive any objections to the personal jurisdiction and venue of such courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.

15. GENERAL.

    a. This Agreement is the entire agreement between Extreme and You regarding the Licensed Materials, and all prior agreements, representations, statements, and undertakings, oral or written, are hereby expressly superseded and canceled.

    b. This Agreement may not be changed or amended except in writing signed by both parties hereto.

    c. You represent that You have full right and/or authorization to enter into this Agreement.

    d. This Agreement shall not be assignable by You without the express written consent of Extreme. The rights of Extreme and Your obligations under this Agreement shall inure to the benefit of Extreme's assignees, licensors, and licensees.

    e. Section headings are for convenience only and shall not be considered in the interpretation of this Agreement.

    f. The provisions of the Agreement are severable and if any one or more of the provisions hereof are judicially determined to be illegal or otherwise unenforceable, in whole or in part, the remaining provisions of this Agreement shall nevertheless be binding on and enforceable by and between the parties hereto.

    g. Extreme's waiver of any right shall not constitute waiver of that right in future. This Agreement constitutes the entire understanding between the parties with respect to the subject matter hereof, and all prior agreements, representations, statements and undertakings, oral or written, are hereby expressly superseded and canceled. No purchase order shall supersede this Agreement.

    h. Should You have any questions regarding this Agreement, You may contact Extreme at the address set forth below. Any notice or other communication to be sent to Extreme must be mailed by certified mail to the following address:

    Extreme Networks, Inc.
    145 Rio Robles
    San Jose, CA 95134 United States
    ATTN: General Counsel

Table of Contents

ExtremeCloud™ IQ Site Enginev26.11.10 User Guide: 1

Comprehensive Configuration, Management, and Advanced Network Features 1

Abstract 2

Extreme Networks® Software License Agreement 4

Table of Contents 9

Getting Started with ExtremeCloud IQ Site Engine 88

Requirements 88

ExtremeCloud IQ Site Engine Access Requirements 89

Use Case 1: Full Read/Write Access 90

Use Case 2: Read-Only Access 91

Use Case 3: Limited Read-Only Access 92

Use Case 4: End-System Information, Read-Only Access 92

Use Case 5: End-System Information, Read/Write Access 92

Browser Requirements 92

Screen Resolution 93

Enable Report Data Collection 93

Enable Device Statistics Collection 93

Enabling Device Statistics Collection 94

Enable Interface Statistics Collection 95

Enabling Interface Statistics Collection 95

Enable Wireless Controller Statistics Collection 96

Enabling Wireless Controller Statistics Collection 96

Enable Flow Collection 97

Enable Flow Collection on a Device 97

Enable Flow Collection on an Interface 97

ExtremeCloud IQ Site Engine Scalability 97

ExtremeCloud IQ Site Engine Timeout 98
Upgrading Fabric Manager (Legacy) 98
Prerequisites 98
Upgrade Procedure 98
Post Upgrade Steps 102
ExtremeCloud IQ Site Engine Licensing 103
ExtremeCloud IQ Pilot Twin Subscription Provides Backwards Compatibility 105
Licensing for Devices in Connected Mode 106
Licensing for Devices in Air Gap Mode 108
Revoke Air Gap License 111
License Limits and Violations 112
Devices Marked as Unmanaged 112
Licensing for ExtremeControl (Network Access Control) 113
After Upgrading from Extreme Management Center 113
Upon Initial Installation 114
ExtremeCloud IQ Site Engine Ports 114
Access Control Ports 117
ExtremeAnalytics Ports 119
FabricManager Ports 121
Ephemeral Ports 121
ExtremeCloud IQ Site Engine Tabs 122
Network 123
Navigating the Network Tab 123
Dashboard 124
Devices 125
Left-Panel Tree 125
Right-Panel Tabs 125
Discovered 125
Firmware 126
Archives 126

Configuration Templates 127
Reports 127
Impact Analysis Dashboard Overview 128
Charts 128
Unavailable Sites Report 134
Endpoints Impacted by Unavailable Sites Report 135
End-System Information 136
Events Log 140
Health Log 143
Site Availability History Report 145
Unavailable Devices Report 146
Sites Impacted by Unavailable Devices Report 149
Endpoints Impacted by Unavailable Devices Report 151
End-System Information 152
Events Log 156
Health Log 159
Device Availability History Report 161
Slow Locations Report 162
Expected Response Time 163
Historical Response Time 164
Applications Impacted by Slow Locations Report 164
Expected Response Time 166
Historical Response Time 167
Network Performance History Report 167
Slow Applications Report 168
Expected Response Time 170
Historical Response Time 171
Locations Impacted by Slow Applications 171
Expected Response Time 173
Historical Response Time 174

Application Performance History Report 174
Highly Utilized Ports Report 175
Sites Impacted by Highly Utilized Ports Report 177
Devices Impacted by Highly Utilized Ports Report 178
Port Capacity History Report 182
High Error Ports Report 183
Sites Impacted by High Error Ports Report 184
Devices Impacted by High Error Ports Report 186
Port Health History Report 190
Unarchived Devices Report 191
Sites Impacted by Unarchived Devices Report 194
Archived Devices History Report 196
Devices Without Reference Firmware Report 197
Sites Impacted by Devices Without Reference Firmware Report 201
Reference Firmware History Report 202
Device Operations 203
Add Device 205
Check for Firmware Updates 206
Export to CSV 206
Menu Options 206
Device View 206
Terminal 206
WebView 206
FlexViews 207
More Views 208
Port Tree 208
Interfaces 209
User Sessions 209
Fabric L2VSNs 210
SDWAN Appliance360 210

Configure 210
Compass Search 211
Rediscover 211
Clear Alarms 211
Upgrade Firmware 211
Add to Device Group 212
More Actions 213
Restart Device 213
Set Device Group's Profile 213
Set/Clear Frozen Ports 213
Import to Site 214
Import to Service Definition 214
View Available Firmware Releases 214
Run Site's Add Actions 214
Contact Device Using Group's Profile 215
Ping Device (ICMP) 215
Authentication Configuration 215
RADIUS Configuration 216
RADIUS Authentication 216
RADIUS Accounting 216
Delete Device 216
Overwrite Local Changes 216
Register Trap Receiver 217
Unregister Trap Receiver 217
Register SysLog Receiver 217
Unregister SysLog Receiver 217
Collect Device Statistics 218
Export Serial Numbers 219
Change Management Status 219

Archives ... 219
Backup Configuration ... 219
Restore Configuration ... 220
Compare Last Configurations ... 220
Inventory Settings ... 220
Tasks ... 220
CLI Commands ... 221
Device Groups ... 222
Selecting the User Device Groups in the left-panel tree of the Devices tab enables you to create, delete, and rename device groups in your network, as well as remove a device from a device group, and remove a port from a device group. ... 222
Creating a Device Group ... 222
Deleting a Device Group ... 222
Renaming a Device Group ... 222
Removing a Device from a Device Group ... 223
Removing a Port from a Device Group ... 223
Maps ... 223
Add to Map ... 223
Create Map ... 224
Create Map for Locations ... 224
Search Maps ... 224
Network ... 225
Policy ... 225
Fabric ... 226
Working in the Devices List ... 226
Devices List Column Definitions ... 226
Buttons, Search Field, and Paging Toolbar ... 231
Local Settings ... 232
Devices Navigation ... 232
Filter by Criteria ... 232

Sort Tree View 234
Status 235
Notes 236
Device Operations 237
Add Device 239
Check for Firmware Updates 239
Export to CSV 239
Menu Options 240
Device View 240
Terminal 240
WebView 240
FlexViews 240
More Views 242
Port Tree 242
Interfaces 242
User Sessions 242
Fabric L2VSNs 243
SDWAN Appliance360 243
Configure 244
Compass Search 244
Rediscover 244
Clear Alarms 244
Upgrade Firmware 245
Add to Device Group 245
More Actions 246
Restart Device 246
Set Device Group's Profile 246
Set/Clear Frozen Ports 247
Import to Site 247

Import to Service Definition 247
View Available Firmware Releases 247
Run Site's Add Actions 248
Contact Device Using Group's Profile 248
Ping Device (ICMP) 248
Authentication Configuration 248
RADIUS Configuration 249
RADIUS Authentication 249
RADIUS Accounting 249
Delete Device 249
Overwrite Local Changes 249
Register Trap Receiver 250
Unregister Trap Receiver 250
Register SysLog Receiver 250
Unregister SysLog Receiver 250
Collect Device Statistics 251
Export Serial Numbers 252
Change Management Status 252
Archives 252
Backup Configuration 252
Restore Configuration 253
Compare Last Configurations 253
Inventory Settings 253
Tasks 253
CLI Commands 254
Device Groups 255
Selecting the User Device Groups in the left-panel tree of the Devices tab enables you to create, delete, and rename device groups in your network, as well as remove a device from a device group, and remove a port from a device group. 255
Creating a Device Group 255

Deleting a Device Group 255
Renaming a Device Group 255
Removing a Device from a Device Group 256
Removing a Port from a Device Group 256
Maps 256
Add to Map 256
Create Map 257
Create Map for Locations 257
Search Maps 257
Network 258
Policy 258
Fabric 259
Working in the Devices List 259
Devices List Column Definitions 259
Buttons, Search Field, and Paging Toolbar 264
Local Settings 265
Add Device 266
Configure Device 267
Device 268
Device Annotation 273
VRF Definition 273
VLAN Definition 274
CLIP Addresses 278
Fabric Connect 280
Services 283
L2 VSN 284
L3 VSN 285
LAG 286
Ports 287

ZTP+ Device Settings 292
Basic Management 293
Configuration/Upgrade 295
Device Protocols/Features 296
Flow Sources 297
Vendor Profile 298
Buttons 301
Device Configuration Enforce Preview 302
Device Details 302
Match Column 303
Status Column 303
Enforce Options 303
Device Configuration Detail Table 305
Device 306
VRF Definitions 306
VLAN Definitions 306
CLIP Addresses 309
Fabric Connect 310
Services 312
L2 VSN 312
L3 VSN 312
LAGs 313
Ports 314
How to Change the Configuration of a Device Included Site 317
Sites 318
Discover 319
Actions 321
Policy 322
Access Control 322

ExtremeAnalytics 323
VRF/VLAN 323
VRF Definition 324
VLAN Definition 325
DHCP Relay Servers 327
Fabric Connect 327
Services 327
L2 VSN 328
L3 VSN 330
LAG Topologies 330
Port Templates 331
Port Templates Panel 331
ZTP+ Automated Templates 336
ZTP+ Device Defaults 340
Basic Management 340
Configuration/Upgrade 344
Device Protocols/Features 346
Global IP To Site Mapping 347
Endpoint Locations 347
Analytics 348
Custom Variables 349
Scope 349
Variable 350
XIQ Location 350
Buttons 351
Site Summary 351
Compare Device Configurations 353
Selecting the Files to Compare 353
Comparing the Files 354

Inventory Settings 355
Pre-Register Device 357
Pre-Register Device Window 358
Pre-Register Device Confirmation Window 359
Sites 360
Discover 362
Actions 363
Policy 365
Access Control 365
ExtremeAnalytics 366
VRF/VLAN 366
VRF Definition 367
VLAN Definition 368
DHCP Relay Servers 370
Fabric Connect 370
Services 370
L2 VSN 371
L3 VSN 373
LAG Topologies 373
Port Templates 374
Port Templates Panel 374
ZTP+ Automated Templates 379
ZTP+ Device Defaults 383
Basic Management 383
Configuration/Upgrade 387
Device Protocols/Features 389
Global IP To Site Mapping 390
Endpoint Locations 390
Analytics 391

Custom Variables ... 392
Scope ... 392
Variable ... 393
XIQ Location ... 393
Buttons ... 394
Services ... 394
VRF Definition ... 395
VLAN Definition ... 396
Service Application Name ... 398
L2 VSN ... 398
L3 VSN ... 400
Fabric Topology Definition on the Sites Tab ... 400
Create a Topology Definition ... 400
Configure a Topology Definition ... 401
Fabric Name Tab ... 401
Fabric Summary tab ... 402
Rename a Topology Definition ... 402
Delete a Topology Definition ... 403
How to Create a Fabric Service Definition ... 404
Create a Service Definition ... 404
Service Definition Panel ... 404
Rename a Service Definition ... 405
Delete a Service Definition ... 405
How to Create a Service Application ... 406
Create a Service Application ... 406
Rename a Service Application ... 407
Delete a Service Application ... 408
Maps Overview ... 408
Accessing Maps ... 409

Navigating Maps 409
Geographic and Floorplan Maps 410
Navigating the Map Tab 414
World Map Navigation Tree 414
Create Map 414
Edit Map 415
Import Map 415
Main Map View 415
File, View, and Tool Menus 415
Pan and Zoom Control 419
Search Field 419
Viewing Alarm/Device Status 420
Accessing Device Information 420
Link Information 421
Network Details Section 423
Map tab 424
Links tab 424
VLAN tab 425
MLAG tab 426
EAPS tab 428
Services tab 432
ISIS Areas tab 432
ISIS Links tab 432
Fabric Attach tab 433
Topology and Geographic map refresh 434
Performing a Search 434
Finding a Wireless Client 435
From the Search Field on the Network Tab 435
From the Wireless Tab 435

Radius Distance Calculation 435
Finding an Access Point 436
From the Wireless Tab 436
From the Reports Page 436
Finding a Device 436
From the Network Page Search Field 436
Finding a Wired Client 437
From the Network Tab Search Field 437
From the Control Tab 437
Using Map Links 437
Navigating the Map Tab 438
To access maps of your devices: 438
World Map Navigation Tree 438
Create Map 439
Edit Map 439
Import Map 439
Main Map View 439
File, View, and Tool Menus 440
Pan and Zoom Control 443
Search Field 444
Viewing Alarm/Device Status 444
Accessing Device Information 444
Link Information 445
Network Details Section 447
Create and Edit Maps 448
Creating a Map 448
Importing a Map 456
Adding Devices/APs from ExtremeCloud IQ Site Engine Devices and Wireless 456
Add to a Specific Map 456

Add to New Maps Based on Location 457
Creating a Manual Link Between Devices 458
Adding Map Links 459
Setting the Map Scale 460
How to Add Devices and APs to Maps 461
Adding Devices/APs from ExtremeCloud IQ Site Engine Devices and Wireless 461
Add to a Specific Map 462
Add to New Maps Based on Location 462
How to Create Maps Using the Map Tab 464
To access maps of your devices: 464
Creating a Map 464
How to Edit Maps 472
To access maps of your devices: 472
Editing a Map 472
Adding Devices, APs and Links to a Map 479
Advanced Map Features Overview 480
Overview 481
Prerequisites 481
Advanced Map Features 483
Overview 483
Prerequisites 484
Designing a Floorplan 484
Drawing Tools 492
Configure Area Window 493
Style Menu 494
Wireless Client Location 494
Time-Lapse Location 496
Wireless Coverage 497
Import and Export Maps 499

Importing Maps 499
Exporting Maps 501
Show Application Data 501
Adding a Map Link with Location 502
Wireless Map Limits 503
Active Client Tracking 503
Maximum Number of Maps 503
Maximum Number of APs per floorplan 503
How to Design Floorplans 503
Designing a Floorplan 503
Drawing Tools 511
Configure Area Window 512
Style Menu 513
How to Add Devices and APs to Maps 514
Adding Devices/APs from ExtremeCloud IQ Site Engine Devices and Wireless 514
Add to a Specific Map 514
Add to New Maps Based on Location 514
How to Display Map Application Data 516
Show Application Data 516
Adding a Map Link with Location 517
How to Use Maps to Locate Wireless Clients 518
Wireless Client Location 518
Time-Lapse Location 520
Wireless Map Limits 521
Active Client Tracking 521
Maximum Number of Maps 522
Maximum Number of APs per Floor Plan 522
How to View Wireless Coverage 522
Wireless Coverage 522

Wireless Map Limits 524
Active Client Tracking 524
Maximum Number of Maps 524
Maximum Number of APs per Floor Plan 525
How to Export Maps 525
Exporting Maps 525
How to Design Floorplans 526
Designing a Floorplan 526
Drawing Tools 534
Configure Area Window 535
Style Menu 536
How to Export Maps 537
Exporting Maps 537
Network Details 538
To access maps of your devices: 538
Accessing Network Details 538
Import Map 540
Import Options 540
EAPS 541
Accessing Network Details 541
EAPS Summary Tab 541
Links 545
Accessing Network Details 545
Links tab 546
VLAN 546
Accessing Network Details 546
VLAN Summary tab 547
MLAG 548
Accessing Network Details 548

MLAG Summary tab 549
VPLS 552
Accessing Network Details 552
VPLS Summary Tab 553
Nodes 553
Pseudowires 554
Map Types 554
Types of Maps 554
How to Perform a Search Using Maps 557
Performing a Search 557
Finding a Wireless Client 558
From the Search Field on the Network Tab 558
From the Wireless Tab 558
Radius Distance Calculation 559
Finding an Access Point 559
From the Wireless Tab 559
From the Reports Page 560
Finding a Device 560
From the Network Page Search Field 560
Finding a Wired Client 561
From the Network Tab Search Field 561
From the Control Tab 561
How to Import Maps 561
Importing a Map 561
How to Create Links Between Devices and Maps 562
Creating a Manual Link Between Devices 562
Adding Map Links 563
How to Set the Map Scale 564
Setting the Map Scale 564

Endpoint Locations 565
Restart Devices 568
Timed Restart Not Supported 568
Timed Restart Supported 569
Fabric 571
Accessing Fabric in ExtremeCloud IQ Site Engine 572
Fabric Tab 572
Fabric Manager Installation (Legacy) 573
Pre-Installation 573
Fabric Manager Installation Static Mode 573
Adding Fabric Manager to ExtremeCloud IQ Site Engine 578
Fabric Connect 579
Left-Panel Tree 579
Fabric Connect Folder 580
Fabric Attach Folder 581
Right-Panel Topology Map 582
Topology Tab Tools 583
Topology Tab Buttons 584
Services 584
VRF Definition 585
VLAN Definition 586
Service Application Name 588
L2 VSN 588
L3 VSN 590
Service Summary 590
Applying Fabric Services 591
Applying a Fabric Topology to a Site 591
Applying a Service Application to a Site 592
Applying Fabric to Port Templates 592

Applying Fabric to Ports 594
Applying Fabric Services to a Device 594
Applying Fabric Topology to a Device 595
Applying Fabric Services to a Device 595
Adding and Deleting VRF Definitions 596
Adding and Deleting VLAN Definitions 597
Enforcing the Fabric Configurations 597
Enforcing Fabric Connect 597
Enforcing Fabric VRF 598
Enforcing Fabric Services 598
Enforcing Fabric VLAN 598
Enforcing Fabric Port 598
Fabric Manager ZTP+ Configuration (Legacy) 598
General Network Configuration 599
How to Add Fabric Manager (Legacy) 599
Adding Fabric Manager to ExtremeCloud IQ Site Engine 599
Add CLI Credentials 600
Create Administration Profile 601
Add Administration Profile to the Fabric Manager engine 601
ZTP+ Discovery 602
Fabric Topology Definition on the Sites Tab 603
Create a Topology Definition 603
Configure a Topology Definition 603
Fabric Name Tab 604
Fabric Summary tab 605
Rename a Topology Definition 605
Delete a Topology Definition 606
How to Create a Fabric Service Definition 607
Create a Service Definition 607

Service Definition Panel 607
Rename a Service Definition 608
Delete a Service Definition 608
How to Create a Service Application 609
Create a Service Application 609
Rename a Service Application 610
Delete a Service Application 611
Upgrading Fabric Manager (Legacy) 611
Prerequisites 611
Upgrade Procedure 612
Post Upgrade Steps 615
Fabric Assist 616
VLAN Trunk Mode 617
Configuring VLAN Trunks on a Port 617
Configuring VLAN Trunks on a Port Template 618
Provision VLAN Trunks Automatically 618
To Provision VLAN Trunks at the Ports Level: 619
To Provision VLAN Trunks at the Port Templates Level: 619
Edit a Port Template 620
VLAN Range 620
Add a Range of VLANs at the Device Level 622
Add a Range of VLANs at the Site Level 623
Add a Range of VLANs at the Service Definition Level 623
Layer 2 VSN Service Creation 624
Enhanced Validation 625
Enabling Fabric Assist 625
Fabric Assist L2 VSN Considerations 626
VLAN Pruning 627
Import to Service Definition 628

Prerequisites 629
Import a Configuration to a Service Definition 629
How to Create an EAPS Domain 633
To create a new EAPS Domain: 633
Changing Device Configurations 634
Discovered 636
Device Grouping 637
Columns 639
Toolbar Buttons 643
Load Configuration on a Discovered Device 644
Clone 644
Template 645
Pre-Register Device 646
Pre-Register Device Window 646
Pre-Register Device Confirmation Window 647
Add Devices 649
Device 650
Device Annotation 652
Add Device Actions 653
Policy 655
Access Control 655
Ports 658
ZTP+ VLAN Definition 659
Device Configuration Enforce Preview 660
Device Details 660
Match Column 660
Status Column 661
Enforce Options 661
Device Configuration Detail Table 663

Device 663
VRF Definitions 664
VLAN Definitions 664
CLIP Addresses 667
Fabric Connect 668
Services 670
L2 VSN 670
L3 VSN 670
LAGs 670
Ports 672
Firmware 675
Firmware Tree 676
Device Type Images Section 677
Details Section 679
Device Type Details 679
Firmware/boot PROM Image Details 682
Archives 685
Archive Name 687
Right-Panel 688
Archive Name (Right-Panel) 689
General 689
Setup 690
Schedule 692
Archive Version 693
Right-Panel 694
Archive Version (Right-Panel) 694
Archive File 696
General Tab 696
Custom Attributes Tab 697

Legacy Devices ... 698
SSR Hardware Attributes ... 698
E5 and E6/E7 Power Supply and Fan Attributes ... 699
RoamAbout Radiocard and Base MAC Address Attributes ... 699
Vertical Horizon Attributes ... 699
ELS Serial Number Attribute ... 700
Archive File (Right-Panel) ... 700
General ... 701
Attributes ... 704
Create Archive ... 708
Select Archive Versions ... 709
Compare Archive Versions ... 710
Devices Table ... 712
Comparison Results Table ... 712
Compare Configurations ... 712
Creating a Configuration Template ... 713
Configuration File Compare ... 716
Configuration File Viewer ... 718
Create Archive ... 719
Archive Name Window ... 720
Archive Setup ... 720
Device Selection Window ... 721
Schedule Window ... 723
Schedule/Process ... 724
Devices ... 724
Restore Archive ... 725
Archive Version Selection Window ... 725
Archives ... 725
Configurations to Restore ... 726

Restore Configurations Window ... 727
Archive ... 728
Creating an Archive ... 729
Saving a New Archive Version ... 732
Editing an Archive ... 732
Renaming an Archive ... 733
Deleting an Archive ... 733
How to Compare Archives ... 733
How to Restore an Archive ... 735
How to Back up, Restore, and Compare Device Configurations ... 736
Device Back up Configuration ... 737
Device Restore Configuration ... 737
Compare Device Configurations ... 737
Configuration Templates ... 738
Templates Tree ... 739
Templates Table ... 740
Details View ... 741
Alarms and Events ... 743
Access Requirements ... 743
Alarms ... 743
Alarm Summary ... 747
Alarm Configuration ... 747
Alarm Configuration Column Definitions ... 748
Events ... 749
Event Log Column Definitions ... 750
Event Configuration ... 751
Buttons, Search Field, and Paging Toolbar ... 751
Alarm History ... 753
Alarm Limits ... 755

Alarm History Options 755
How to Configure Alarms 756
Defining an Alarm 757
Copying an Alarm 771
Disabling Alarms 771
Deleting Alarms 772
Configuring Email Settings 772
Resetting Alarm Action Limits 772
Enabling/Disabling All 772
Restoring Default Alarms 772
Viewing Alarms 773
ExtremeCloud IQ Site Engine 773
Alarms & Events Tab 773
Network Tab 774
Clearing Alarms 776
Buttons, Search Field, and Paging Toolbar 776
Event Configuration Tab 777
Event Type 777
Event Logs 779
Event Patterns 780
Field Types 781
Delimiters 782
Getting Started with ExtremeControl 783
Access Requirements 783
Navigating the Control Tab 783
Dashboard 784
Policy 784
Access Control 784
End-Systems 784
Reports 784

Policy 785
Understanding Policy Domains 787
Understanding Roles 788
Role Summary Column 790
Understanding Services 790
Working with Service Groups 791
Understanding Traffic Classification Rules 792
Adding Devices 792
Viewing Port Configuration Information 793
Working with Port Groups 793
Working with VLANS 794
Viewing Classes of Service 794
Saving the Domain 795
Enforcing 795
Enforce Preview 796
Rule Counts Reported by Devices 796
Verifying 797
AP Aware 797
Policy Configuration Considerations 798
General Considerations 798
Authenticating without Policy 798
Terminating Role Override Sessions 800
Port-Level MAC to Role Mappings 800
Import From Device 800
Flood Control 800
C1 Considerations 800
Policy Support 800
Rule Limits 801
N-Series Considerations 801

Role Precedence for the N-Series Platinum 801
C2 and B2 Considerations 802
C3 and B3 Considerations 802
Mixed-Stack C2/C3 and B2/B3 Considerations 803
7100 Considerations 804
ExtremeControl Controller Configuration 804
ExtremeControl Controllers Require Separate Domains 804
Modifying ExtremeControl Controllers Preconfigured Policy 804
Modifying the Downstream Default Policy 805
Configuring LAG on ExtremeControl Controllers 805
Configuring LAG on Layer 3 ExtremeControl Controllers - Upstream Ports 805
Configuring LAG on Layer 3 ExtremeControl Controllers - Downstream Ports 805
Configuring LAG on Layer 2 ExtremeControl Controllers - Upstream Ports 805
Configuring LAG on Layer 2 ExtremeControl Controllers - Downstream Ports 805
ExtremeWireless Controller Configuration 806
Version Supported 806
Policy Rules 806
Supported Rule Types 806
"No Change" Filter Sets 807
Rule Actions 807
Rule Directions 807
Rule Limits 808
Role Default Actions 808
Class of Service 808
Rate Limits 808
Internal VLAN 809
Policy Inheritance 809
Configuring RADIUS Servers 810
Other Considerations 810

ExtremeCloud IQ Site Engine Policy 811
Policy Tab Overview 811
Details View 811
General 812
Policy Menus 812
Open/Manage Domains Menu 812
Global Domain Settings Menu 813
Tools Menu 814
Policy Enforce Preview 816
Left Panel 816
Right Panel 817
Import from Domain 820
Data Elements to Import 821
Application of Imported Data Elements 823
Import from File 824
Data Elements to Import 825
Global Domain Data 827
Application of Imported Data Elements 828
Assign Devices to Domain 829
Authentication Configuration 831
Device Selection 831
Port Selection 831
Device Configuration 832
Authentication Status 832
Global Authentication Settings 833
MAC Authentication Settings 834
Web Authentication Settings 835
General 835
Guest Networking 837

Web Page Banner 838
Convergence End-Point Settings 839
CEP Role Mappings 839
CEP Detection Tab 840
Port Configuration 842
Authentication Mode 842
Port Mode 843
RFC3580 VLAN Authorization Tab 845
Login Settings 846
Automatic Re-Authentication 847
Authenticated User Counts 848
Convergence End-Point Access 849
Policy Main Window 850
Menu Tabs 850
Dialog Boxes (Messages) 851
Icons 851
Open/Manage Domain Menu Icons 852
Policy Windows 852
Policy Concepts 852
Policy 853
Role 853
What is a Role 853
Default Role 854
Policy Domains 854
Service 855
Rule 855
What is a Rule 855
Disabling Rules 856
Conflict Checking 856

Packet Tagging 856
VLAN to Role Mapping 857
Dynamic Egress 858
Setting Domain GVRP Status 861
Policy VLAN Islands 862
Traffic Mirroring 862
Port Groups 863
User-Defined Port Groups 863
Network Resource Groups 863
Network Resource Topologies 863
Verifying 864
Enforcing 864
Controlling Client Interactions with Locks 865
Policy Tab Right-Panel 866
Policy Left Panel 866
Roles/Services Tab 867
Roles Tree 867
Service Repository Tree 868
Class of Service Tab 870
VLAN Tab 872
Network Resources Configuration 873
Devices/Port Groups Tab 875
Devices Tree 875
Summary (Roles) 877
General (Role) 877
Default Actions 879
Services 880
VLAN Egress (Role) 880
Add Egress VLAN Window 881

Mappings (Role) 882
MAC to Role Mapping 883
IP to Role Mapping 884
Tagged Packet VLAN to Role Mapping 884
Authentication-Based VLAN to Role Mapping 884
Pre-configured Domains (Legacy) 884
Access Pre-Configured Domains 885
Pre-configured Domain Descriptions 885
Embedded NAC Domain 885
Generic Services N-Series 886
Generic Services SecureStack 886
HealthCare Services 886
Quickstart 886
Secure Guest 887
ShoreTel 887
VPN Termination Point 887
Add/Remove Services (Roles) 887
Details View (Service) 889
Service Repository 893
Local/Global Services 894
Details View (Services) 894
Details View (Service Group) 895
Add/Remove Services (Service Groups) 896
Rule 898
General Area 898
Traffic Description Area 899
Actions Area 900
Create Rule 902
Edit Rule 903

Layer Area 904
Value Area 904
Class of Service Overview 904
Getting Started with Class of Service 905
Class of Service Overview 906
Implementing CoS 907
Configuring CoS 907
Rate Limits 908
Transmit Queues 909
Flood Control 910
Class of Service 911
General 912
Rate Limiting/Rate Shaping 912
Index Numbers 913
General (CoS Components Folder) 914
General (Rate Limits) 915
Details View (Rate Limits Folder) 917
Priority-Based Rate Limits 918
Add/Edit CoS to Rate Limit Mapping 919
Advanced Rate Limiting by Port Type 920
Configuring Rate Limit Mappings 920
Associating Rate Limits with a Class of Service 921
Summary (Rate Limit Port Groups Folder) 921
CoS - Rate Limit Mappings (Rate Limit Port Group) 922
Ports (Rate Limit Port Group) 924
Automated Service 926
Traffic Description Area 927
Actions Area 927
Traffic Classification Rules 929

Traffic Descriptions 930
Actions 931
VLAN Membership (Access Control) 931
Priority (Class of Service) 932
Classification Types and their Parameters 932
Layer 2 -- Data Link Classification Types 932
Layer 3 -- Network Classification Types 934
Layer 4 -- Application Transport Classification Types 940
Layer 7 -- Application Classification Types 944
Examples of How Rules are Used 945
Traffic Containment 945
Traffic Filtering 946
Traffic Security 946
Traffic Prioritization 947
Ports (Transmit Queue Port Group) 948
Summary (Transmit Queue Port Groups) 950
CoS - Transmit Queue Mappings (Transmit Queue Port Group) 951
Ports (Flood Control Port Groups) 953
Flood Control Port Groups 955
Flood Control Rate Limits (Flood Control Port Groups) 955
Class of Service Example 956
Configure the Classes of Service 959
Create the VoIP Core Role 959
Create a VoIP Core Service 959
Create a Rule 959
Creating the VoIP Edge Role 960
Create a VoIP Edge Service 960
Create a Rule 960
Creating the H.323 Call Setup Role 960

Create a H.323 Call Setup Service 960
Create a Rule 960
Apply the Roles to Network Devices 961
ToS/DSCP Value Definition Chart 961
Policy VLAN Tab Overview 962
General 963
Authentication-Based VLAN to Role Mapping 963
Tagged Packet VLAN to Role Mapping 964
Global VLANs 965
Create VLAN 966
Editing an existing VLAN/Class of Service 966
Selection View (Roles) 966
Policy VLAN Islands 967
(VLANs) - VIDs Tab 967
(VLANs) - Role Mappings Tab 968
General 969
Authentication-Based VLAN to Role Mapping 970
Tagged Packet VLAN to Role Mapping 970
Add Devices (VLAN Islands) 971
Island Topology (Policy VLAN Islands) 972
(Island) - VIDs Tab 973
(Island) - Devices Tab 974
Packet Flow Diagram 975
Network Resources Tab Overview 976
Network Resource Group General Tab 977
Network Resource Topology Tab 978
Network Resource Topology Island Domain Wide 979
Details View (Network Resource Topologies Folder) 980
Devices (Devices) 980

User Sessions (Devices) ... 981
User Sessions Tab ... 981
Authentication (Device) ... **986**
Authentication Status ... 986
Current User Counts ... 988
Global Authentication Settings ... 989
MAC Authentication Settings ... 989
Web Authentication Settings ... 990
General ... 990
Guest Networking ... 992
Web Page Banner ... 993
Convergence End-Point Settings ... 994
CEP Role Mappings ... 994
CEP Detection Tab ... 995
Add/Edit CEP Detection Rule ... **998**
CEP Detection Settings ... 999
Ports (Authentication) ... **1000**
Authentication Mode ... 1001
RFC3580 VLAN Authorization ... 1002
Login Settings ... 1003
MAC ... 1004
802.1X ... 1004
Web Auth ... 1004
Quarantine ... 1005
Auto Tracking ... 1005
Automatic Re-Authentication ... 1005
Authenticated User Counts ... 1006
Convergence End-Point Access ... 1007
RADIUS (Device) ... **1008**

Authentication Tab 1008
RADIUS Authentication Client Settings 1008
Authentication RADIUS Server(s) Table 1010
Accounting Tab 1012
RADIUS Accounting Client Settings 1013
Accounting RADIUS Servers Table 1014
RADIUS Authentication (Device) **1016**
RADIUS Authentication Client Settings 1016
Authentication RADIUS Server(s) Table 1018
RADIUS Authentication (Devices) **1021**
RADIUS Accounting (Device) **1023**
RADIUS Accounting Client Settings 1024
Accounting RADIUS Servers Table 1025
RADIUS Accounting (Devices) **1027**
Add/Edit RADIUS Server **1028**
Add RADIUS Accounting Server **1031**
Ports (Device) 1033
Ports (Port Group) **1035**
Details View (Port Groups) 1036
Add/Remove Ports (User-Defined Port Groups) 1036
Add/Remove Ports 1038
Port Authentication Configuration **1040**
Authentication Mode 1040
Port Mode 1040
RFC3580 VLAN Authorization Tab 1042
Login Settings 1043
Automatic Re-Authentication 1045
Authenticated User Counts 1046
Convergence End-Point Access 1047

How To Use Policy 1048
How to Select on Add/Remove Windows 1048
Selecting single items 1049
Selecting multiple sequential items 1049
Selecting multiple non-sequential items 1049
How to Create and Use Domains 1049
Creating a New Domain 1050
Opening a Domain 1050
Assigning Devices to a Domain 1051
Removing Devices From a Domain 1051
Importing a File into a Domain 1052
Exporting a Domain to a File 1052
Importing Data from a Domain 1053
Saving a Domain 1053
Renaming a Domain 1053
Deleting a Domain 1053
How to Create a Role 1054
Using the Role Tabs 1054
Modifying a Role 1055
Adding Services to Roles 1055
Removing Services from a Role 1056
Modifying a Role's Default Class of Service 1056
Modifying a Role's Default Access Control 1056
Modifying a Role's Description 1056
Modifying a Role's Ports 1056
Mapping a Role to an HTTP Redirect Group 1057
Deleting a Role 1057
How to Assign a Default Role to a Port 1057
Assigning and Clearing a Default Role 1057

Assigning Default Roles to Ports 1057
Clearing Default Roles from Ports 1058
How to Create a Quarantine Role 1058
Modifying the Quarantine Role 1059
Modifying Default Values 1059
Adding/Removing Services 1059
Setting the Quarantine Role as the Default Role on a Port 1060
How to Create a Service 1060
Using the Service Tabs 1061
Creating an Automated Service 1061
Creating a Manual Service 1061
Modifying a Service 1062
Modifying a Service Description 1062
Modifying a Service Name 1062
Modifying the Roles for a Service 1062
Adding a Service to Roles 1063
Modifying the Rules for a Manual Service 1063
Modifying an Automated Service 1063
Deleting a Service 1063
How to Create a Service Group 1064
Creating a Service Group 1064
Adding Services to a Service Group 1064
Removing Services from a Service Group 1065
How to Create or Modify a Rule 1065
Creating a Rule 1065
Disabling/Enabling a Rule 1066
Deleting a Rule 1067
How to Define Rate Limits 1067
Defining Rate Limits 1068

Removing a Rate Limit 1068
How to Create a Class of Service 1069
Creating a Class of Service 1069
Creating Class of Service Port Groups 1070
Deleting a Class of Service 1071
How to Configure Transmit Queues 1071
Transmit Queue Configuration 1072
Transmit Queue Rate Shapers 1072
How to Define Traffic Descriptions 1073
How to Use Compressed Dynamic ACLs 1073
Using Range Compression 1075
Automatic Command Appreviation 1075
Viewing Compressed ACLs on the Fabric Engine Switch 1075
How to Configure Flood Control 1076
How to Create Global and Island VLANs 1077
Creating a VLAN 1078
Editing an Island VLAN ID 1078
Deleting a VLAN 1078
How to Create a Policy VLAN Island 1079
Creating a VLAN Island 1079
Modifying a VLAN Island 1079
Deleting a VLAN Island 1079
How to Create a Network Resource 1080
How to Add and Delete Devices 1081
Adding a Single Device 1082
Deleting Devices from the Database 1082
How to Create a Port Group 1083
Creating a Port Group 1083
Adding Ports to a Port Group 1083

Removing Ports from a Port Group 1083
ExtremeControl Access Control 1084
Access Control Configuration 1084
Access Control Group Editor 1085
All Access Control Engines 1085
Access Control Configuration Considerations 1085
ExtremeControl Configuration Tables 1086
General Considerations 1092
Considerations When Implementing Policy Roles 1096
Considerations when Implementing Compound Rules 1097
ExtremeWireless Controller Configuration 1097
DNS Proxy Functionality for Registration and Remediation 1098
Basic Operation 1098
Enabling DNS Proxy 1099
Backup DNS Server 1099
Troubleshooting 1099
Install the Assessment Agent Adapter on a Nessus Server 1100
How to Configure Local RADIUS Termination at the ExtremeControl Engine 1102
LDAP Authentication 1103
User Authentication Considerations 1103
Active Directory 1103
Other LDAP Servers 1105
Local Authentication 1105
User Password Considerations 1105
Certificate Configuration 1105
EAP-TLS Certificate Requirements 1106
Deploy ExtremeControl in an MSP or MSSP Environment 1107
Configuring ExtremeCloud IQ Site Engine Behind a NAT Router 1107
Defining Interface Services 1108

ExtremeControl Concepts 1109
Overview of the Access Control Tab 1109
Access Control Engines 1110
Use Scenario 1110
ExtremeControl VPN Deployment 1112
Access Control Tab Structure 1113
ExtremeControl Configuration 1114
Rule Components 1114
Compound Rules 1115
ExtremeControl Profiles 1115
AAA Configurations 1116
Portal Configurations 1116
Access Policies 1116
Registration 1118
How Registration Works 1119
Assessment 1120
Assessment Remediation 1122
How Remediation Works 1123
End-System Zones 1123
End-System Zone Use Cases 1124
Enforcing 1125
Advanced Enforce Options 1126
MAC Locking 1126
Notifications 1127
Access Control 1127
Configurations 1128
AAA 1129
Profiles 1129
Captive Portals 1129

Notifications 1130
Vendor RADIUS Attributes 1130
Add Radius Dictionary to ExtremeControl. 1130
Global & Engine Settings 1130
Configuration Evaluation Wizard 1132
User Input 1132
Authentication Results Tab 1132
Authorization Results Tab 1133
Compound Criteria Evaluation Results 1135
Access Control Configuration Rules 1136
Accessing ExtremeControl Configuration Rules 1136
Viewing Rules in the Table 1136
Creating and Editing Rules 1138
Add/Edit Rule 1140
Multi-Select Criteria for Compound Rules 1143
Authentication Rules and Add User to Authentication Mapping Window 1144
AAA Configurations Panel 1148
AAA Configurations 1150
Accessing the AAA Configuration 1150
Basic AAA Configuration 1150
Advanced AAA Configuration 1152
AAA Configurations Panel 1158
Manage LDAP Configurations 1160
Add LDAP Configuration 1161
Edit LDAP Configuration 1167
Manage RADIUS Servers 1173
Add/Edit RADIUS Server 1176
Authentication Via ExtremeCloud IQ Site Engine or Captive Portal 1177
Configuration 1177
Change Server Shared Secret 1179

Manage RADIUS Attribute Configurations Window 1180
Advanced RADIUS Server Configuration 1181
Health Check for UDP 1182
Manage RADSec Certificates 1184
RADSec Client CA Certificate 1184
RADSec Client Certificate 1184
Assign Certificate to RADSec Clients 1185
Assign Certificate to RADSec Clients 1186
Manage Entra ID (formerly Azure AD) Configurations 1187
Policy Mapping Configuration 1189
Column Definitions 1190
Add/Edit Policy Mapping 1193
Add LDAP Policy Mappings 1197
Add Attribute Value to Policy Mapping 1198
Edit LDAP Policy Mappings 1199
Edit Attribute Value to Policy Mapping Window 1200
Access Control Profiles 1200
New/Edit ExtremeControl Profile 1204
Authorization 1205
Assessment 1206
Edit Assessment Configuration 1209
Test Sets 1210
Buttons 1211
Manage Assessment Servers 1211
Manage Assessment Settings 1214
Create a Custom Scan for Agent-less Assessment 1214
Portal Configuration Overview 1218
Accessing the Portal Configuration 1218
Default Portal Configuration 1218

Network Settings 1218
Administration 1218
Website Configuration 1219
Look and Feel 1219
Guest Access and Registration 1219
Authenticated Web Access 1219
Authenticated Registration 1219
Assessment / Remediation 1219
External Captive Portal 1220
Portal Configuration Network Settings 1220
Portal Registration Administration 1222
Administration 1222
Administration Web Page Settings 1223
Portal Configuration Website Configuration 1224
Portal Configuration Look & Feel 1225
Message Strings 1226
Images 1228
Colors 1229
Style Sheets 1230
Locales 1230
Message String Editor 1230
Portal Configuration Authenticated Access and Registration 1234
Authenticated Web Access 1234
Authentication 1236
Redirection 1236
Web Access Settings 1237
Authenticated Registration 1237
Authentication 1239
Redirection 1239

Registration Settings ... 1240
Portal Configuration Guest Access ... **1243**
Registration Settings ... 1244
Secure Guest Access ... 1246
Secure Access Settings ... 1248
Sponsorship ... 1250
Portal Configuration Assessment / Remediation ... **1251**
Web Page Settings ... 1253
Remediation Attempt Limits ... 1255
Remediation Links ... 1255
Custom Remediation Actions ... 1255
Portal Web Page URLs ... 1256
Portal Configuration Guest Registration ... **1257**
Registration Settings ... 1259
Sponsorship ... 1260
Portal Web Page URLs ... 1261
Portal Configuration Provider Registration ... 1261
Facebook Registration ... 1262
Google Registration ... 1263
Microsoft Registration ... 1263
Yahoo Registration ... 1263
Salesforce Registration ... 1264
Provider Registration (Generic) ... 1264
Portal Configurations ... **1266**
Manage Custom Fields ... **1267**
Keywords ... 1270
Keyword Definitions ... 1270
Allowed Web Sites ... **1278**
Allowed URLs ... 1278

Allowed Domains 1279
Web Proxy Servers 1281
Manage Notifications 1281
Notifications Table Buttons 1282
Notifications Table 1283
Enable Default Notifications 1283
Add/Edit Notification 1285
Conditions 1287
Actions 1288
Result 1289
MAC Locking 1289
MAC to IP Mappings 1291
Access Control Engine Settings 1292
Credentials 1292
Switch Configuration 1293
Admin Web Page Credentials 1294
Admin Web Page Authentication 1294
EAP-TLS Configuration 1295
Network Settings 1295
Manage DNS Configuration 1297
Manage NTP Configuration 1297
Manage SSH Configuration 1297
SNMP Configuration 1298
Device Type Detection 1299
IP Address Resolution 1301
Hostname Resolution 1305
Username Resolution 1307
Reauthentication 1308
Miscellaneous 1310
Port Link Control 1312

NTLM Health Check ... 1312
OCSP Responder Health Check ... 1313
Entra ID Attributes ... 1313
NetBIOS ... 1314
Kerberos ... 1314
Microsoft NAP ... 1315
Auditing ... 1316
Advanced Settings ... 1316
Thread Pool Configuration ... 1317
SNMP Port Discovery Configuration ... 1318
Use Local Switch Data Lookup ... 1318
Verbosity Level Persistence ... 1318
Access Control Engine Groups ... 1319
ExtremeControl Access Control Group Editor ... 1320
Add/Edit Device Type Group ... 1324
End-Systems ... 1326
End-Systems ... 1326
Actions ... 1332
Menu Buttons ... 1333
End-System Events Tab ... 1334
Add/Edit End-System Group ... 1338
End-System Details ... 1341
Access Profile Tab ... 1341
End-System Tab ... 1343
End-System Events Tab ... 1344
Health Results Tab ... 1345
Health Results ... 1346
Health Result Details ... 1348
Buttons and Paging Toolbar ... 1349

Add/Edit Location Group **1351**
Create Time Group Window **1353**
Add/Edit User Group **1355**
Add/Edit User Group Window **1358**
Switches 1359
Edit Switches in Access Control Engine Group 1362
Add Switches to Access Control Engine Group 1366
Advanced Switch Settings 1371
All Access Control Engines 1372
Access Control Engine Enforce Preview **1375**
Details (ExtremeControl Engine) 1375
Details (ExtremeControl Engine Groups) 1378
Status 1379
Group 1379
Engines 1379
Access Control Configuration - Default 1379
Load Balancing 1380
Interfaces Window **1381**
Interface Modes 1381
Services 1382
DHCP/Kerberos Snooping 1384
Captive Portal HTTP Mirroring 1384
Tagged VLANs 1384
Static Route Configuration Window **1385**
How To Use Access Control **1386**
How to Use Device Type Profiling **1387**
Device Profiling Use Case 1387
How to Configure LDAP for End Users and Hosts via Active Directory **1397**
How to Change the Assessment Agent Adapter Password **1406**

How to Set ExtremeControl Options **1407**
Advanced Settings 1407
Assessment Server 1408
Data Persistence 1408
End-System Event Cache 1410
Enforce Warning Settings 1410
Setting Features Options 1411
Notification Engine Options 1411
Policy Defaults 1412
Status Polling and Timeout 1412
How to Set Up Registration **1414**
ExtremeControl Configuration 1415
Identifying Access Control Engines Location 1415
Defining the Unregistered Access Policy 1415
Creating the Unregistered Access Policy 1416
Configuring the Unregistered ExtremeControl Profile 1419
Configuring Policy-Based Routing 1419
Configuring the Access Control Tab (for ExtremeControl Engines and Controllers) 1421
How to Configure Pre-Registration **1423**
Configuring Pre-Registration 1423
Pre-Registering Guest Users 1428
Pre-Registering a Single User 1429
Pre-Registering Multiple Users 1430
How to Enable RADIUS Accounting **1434**
Considerations for Fixed Switching Devices 1435
Considerations for ExtremeXOS/Switch Engine Devices 1436
Guest and IoT Manager Configuration in ExtremeCloud IQ Site Engine and Access Control (Legacy) **1437**
Connecting GIM to ExtremeControl 1437
Configuring the RADIUS Protocol for GIM Authentication 1438

Creating and Configuring a GIM Domain 1439
Configuring GIM Authentication 1441
Local Password Repository 1441
LDAP 1441
Configuring Multiple Active Directory Domains 1443
Requirements 1443
Validating Multiple AD Domain Functionality 1443
Joining Multiple Active Directory Domains 1443
Important Note 1444
How to Set Up Access Policies and Policy Mappings 1445
Setting Up Your Access Policies 1446
How to Configure Credential Delivery for Secure Guest Access 1450
Configuration Steps 1450
How Secure Guest Access Works 1457
How to Configure Verification for Guest Registration 1461
Configuration Steps 1461
How User Verification Works 1465
Configure Sponsorship for Guest Registration 1468
How to Implement Facebook Registration 1471
Requirements 1471
Creating a Facebook Application 1472
Portal Configuration 1478
How Facebook Registration Works 1480
Special Deployment Considerations 1480
Wireless Clients 1480
Networks using DNS Proxy 1480
How to Implement Google Registration 1482
Requirements 1482
Creating a Google Application 1483
Portal Configuration 1488

How Google Registration Works 1490
Special Deployment Considerations 1490
Networks using DNS Proxy 1490
How to Implement Microsoft Registration 1492
Requirements 1492
Creating a Microsoft Application 1493
Portal Configuration 1498
How Microsoft Registration Works 1500
Special Deployment Considerations 1500
Networks using DNS Proxy 1500
How to Implement Yahoo Registration 1502
Requirements 1502
Creating a Yahoo Application 1503
Portal Configuration 1505
How Yahoo Registration Works 1507
Special Deployment Considerations 1507
Networks using DNS Proxy 1507
How to Implement Salesforce Registration 1509
Requirements 1509
Creating a Salesforce Application 1510
Portal Configuration 1519
How Salesforce Registration Works 1521
Special Deployment Considerations 1521
Networks using DNS Proxy 1521
How to Implement Microsoft Entra ID Registration with OpenID 1523
Requirements for Entra ID Registration 1523
Create an Entra ID Application 1524
Configure the Captive Portal 1528
Configure User Groups 1530
Configure Access Control Rules 1531
Configure Custom Security Attributes and Extension Attributes 1531

Configure a Multiple NIC Environment ... 1532
Deployment Considerations ... 1532
How to Implement 802.1X EAP-TTLS Authentication with Microsoft Entra ID ... 1534
Requirements for Entra ID Registration ... 1534
Create an Entra ID Application ... 1535
Configure AAA Rules ... 1539
Configure User Groups ... 1541
Configure Access Control Rules ... 1542
Configure Custom Security Attributes and Extension Attributes ... 1542
Configure 802.1X on the End-System ... 1543
How to Implement 802.1X EAP-TLS Authentication with Microsoft Entra ID ... 1545
Requirements for Entra ID Registration ... 1545
Generate a RADIUS Certificate for Each Access Control Engine ... 1546
Upload Certificates ... 1546
Create an Entra ID Application ... 1546
Configure AAA Rules ... 1551
Configure User Groups ... 1553
Configure Access Control Rules ... 1553
Configure 802.1X on the End-System ... 1554
How to Implement Keycloak Registration with OpenID ... 1556
Requirements for Keycloak Registration ... 1556
Prepare the Keycloak Realm, Roles, Groups, and Users ... 1557
Create a Keycloak Client ... 1559
Configure the Captive Portal ... 1562
Configure User Groups ... 1565
Configure Access Control Rules ... 1566
Verify the Configuration ... 1567
Configure a Multiple NIC Environment ... 1568
Deployment Considerations ... 1569
How to Integrate and Configure Microsoft MDM Intune/Defender ... 1571
Solution Overview ... 1571

Requirements 1571
Creating an Entra ID Application 1572
Intune Compliance Module Configuration 1575
End-System 802.1X Configuration 1576
Example of an End-System's Certificate 1577
How to Integrate and Configure VMware Workspace ONE UEM 1579
Solution Overview 1579
Requirements 1579
Workspace ONE UEM Compliance Module Configuration 1580
End-System Groups 1581
System-Generated Ownership Groups 1581
Non-Compliant Group 1581
End-System Table Columns 1582
Creating NAC Rules Based on Workspace ONE UEM Attributes 1582
Fallback Behavior 1583
Logging 1583
How to Integrate and Configure Microsoft Sentinel Export 1584
Solution Overview 1584
Requirements 1585
Deploying the ARM Template in Microsoft Azure 1588
Assigning the Monitoring Metrics Publisher Role 1589
Configuring Microsoft Sentinel Export in ExtremeCloud IQ Site Engine 1590
Custom Table Schema 1591
Logging and Reliability 1592
Add/Edit MAC Lock 1593
Getting Started with ExtremeAnalytics 1595
ExtremeAnalytics Access Requirements 1595
ExtremeAnalytics Engine Configuration 1595
Enable Flow Collection 1595
Enable Jumbo Frames 1595

Configuring Enhanced Netflow for Extreme Analytics and Extreme Wireless Controller Version 10.21 1596
How to Deploy ExtremeAnalytics in an MSP or MSSP Environment 1602
Configuring ExtremeCloud IQ Site Engine Behind a NAT Router 1602
Wireless 1604
Dashboard 1604
Overview Report 1605
Wireless Network Summary Report 1605
Network 1605
Controllers 1605
Access Points 1606
Clients 1607
Client Events Report Options 1608
Client Location Information 1608
Event Analyzer 1608
Threats (Legacy) 1608
Reports 1611
Report Features 1611
Event Analyzer 1613
RSS Graph 1615
Events Table 1616
ExtremeCompliance Overview (Legacy) 1618
Dashboard 1619
Audit Tests 1619
ExtremeCompliance Integration with Workflows 1619
ExtremeCompliance Overview (Legacy) 1619
Dashboard 1620
Audit Tests 1620
ExtremeCompliance Integration with Workflows 1620

Compliance Dashboard (Legacy) 1621
Test Results 1621
Score Over Time 1622
Device Scores 1622
Tests Run 1623
Audit Tests (Legacy) 1623
Run Regime (Legacy) 1625
Create/Edit Audit Test (Legacy) 1627
Dependent Tests 1631
Add a New Regime in ExtremeCloud IQ Site Engine (Legacy) 1632
Third Party Device Support in ExtremeCompliance (Legacy) 1633
Introduction 1633
Prerequisite 1634
Steps 1634
Adding a new audit test and verifying that the ExtremeCompliance audit was run successfully 1634
Sample regex for audit tests for Aruba devices (Legacy) 1637
Sample regex for audit tests for Cisco devices (Legacy) 1638
Reports Tab Overview 1639
Requirements 1640
Custom Report 1640
Report Designer 1640
Report Features 1640
Reports Features 1642
Reports Features 1642
Reports Catalog 1645
Reports Catalog 1645
Report Designer Overview 1647
Creating a Report 1647
Customize a System Report 1647

Create a New Report ... 1647
Modifying a Report ... 1647
Deleting a Report ... 1648
Custom Components ... 1648
How to Create a New Report Using the Report Designer ... 1648
Creating a New Report ... 1648
How to Modify a Report Using the Report Designer ... 1650
How to Customize a Report Using the Report Designer ... 1651
Customizing a System Report ... 1651
Custom Components in Report Designer ... 1652
Create a New Component ... 1652
Administration ... 1655
Profiles ... 1655
Users ... 1656
Server Information ... 1656
Licenses ... 1656
Certificates ... 1658
Options ... 1659
Device Types ... 1660
Detection and Profiling ... 1660
Table Functions ... 1660
Columns ... 1660
Buttons ... 1661
MAC OUI Vendors ... 1661
Backup/Restore ... 1661
Diagnostics ... 1662
Vendor Profiles ... 1663
Client API Access ... 1663
Profiles ... 1664
Profiles Section ... 1664
SNMP Credentials Subtab ... 1665

CLI Credentials Subtab ... 1666
Device Mapping Subtab ... 1667
Add/Edit Profile Window ... 1668
Add/Edit SNMP Credential Window ... 1670
Add/Edit CLI Credential Window ... 1672
Vendor Profiles ... **1674**
Vendor Profiles List ... 1675
Vendor Profile Details ... 1677
Users ... **1678**
Users/Groups Access ... 1679
Authentication Method ... 1679
OS Authentication (Default) ... 1680
LDAP Authentication ... 1680
RADIUS Authentication ... 1681
TACACS+ Authentication ... 1682
Okta SSO Authentication ... 1682
Network Settings ... 1683
Authorized Users Table ... 1685
Authorization Groups Table ... 1686
Add/Edit User Window ... 1688
Add/Edit Group Window ... 1689
Add Users ... 1690
Create Authorization Groups ... 1691
Add Users to Authorization Groups ... 1692
Select the Authentication Method ... 1692
Server Information ... **1693**
Client Connections ... 1693
Current Locks ... 1694
Updating a License ... **1695**
Certificates ... **1698**

Update Legacy Client Trust Mode Window 1700
Update Server Certificate Window 1702
Add Fabric Manager Certificate (Legacy) 1705
Update Server Trust Mode Window 1708
Update the Server Certificate 1710
Certificate Requirements 1710
Replacing the Certificate 1711
Verifying the Certificate 1712
Use a Browser 1712
Use OpenSSL 1712
Generating a Server Private Key and Server Certificate 1713
Generating a Server Private Key and Server Certificate using CLI 1714
Authorization Group Capabilities 1716
ExtremeCloud IQ Site Engine Event Correlation 1717
ExtremeCloud IQ Site Engine Fabric Manager 1717
Northbound API 1717
XIQ-SE Console 1719
XIQ-SE Mediation Agent 1720
XIQ-SE NAC Manager 1720
XIQ-SE OneView 1721
Administration 1722
Alarms and Events 1724
Application Analytics 1724
Compliance 1725
Network 1725
Devices 1725
Firmware 1727
Reports 1727
Wireless Manager 1727
Workflows/Scripts 1728

XIQ-SE Suite 1728
Authorization/Device Access 1728
Common Web Services 1729
Device Local Management WebView 1729
Web Service Credentials 1729
ExtremeCloud IQ Site Engine All User Options 1730
ZTP+ Registration 1730
Access Control Options 1731
Advanced 1731
Assessment Agent Adapter Credentials 1732
Data Persistence 1733
Daily Persistence 1733
Age End-Systems 1734
End-System Events 1734
Transient End-Systems 1734
End-System Information Events 1734
Health Results 1735
Wireless End-System Events 1735
Display 1735
End-System Event Cache 1736
Enforce Warnings to Ignore 1737
Entra ID Registered User Status Monitor 1737
Features 1738
Intune Compliance Module 1738
Workspace ONE UEM Compliance Module 1739
Microsoft Sentinel 1740
Notification Engine 1741
Policy Defaults 1743
Status Polling and Timeout 1744
Alarm Options 1746

Advanced 1746
Action Dispatcher Options 1747
Alarm Dispatcher Options 1748
Alarm Tracker Options 1748
Persistence Options 1748
Alarm Action Defaults 1749
Alarm History 1750
Consolidate Email 1751
Override Email 1751
Alarm/Event Logs and Tables Options 1752
Analytics Options 1755
Configuration 1755
1756
Compass Options 1757
Search Limits 1760
Search Access Control Database 1760
Search SNMP MIBs with Database Match 1760
Database Backup Options 1761
Backup Location 1762
Include Additional Data 1762
Schedule Database Backup 1762
Device Terminal Options 1764
Configuration 1764
Event Analyzer Options 1765
Proxy Server 1766
FlexView Options 1767
FlexView Display 1767
FlexView Selector 1767
Memory Usage 1768
SNMP 1768

Compliance Options (Legacy) 1769
Impact Analysis Options 1770
Availability Collector 1770
Device Availability Chart 1771
Report Generation 1771
Site Availability Chart 1771
Capacity/Health Collector 1771
Port Capacity Chart 1772
Port Health Chart 1772
Report Generation 1773
Configuration Collector 1773
Archived Devices Chart 1774
Devices with Reference Firmware Chart 1775
Report Generation 1775
Performance Collector 1775
Application Performance Chart 1776
Network Performance Chart 1776
Inventory Manager Options 1777
Data Storage Directory Path Setting 1777
File Transfer Settings 1777
FTP Server Properties Settings 1777
SCP Server Properties Settings 1779
SFTP Server Properties Settings 1782
TFTP Server Properties Settings 1785
Firmware Refresh Settings 1786
ExtremeCloud IQ Site Engine Options 1787
Data Display 1788
Date Time Format 1788
Device Tree 1789

MAC Address Display 1789
MAC OUI Web Update URL 1789
Map 1790
Message of the Day 1790
Session Limits 1790
Status Bar Message 1790
ExtremeCloud IQ Site Engine Collector Options 1791
Access Control Collection 1791
Capacity Collection 1791
Device Collection 1792
Port Collection 1793
Wireless Collection 1794
Advanced 1796
Engine Options 1798
Data Retention 1800
Server CPU Reporting 1800
Advanced 1801
Server Health Options 1803
Database Connection Monitoring 1804
Disk Usage Monitoring 1804
Low Memory Monitoring 1804
Name Resolution Options 1805
Host Name Resolution 1805
Port Name Resolution 1806
NetFlow Collector Options 1808
Configuration 1810
Alarm Dispatcher 1810
Socket 1811
Name Resolution 1811
Version 9 Template 1812
Network Monitor Cache Options 1813

Monitor Cache ... 1813
Network Monitor Trap Refresh ... 1814
Policy Options ... **1815**
Default Class of Service Mode ... 1815
Enforce/Verify ... 1816
Site Options ... **1818**
Configure Device ... 1818
Discover First SNMP Request ... 1819
Discover Seed MIBs ... 1819
Email Configuration (SMTP/API) Options ... **1820**
Email ... 1820
SMTP Email Advanced Configuration ... 1821
SMTP OAUTH Configuration ... 1821
Examples and How-tos for using OAUTH with Gmail ... 1821
How-to Enable SMTP with Microsoft Office 365 ... 1823
SNMP Options ... **1825**
Configuration ... 1825
MIB Directories on Server ... 1826
Manage SNMP Configuration ... 1826
Status Polling Options ... **1828**
Events ... 1829
Ping ... 1829
Poll Groups ... 1830
SNMP ... 1831
Syslog Options ... **1832**
Configuration ... 1832
Advanced ... 1833
TopN Collector Options ... **1834**
History ... 1836
NetFlow ... 1836

Collect Top Applications ... 1836
Collect Top Clients ... 1837
Collect Top Servers ... 1837
Wireless Event ... 1838
Trap Options ... 1839
Configuration ... 1840
Device Topology Change Trap Threshold ... 1841
Trap Engine ... 1841
Trap Poller ... 1841
Web Server Options ... 1843
HTTP Session Timeout ... 1843
HTTP Web Server ... 1843
Password Auto Complete ... 1844
Wireless Manager Options ... 1845
ZTP+ Options ... 1847
Configuration ... 1848
License Signaling ... 1849
Add Device Type Profile ... 1850
Edit Device Type Profile ... 1851
Backup/Restore ... 1853
Backup ... 1853
Restore ... 1854
Advanced ... 1854
Client API Access ... 1856
Add/Edit Client ... 1858
Using the Northbound Interface to Integrate with Third-Party Software ... 1859
Accessing NBI Tools in ExtremeCloud IQ Site Engine ... 1859
Using the NBI Explorer ... 1860
Compound Rules NAC Rule Criteria for NBI ... 1864
Link-Based Response Format ... 1864

Legacy Single-Value Parameters ... 1864
Tasks ... 1865
Workflow Dashboard ... 1865
Scheduled Tasks ... 1865
Saved Tasks ... 1865
Scripts ... 1865
Workflows ... 1866
Workflow Dashboard ... 1866
Workflow Charts ... 1867
Workflow Results ... 1868
Workflow Details ... 1870
Workflow Summary ... 1871
Activities ... 1872
Graph View ... 1873
Table View ... 1875
Devices Grid ... 1876
Buttons ... 1878
Scheduled Tasks Overview ... 1878
Saved Tasks ... 1879
Scripts Overview ... 1881
Workflows ... 1883
Workflows List ... 1884
Palette ... 1886
Designer ... 1889
Details ... 1891
General (Workflow) ... 1891
General (Element) ... 1892
Condition ... 1892
Evaluate Status ... 1894

Evaluate Variables 1894
Expression 1894
Variables 1895
Inputs 1897
Workflow 1898
Script 1898
Shell 1900
HTTP 1902
Mail 1905
CLI 1906
Outputs 1907
Menus 1908
Network OS 1911
System Workflows 1912
Compliance 1913
Config 1914
Basic Support 1914
EXOS-VPEX 1915
LAG-MLAG 1915
Inventory 1915
Backup 1915
Restart 1916
Restore 1916
Upgrade 1916
Network Essentials SLX VDX 1916
ACL Management 1916
Edge Ports Configuration 1917
Utility Actions 1918
Validation and Troubleshooting 1918

Security ... 1918
Importing Workflows ... 1919
Manage Inputs ... 1921
Search Network ... 1923
Using ExtremeCloud IQ Site Engine Search ... 1924
Search ... 1924
Search Maps ... 1924
Search with Compass ... 1924
Compass Search Types ... 1925
Search Examples ... 1926
Search your Network for an End-System MAC Address ... 1926
Search your Network for an ExtremeControl Authenticated Client IP Address ... 1926
Search your Network for a Device IP Address ... 1926
Search Options/Limitations ... 1926
Compass SNMP MIBs Descriptions ... 1927
Site Engine How-tos ... 1930
Discover Devices ... 1930
Discovering Devices ... 1931
Adding Devices ... 1932
Add Users ... 1933
Create Authorization Groups ... 1933
Add Users to Authorization Groups ... 1934
Select the Authentication Method ... 1934
How to Configure 2FA ... 1935
How to Pair a 2FA Authenticator App with your Account ... 1935
How to Reset 2FA ... 1936
Compare Device Configurations ... 1937
Selecting the Files to Compare ... 1937
Comparing the Files ... 1937

Device View 1938
Requirements 1939
Access Requirements 1939
Data Collection Requirements 1939
Device View Panels 1939
Left-Panel Device Summary 1940
Right-Panel Device Summary 1942
Launching Device View 1945
Network Tab 1945
Control Tab 1945
ExtremeCloud IQ Site Engine Maps 1945
Search 1945
Upgrade Firmware 1946
Upgrading for a Device 1946
Upgrading for a Device Type 1949
Upgrading for Fabric Manager 1951
Restart a Device 1951
Add a New Regime (Legacy) 1952
ZTP+ Device Configuration 1953
Prerequisites 1953
Select the Reference Firmware Image Location 1954
Default Device Configuration in ExtremeCloud IQ Site Engine 1955
Download XMODs (ExtremeXOS/Switch Engine devices only) 1956
General Network Configuration 1956
NOS Persona Change from Switch Engine to Fabric Engine 1957
Adding the Device to the ExtremeCloud IQ Site Engine Database 1957
General Network Configuration 1961
Adding the Device to the ExtremeCloud IQ Site Engine Database 1962
Completing Configuration and Enforcing the Engine in ExtremeAnalytics 1964
PortView 1965

Requirements ... 1965
License and Data Collection Requirements ... 1965
Access Requirements ... 1966
Launching PortView ... 1967
Launching from ExtremeCloud IQ Site Engine ... 1967
ExtremeCloud IQ Site Engine Search Tab ... 1967
ExtremeCloud IQ Site Engine Interface Summary FlexView ... 1968
Launching from Console ... 1968
Launching from NAC Manager ... 1968
AP Wireless Real Capture ... 1968
Configure and Use Real Capture ... 1969
Real Capture Example ... 1973
Restoring the Database Using the CLI ... 1975
Restore Device Configuration ... 1976
Preliminary Steps ... 1977
Required Capabilities ... 1977
Device Firmware ... 1977
Restoring a Configuration ... 1978
Cloning a Device Configuration ... 1978
Using a Configuration Template ... 1979
Configuring Enhanced Netflow for Extreme Analytics and Extreme Wireless Controller Version 10.21 in ExtremeCloud IQ Site Engine ... 1980
Configure ExtremeXOS/Switch Engine Identity Manager to Send Events to ExtremeCloud IQ Site Engine ... 1985
Schedule Tasks ... 1987
Create a New Scheduled Task ... 1987
Create a Variable ... 1990
Creating Scripts ... 1991
ExtremeCloud IQ Site Engine Scripts Overview ... 1991
Bundled ExtremeCloud IQ Site Engine Scripts ... 1992

The ExtremeCloud IQ Site Engine Script Interface 1993
Managing ExtremeCloud IQ Site Engine Scripts 1995
Create an ExtremeCloud IQ Site Engine Script 1995
Specify Runtime Settings for a Script 1998
Specify Permissions and Run Locations for Scripts 1999
Specify Network Operating System 2000
Run a Script 2001
From the Network tab 2001
From the Tasks tab 2002
View Script Results 2004
Edit a Script 2004
Delete a Script 2005
Import Scripts into ExtremeCloud IQ Site Engine 2005
Export a Script 2006
Save Script as a Task 2007
ExtremeCloud IQ Site Engine Script Reference 2007
ExtremeCloud IQ Site Engine-Specific Python Scripting Constructs 2008
Specifying the Wait Time Between Commands 2008
Metadata Tags 2008
#@MetaDataStart and #@MetaDataEnd 2008
#@ScriptDescription 2008
#@DetailDescriptionStart and #@DetailDescriptionEnd 2008
#@SectionStart and #@SectionEnd 2009
#@VariableFieldLabel 2009
ExtremeCloud IQ Site Engine-Specific TCL Scripting Constructs 2010
Specifying the Wait Time Between Commands 2010
Printing System Variables 2010
Configuring a Carriage Return Prompt Response 2011
Synchronizing the Device with ExtremeCloud IQ Site Engine 2011

Saving the Configuration on the Device Automatically 2012
Printing a String to the Output File 2012
TCL Support in ExtremeCloud IQ Site Engine Scripts 2012
Entering Special Characters 2012
Line Continuation Character 2013
Case Sensitivity in ExtremeCloud IQ Site Engine Scripts 2013
Reserved Words in ExtremeCloud IQ Site Engine Scripts 2013
ExtremeXOS/Switch Engine CLI Scripting Commands Supported in ExtremeCloud IQ Site Engine Scripts 2013
$VAREXISTS 2014
$TCL 2014
$UPPERCASE 2014
show var 2015
delete var 2015
configure cli mode scripting abort-on-error 2015
ExtremeCloud IQ Site Engine-Specific System Variables 2015
FlexViews 2017
Browser Requirements 2017
Launching FlexViews 2017
Using FlexViews 2019
Editing Writable Values 2019
Bookmarking FlexViews 2020
Exporting Table Data 2020
Add Custom FlexViews and MIBs 2021
VLAN Concepts 2021
Egress Rules (Transmitting Frames) 2022
Dynamic Egress 2022
GVRP 2025
GARP Timers 2025

Enforcing 2025
Frame Types 2025
IGMP 2026
IGMP Intervals 2026
Ingress Filtering 2027
Priority Classification 2027
Weighted Priority 2027
Verifying 2028
VLAN Identification 2028
VLAN ID (VID) 2028
PVID (Port VLAN ID) 2029
VLAN Model 2029
VLAN Learning 2029
Create and Edit a VLAN on a Device 2030
To create a new VLAN: 2030
To configure the VLAN(s) on the ports 2033
To edit the name of a VLAN: 2035
To remove devices from a VLAN: 2036
Discover Devices 2037
Discovering Devices 2038
Adding Devices 2040
Add Users 2040
Create Authorization Groups 2041
Add Users to Authorization Groups 2041
Select the Authentication Method 2041
How to Integrate and Configure Okta SSO Authentication for ExtremeCloud IQ Site Engine Users 2042
Requirements 2042
Create the Application in Okta 2042

Save the Values Required for the ExtremeCloud IQ Site Engine Configuration 2044
Assign Users to the Okta Application 2047
Configure the Okta Authentication Method in ExtremeCloud IQ Site Engine 2048
Compare Device Configurations 2051
Selecting the Files to Compare 2051
Comparing the Files 2051
Device View 2052
Requirements 2053
Access Requirements 2053
Data Collection Requirements 2053
Device View Panels 2053
Left-Panel Device Summary 2054
Right-Panel Device Summary 2056
Launching Device View 2059
Network Tab 2059
Control Tab 2059
ExtremeCloud IQ Site Engine Maps 2059
Search 2059
Upgrade Firmware 2060
Upgrading for a Device 2060
Upgrading for a Device Type 2063
Upgrading for Fabric Manager 2065
How to Restart a Device 2065
Add a New Regime in ExtremeCloud IQ Site Engine (Legacy) 2066
ZTP+ Device Configuration 2068
Prerequisites 2068
Select the Reference Firmware Image Location 2068
Default Device Configuration in ExtremeCloud IQ Site Engine 2069
Download XMODs (ExtremeXOS/Switch Engine devices only) 2070

General Network Configuration 2071
NOS Persona Change from Switch Engine to Fabric Engine 2071
Adding the Device to the ExtremeCloud IQ Site Engine Database 2071
General Network Configuration 2075
Adding the Device to the ExtremeCloud IQ Site Engine Database 2076
Completing Configuration and Enforcing the Engine in ExtremeAnalytics 2078
PortView 2079
Requirements 2079
License and Data Collection Requirements 2079
Access Requirements 2080
Launching PortView 2081
Launching from ExtremeCloud IQ Site Engine 2081
ExtremeCloud IQ Site Engine Search Tab 2081
ExtremeCloud IQ Site Engine Interface Summary FlexView 2082
Launching from Console 2082
Launching from NAC Manager 2082
AP Wireless Real Capture 2083
Configure and Use Real Capture 2083
Real Capture Example 2087
Restoring the Database Using the CLI 2088
Restore Device Configuration 2091
Preliminary Steps 2091
Required Capabilities 2091
Device Firmware 2091
Restoring a Configuration 2092
Cloning a Device Configuration 2092
Using a Configuration Template 2093
Configuring Enhanced Netflow for Extreme Analytics and Extreme Wireless Controller Version 10.21 2094

Configure ExtremeXOS/Switch Engine Identity Manager to Send Events to ExtremeCloud IQ Site Engine 2099
Schedule Tasks 2101
Create a New Scheduled Task 2101
Create a Variable 2104
Creating Scripts 2105
ExtremeCloud IQ Site Engine Scripts Overview 2105
Bundled ExtremeCloud IQ Site Engine Scripts 2106
The ExtremeCloud IQ Site Engine Script Interface 2106
Managing ExtremeCloud IQ Site Engine Scripts 2109
Create an ExtremeCloud IQ Site Engine Script 2109
Specify Runtime Settings for a Script 2112
Specify Permissions and Run Locations for Scripts 2113
Specify Network Operating System 2114
Run a Script 2115
From the Network tab 2115
From the Tasks tab 2116
View Script Results 2118
Edit a Script 2118
Delete a Script 2119
Import Scripts into ExtremeCloud IQ Site Engine 2119
Export a Script 2120
Save Script as a Task 2121
ExtremeCloud IQ Site Engine Script Reference 2121
ExtremeCloud IQ Site Engine-Specific Python Scripting Constructs 2122
Specifying the Wait Time Between Commands 2122
Metadata Tags 2122
#@MetaDataStart and #@MetaDataEnd 2122
#@ScriptDescription 2122

#@DetailDescriptionStart and #@DetailDescriptionEnd 2122
#@SectionStart and #@SectionEnd 2123
#@VariableFieldLabel 2123
ExtremeCloud IQ Site Engine-Specific TCL Scripting Constructs 2124
Specifying the Wait Time Between Commands 2124
Printing System Variables 2124
Configuring a Carriage Return Prompt Response 2125
Synchronizing the Device with ExtremeCloud IQ Site Engine 2125
Printing a String to the Output File 2125
TCL Support in ExtremeCloud IQ Site Engine Scripts 2126
Entering Special Characters 2126
Line Continuation Character 2127
Case Sensitivity in ExtremeCloud IQ Site Engine Scripts 2127
Reserved Words in ExtremeCloud IQ Site Engine Scripts 2127
ExtremeXOS/Switch Engine CLI Scripting Commands Supported in ExtremeCloud IQ Site Engine Scripts 2127
$VAREXISTS 2128
$TCL 2128
$UPPERCASE 2128
show var 2128
delete var 2128
configure cli mode scripting abort-on-error 2129
ExtremeCloud IQ Site Engine-Specific System Variables 2129
FlexViews 2131
Browser Requirements 2131
Launching FlexViews 2131
Using FlexViews 2133
Editing Writable Values 2133
Bookmarking FlexViews 2134

Exporting Table Data 2134
Add Custom FlexViews and MIBs 2135
VLAN Concepts 2135
Egress Rules (Transmitting Frames) 2136
Dynamic Egress 2136
GVRP 2139
GARP Timers 2139
Enforcing 2139
Frame Types 2139
IGMP 2140
IGMP Intervals 2140
Ingress Filtering 2141
Priority Classification 2141
Weighted Priority 2141
Verifying 2142
VLAN Identification 2142
VLAN ID (VID) 2142
PVID (Port VLAN ID) 2143
VLAN Model 2143
VLAN Learning 2143
Create and Edit a VLAN on a Device 2144
To create a new VLAN: 2144
To configure the VLAN(s) on the ports 2148
To edit the name of a VLAN: 2150
To remove devices from a VLAN: 2151
Troubleshooting 2153

Getting Started with ExtremeCloud IQ Site Engine

This topic provides information to help you get started using ExtremeCloud IQ Site Engine to view network data. It includes information on configuring ExtremeCloud IQ Site Engine access requirements, including several different access scenarios. It also provides steps for enabling the statistics and flow collection that provides ExtremeCloud IQ Site Engine reporting data, and information on ExtremeCloud IQ Site Engine scalability.

- Requirements
  - ExtremeCloud IQ Site Engine Access Requirements
    - Full Read/Write Access
    - Read-Only Access
    - Limited Read-Only Access
    - End-System Information, Read-Only Access
    - End-System Information, Read/Write Access
  - Browser Requirements
  - Screen Resolution
- Enable Report Data Collection
  - Enable Device Statistics Collection
  - Enable Interface Statistics Collection
  - Enable Wireless Controller Statistics Collection
- Enable Flow Collection
  - Enable Flow Collection on a Device
  - Enable Flow Collection on an Interface
- ExtremeCloud IQ Site Engine Scalability
- ExtremeCloud IQ Site Engine Timeout

Requirements

This section provides information on license requirements for the different ExtremeCloud IQ Site Engine features, as well as access requirements, browser requirements, and screen resolution requirements.

ExtremeCloud IQ Site Engine Access Requirements

Access to the ExtremeCloud IQ Site Engine application and its features is determined by the user's membership in an ExtremeCloud IQ Site Engine authorization group and the group's assigned capabilities. The following table lists the different ExtremeCloud IQ Site Engine access options and features, and their corresponding capabilities.

To have full read/write access to all ExtremeCloud IQ Site Engine functionality, a user must be a member of an authorization group with the capabilities shown in the following table. Optionally, users can be configured to have read-only and limited read-only access to ExtremeCloud IQ Site Engine functionality by selecting a combination of capabilities.

ExtremeCloud IQ Site Engine Access Options and Features	Required Capabilities
Launch ExtremeCloud IQ Site Engine. Allows the ability to launch the ExtremeCloud IQ Site Engine application.	XIQ-SE OneView > Access OneView
View ExtremeCloud IQ Site Engine Reports. Adds the ability to view reporting data.	XIQ-SE OneView > Access OneView Reports
View ExtremeCloud IQ Site Engine Maps. Adds the ability to view maps.	XIQ-SE OneView > Maps > Maps Read Access
View and Configure ExtremeCloud IQ Site Engine Maps. Adds the ability to view and configure maps.	XIQ-SE OneView > Maps > Maps Read/Write Access
View ExtremeCloud IQ Site Engine Wireless. Adds the ability to view wireless data.	XIQ-SE Console > Wireless Manager > Launch
View ExtremeCloud IQ Site Engine Administration. Adds access to the ExtremeCloud IQ Site Engine administration tools and the ability to enable data collection.	XIQ-SE OneView > Access OneView Administration
View ExtremeCloud IQ Site Engine Search. Adds the ability to use the ExtremeCloud IQ Site Engine Search functionality.	XIQ-SE OneView > Access OneView Search
View ExtremeCloud IQ Site Engine Network and Alarms and Events. Adds the ability to view device information and event log details.	XIQ-SE OneView > Events and Alarms > OneView Event Log Access
View ExtremeCloud IQ Site Engine alarms. Adds the ability to view current alarms in the Alarms and Events page.	XIQ-SE OneView > Events and Alarms > OneView Alarms Read Access
View and clear ExtremeCloud IQ Site Engine alarms. Adds the ability to view and clear alarms in the Alarms and Events page.	XIQ-SE OneView > Events and Alarms > OneView Alarms Read/Write Access
View ExtremeCloud IQ Site Engine Control. Adds the ability to view Dashboard, System, Health, and Data Center reports under the **Control** tab.	XIQ-SE OneView > Identity and Access > Access OneView Identity and Access Reports
View ExtremeCloud IQ Site Engine Control end-systems table. Adds the ability to view end-system information under the **Control** tab.	XIQ-SE OneView > Identity and Access > OneView End-Systems Read Access
View and modify ExtremeCloud IQ Site Engine Control end-systems table. Adds the ability to perform actions in the end-systems table, such as forcing reauthentication.	XIQ-SE OneView > Identity and Access > OneView End-Systems Read/Write Access

ExtremeCloud IQ Site Engine Access Options and Features	Required Capabilities
View ExtremeCloud IQ Site Engine Control Group Information. Adds the ability to launch the Group Editor tool from the **Control** tab > End-Systems view, and view group information.	XIQ-SE OneView > Identity and Access > OneView Group Read Access
View and Edit ExtremeCloud IQ Site Engine Control tab Group Information. Adds the ability to launch the Group Editor tool from the **Control** tab > End-Systems view, and add, edit, delete groups, and add, remove, edit group membership.	XIQ-SE OneView > Identity and Access > OneView Group Read/Write Access
View ExtremeCloud IQ Site Engine Flows. Adds the ability to view NetFlow data for devices in the network.	XIQ-SE OneView > NetFlow Read Access
View ExtremeCloud IQ Site Engine Flows and allow NetFlow Sensor Write access. Adds the ability to view NetFlow data and configure the Console NetFlow Sensor Configuration view.	XIQ-SE OneView > NetFlow Read/Write Access
Allow Web FlexView read access. Adds the ability to launch a FlexView from the ExtremeCloud IQ Site Engine **Network** tab.	XIQ-SE OneView > FlexView > OneView FlexView Read Access
Allow Web FlexView Write access. Adds the ability to launch and edit a FlexView from the ExtremeCloud IQ Site Engine **Network** tab.	XIQ-SE OneView > FlexView > OneView FlexView Read/Write Access
Allow Wireless Controller Automatic WebView Login ability. Adds the ability to launch local management for wireless controllers without requiring a login, as long as the user's credentials are good. Users who do not have this capability are required to log in.	XIQ-SE Suite > Device Local Management WebView > Auto Login to Web Local Management for ExtremeWireless Wireless Controllers
Allow Check for Firmware Updates ability. Adds the ability to check for firmware updates from the ExtremeCloud IQ Site Engine **Network** tab.	XIQ-SE Suite >XIQ-SE All User Options > Request and Configure ExtremeNetworks.com Support
Allow Create Policy Rule ability. Adds the ability to create a policy rule in NetFlow tables.	XIQ-SE > Access Control > Policy
Add Devices. Adds the ability to add devices in the ExtremeCloud IQ Site Engine **Network** tab.	XIQ-SE Suite > Devices > Add, Discover and Import
Delete Devices. Adds the ability to delete devices in the ExtremeCloud IQ Site Engine **Network** tab.	XIQ-SE Suite > Devices > Delete
Compare Configurations. Adds the ability to compare archived device configurations in either the ExtremeCloud IQ Site Engine **Network** tab or the Archive Details Report available in the ExtremeCloud IQ Site Engine **Reports** tab.	Inventory Manager > Configuration Archive Management > View/Compare Configurations

Here are several scenarios that show how different ExtremeCloud IQ Site Engine user access levels can be configured based on assigned capabilities.

Use Case 1: Full Read/Write Access

To provide full read/write access to all ExtremeCloud IQ Site Engine functionality, configure user membership in an authorization group assigned the following capabilities:

- XIQ-SE OneView > Access OneView
- XIQ-SE OneView > Access OneView Reports
- XIQ-SE OneView > Access OneView Search
- XIQ-SE OneView > Access OneView Administration
- XIQ-SE OneView > NetFlow Read/Write Access
- XIQ-SE OneView > Maps > Maps Read/Write Access
- XIQ-SE Console > Wireless Manager > Launch
- XIQ-SE OneView > Events and Alarms > OneView Event Log Access
- XIQ-SE OneView > Events and Alarms > OneView Alarms Read/Write Access
- XIQ-SE OneView > FlexView > OneView FlexView Read/Write Access
- XIQ-SE OneView > Identity and Access > Access OneView Identity and Access Reports
- XIQ-SE OneView > Identity and Access > OneView End-Systems Read/Write Access
- XIQ-SE OneView > Identity and Access > OneView Group Read/Write Access
- XIQ-SE OneView > Access Control > Policy
- XIQ-SE > Device Local Management WebView > Auto Login to Web Local Management for ExtremeWireless Wireless Controllers
- XIQ-SE Suite > XIQ-SE All User Options > Request and Configure ExtremeNetworks.com Support
- XIQ-SE Suite > Devices > Add, Discover and Import
- XIQ-SE Suite > Devices > Delete
- Inventory Manager > Configuration Archive Management > View/Compare Configurations

Use Case 2: Read-Only Access

To provide read-only access to all ExtremeCloud IQ Site Engine reports and FlexViews, configure user membership in an authorization group assigned the following capabilities:

- XIQ-SE OneView > Access OneView
- XIQ-SE OneView > Access OneView Reports
- XIQ-SE OneView > Access OneView Search
- XIQ-SE OneView > NetFlow Read Access
- XIQ-SE OneView > Maps > Maps Read Access
- XIQ-SE Console > Wireless Manager > Launch
- XIQ-SE OneView > Events and Alarms > OneView Event Log Access
- XIQ-SE OneView > Events and Alarms > OneView Alarms Read Access

- XIQ-SE OneView > FlexView > OneView FlexView Read Access
- XIQ-SE OneView > Identity and Access > Access OneView Identity and Access Reports
- XIQ-SE OneView > Identity and Access > OneView End-Systems Read Access
- XIQ-SE OneView > Identity and Access > OneView Group Read Access

Use Case 3: Limited Read-Only Access

To provide limited read-only access to only ExtremeCloud IQ Site Engine reporting and wireless data, configure user membership in an authorization group assigned the following capabilities:

- XIQ-SE OneView > Access OneView
- XIQ-SE OneView > Access OneView Reports
- XIQ-SE Console > Wireless Manager > Launch

Use Case 4: End-System Information, Read-Only Access

To provide read-only access to ExtremeCloud IQ Site Engine end-system information, configure user membership in an authorization group assigned the following capabilities:

- XIQ-SE OneView > Access OneView
- XIQ-SE OneView > Identity and Access > OneView End-Systems Read Access

Use Case 5: End-System Information, Read/Write Access

To provide read/write access to ExtremeCloud IQ Site Engine end-system information, configure user membership in an authorization group assigned the following capabilities:

- XIQ-SE OneView > Access OneView
- XIQ-SE OneView > Identity and Access > OneView End-Systems Read/Write Access

Browser Requirements

The following web browsers are supported:

- Microsoft Edge
- Mozilla Firefox 34 and later
- Google Chrome 33.0 and later

Browsers must have JavaScript enabled in order for the web-based views to function.

While it is not required that cookies are enabled, impaired functionality results if they are not. This includes (but is not limited to) the ability to generate PDFs and persist table configurations such as filters, sorting, and column selections.

Screen Resolution

For optimum display of graphs and tables, ExtremeCloud IQ Site Engine is best viewed on a system with a minimum screen resolution of 1280x1024.

Enable Report Data Collection

To view ExtremeCloud IQ Site Engine reporting data, you must enable statistics collection for your network devices. You must be a member of an authorization group that has been assigned the XIQ-SE OneView > Access XIQ-SE OneView and Administration capability to enable data collection. Data collection is only available with the NMS license and above.

Enable Device Statistics Collection

To view ExtremeCloud IQ Site Engine device reports, you must enable statistics collection for your network devices from either ExtremeCloud IQ Site Engine Devices, or the Console device tree or **Device Properties** tab. Statistics can be collected in a historical or threshold alarms collection mode.

- **Historical Mode** — Device and physical port statistics are saved to the database and aggregated over time, and are then used in ExtremeCloud IQ Site Engine reports. The device statistics are also used for active threshold alarms configured in the Console Alarms Manager.

  NOTE: Enabling Historical Device Statistics Collection may use substantial disk space.

- **Threshold Alarms Mode (formerly Monitor Mode**) — Device statistics are saved to a Threshold Alarms cache for one hour and then dropped. These statistics are used for active threshold alarms, configured in the Console Alarms Manager, but not for ExtremeCloud IQ Site Engine reporting.

  NOTE: The Threshold Alarms mode option is not available if you have disabled Threshold Alarms Collection in the OneView Collector Advanced Settings window in Administration > Options.

If you are enabling statistics collection on an ExtremeControl engine, Application Detection engine, or ExtremeWireless Controller, read through the following notes:

- **Access Control Engine**
  When collecting statistics on an Access Control engine, the engine must be added to ExtremeCloud IQ Site Engine to collect all engine statistics. In addition, Threshold Alarms mode is not supported on Access Control engines.
- **Application Detection Engine**
  When collecting statistics on an Application Detection engine, the engine must be added to the Analytics > Configuration > ExtremeAnalytics Engines table in order for ExtremeCloud IQ

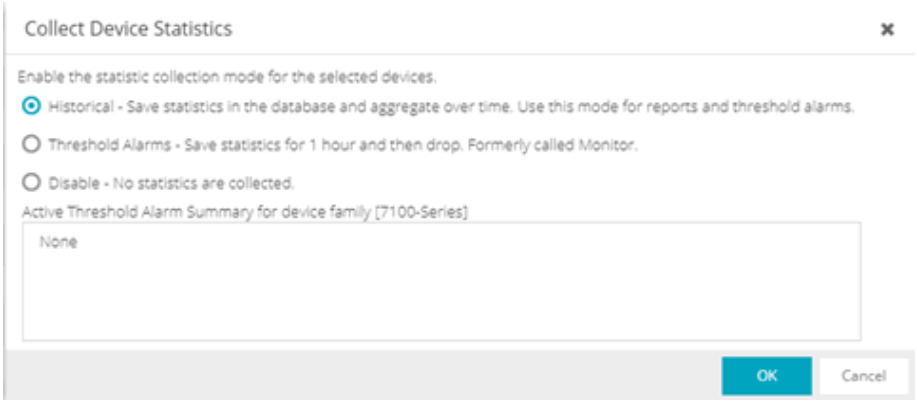
Site Engine to collect all Application Detection statistics. In addition, Threshold Alarms mode is not supported on Application Detection engines.

- **ExtremeWireless Controller**
  Wireless Controller statistics collection is configured separately from other devices.

Enabling Device Statistics Collection

Use the following steps to enable device statistics collection.

1. You can enable statistics collection from either ExtremeCloud IQ Site Engine or Console:
   - In the **Network** tab, right-click one or more devices (multiple devices must be in the same device family) and select **Device > Collect Device Statistics**. You can also select the **Menu** icon ( ) in the upper left corner of the **Network** tab and select **Device > Collect Device Statistics**.
   - In the Console device tree or **Device Properties** tab, right-click one or more devices (multiple devices must be in the same device family) and select OneView > Collect Device Statistics.
2. From the Collect Device Statistics window, select the statistic collection mode you want to use: **Historical, Threshold Alarms (formerly Monitor), or Disable**.



All active threshold alarms configured in the ExtremeCloud IQ Site Engine **Alarms and Events** tab (for the selected device family) that use the collected statistics display in the Active Threshold Alarms Summary box. If the selected devices do not match any active threshold alarms, this box is blank. To reduce unnecessary statistic collection, do not enable Threshold Alarms mode on devices that do not match any active threshold alarms.

TIP: A summary event is generated daily in the **Alarms and Events** > **Events** tab that shows the number of device with statistic collection enabled where corresponding threshold alarms are not configured.

3. Select **OK**. ExtremeCloud IQ Site Engine begins collecting statistics for the selected devices.

Enable Interface Statistics Collection

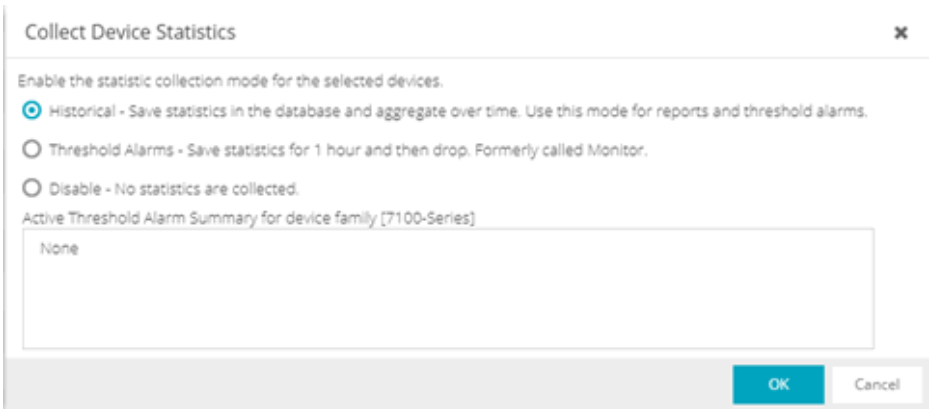
To view ExtremeCloud IQ Site Engine interface reports, you must enable statistics collection for your device interfaces from either the ExtremeCloud IQ Site Engine **Network** tab, or the **Console Port Properties** tab or Interface Summary FlexView. Statistics can be collected in a historical collection mode or a threshold alarms collection mode.

- Historical Mode — Interface statistics are saved to the database and aggregated over time, used in ExtremeCloud IQ Site Engine reports. The interface statistics are also used for active threshold alarms configured in the **Alarms and Events** tab.
- Threshold Alarms Mode (formerly Monitor Mode) — Interface statistics are saved for one hour and then dropped. These statistics are used for active threshold alarms configured in the Console Alarms Manager, but not for ExtremeCloud IQ Site Engine reporting. (Note that the Threshold Alarms mode option is not available if you have disabled Threshold Alarms Collection in the OneView Collector Advanced Settings window in the **Administration** > **Options** tab.)

Enabling Interface Statistics Collection

Use the following steps to enable interface statistics collection.

1. You can enable statistics collection from either ExtremeCloud IQ Site Engine or Console:
    - On the **Network** tab, select the device name link to open the Interface Summary FlexView. In the FlexView, right-click on one or more interfaces and select Collect Interface Statistics.
    - On the **Network** tab, right-click on a device and select Port Tree. In the Port Tree, select an interface, right-click and select **Collect Interface Statistics**.
    - In the **Console Port Properties** tab or Interface Summary FlexView, right-click one or more interfaces and select the OneView > Collect Interface Statistics.
2. From the Collect Device Statistics window, select the statistic collection mode you want to use: **Historical, Threshold Alarms (formerly Monitor), or Disable**.



All active threshold alarms configured in the ExtremeCloud IQ Site Engine **Alarms and Events** tab (for the selected device family) that use the collected statistics display in the Active Threshold Alarm Summary box. If the selected devices do not match any active threshold alarms, this box is blank. To reduce unnecessary statistic collection, do not enable Threshold Alarms mode on devices that do not match any active threshold alarms.

TIP: A summary event is generated daily in the **Alarms and Events** > **Events** tab that shows the number of device with statistic collection enabled where corresponding threshold alarms are not configured.

3. Select **OK**. ExtremeCloud IQ Site Engine begins collecting statistics for the selected interfaces.

Enable Wireless Controller Statistics Collection

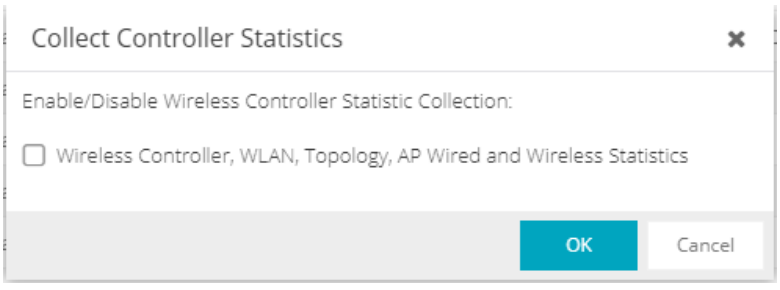
Wireless Controller statistics collection is configured separately from other devices. When you enable Wireless Controller statistics collection, it includes Wireless Controller, WLAN, Topology, and AP wired and wireless statistics, and you also have the option to collect wireless client statistics.

You can enable statistics collection for multiple controllers, however the group cannot contain a mix of devices and wireless controllers. The group must include only controllers.

Enabling Wireless Controller Statistics Collection

Use the following steps to enable wireless controller statistics collection.

1. You can enable statistics collection from either ExtremeCloud IQ Site Engine or Console:
   - On the **Network** tab, right-click one or more wireless controllers and select **Device** > **Collect Device Statistics**. You can also select the menu icon (☰) in the upper left corner of the **Network** tab and select **Device** > **Collect Device Statistics**.
   - In the Console device tree or **Device Properties** tab, right-click one or more wireless controllers and select OneView > Collect Device Statistics.
2. From the Collect Controller Statistics window, select the statistics you want to collect.



3. Select **OK**. ExtremeCloud IQ Site Engine begins collecting statistics for the selected controllers.

Enable Flow Collection

To view ExtremeCloud IQ Site Engine Flow and Application reports, you must enable NetFlow or application telemetry on the device and enable flow collection for the device interfaces. N-Series, S-Series, and K-Series devices support NetFlow flow collection and ExtremeXOS/Switch Engine devices support application telemetry flow collection. You must be a member of an authorization group assigned the XIQ-SE OneView > NetFlow Read/Write Access capability to view NetFlow data or the **XIQ-SE OneView > Application Telemetry Read/Write Access** capability to view application telemetry data and enable flow collection in ExtremeCloud IQ Site Engine.

Enable Flow Collection on a Device

In ExtremeCloud IQ Site Engine, open the Advanced Configuration panel. Select an ExtremeAnalytics engine and use the **Flow Collection Type** drop-down to select the type of flow collection supported by your device. Use the **Flow Sources** or **Application Telemetry Sources** section of the window (depending on the **Flow Collection Type** selected) to add a device as a flow collection source.

Enable Flow Collection on an Interface

In PortView, you can enable flow collection from the Configure Collection State section of the **Interface Details** tab.

ExtremeCloud IQ Site Engine Scalability

ExtremeCloud IQ Site Engine supports reporting on 20,000 objects as determined by the number of devices and interfaces being monitored, along with polling interval and data storage periods. Below are two example network configurations resulting in collected objects under 20,000. For additional information on tuning your deployment, please contact Extreme Networks Support.

Variables		Scenario 1	Scenario 2
Data Retention	Raw Data	7 Days	7 Days
	Hourly Rollups	8 Weeks	8 Weeks
	Daily Rollups	6 Months	6 Months
Polling Interval		15 Minutes	15 Minutes
Devices	Wireless Controllers	5	10
	Wireless APs	1000	2000
	Advanced Switch/Routers	150	50
	Advanced Interfaces	1000	200
	Servers	150	50

Variables	Scenario 1	Scenario 2
Collected Objects	19,450	18,630

ExtremeCloud IQ Site Engine Timeout

ExtremeCloud IQ Site Engine automatically times out after a specified amount of time, specified in the **HTTP Session Timeout** section of the Web Server view in the **Administration** > **Options** tab. A dialog box appears to warn you when you are two minutes from timing out of an ExtremeCloud IQ Site Engine web page. For additional information, see the Web Server Options Help topic.

NOTE: The ExtremeCloud IQ Site Engine, ExtremeControl, and ExtremeAnalytics Virtual Engine Installation Guide includes an overview of ExtremeCloud IQ Site Engine, ExtremeControl, and ExtremeAnalytics virtual engine deployment requirements and how to deploy a virtual engine on a VMware® and Hyper-V server.

Upgrading Fabric Manager (Legacy)

Use the following procedure to upgrade your version Fabric Manager.

Prerequisites

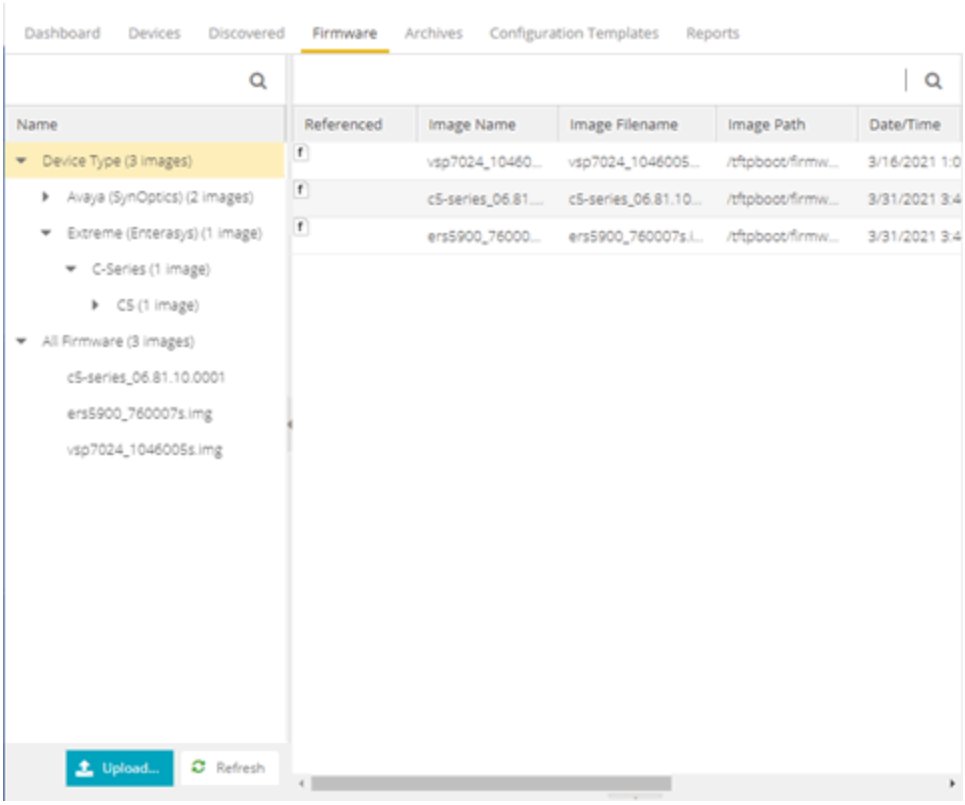
- Upgrade ExtremeCloud IQ Site Engine to the later version before you upgrade Fabric Manager to the corresponding build number.
- Ensure that both the current and target ExtremeCloud IQ Site Engine and Fabric Manager build numbers are the same.
- Download the latest upgrade bundle from the Extreme Networks software download Portal.
- Change **Login Information** from **Anonymous** to appropriate SCP credentials in the SCP Server Properties section in the **Administration** > **Options** > **Inventory Manager** > **File Transfer** tab.

NOTE: After you deploy Fabric Manager and then register with ExtremeCloud IQ Site Engine, only the user credential associated with the Fabric Manager profile has SSH login access.

Upgrade Procedure

1. Open the **Network** tab in ExtremeCloud IQ Site Engine.

2. Select the **Firmware** tab.

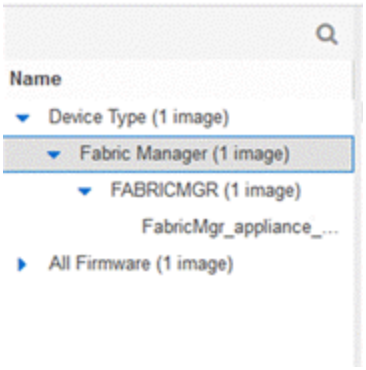


3. On the left panel, select **Upload** .
4. In the Directory field, select the **SCP** radio button and select **Upload**.

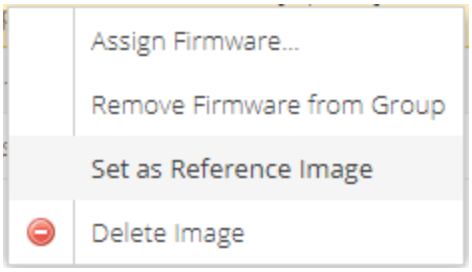


5. Select on **Drop files here or select to browse** and select the previously downloaded upgrade bundle.
6. Select the **Upload** button to initiate the bundle upload to the ExtremeCloud IQ Site Engine server.

   Once the upload is completed successfully, if not previously added after selecting the **Refresh** button, a new entry appears under Device Type called Fabric Manager.

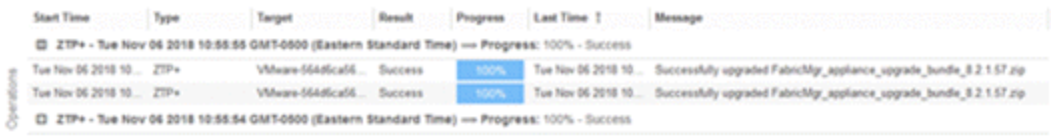


7. Navigate through the newly added Device type until you see the bundle image listed.
8. Right-click the bundle listed on the main panel and select **Set as Reference Image**.

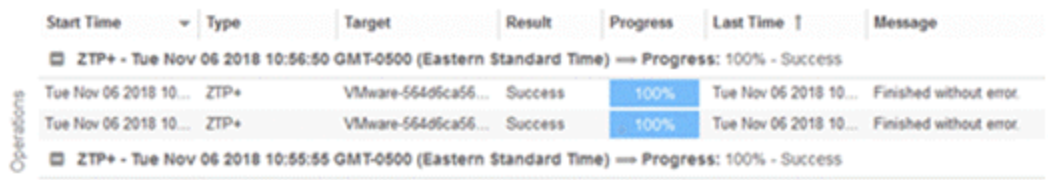


This step sets this image bundle as the Reference upgrade image for Fabric Manager. The upgrade process to get triggered by default can take **up to five minutes** depending on the poll interval set on ExtremeCloud IQ Site Engine.

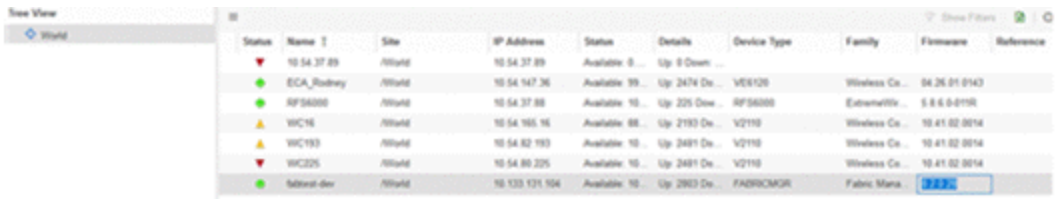
9. Open the **Operations** log on ExtremeCloud IQ Site Engine and wait until a log of type 'ZTP+' with the message `Successfully upgraded FabricMgr_appliance_upgrade_bundle_<version_number>.zip` appears.



This is followed by a message `Finished without error` to indicate the upgrade operation has been completed by the ZTP+.



10. When the upgrade is complete, the details on Fabric Manager are updated to the latest version.



Post Upgrade Steps

1. Ensure that the same user credential associated with the Fabric Manager profile has SSH login access.
2. Navigate to the previously added and referenced upgrade image and un-reference it by right selecting the bundle and then selecting **Unset as Reference Image**.

- ExtremeCloud IQ Site Engine Fabric
- Fabric Connect

ExtremeCloud IQ Site Engine Licensing

ExtremeCloud IQ Site Engine includes all the features and functionality of Extreme Management Center. If you are an existing Extreme Management Center customer, contact your representative to have your Extreme Management Center license migrated to an ExtremeCloud IQ Site Engine license. The ExtremeCloud IQ Site Engine license also includes licensing for ExtremeAnalytics.

NOTES:

- ExtremeCloud IQ Site Engine is a subscription-based -only licensing model.
- ExtremeCloud IQ Site Engine is not compatible with ExtremeCloud IQ Connect level account. The account level must be Pilot or Extreme Platform ONE.
- ExtremeCloud IQ Site Engine in Connected mode is fully compatible with the Extreme Platform ONE licensing model starting in version 25.02.10
- ExtremeCloud IQ Site Engine in Air Gap mode is fully compatible with the Extreme Platform ONE licensing model starting in version 25.05.10

You can view ExtremeCloud IQ and ExtremeCloud IQ Site Engine license information by accessing Administration > Licenses.

This Help topic includes information on the following:

- ExtremeCloud IQ Pilot Twin Subscription Provides Backwards Compatibility
- Licensing for Devices in Connected Mode
- Licensing for Devices in Air Gap Mode
- Revoke Air Gap License
- License Limits and Violations
- Licensing for ExtremeControl

There are tiers of licenses for ExtremeCloud IQ Site Engine and devices:

- No License - Status-Only devices
- Platform ONE Tier 3rd Party - 3rd party devices, Extreme Campus Controller, ExtremeCloud IQ Controller, WiNG wireless devices, and devices not natively supported by ExtremeCloud IQ Site Engine
- Navigator - 3rd party devices, Extreme Campus Controller, ExtremeCloud IQ Controller, WiNG wireless devices, and devices not natively supported by ExtremeCloud IQ Site Engine
- Platform ONE Tier A - Natively supported Extreme devices of tier A
- Platform ONE Tier B - Natively supported Extreme devices of tier B
- Platform ONE Tier C - Natively supported Extreme devices of tier C

- Platform ONE Tier D - Natively supported Extreme devices of tier D
- Pilot - Natively supported Extreme devices of any tier

NOTE:

- If the license of the appropriate tier is not available then you can use a higher license tier instead.
- The license tier hierarchy from lowest to highest is: No License - Tier 3rd Party - Navigator - Tier A - Tier B - Tier C - Tier D - Pilot.
- In Air Gap deployment, the **Administration > Licenses > Realign License Assignment** button triggers the process of automatic realignment of licenses to devices. The device is assigned the best-fit available Tier. In Connected mode deployment, use Unmanage/Manage in Extreme Platform ONE or ExtremeCloud IQ to realign licenses.
- Device stacks can include devices from different families and use licenses of different tiers, subject to the following requirements:
    - Licenses must all be of the same Standard or Pilot level. Combinations are not allowed.
    - Each unit in a stack requires a license. If there are insufficient subscriptions to license all devices in a stack, then the entire stack is unmanaged.

ExtremeCloud IQ Site Engine can be deployed in two ways, using Connected mode or Air Gap mode:

- Connected mode:
    - ExtremeCloud IQ - Site Engine uses ExtremeCloud IQ to determine if you meet or exceed the license limits for each license type.
    - All ExtremeCloud IQ - Site Engines connected to the same customer account share a pool of licenses, one serial number consumes one license entitlement, regardless of the number of monitoring entities.
    - ExtremeCloud IQ - Site Engine shares information with ExtremeCloud IQ.
    - ExtremeCloud IQ can cooperate with ExtremeCloud IQ - Site Engine.
- Air Gap mode:
    - ExtremeCloud IQ - Site Engine does not require internet access.
    - ExtremeCloud IQ - Site Engine uses a license file to determine if you meet or exceed the license limits for each license type.
    - ExtremeCloud IQ - Site Engines can not share licenses.

	Devices that do not have serial numbers or MAC addresses in Extreme Management Center must be Rediscovered after you upgrade to ExtremeCloud IQ Site Engine in Connected mode before they can be onboarded to ExtremeCloud IQ.
NOTE:	If your number of devices exceeds your licenses available, ExtremeCloud IQ Site Engine transitions to a license violation state and your access to ExtremeCloud IQ Site Engine features and functionality is degraded. To resolve the license shortage you need to access the Extreme Networks License Portal or ExtremeCloud IQ to evaluate the quantities of available Pilot, Navigator, Platform ONE, and NAC licenses versus the number of licenses required by ExtremeCloud IQ Site Engine.

ExtremeCloud IQ Pilot Twin Subscription Provides Backwards Compatibility

Some versions of ExtremeCloud IQ Site Engine and ExtremeCloud IQ Controller do not support Extreme Platform ONE subscriptions. To provide you with the necessary time to upgrade to later versions, Extreme Networks provides every Extreme Platform ONE standard subscription with an ExtremeCloud IQ Pilot Twin subscription with the same start date, end date, and licensed quantity.

- The Extreme Portal shows both Extreme Platform ONE Standard and ExtremeCloud IQ Pilot Twin subscriptions
- ExtremeCloud IQ does not show ExtremeCloud IQ Pilot Twin subscriptions
- Extreme Platform ONE does not show ExtremeCloud IQ Pilot Twin subscriptions
- ExtremeCloud IQ Site Engine version 25.2 and earlier supports ExtremeCloud IQ Pilot and ExtremeCloud IQ Pilot Twin subscriptions
- ExtremeCloud IQ Site Engine version 25.5 and later supports ExtremeCloud IQ Pilot and Extreme Platform ONE subscriptions
- ExtremeCloud IQ Controller versions support ExtremeCloud IQ Pilot and ExtremeCloud IQ Pilot Twin subscriptions

NOTE:	If you purchased an Extreme Platform ONE subscription and are running management application versions which are not compatible with Extreme Platform ONE subscriptions, you can use the provided ExtremeCloud IQ Pilot Twin subscription.

Licensing for Devices in Connected Mode

When ExtremeCloud IQ Site Engine has been onboarded, it starts sending requests to add the devices from its database to ExtremeCloud IQ.

As devices are added and discovered in ExtremeCloud IQ Site Engine, they are onboarded to ExtremeCloud IQ, with a request for a license of the appropriate tier (Navigator, Pilot, Extreme Platform ONE, or No License) that each device will require. ExtremeCloud IQ assigns a license of the appropriate tier (No License, Tier 3rd Party, Navigator, Tier A, Tier B, Tier C, Tier D, Pilot).

Devices may be marked as Unmanaged in ExtremeCloud IQ, which means they are not using a license and available features are very limited.

The following grid details the type of license required by each device and engine type:

Device Type	License Tier Type	Number of Licenses Per Device
Extreme-supported Device Tier D (Includes: Universal Platform Fabric Engine 5720, Universal Platform Switch Engine 5720, Universal Platform Fabric Engine 7520, Universal Platform Switch Engine 7520, Universal Platform Fabric Engine 7720, Universal Platform Switch Engine 7720, Universal Platform Fabric Engine 7830, Universal Platform Switch Engine 7830, Summit Series X670, Summit Series X670V, Summit Series X670-G2, Summit Series X690, Summit Series X695, Summit Series X770, Summit Series X870)	Tier D	1 for each unit
Extreme-supported Device Tier D (Includes: VSP series 7200, VSP series 7400, VSP series 8000, VSP series 8600)	Tier D	1
Extreme-supported Device Tier C (Includes: Universal Platform Fabric Engine 5520, Universal Platform Switch Engine 5520, Summit Series X460-G2, Summit Series X465, Summit Series X590, Summit Series X620, ERS Series 5900)	Tier C	1 for each unit
Extreme-supported Device Tier C (Includes: VSP series 4000, VSP series 4900)	Tier C	1

Device Type	License Tier Type	Number of Licenses Per Device
Extreme-supported Device Tier B (Includes: Universal Platform Fabric Engine 5420, Universal Platform Switch Engine 5420, Summit Series X450-G2, ERS Series 4800, ERS Series 4900)	Tier B	1 for each unit
Extreme-supported Device Tier A (Includes: Universal Platform Fabric Engine 5320, Universal Platform Switch Engine 5320, Universal Platform Fabric Engine 5322, Universal Platform Switch Engine 5322, Universal Platform Fabric Engine 5120, Universal Platform Switch Engine 5120, Universal Platform Fabric Engine 4220, Universal Platform Switch Engine 4220, Universal Platform Switch Engine 4120, Summit Series X440-G2)	Tier A	1 for each unit
Extreme-supported Devices (Includes: SLX, Extreme Access Series, Fabric Manager, ICX Series, Security Appliances, MLXe Series, VDX Series, Summit Series X435)	Tier A	1
Extreme-supported Legacy Devices (includes: A Series, B Series, C Series, 7100 Series, 200 Series, SSA Series, ERS Series 8xxx, ERS Series 3xxx)	Tier A	1 for each unit
Extreme-supported Chassis (Includes S series, K series, N series, E series, Black Diamond, Black Diamond X, X series, MLXe series, VDX series, SLX series)	Tier A	1 for each chassis
ExtremeControl Engine, ExtremeAnalytics Engine, vSensor	Tier A	1
ExtremeCloud IQ Site Engine*	Tier A	1
All Other Devices (Includes Non-Extreme Device)	Tier 3rd Party	1
Devices with Ping-Only profile	No License	0

*There is one license required for the ExtremeCloud IQ Site Engine itself. Each ExtremeCloud IQ Site Engine consumes only one license even if there are multiple ExtremeCloud IQ Site Engine devices in the device list.

NOTE: For Port Extenders V300, Port Extenders V400, HiveOS APs (IQE) and Dell N-Series, a Tier A license is required, but currently not enforced in ExtremeCloud IQ Site Engine. These devices are not onboarded to ExtremeCloud IQ through ExtremeCloud IQ Site Engine.

For WiNG APs, a Tier 3rd party license is required, but currently not enforced in ExtremeCloud IQ Site Engine. These devices are not onboarded to ExtremeCloud IQ through ExtremeCloud IQ Site Engine.

Licensing for Devices in Air Gap Mode

ExtremeCloud IQ Site Engine uses licenses stored locally in a license file. This ensures ExtremeCloud IQ Site Engine does not require an internet connection to verify licenses are available as you add devices.

NOTE: Licenses in one installation of ExtremeCloud IQ Site Engine in Air Gap mode cannot be shared with other installations of ExtremeCloud IQ Site Engine.

As devices are added and discovered in ExtremeCloud IQ Site Engine, they consume a license of the appropriate tier (No License, Navigator, Tier A, Tier B, Tier C, Tier D, Pilot) that each device requires against the total listed in the license file.

Devices may be marked as Unmanaged, which means they are not using a license and available features are very limited.

The following grid details the type of license required by each device and engine type:

Device Type	License Tier Type	Number of Licenses Per Device
Extreme-supported Device Tier D (Includes: Universal Platform Fabric Engine 5720, Universal Platform Switch Engine 5720, Universal Platform Fabric Engine 7520, Universal Platform Switch Engine 7520, Universal Platform Fabric Engine 7720, Universal Platform Switch Engine 7720, Universal Platform Fabric Engine 7830, Universal Platform Switch Engine 7830, Summit Series X670, Summit Series X670V, Summit Series X670-G2, Summit Series X690, Summit Series X695, Summit Series X770, Summit Series X870)	Tier D	1 for each unit
Extreme-supported Device Tier D (Includes: VSP series 7200, VSP series 7400, VSP series 8000, VSP series 8600)	Tier D	1
Extreme-supported Device Tier C (Includes: Universal Platform Fabric Engine 5520, Universal Platform Switch Engine 5520, Summit Series X460-G2, Summit Series X465, Summit Series X590, Summit Series X620, ERS Series 5900)	Tier C	1 for each unit
Extreme-supported Device Tier C (Includes: VSP series 4000, VSP series 4900)	Tier C	1
Extreme-supported Device Tier B (Includes: Universal Platform Fabric Engine 5420, Universal Platform Switch Engine 5420, Summit Series X450-G2, ERS Series 4800, ERS Series 4900)	Tier B	1 for each unit

Device Type	License Tier Type	Number of Licenses Per Device
Extreme-supported Device Tier A (Includes: Universal Platform Fabric Engine 5320, Universal Platform Switch Engine 5320, Universal Platform Fabric Engine 5322, Universal Platform Switch Engine 5322, Universal Platform Fabric Engine 5120, Universal Platform Switch Engine 5120, Universal Platform Fabric Engine 4220, Universal Platform Switch Engine 4220, Universal Platform Switch Engine 4120, Summit Series X440-G2)	Tier A	1 for each unit
Extreme-supported Devices (Includes: SLX, Extreme Access Series, Fabric Manager, ICX Series, Security Appliances, MLXe Series, VDX Series, Summit Series X435, HiveOS (IQE), Dell N-Series)	Tier A	1
Extreme-supported Legacy Devices (includes: A Series, B Series, C Series, 7100 Series, 200 Series, SSA Series, Port Extenders V300, Port Extenders V400, ERS Series 8xxx, ERS Series 3xxx)	Tier A	1 for each unit
Extreme-supported Chassis (Includes S series, K series, N series, E series, Black Diamond, Black Diamond X, X series, MLXe series, VDX series, SLX series)	Tier A	1 for each chassis
ExtremeControl Engine, ExtremeAnalytics Engine, vSensor	Tier A	1
ExtremeCloud IQ Site Engine*	Tier A	1
All Other Devices (Includes Non-Extreme Device)	Tier 3rd Party	1
Devices with Ping-Only profile	No License	0

*There is one license required for the ExtremeCloud IQ Site Engine itself. Each ExtremeCloud IQ Site Engine consumes only one license even if there are multiple ExtremeCloud IQ Site Engine devices are in the device list.

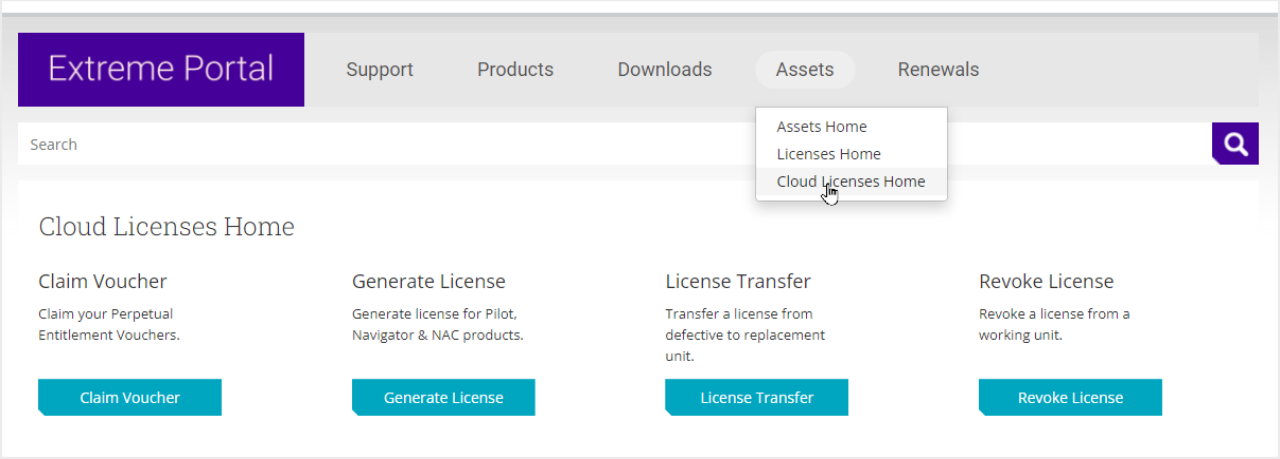
Revoke Air Gap License

NOTE: A maximum of 10 Air Gap licenses can be revoked in one revocation file.

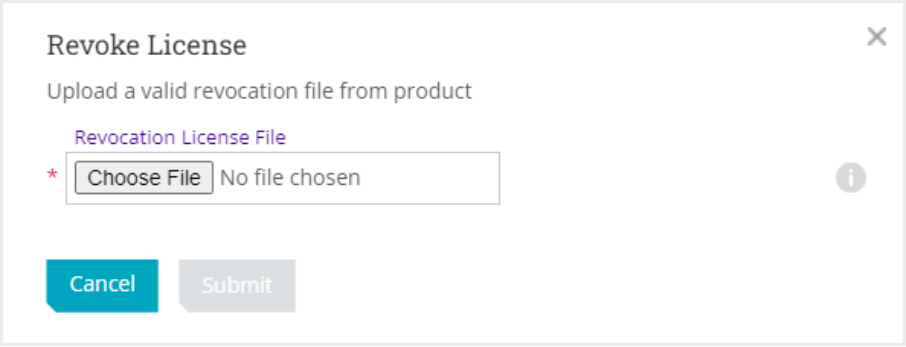
Follow this procedure to revoke your Air Gap license.

1. Open **Administration > Licenses** or enter this URL.
   `https://<Server>:/8443/xiqLicenseSetup.jsp?setupMode=Airgap`
2. Select either the Pilot, Navigator, Platform ONE, or NAC license to revoke.

   ExtremeCloud IQ Site Engine generates a revocation file.
3. Download the file to your computer.
4. Log into the Extreme Portal (https://extreme-networks.my.site.com/ExtrCloudLicenseLanding).
5. Select **Assets > Cloud Licenses Home > Revoke License**.



6. Upload the revocation file and select **Submit**.



The revoked licenses are returned to the license pool. Contact support if you encounter an error. You will need to provide the revocation file (`.rvk`) and the error message.

License Limits and Violations

For each request to add a device to ExtremeCloud IQ Site Engine:

- **In Connected mode**: ExtremeCloud IQ determines if there are enough licenses of that type available.
- **In Air Gap mode**: ExtremeCloud IQ Site Engine uses the license file to determine if there are enough licenses of that type available.

As a result for both modes, one of the following actions happens:

- If there are enough licenses of the optimal type, device onboarding is successful.
- If there are not enough optimal type licenses, a license of the higher type is used instead.
- If there are not enough licenses, the request is considered a license violation.

NOTE: When an evaluation license is used for ExtremeCloud IQ Site Engine, all devices are managed with Tier D licenses.

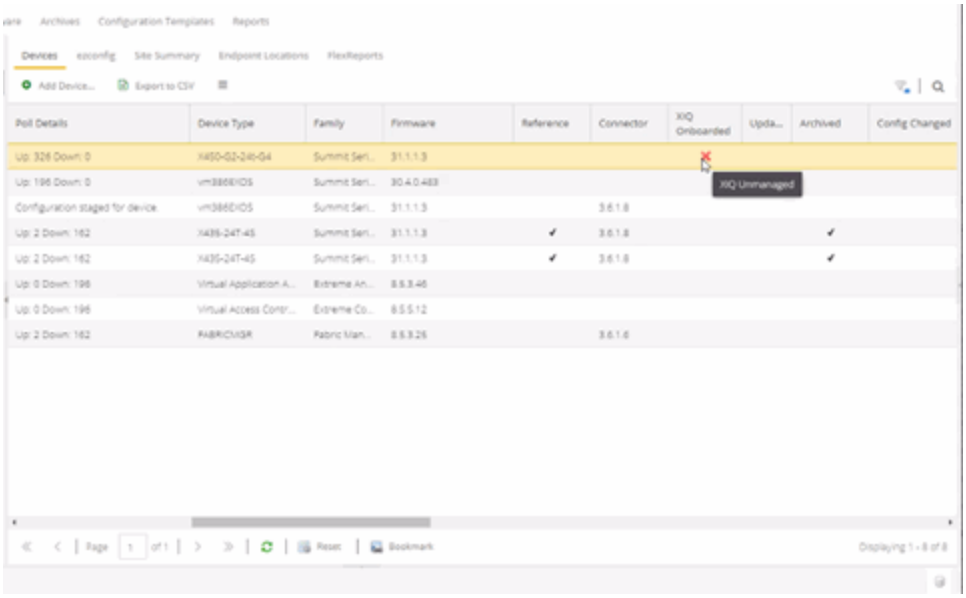
To correct a license limit violation:

- **In Connected mode**: You must acquire more licenses (and, when the updated licenses are available in ExtremeCloud IQ, they are used by ExtremeCloud IQ Site Engine).
- **In Air Gap mode**: You must acquire more licenses by generating a new licensing file from the licensing portal, then install the licensing file in ExtremeCloud IQ Site Engine.

Devices Marked as Unmanaged

When devices are marked as Unmanaged in ExtremeCloud IQ, they are also Unmanaged in ExtremeCloud IQ Site Engine.

Onboarded Unmanaged devices are indicated in the XIQ Onboarded column of the **Network > Site > Device** table by a red **X**.



For more details on the **Network > Site > Device** table, visit Onboarding Unmanaged Devices.

Licensing for ExtremeControl (Network Access Control)

If the ExtremeCloud IQ Site Engine was onboarded to ExtremeCloud IQ, ExtremeCloud IQ provides the Network Access Control (NAC) entitlements to ExtremeCloud IQ Site Engine. There is an option to allocate a portion of the available license pool in ExtremeCloud IQ. The full 100% NAC entitlements should be allocated automatically to the first ExtremeCloud IQ Site Engine. If there are more Site Engines, for example, a lab instance and a production instance, then the NAC entitlements allocation can be changed in the ExtremeCloud IQ GUI. It is recommended to check the NAC entitlements allocation in ExtremeCloud IQ.

If the ExtremeCloud IQ Site Engine is operated in Air Gap deployment mode, the licensed quantity for ExtremeControl is provided through a license file. The license file is generated in Extreme Portal. The licensed quantity for ExtremeControl varies depending on whether ExtremeCloud IQ Site Engine is initially installed or it was upgraded from the Extreme Management Center.

After Upgrading from Extreme Management Center

If you are upgrading from Extreme Management Center to ExtremeCloud IQ Site Engine, the licensing and capabilities of ExtremeControl do not change. The following are included in the licenses:

- NMS-ADV License includes 500 Access Control End-Systems.
- NMS-xx License includes 250 Access Control End-Systems.

NOTE: If your version of ExtremeControl contains NMS or NMS-ADV licenses described above and licenses are used through ExtremeCloud IQ (in Connected mode) or in a locally stored license file (in Air Gap mode), ExtremeControl will sum those licensed quantities.

Upon Initial Installation

If you are completing an initial install of ExtremeCloud IQ Site Engine, there is no end-system license included. The evaluation license can be generated on the Extreme Portal which includes unlimited end-systems.

ExtremeCloud IQ Site Engine Ports

ExtremeCloud IQ Site Engine Inbound Communication (Local Ports)

Type	Port	Description	Purpose
TCP	20	FTP Data	Device software and configuration upload/download
TCP	21	FTP Control	Device software and configuration upload/download
TCP	22	SSH	Shell access Device software and configuration upload/download
TCP	8080	HTTP	Web browser access to ExtremeCloud IQ Site Engine user interface (redirects to port 8443) Communication with ExtremeControl and ExtremeAnalytics
TCP	8443	HTTPS	Web browser access to ExtremeCloud IQ Site Engine user interface Northbound Interface (NBI) ExtremeControl, ExtremeAnalytics, and Fabric Manager communication ZTP+ (cloud connector) communication
TCP	8444	HTTPS	ExtremeControl engine communication
TCP	8445	HTTPS	ExtremeControl Assessment communication
TCP	20504	ExtremeWireless Protocol	ExtremeWireless Controller communication
TCP	20505	ExtremeWireless Protocol	ExtremeWireless Controller communication
UDP	69	TFTP	Device software and configuration upload/download

ExtremeCloud IQ Site Engine Inbound Communication (Local Ports)

Type	Port	Description	Purpose
UDP	123	NTP	
UDP	161	SNMP	SNMP agent (if enabled)
UDP	162	SNMP Traps	Reception of SNMP traps from all managed devices Reception of SNMP traps from ExtremeControl and ExtremeAnalytics engines, Guest & IoT Manager, Fabric Manager, ExtremeWireless Controller, and Virtual Sensors.
UDP	514	Syslog	Reception of syslog messages from monitored devices
UDP	2055	NetFlow	Default NetFlow collector

ExtremeCloud IQ Site Engine Outbound Communication (Remote Ports)

Type	Port	Description	Purpose
TCP	22	SSH	CLI access to managed devices Shell access to ExtremeControl and ExtremeAnalytics engines, Guest & IoT Manager, Fabric Manager, and ExtremeWireless controllers
TCP	23	Telent	If used for CLI communication in lieu of SSH
TCP	25	SMTP	Communication with SMTP server (port is configurable, most common values: 25, 465, and 587)
TCP	49	TACACS+	Required when using TACACS+ for user authentication
TCP	80	HTTP	Internet for ExtremeControl Assessment Agent updates (extremenetworks.com) Virtual sensor communication
TCP	389	LDAP	Required when using LDAP for user authentication

ExtremeCloud IQ Site Engine Outbound Communication (Remote Ports)

Type	Port	Description	Purpose
TCP	443	HTTPS	Allows ExtremeCloud IQ Site Engine to connect to ExtremeCloud IQ ExtremeAnalytics Fingerprint updates (services.enterasys.com) Required when using Microsoft Entra ID (formerly Azure AD), Intune Compliance Module, or OpenID integration. URLs: graph.microsoft.com, sts.windows.net, customer-defined Token Endpoint login.microsoftonline.com Required when using Okta Required when using Microsoft Sentinel Required when using VMware Workspace ONE UEM (formerly AirWatch)
TCP	443	Connect	Connect modules can be configured to communicate with third party solutions. The destination is defined in the Connect modules.
TCP	443	OAUTH	Required when automatic access tokens update is enabled in Administration > Options > SMTP Email.
TCP	636	LDAPs	Required when using LDAP for user authentication
TCP	8080	HTTP	ExtremeControl and ExtremeAnalytics engine communication
TCP	8443	HTTPS	ExtremeControl, ExtremeAnalytics, Guest & IoT Manager, Fabric Manager, and Virtual Sensor communication
TCP	8444	HTTPS	ExtremeControl engine communication
TCP	8090	HTTPS	Integration with Extreme Platform ONE Security
TCP	20506	ExtremeWireless Protocol	ExtremeWireless Controller communication
UDP	53	DNS	Domain Name Server
UDP	123	NTP	Network Time Protocol
UDP	161	SNMP	SNMP Management of all managed devices SNMP Management of ExtremeControl and ExtremeAnalytics engines, Guest & IoT Manager, Fabric Manager, ExtremeWireless Controller, and Virtual Sensors.

ExtremeCloud IQ Site Engine Outbound Communication (Remote Ports)

Type	Port	Description	Purpose
UDP	162	SNMP Trap	Send SNMP traps to external trap receivers
UDP	514	Syslog	Send syslog messages to external syslog receivers
UDP	1812	RADIUS authentication	Required when using RADIUS for user authentication

ExtremeCloud IQ Site Engine Outbound Internet Connections (not mandatory in air gap deployment)

Type	Port	Description	Purpose
			Allows ExtremeCloud IQ Site Engine to connect to ExtremeCloud IQ (`*.extremecloudiq.com` - Check the specifics for your RDC. Login to **ExtremeCloud IQ > About ExtremeCloud IQ > Firewall Configuration Guide**)
TCP	443	HTTPS	ExtremeAnalytics Fingerprint updates (services.enterasys.com)
TCP	80	HTTP	ExtremeControl Assessment Agent download (`extremenetworks.com`)

Access Control Ports

Access Control Inbound Communication (Local Ports)

Type	Port	Description	Purpose
TCP	22	SSH	Shell access Device software and configuration upload/download
TCP	80	HTTP	Captive Portal listening
TCP	443	HTTPS	Captive Portal listening
TCP	8080	HTTP	ExtremeControl web browser access (redirects to port 8443) ExtremeCloud IQ Site Engine communication Communication between multiple ExtremeControl engines From every end-system subnet subject to ExtremeControl assessment agent in order to support agent mobility

Access Control Inbound Communication (Local Ports)

Type	Port	Description	Purpose
TCP	8443	HTTPS	ExtremeControl web browser access ExtremeCloud IQ Site Engine communication Communication between multiple ExtremeControl engines From every end-system subnet subject to ExtremeControl assessment agent in order to support agent mobility
TCP	8444	HTTPS	ExtremeControl web browser access (redirects to port 8443) ExtremeCloud IQ Site Engine communication Communication between multiple ExtremeControl engines
TCP	8445	HTTPS	ExtremeControl Assessment communication
UDP	123	NTP	Network Time Protocol
UDP	161	SNMP	SNMP agent managed by ExtremeCloud IQ Site Engine
UDP	1812	RADIUS authentication	ExtremeControl RADIUS server
UDP	1813	RADIUS accounting	ExtremeControl RADIUS server
TCP	2083	RADIUS over TCP (secured by TLS)	ExtremeControl RADIUS server
		Connect	Distributed IPS module can be configured to receive information from third party solutions. Source (Protocol and Port and IP) is defined in the Distributed IPS module.

Access Control Outbound Communication (Remote Ports)

Type	Port	Description	Purpose
TCP	22	SSH	Configuration of devices running VOSS/Fabric Engine (if ssh is configured in the CLI profile)
TCP	23	Telnet	Configuration of devices running VOSS/Fabric Engine (if telnet is configured in the CLI profile)
TCP	135	RPC	Remote Procedure Calls to Active Directory
TCP	389	LDAP	User-based network authentication and directory services
TCP	80/443	HTTPS	Certificate verification by CRL or OCSP

Access Control Outbound Communication (Remote Ports)

Type	Port	Description	Purpose
TCP	443	HTTPS	Required when using Microsoft Entra ID (formerly Azure AD), Intune Compliance Module, or OpenID integration. URLs: graph.microsoft.com, sts.windows.net, customer-defined Token Endpoint login.microsoftonline.com
TCP	445	DCERPC	Distributed Computing Environment/Remote Procedure Calls
TCP	636	LDAP	User-based network authentication and directory services
TCP	8080	HTTP	ExtremeCloud IQ Site Engine communication Communication between multiple ExtremeControl engines
TCP	8443	HTTPS	ExtremeCloud IQ Site Engine communication Communication between multiple ExtremeControl engines
TCP	8444	HTTPS	ExtremeCloud IQ Site Engine communication Communication between multiple ExtremeControl engines
UDP/TCP	88	Kerberos	Kerberos Protocol
UDP	123	NTP	Network Time Protocol
UDP	161	SNMP	Communication to authenticators
UDP	162	SNMP Trap	SNMP traps sent to ExtremeCloud IQ Site Engine
UDP	389	CLDAP	Winbind discovery
UDP	1700	RADIUS CoA	ExtremeControl RADIUS server to authenticators
UDP	1812	RADIUS authentication	Proxy authorization to remote RADIUS Server
UDP	1813	RADIUS accounting	Proxy accounting to remote RADIUS Server
UDP	3799	RADIUS CoA	ExtremeControl RADIUS server to authenticators

ExtremeAnalytics Ports

ExtremeAnalytics Inbound IP Protocols

Type	Protocol	Description	Purpose
IP	47	GRE	Mirror Traffic for CoreFlow, Virtual Sensor, Wireless Controller, and App Telemetry application identification.

ExtremeAnalytics Inbound Communication (Local Ports)

Type	Port	Description	Purpose
TCP	22	SSH	Shell access
TCP	8080	HTTP	ExtremeCloud IQ Site Engine communication
TCP	8443	HTTPS	ExtremeCloud IQ Site Engine communication
UDP	123	NTP	Network Time Protocol
UDP	161	SNMP	SNMP agent managed by ExtremeCloud IQ Site Engine
UDP	2055	NetFlow	NetFlow Collector
UDP	2058	IPFIX	VMWare NSX IPFIX collector
UDP	2075	IPFIX	IPFIX collector
UDP	2095	NetFlow	ExtremeWireless NetFlow collector
UDP	4739	IPFIX	ExtremeXOS/Switch Engine IPFIX collector, VTAP IPFIX collector from Virtual Sensor
UDP	6343	SFlow	SFlow for ExtremeAnalytics Application Telemetry

ExtremeAnalytics Outbound Communication (Remote Ports)

Type	Port	Description	Purpose
TCP	80	HTTP	Virtual Sensor configuration
TCP	443	HTTPS	Virtual Sensor configuration
TCP	8080	HTTP	ExtremeCloud IQ Site Engine communication
TCP	8443	HTTPS	ExtremeCloud IQ Site Engine communication
UDP	123	NTP	
UDP	162	SNMP Trap	SNMP traps sent to ExtremeCloud IQ Site Engine
UDP		IPFIX	Flow export. Destination and port is defined in the configuration of the Analytics Engine

FabricManager Ports

Fabric Manager Outbound Communication (Remote Ports)

Type	Port	Description	Purpose
UDP	161	SNMP	Communicating with the devices
TCP	22	SSH	Communication between ExtremeCloud IQ - Site Engine and FM for SSH
TCP	8443	HTTP	Communication between ExtremeCloud IQ - Site Engine and FM for REST & ZTP+

Fabric Manager Inbound Communication (Local Ports)

Type	Port	Description	Purpose
TCP	22	SSH	Communication between ExtremeCloud IQ - Site Engine and FM for SSH

Ephemeral Ports

The port range 32768 to 61000 is reserved for dynamically allocated port numbers used by most TCP and UDP based protocols, such as TFTP and FTP.

ExtremeCloud IQ Site Engine Tabs

ExtremeCloud IQ Site Engine includes the following tabs:

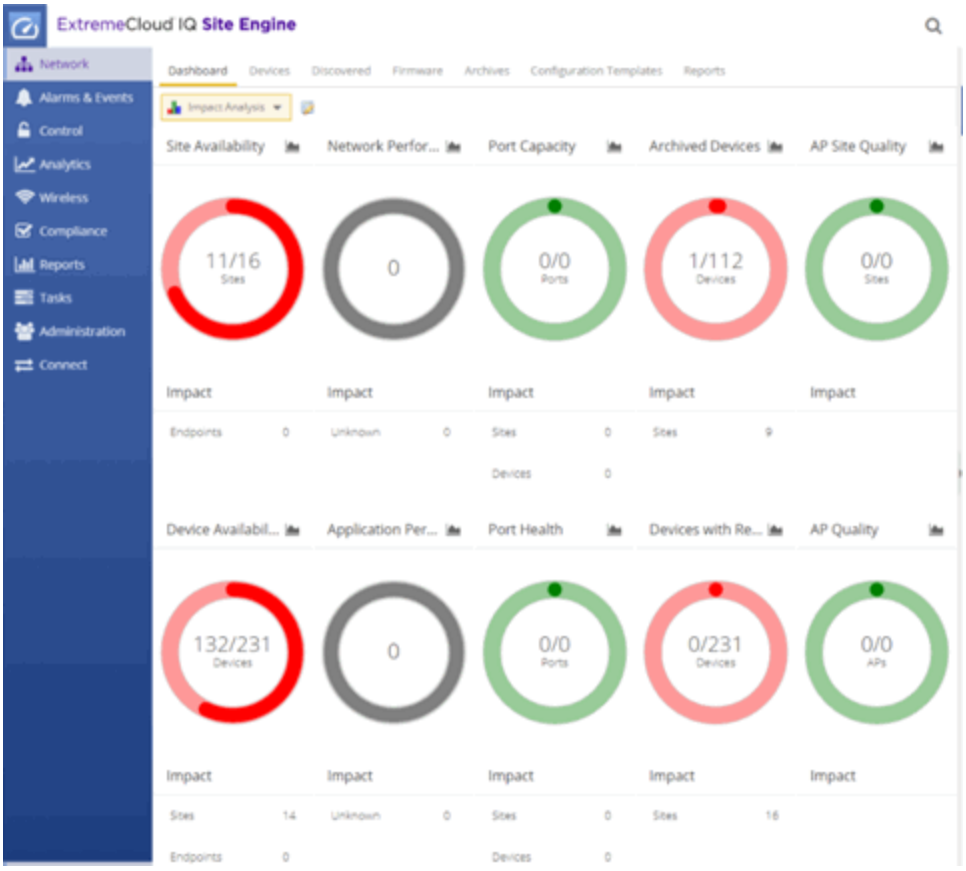
- Network — Device details for all managed devices in the network with sorting and filtering of relevant information for network troubleshooting and forensics. Additionally, create maps of the devices and wireless APs on your network. Import images of maps and building/floor plans, and then drag and drop your managed devices and wireless APs in the map. Use the Search to find a device, AP, or wired/wireless client or locate end-systems for a single AP on the map using RSS-based location services. This feature also includes maps with triangulated location.
- Alarms & Events — Alarm and event details for all managed devices in the network with sorting and filtering of relevant information for network troubleshooting and forensics.
- Control — Dashboards, reports, and control capabilities extending network management to the network attached end-systems. Allows better visibility and control for IT analysts, troubleshooters, and help desk based on end-system and user identity. Create policies for users and ports, enabling network engineers, information technology administrators, and business managers to work together to create the appropriate network experience for each user in their organization.
- Analytics — Real-time NetFlow data for enhanced network diagnostics such as flow details, applications, senders, and receivers.
- Wireless — Wireless monitoring providing details, dashboards, and Top N information to monitor the overall status of the wireless network, as well as the ability to drill in to details as needed.
- Compliance — Oversight into the configuration of your devices and wireless threat alerts to ensure you are compliant with industry best practices.
- Reports — Historical and real-time reporting offering high-level network summary information as well as detailed reports and drill-downs.
- Tasks — Create scripts and workflows and use them to configure tasks.
- Administration — ExtremeCloud IQ Site Engine administration tools to monitor and maintain the ExtremeCloud IQ Site Engine application and its components.
- Connect — Provides configuration to allow you to integrate third-party software with ExtremeCloud IQ Site Engine's ExtremeControl solution.
- Search — A powerful diagnostic tool to search end-systems by MAC address, IP address, end-system name, or user name for fast troubleshooting. Includes a Search with Compass option that uses SNMP to provide information about the status, configuration, and activities at the ingress points of your network, and is an easy way to search for end stations or users on end stations.

Network

Selecting the **Network** tab displays details for the managed devices in ExtremeCloud IQ Site Engine, with sorting and filtering of relevant information for network troubleshooting.

Navigating the Network Tab

To access the **Network** tab, select it in the ExtremeCloud IQ Site Engine menu.



The **Network** tab provides access to the following sub-tabs:

- **Dashboard** — Presents a summary of ExtremeCloud IQ Site Engine data via a variety of dashboards, including the Impact Analysis, Overview, Multi Cloud, and Inventory dashboards.
- **Devices** — Provides you with information about the devices on your network and the relationships between devices. The **Devices** tab also allows you to organize devices into groups, geographically in maps, and configure default settings for newly discovered devices using sites.

- **Discovered** — Displays newly discovered devices on your network and allows you to configure those devices.
- **Firmware** — Allows you to view and upgrade firmware for network devices.
- **Archives** — Displays all device archives, or saved device configurations grouped by device type.
- **Configuration Templates** — Provides you with device configurations you can use as a template for your device types.
- **Reports** — Provides a variety of system reports that give information about your devices, ports, and network traffic.

Additionally, the **Menu** icon (☰) at the top of the screen provides links to additional information about your version of ExtremeCloud IQ Site Engine.

Dashboard

Select the **Dashboard** tab to view graphical data about devices on your network.

The **Dashboard** contains four options, the Impact Analysis, Overview, Multi Cloud, and Inventory dashboards.

Impact Analysis

The Impact Analysis dashboard displays a real-time summary of Availability, Performance, Capacity/Health, and Configuration data for your network. The dashboard provides you with charts that identify the scope and scale of faulting elements in the network or location. Charts display an impact status and an impact summary for a particular factor that are updated automatically when conditions change.

Overview

The Overview dashboard displays several reports containing statistical information about the devices on your network. The information presents a sampling of the performance of individual devices.

Multi Cloud

The Multi Cloud dashboard provide an overview of all virtual machines on the network broken down into VM distribution per ExtremeControl profile, Operating System, Switch, and Hypervisor technology. It also provides detailed information on all VMs. For each supported Hypervisor technology, sub-reports provide more in-depth data. Additionally, the Multi Cloud dashboard includes information about Google Compute, Amazon Web Service, and Microsoft Azure instances.

Inventory

The Inventory Dashboard includes a Summary tab, which displays several pie charts that enable you to view the activity and status of the devices and ports that comprise your network. The criteria for each chart is configurable, and you can drill down from each chart to access reports displaying details about the device and port activity.

The Inventory Dashboard also includes Asset Tracking and Device Tracking tabs. Use these tables to monitor changes made to assets and devices in your network.

Devices

Select the **Devices** tab to display information about devices in your network and the maps and sites in which they are added.

Left-Panel Tree

The left-panel of the **Devices** tab contains a drop-down list, enabling you to view all of your devices, a subset of devices, your maps, or your sites.

Selecting a device, device group, map, or site in the Groups/Maps navigation tree displays details about that item in the right-panel. Additionally, you can contact the selected devices with the currently configured profile and execute CLI commands on devices or device groups.

Right-Panel Tabs

The information in the right-panel is organized into tabs. The tabs available depends on the item selected in the left-panel.

- **Devices** — The **Devices** tab contains a table of information about the devices selected in the left-panel (or the devices included in the map or site selected in the left-panel), including the status of the device, the IP address, the device type, the firmware version, and the serial number.
- **Site** — The **Site** tab allows you to create a default configuration for devices being added to the selected site.
- **Summary** — The **Summary** tab opens the Device View for the device selected.
- **Map** — The **Map** tab displays the geographic, topology, or floor plan map as well as a graphic representation of the devices contained in that map.
- **Site Summary** — The **Site Summary** tab contains a table of information about the sites on your network, including the path, addresses, and configuration.
- **Endpoint Locations** — The **Endpoint Locations** tab displays the geographic locations of your devices and sites.
- **FlexReports** — The **FlexReports** tab contains reports available for the device, controller, map, or site selected in the left-panel.

Discovered

Select the **Discovered** tab to view devices new to your network not yet added to the ExtremeCloud IQ Site Engine database. Devices appear on the **Discovered** tab when they are:

- Discovered via the **Site** tab and one of the following occurs:
  - The **Automatically Add Devices** checkbox is not selected in the Site Actions section of the tab.
  - The serial number of the device matches:
    - The serial number of another device being discovered.
    - The serial number of a device already in the ExtremeCloud IQ Site Engine database.
  - The serial number is not defined for a device and the base MAC address matches:
    - The base MAC address of another device being discovered.
    - The base MAC address of a device already in the ExtremeCloud IQ Site Engine database.
  - The serial number and base MAC address are not defined for a device and the IP address matches:
    - The IP address of another device being discovered.
    - The IP address of a device already in the ExtremeCloud IQ Site Engine database.
  - The device uses a profile different than those associated with devices that already exist in the ExtremeCloud IQ Site Engine database.
- Discovered using the Pre-Register Device window for your ZTP+ (Zero Touch Provisioning Plus) enabled devices.

  NOTE: ZTP+ functionality is supported on ExtremeXOS/Switch Engine devices on which version 21.1 (or greater) is installed, FastPath devices, Fabric Manager, ExtremeAnalytics engines, and Access Control engines.

- Discovered using a trap to discover a ZTP (Zero Touch Provisioning) enabled device.

  NOTE: ZTP functionality is not identical to ZTP+ functionality.

Firmware

Select the **Firmware** tab to assign a firmware or boot PROM image to one or more product families or device types. This enables you to download the assigned image to any of your network devices of that family or type. Use the Details section of the tab to display the firmware or boot PROM image details and save the image to the device.

Archives

Select the **Archives** tab to create new archives for your devices and view a list of existing archives grouped by device type in the left-hand panel. This tab provides information about archive operations

performed on the selected device or device group. Additionally, use your archives to compare your device configurations against industry best practices.

Configuration Templates

Select the **Configuration Templates** tab to view and use device configuration templates grouped by device type in the left-hand panel. This tab provides information about configurations you can use as templates for your devices.

Reports

Select the **Reports** tab to view information about the devices and ports on your network as well as information about network traffic. Available reports are accessible via the **Reports** drop-down list at the top of the tab and are grouped into the following three reporting areas:

- Device
- Interface
- Network

Select **Information** ( ) in the top-right corner of a report to view more information about that report.

Select **Export to CSV** ( ) to export the information contained in the report to your default CSV application, where it can then be manipulated or saved.

For information on related topics:

- How to Add Fabric Manager
- Fabric Manager ZTP+ Configuration
- Device Operations
- Search

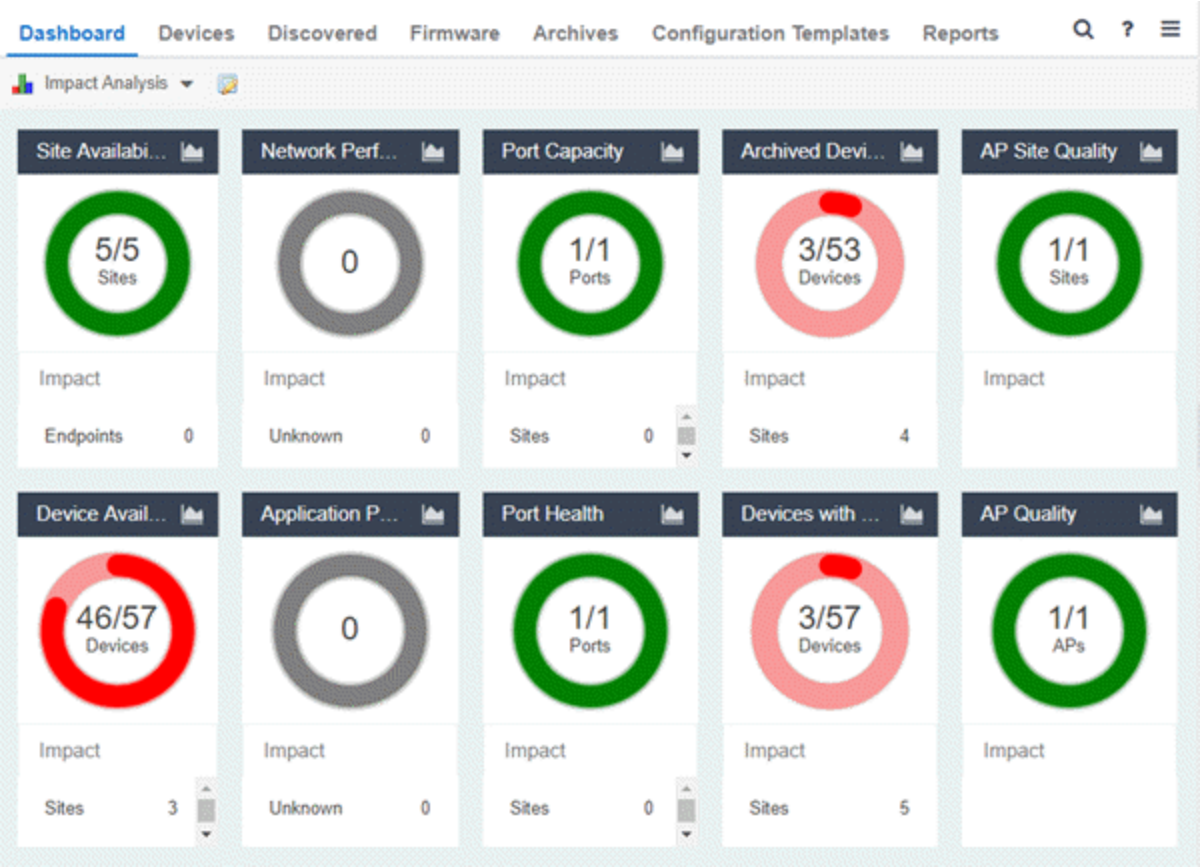
For information on related tasks:

- Add to Device Group
- Add Devices to Maps
- New Device Configuration in ExtremeCloud IQ Site Engine

Impact Analysis Dashboard Overview

Use the **Impact Analysis Dashboard** to view a real-time summary of Availability, Performance, Capacity/Health, Configuration, and Quality data for your network. To access the Impact Analysis Dashboard, navigate to the **Network** tab and select the **Dashboard** tab.

Select the report button ( ) to open the Impact Analysis Report page window in the Reports Designer tab.



Charts

The dashboard provides you with ring charts and data that identify the scope and scale of faulting elements in the network or site. Charts display a name and impact status for a particular factor, and are updated automatically when conditions change.

NOTES: A network element is considered **"faulting"** if it is non-optimal relative to a certain factor; for example, a device that has not been archived recently or an application that is responding poorly.

A network element is considered **"impacted"** if it has a relationship to a faulting element which might affect its operation; for example, an endpoint connected to a device that failed.

The center of each chart contains a ratio of the non-faulting elements compared to the total number of elements. Hover over a ring color to display a complete description of the ratio. ExtremeCloud IQ Site Engine uses these ratios, converts them to a percentage, and uses them to determine the impact status. Below each chart is an Impact Summary, which displays the network elements impacted by any faulting elements.

The Impact Status is reflected by color:

Impact Status	Color	Description
Low		None, or few, faulting elements
Medium		Some, but not many, faulting elements
High		Many faulting elements

The thresholds that determine the Impact Status (Low, Medium, or High) for each chart is configurable in the Impact Analysis options on the **Administration** tab.

When the Impact Status changes for network elements (e.g. device availability changes from Low to Medium or from Medium to High), an event is generated and is available in the event log on the Events tab.

Site Availability

The center of the Site Availability ring chart indicates the ratio of sites with which ExtremeCloud IQ Site Engine can communicate to the total number of sites with at least one device. The number of end-points impacted by sites ExtremeCloud IQ Site Engine can not reach is listed in the Impact Summary beneath the ring chart.

- Select the ring chart to open the Unavailable Sites report that displays sites ExtremeCloud IQ Site Engine can not reach.
- Select **Endpoints** in the Impact Summary beneath the ring chart to open the Endpoints Impacted by Unavailable Sites report that provides more details about endpoints with devices.
- Select the report button ( ) to open the Site Availability History report that provides a historical view of the Site Availability chart.

Device Availability

The center of the Device Availability ring chart indicates the ratio of devices with which ExtremeCloud IQ Site Engine can communicate to the total number of devices. The number of

sites and endpoints that contain devices with which ExtremeCloud IQ Site Engine can not communicate are listed in the Impact Summary beneath the ring chart.

- Select the ring chart to open the Unavailable Devices report that provides detailed data for all unavailable devices.
- Select **Sites** in the Impact Summary beneath the ring chart to open the Sites Impacted by Unavailable Devices report that provides more details about sites with unavailable devices.
- Select **Endpoints** in the Impact Summary beneath the ring chart to open the Endpoints Impacted by Unavailable Devices report that provides more details about endpoints with unavailable devices.
- Select the report button () to open the Device Availability History report that provides a historical view of the Device Availability chart.

Network Performance

The center of the Network Performance ring chart indicates the ratio of sites with a network response time in the expected or better-than-expected range to the total number of sites. The number of tracked applications and network services and endpoints with a slower-than-expected response time are listed in the Impact Summary beneath the ring chart. Data displayed in the chart includes all engines on your network. Applications at different sites are counted separately.

NOTE: If you do not use ExtremeAnalytics, you can remove this chart from the Impact Analysis dashboard in the Report Designer.

- Select the ring chart to open the Slow Sites report that displays sites with slower-than-expected network response times.
- Select **Applications** in the Impact Summary beneath the ring chart to open the Applications Impacted by Slow Sites report that provides more details about the tracked applications and network services impacted by slower-than-expected network response time.

  NOTE: Enable Event Collection to allow ExtremeCloud IQ Site Engine to report specific end-points impacted by slower-than-expected response times.

- Select **Endpoints** in the Impact Summary beneath the ring chart to open the Endpoints Impacted by Network Response Time report that provides more details about endpoints impacted by slower-than-expected network response time.
- Select the report button () to open the Network Performance History report that provides a historical view of the Network Performance chart.

Application Performance

The center of the Application Performance ring chart indicates the ratio of tracked applications and network services with an application response time in the expected or better-than-expected range to the total number of tracked applications and network services. The number of sites that contain tracked applications and network services with slower-than-expected application response times are listed in the Impact Summary beneath the ring chart. Data displayed in the chart includes all engines on your network. Applications at different sites are counted separately.

NOTE: If you do not use ExtremeAnalytics, you can remove this chart from the Impact Analysis dashboard in the Report Designer.

- Select the ring chart to open the Slow Applications report, which is filtered to display tracked applications and network services with slower-than-expected application response times.
- Select **Sites** in the Impact Summary beneath the ring chart to open the Sites Impacted by Slow Applications report that provides more details about the sites impacted by tracked applications and network services with slower-than-expected response times.
- Select **Endpoints** in the Impact Summary beneath the ring chart to open the Endpoints Impacted by Slow Applications report that provides more details about endpoints impacted by slower-than-expected application response time.

  NOTE: Enable Event Collection to allow ExtremeCloud IQ Site Engine to report specific end-points impacted by slower-than-expected response times.

- Select the report button () to open the Application Performance History report that provides a historical view of the Application Performance chart.

Port Capacity

The center of the Port Capacity ring chart indicates the ratio of ports with an acceptable level of utilization to the total number of ports on which data collection is enabled and which recently reported utilization measurements. The number of sites and devices that contain ports with excessive utilization are listed in the Impact Summary beneath the ring chart.

- Select the ring chart to open the Highly Utilized Ports report that displays the utilization of ports filtered to include only those ports with an excessive port rate.
- Select **Sites** in the Impact Summary beneath the ring chart to open the Sites Impacted by Highly Utilized Ports report that provides more details about sites impacted by port capacity.
- Select **Devices** in the Impact Summary beneath the ring chart to open the Devices Impacted by Highly Utilized Ports report that provides more details about devices impacted by port capacity.

- Select the report button ( ) to open the Port Capacity History report that provides a historical view of the Port Capacity chart.

Port Health

The center of the Port Health ring chart indicates the ratio of ports with an acceptable error rate to the total number of ports on which data collection is enabled and which recently reported error rate measurements. The number of sites and devices that contain ports with an excessive error rate are listed in the Impact Summary beneath the ring chart.

- Select the ring chart to open the High Error Ports report that lists the ports with an excessive error rate.
- Select **Sites** in the Impact Summary beneath the ring chart to open the Sites Impacted by High Error Ports report that provides a list of sites with ports with an unacceptable error rate.
- Select **Devices** in the Impact Summary beneath the ring chart to open the Devices Impacted by High Error Ports report that provides a list of devices with ports with an unacceptable error rate.
- Select the report button ( ) to open the Port Health History report that provides a historical view of the Port Health chart.

Archived Devices

The center of the Archived Devices ring chart indicates the ratio of devices for which an archive was created in the past 30 days to the total number of devices that support archiving. The number of sites with devices not archived in the past 30 days is listed in the Impact Summary beneath the ring chart.

- Select the ring chart to open the Unarchived Devices report that provides a list of the devices not archived in the last 30 days.
- Select **Sites** in the Impact Summary beneath the ring chart to open the Sites Impacted by Unarchived Devices report that provides a list of the sites associated with devices with no archive in the last 30 days.
- Select the report button ( ) to open the Archived Devices History Report that provides a historical view of the Archived Devices chart.

Devices with Reference Firmware

The center of the Devices with Reference Firmware ring chart indicates the ratio of devices on which firmware you define as a reference image is installed to the total number of devices. The number of sites containing devices on which reference firmware is not installed is listed in the Impact Summary beneath the ring chart.

NOTE: The Devices with Reference Firmware ring chart only includes devices discovered via SNMP.

- Select the ring chart to open the Devices Without Reference Firmware report that displays a list of affected devices not running reference firmware.
- Select **Sites** in the Impact Summary beneath the ring chart to open the Sites Impacted by Devices Without Reference Firmware report that provides a list of the sites with devices not running reference firmware.
- Select the report button () to open the Reference Firmware History Report that provides a historical view of the Devices with Reference Firmware chart.

AP Site Quality

The center of the AP Site Quality ring chart indicates the ratio of ExtremeCloud IQ sites with applications that meet the required RFQI or quality standards to the total number of sites. Quality indicators of 1 (low) to 5 (good) are determined via the ExtremeCloud IQ engine.

- Select the ring chart to open the **AP Sites with Low Quality** report that includes details about the sites with APs that are experiencing both good and poor quality.
- Select **Impact** in the Impact Summary beneath the ring chart to open the **Sites Impacted by APs with Low Quality** report that provides a list of the sites with devices not running reference firmware.
- Select the report button () to open the **AP Site Quality History Report**, which provides a historical view of AP site quality totals and counts.

AP Quality

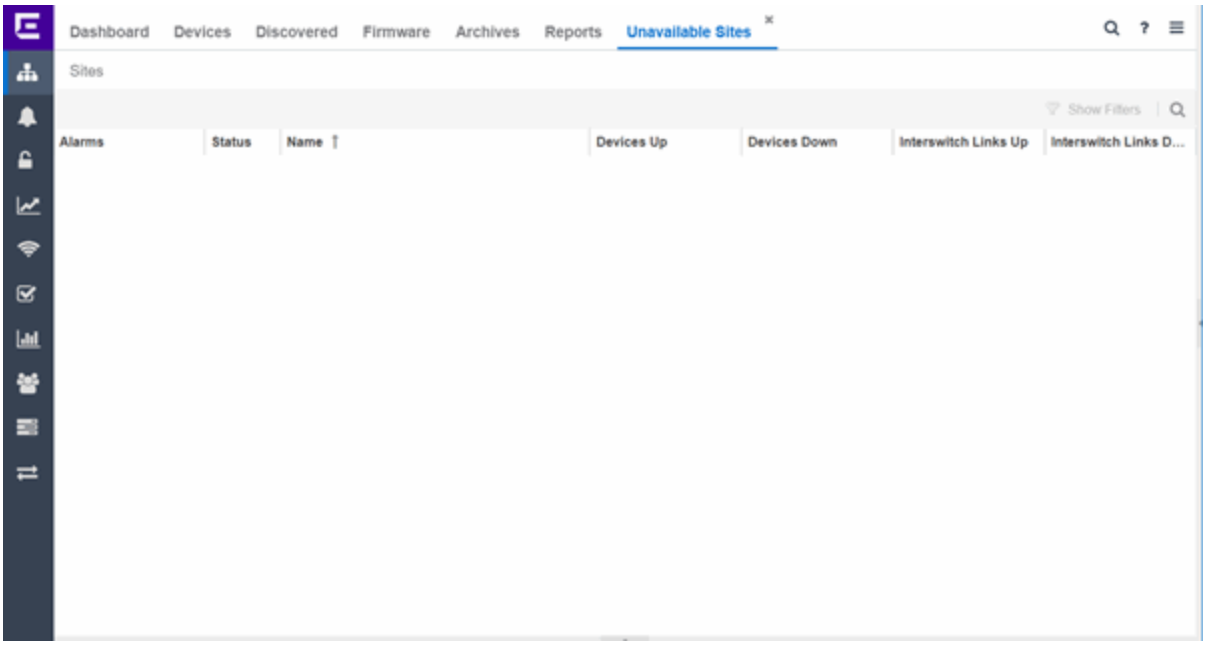
The center of the AP Quality ring chart indicates the ratio of applications that meet the required RFQI or quality standards to the total number of APs. The number of APs experiencing low quality is listed in the Impact Summary beneath the ring chart. Quality indicators of 1 (low) to 5 (good) are determined via the ExtremeCloud IQ engine.

- Select the ring chart to open the **APs with Low Quality** report that displays details about APs experiencing low quality.
- Select **Impact** in the Impact Summary beneath the ring chart to open the **APs Impacted by Low Quality** report that provides a list of the APs experiencing low quality.
- Select the report button () to open the **AP Quality History Report**, which provides a historical view of the quality experienced by APs.

- Impact Analysis Options
- ExtremeCloud IQ Site Engine Network Overview

Unavailable Sites Report

The Unavailable Sites report provides a list of sites ExtremeCloud IQ Site Engine considers to be down. Use the **Devices Up for Site Up (percent)** field on the **Impact Status Options** tab to configure the threshold ExtremeCloud IQ Site Engine uses to determine if a site is up. The threshold is calculated as the ratio of devices in a site with a **Status** of **Up** to the total number of devices in the site.



The following columns are included in the report:

Alarms:

Shows the most severe alarm triggered by a device included in the site. The severity of the alarm is indicated by the following icons:

- Critical (▼) — A problem with significant implications.
- Error (▶) — A problem with limited implications.
- Warning (▲)— A condition that might lead to a problem.
- Info (■) — Information only; not a problem.
- None ( ) — No alarms on the device.

Status:

Indicates whether the site is up or down, based on the percentage of devices in the site with which ExtremeCloud IQ Site Engine can communicate (**Status** of **Up**). A green check mark indicates the site is up, while a red X icon indicates the site is down.

Use the **Devices Up for Site Up (percent)** field on the **Impact Status Options** tab to

configure the threshold ExtremeCloud IQ Site Engine uses to determine if a site is up. The threshold is calculated as the ratio of devices in a site with a **Status** of **Up** to the total number of devices in the site.

Name:
The name of the site.

Devices Up
This column indicates the number of devices with a **Status** of **Up** in the site.

Devices Down
This column indicates the number of devices with a **Status** of **Down** in the site.

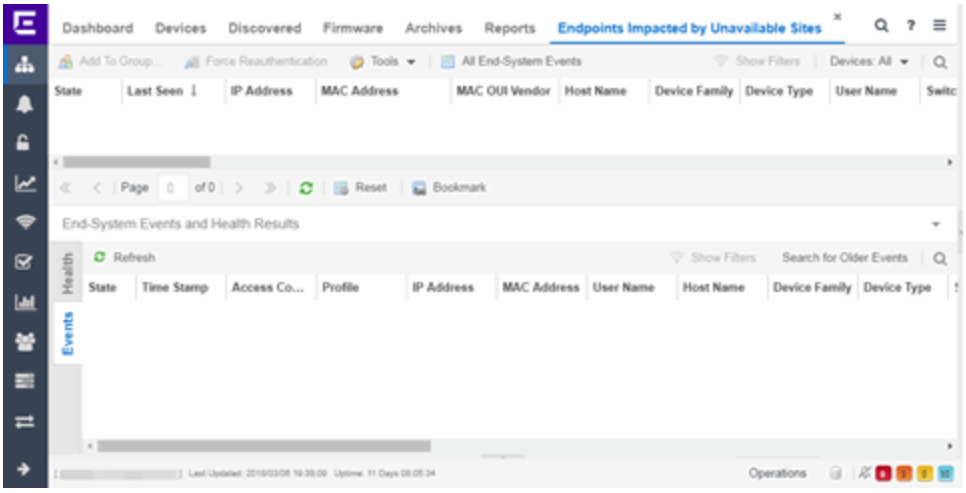
Interswitch Links Up
This column indicates the number of Interswitch Links with a **Status** of **Up** in the site.

Interswitch Links Down
This column indicates the number of Interswitch Links with a **Status** of **Down** in the site.

- Impact Analysis Dashboard Overview

Endpoints Impacted by Unavailable Sites Report

This report provides detailed information about end-systems impacted as the result of ExtremeCloud IQ Site Engine unable to communicate with a site (**Status** of **Down**). The report also shows any events that pertain to the end-systems selected in the top table. Additionally, the report lists the risks and vulnerabilities for the device and assigns a score based on the severity of the risk.



The report contains three tables:

- End-System Information
- Events

- Health

End-System Information

The table at the top of the report lists the end-systems that are affected as the result of unavailable sites.

ID
: The identification number for the end-system. This column is hidden by default.

State
: The end-system's connection state:

  - Scan - The end-system is currently being scanned.
  - Accept - The end-system is granted access with either the Accept policy or the policy returned from the RADIUS server in the filter-ID.
  - Quarantine -The end-system is quarantined because the scanning test failed.
  - Reject - The end-system was rejected because the assigned ExtremeControl profile was set to Reject, the MAC Locking test failed, or the RADIUS server was reachable but rejected the authentication request.
  - Error - Indicates one of nine problems:
    - the MAC to IP resolution failed, if assessment is enabled
    - the MAC to IP resolution timed out, if assessment is enabled
    - all RADIUS servers are unreachable
    - the RADIUS request was non-compliant
    - all assessment servers are unavailable
    - the assessment server can't reach the end-system
    - no assessment servers are configured
    - the assessment server is not compatible with the current version of ExtremeCloud IQ Site Engine
    - the username and password configured in the Assessment Server section of the Access Control options (Administration > Options > Access Control) are incorrect for the assessment server

Last Seen
: The last date and time the end-system was seen by the ExtremeControl engine.

IP Address
: The end-system's IP address.

OV MAC Key
: OV MAC Key. This column is hidden by default.

MAC Address
: The end-system's MAC address. MAC addresses are displayed as a full MAC address or with a MAC OUI (Organizational Unique Identifier) prefix, depending on the option you select the **Access Control Options** tab.

MAC OUI Vendor
: The vendor associated with the MAC OUI.

Host Name
: The end-system's host name.

Device Family
: The hardware family or the operating system family for the end-system.

Device Type
: The hardware type or the operating system type for the end-system.

User Name
: The User Name used for device access.

Switch IP
: The IP address of the switch to which the end-system is connected.

Switch Nickname
: The nickname defined for the switch to which the end-system is connected.

Switch Port
: The port alias (if defined) followed by the switch port number to which the end-system is connected.

Policy
: The policy role assigned to the end-system.

Authorization
: The Authorization granted to allow access to the end-system.

Risk Level
: The overall risk level assigned to the end-system based on the health result of the scan:

  - Red - High Risk
  - Orange - Medium Risk
  - Yellow - Low Risk
  - Green - No Risk
  - Gray - Unknown

Profile Name
: The name of the profile assigned to the end-system when it connected to the network.

Reason
: Provides additional information about the reasons why the end-system is in its particular connection state. It gives you an idea as to why a certain policy was applied to the end-system or why the end-system was rejected.

Authentication Type
: Identifies the latest authentication method used by the end-system to connect to the network.

State Description
: This column provides more details about the end-system state. For example, if the end-system's connection state is Reject, this column might list the RADIUS server (primary or secondary) that rejected the authentication request.

Extended State
: Provides additional information about the end-system's connection state.

Access Control Engine/Source IP
: The Engine to which the end-system is connecting.

Engine Group
: Displays what Engine group the ExtremeControl engine was in when the end-system event was generated. For example, if the Engine was in Engine group A when an end-system connected, but then later the Engine was moved to Engine group B, this column still list Engine group A for that end-system's entry.

RFC 3580 VLAN ID
: For end-systems connected to RFC 3580-enabled switches, this is the RFC3580 VLAN ID assigned to the end-system.

Warning Time
: Shows the time for warning. This column is hidden by default.

Last Quarantined
: The last date and time the end-system was quarantined. This column is hidden by default.

Score
: The total sum of the scores for all the health details that were included as part of the quarantine decision.

Top Score
: The highest score received for a health detail in the health result.

Actual
: The actual score is what the total score would be if all the health details including those marked Informational and Warning were included in the score.

Switch Port Index
: The SNMP index (ifIndex) of the port to which the end-system connected.

Switch Location
: The physical location of the switch to which the end-system connected.

ELIN
: An extended set of data for an end-system based on a MAC address.

Port Info Raw
: Displays unformatted information as it is received from the port.

All Authentication Types
: This column displays all the authentication methods the end-system has used to authenticate.

Last Scan Result State
: The last scan result assigned to the end-system: Scan, Accept, Quarantine, Reject, Error. This is the state that was assigned to the end-system as a result of the last completed scan. This will typically match the end-system State if scanning is currently enabled and has been performed recently.

Last Scanned Time
: The last time an assessment (scan) was performed on the end-system.

First Seen Time
: he first time the end-system was seen by the ExtremeControl engine.

NAP Capable
: Indicates whether the end-system is Microsoft NAP (Network Access Protection) capable: **Yes** or **No**

Custom 1-4
: Use these column to add additional information you want to display. You can add information for up to four Custom columns.

Registered User
: The registered username supplied by the end user during the registration process.

Registered Email
: The registered email address supplied by the end user during the registration process.

Registered Phone
: The registered phone number supplied by the end user during the registration process.

Sponsor
: The registered user's sponsor, if sponsorship is enabled.

Registration 1-5
: The text from the Custom 1-5 registration fields supplied by the end user during the registration process.

Registration Description
: The device description supplied by the end user during the registration process.

Groups
: End-system groups are rule components that allow you to group together devices having similar network access requirements or restrictions.

Group 1-3
: Displays the names of up to three end-system groups.

Zone
: This field only displays if you have displayed the Zone column in the Access Control Configuration Rules table. Select the end-system zone assigned to any end-system matching this rule. See End-System Zones for more information.

Request Attributes
: Displays the RADIUS attributes injected when the end-system requested authentication.

Registration Type
: Shows the type of registration

RADIUS Server IP
: The IP address of the RADIUS server with which the end-system is associated.

Source
: Displays the origin of the event:

  - Access Controlengine — An Access Controlengine.
  - Wireless Manager — An ExtremeWireless Controller or AP.
  - ExtremeXOS/Switch Engine ID Manager — An Extreme switch running ExtremeXOS/Switch Engine with the Identify Manager feature configured to send events to ExtremeCloud IQ Site Engine.
  - OneFabric Connect — An ExtremeConnect module (e.g. Solutions Architecture and Innovation (SAI) integration)
  - One Controller — The Extreme SDN Controller.

DCM
: Data Center Manager. This column is hidden by default.

TLS Client Certificate Expiration
: Expiration date of the TLS Client Certificate issued for 802.1x authentication.

TLS Client Certificate Issuer
: Name of the issuer of the TLS Client Certificate issued for 802.1x authentication.

Events Log

The Events table displays end-system events related to the unavailability of the site.

ID

The identification number for the end-system. This column is hidden by default.

State

The end-system's connection state:

- Scan - The end-system is currently being scanned.
- Accept - The end-system is granted access with either the Accept policy or the policy returned from the RADIUS server in the filter-ID.
- Quarantine -The end-system is quarantined because the scanning test failed.
- Reject - The end-system was rejected because the assigned ExtremeControl profile was set to Reject, the MAC Locking test failed, or the RADIUS server was reachable but rejected the authentication request.
- Error - Indicates one of nine problems:
    - the MAC to IP resolution failed, if assessment is enabled
    - the MAC to IP resolution timed out, if assessment is enabled
    - all RADIUS servers are unreachable
    - the RADIUS request was non-compliant
    - all assessment servers are unavailable
    - the assessment server can't reach the end-system
    - no assessment servers are configured
    - the assessment server is not compatible with the current version of NAC Manager
    - the username and password configured in the Assessment Server section of the Access Control options (Administration > Options > Assessment Server) are incorrect for the assessment server

Timestamp

Shows the date and time when an event occurred.

ExtremeControl engine / Source IP

The ExtremeControl engine to which the end-system is connecting.

Profile

The Profile assigned to the end-system in the ExtremeCloud IQ Site Engine database.

IP Address

The end-system's IP address.

MAC Address

The end-system's MAC address. MAC addresses are displayed as a full MAC address or with a MAC OUI (Organizational Unique Identifier) prefix, depending on the option you have selected

in the Display section of the Access Control Options (Administration > Options > Access Control).

User Name
The name of the user that triggered the event.

Host Name
The end-system's host name.

Device Family
The hardware family or the operating system family for the end-system.

Device Type
The hardware type or the operating system type for the end-system.

State Description
This column provides more details about the end-system's state. For example, if the end-system's connection state is Reject, this column might list the RADIUS server (primary or secondary) that rejected the authentication request.

Extended State
Provides additional information about the end-system's connection state.

Reason
Provides additional information about the reasons why the end-system is in its particular connection state. It gives you an idea as to why a certain policy was applied to the end-system or why the end-system was rejected.

Authorization
The attributes returned by the RADIUS server for this end-system. If the end-system is connected to a switch that supports multi-authentication, then this column may not reflect the actual active policy for the authenticated user. For Layer 3 Access Control Controller engines, this column displays the policy assigned to the end-system for its authorization.

Auth Type
Identifies the authentication method used by the end-system to connect to the network. For Layer 3 Access Control Controller engines, this column shows **IP**.

Switch IP
The IP address of the switch to which the end-system connected. If the end-system is connected to an Access Control Controller engine, this is the Access Control Controller PEP (Policy Enforcement Point) IP address..

Switch Nickname
The nickname defined for the switch to which the end-system is connected.

Switch Port Index
The switch port index to which the end-system is connected.

Switch Port
The switch port interface name to which the end-system is connected.

Switch Location
The physical location of the switch to which the end-system connected. If the end-system is connected to an Access Control Controller engine, this is the Access Control Controller PEP (Policy Enforcement Point) location.

ELIN
An extended set of data for an end-system based on a MAC address.

Port Info Raw
Displays unformatted information as it is received from the port.

Last Scan Time
The last time an assessment (scan) was performed on the end-system.

Zone
Displays the end-system zone to which the end-system is assigned.

Registration Type
The end-system type supplied by the end user during the registration process.

RADIUS Server IP
The IP address of the RADIUS server with which the end-system is associated.

Event Source
Displays the origin of the event:

- Access Control Engine — A Access Control engine.
- Wireless Manager — An ExtremeWireless Wireless Controller or AP.
- ExtremeXOS/Switch Engine ID Manager — An Extreme switch running ExtremeXOS/Switch Engine with the Identify Manager feature configured to send events to ExtremeCloud IQ Site Engine.
- OneFabric Connect — A custom project (e.g. Solutions Architecture and Innovation (SAI) integration)
- One Controller — The Extreme SDN Controller.

Health Log

This tab provides summary information on health results (assessment results) obtained for the end-system selected in the table above. You can specify the number of health result summaries displayed using the Health Result Persistence options in the Data Persistence Options.

Risk
The risk level assigned to the end-system based on the health result of the scan: High Risk, Medium Risk, Low Risk, or No Risk.

Name
This column lists the name of the test that is reported by the health result detail.

Test Case ID
The unique number assigned to the test case.

Score
The score assigned to the test case. The score is a value between 0.0 and 10.0. In the case of agent-based test cases, the score is either 0.0 for a passed test, or 10.0 for a failed test, unless specifically overwritten by the scoring override configuration.

Scoring Mode
The scoring mode that was used at the time the test was performed.

- Applied — The score returned by this test was included as part of the quarantine decision.
- Informational — The score returned by this test was reported, but did not apply toward a quarantine decision.
- Warning — The score returned by this test was only used to provide end user assessment warnings via the Notification portal web page.

CVE IDs
The CVE (Common Vulnerability and Exposures) ID assigned to the security vulnerability or exposure. For more information on CVE IDs, refer to the following URL: https://cve.mitre.org/.

Description
This column lists information about the health result detail.

Solution
This column lists a solution for the health result.

Port ID
The port on which the end-system the security risk was detected.

Protocol ID
The well-known number (ID) assigned to the IP Protocol Type.

Assessment
The list of test sets that were run during assessment, for example, Default Nessus, Default Agent-less, and Default Agent-based. Test sets are defined as part of the assessment configuration. If the end-system is NAP capable, then this column displays Microsoft NAP indicating that NAP performed the assessment.

Remediation
For agent-based assessment, this column lists the results of remediation attempts: Success, Failed, or Not Attempted.

Type

A "type" is assigned to each security risk found on a port during an assessment, and is used to determine whether to Quarantine an end-system. Types are configurable on the assessment agent. There are three types:

- Hole — The port is vulnerable to attack.
- Warning — The port may be vulnerable to attack.
- Note — There may be a security risk on the port.

- Impact Analysis Dashboard Overview

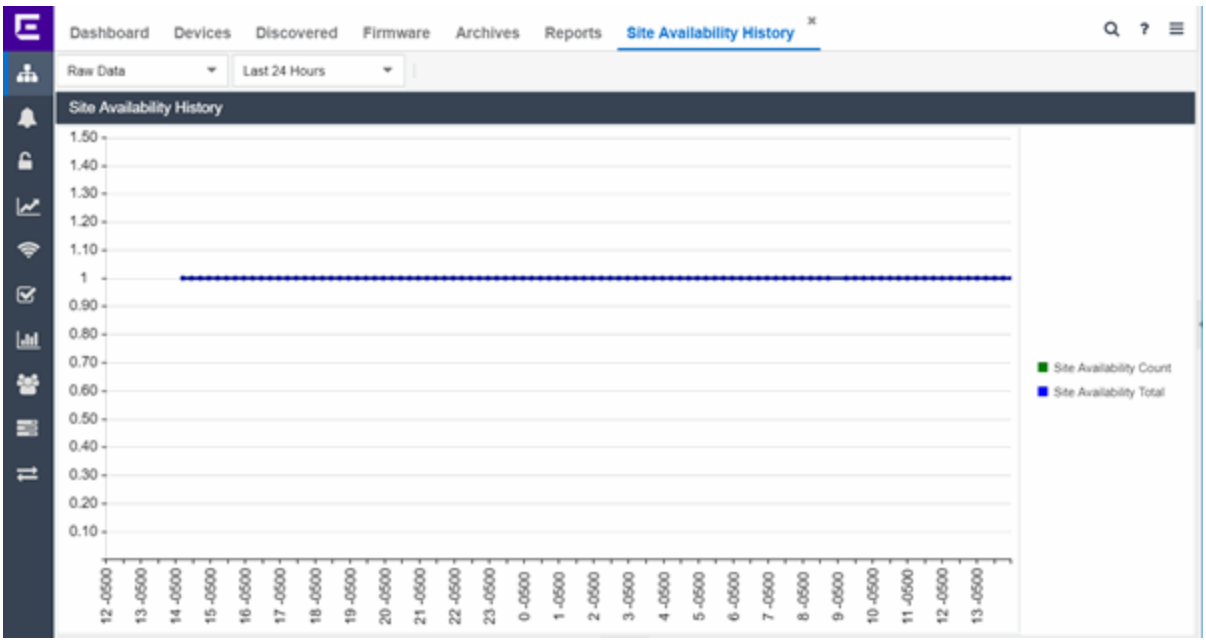
Site Availability History Report

The Site Availability History report contains a graph that displays the number of sites with a **Status** of **Up** (depending on the number of devices with which ExtremeCloud IQ Site Engine can communicate) (green), and the total number of sites that have devices (blue) for the duration you define. The values here are the values displayed in the Site Availability ring chart over the time span you define.

Use the **Devices Up for Site Up (percent)** field on the **Impact Status Options** tab to configure the threshold ExtremeCloud IQ Site Engine uses to determine if a site is up. The threshold is calculated as the ratio of devices in a site with a **Status** of **Up** to the total number of devices in the site.

Select the increment between which ExtremeCloud IQ Site Engine analyzes sites from the data drop-down list. Available options are **Raw**, **Hourly**, or **Daily** data.

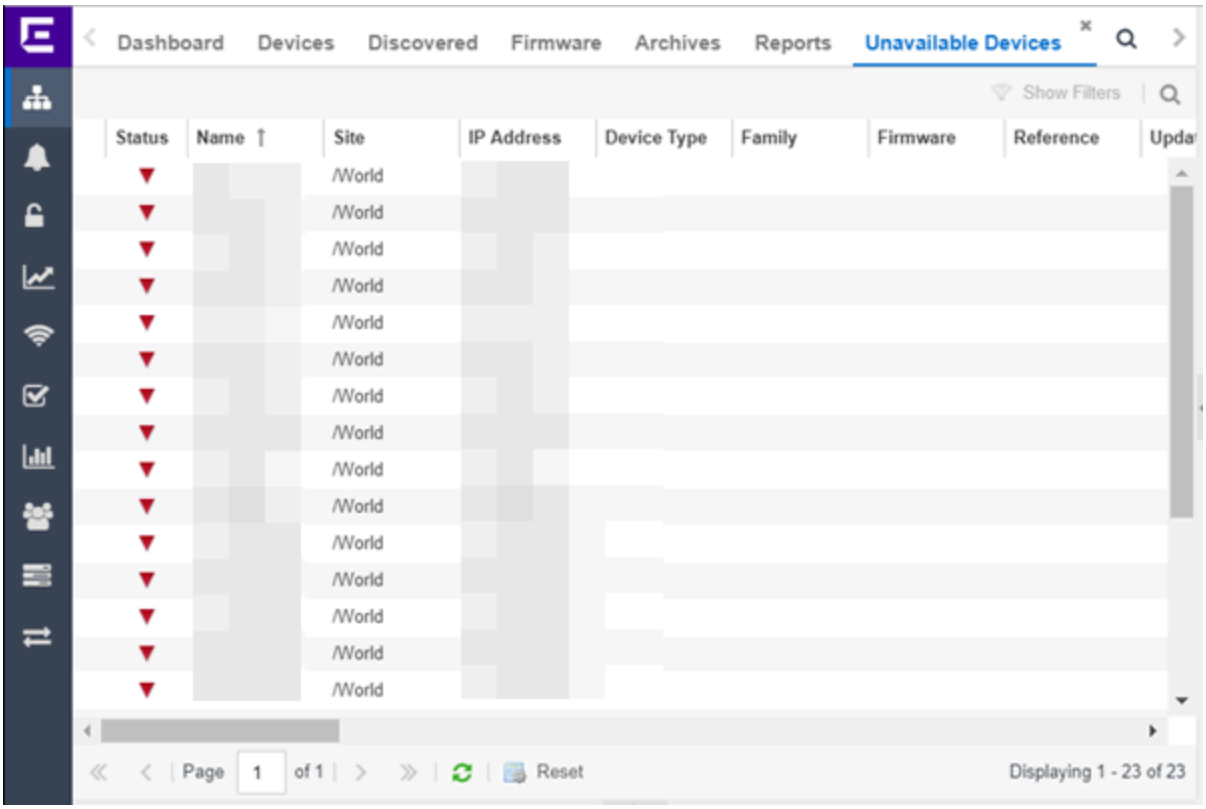
Select the time span for which the report displays from the time span drop-down list. Available options are **Last 24 Hours**, **Yesterday**, **Last 3 Days**, **Last Week**, **Last 2 Weeks**, **Last Month**.



- Impact Analysis Dashboard Overview

Unavailable Devices Report

The Unavailable Devices report provides detailed information for devices with which ExtremeCloud IQ Site Engine cannot communicate (**Status** of **Down**).



The following columns are included in the report:

Device Status

This column, hidden by default, indicates whether there is contact with the device. The color of the circle indicates the degree to which the device is communicating:

- Green icon (●) — Indicates ExtremeCloud IQ Site Engine is in contact with the device.
- Yellow icon (●) — Indicates ExtremeCloud IQ Site Engine has issues contacting the device.
- Red icon (●) — Indicates ExtremeCloud IQ Site Engine can not contact the device.

Hover over the Device Status icon to view additional details about the status for that device.

Status
: Indicates the device/alarm status for the device. The icon indicates the severity of the most severe alarm on the device:

  - Red icon () — A critical problem with significant implications.
  - Orange icon () — An error with limited implications.
  - Yellow icon () — A warning that might lead to a problem.
  - Blue icon () — Information only; not a problem.
  - Green icon () — ExtremeCloud IQ Site Engine can contact the device.

  Hover over the status icon to view the number of alarms. Select the alarm/device status icon to open a new page with detailed information about the alarms for that device.

Device ID
: This column, hidden by default, displays a number that serves as a database identifier automatically created for the device. This number increments as you add additional devices.

Name
: The device name, nickname, or IP address.

Site
: The site in which the device is located.

Poll Type
: This column, hidden by default, indicates the poll type ExtremeCloud IQ Site Engine uses to discover devices: SNMP, Ping or Not Polled.

Poll Group Name
: This column, hidden by default, indicates the name of the Poll Group you define in the Poll Groups section of the Status Polling options.

Admin Profile
: This column, hidden by default, indicates the access Profile that gives ExtremeCloud IQ Site Engine administrative access to the device.

Client Profile
: This column, hidden by default, indicates the access Profile that gives ExtremeCloud IQ Site Engine client access to the device.

IP Address
: The device's IP address.

Context
: The Context column, hidden by default, displays a string that indicates how the device behaves, depending on whether the device is a router or a switch.

IP Context
: The IP Context column, hidden by default, displays a device's IP address with the context appended to the end of the address following a colon.

Trap Status
: Indicates whether a trap receiver is configured, not configured, or not supported for the device. This column is hidden by default.

Syslog Status
: Indicates whether the device is configured to send information to the syslog or if it is not supported for the device. This column is hidden by default.

Display Name
: The IP address of the device. This column is hidden by default.

Device Type
: The type of device.

Family
: The device product family.

Firmware
: The revision for the firmware running in the device.

Running Reference Firmware
: Indicates if the device's thresholds have been configured for Reference Firmware

Updates
: The firmware release status for the device according to the results from the latest Check for Firmware Updates operation. Place your cursor on the column to see a tooltip describing the status.

Archived
: Indicates if the device has been archived in the last 30 days.

Config Changed
: Indicates if the archived configuration for the device has changed in the last 30 days.

Policy Domain
: The policy domain assigned to the device.

Boot PROM
: The revision for the BootPROM installed on the device.

Base MAC
: The base MAC address for the device.

Serial Number
: The serial number for the device.

Stats
: Displays whether statistics collection is enabled or disabled on the device. A black check mark indicates that historical collection is enabled, a blue check mark indicates that threshold alarms collection (formerly monitor collection) is enabled.

Location
: The physical location of the device. You can set the location for one or more devices by selecting the devices in the table, right-clicking, and selecting Set Selected Location from the menu.

Contact
: The name of the responsible contact person. You can set the contact for one or more devices by selecting the devices in the table, right-clicking, and selecting Set Selected Contact from the menu.

System Name
: Hostname for the device taken from the **System Name** field on the **Device** tab of the **Configure Device** window. You can set the system name for a device by selecting the device in the table, right-clicking, and selecting **Device** > **Configure Device**.

Uptime
: The amount of time, in a days hh:mm:ss format, that the device has been running since the last start-up.

Nickname
: The user-defined nickname for the selected device.

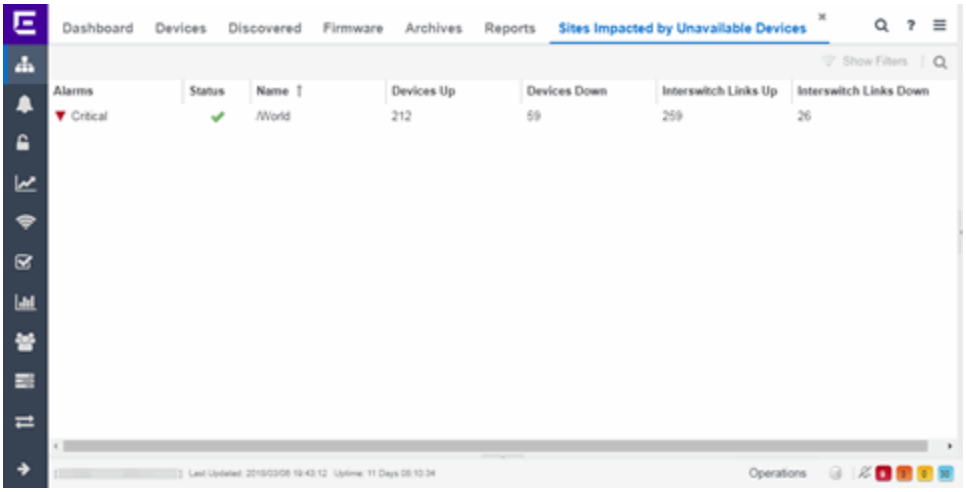
Description
: A description of the unavailable device.

User Data 1-4, Notes
: These columns can provide additional information about the device.

- Impact Analysis Dashboard Overview

Sites Impacted by Unavailable Devices Report

The Sites Impacted by Unavailable Devices report provides detailed information about sites that have one or more unavailable devices within your network.



The following columns are included in the report:

Alarms
: Shows the most severe alarm triggered by a device included in the site. The severity of the alarm is indicated by the following icons:

- Critical (▼) — A problem with significant implications.
- Error (▶) — A problem with limited implications.
- Warning (▲)— A condition that might lead to a problem.
- Info (■) — Information only; not a problem.
- None ( ) — No alarms on the device.

Status
: Indicates whether the site is up or down, based on the percentage of devices in the site with which ExtremeCloud IQ Site Engine can communicate (**Status** of **Up**). A green check mark indicates the site is up, while a red X icon indicates the site is down.

  Use the **Devices Up for Site Up (percent)** field on the **Impact Status Options** tab to configure the threshold ExtremeCloud IQ Site Engine uses to determine if a site is up. The threshold is calculated as the ratio of devices in a site with a **Status** of **Up** to the total number of devices in the site.

Name
: The name of the site.

Devices Up
: This column indicates the number of devices with a **Status** of **Up** in the site.

Devices Down
: This column indicates the number of devices with a **Status** of **Down** in the site.

Interswitch Links Up
: This column indicates the number of Interswitch Links with a **Status** of **Up** in the site.

Interswitch Links Down
: This column indicates the number of Interswitch Links with a **Status** of **Down** in the site.

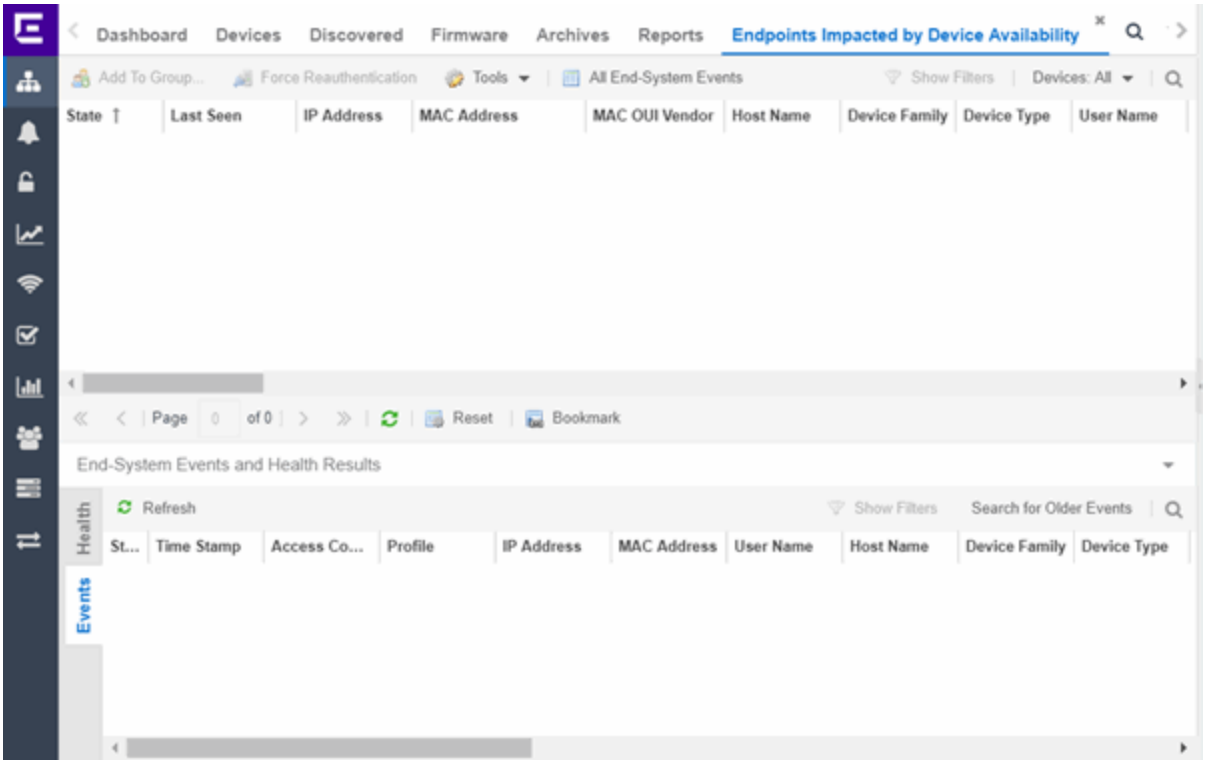
- Impact Analysis Dashboard Overview

Endpoints Impacted by Unavailable Devices Report

This report provides detailed information about end-systems impacted as the result of failing devices (**Status** of **Down**). An end-system is considered impacted if it was session-authenticated on the device at the time that the device became failing.

NOTE: Use the **Devices Up for Site Up (percent)** field on the **Impact Status Options** tab to configure the threshold ExtremeCloud IQ Site Engine uses to determine if a site is up. The threshold is based on the percentage of devices in a site with which ExtremeCloud IQ Site Engine can communicate.

The report also shows any events from the event log that pertain to the device selected in the top table. Additionally, the report lists the risks and vulnerabilities for the device and assigns a score based on the severity of the risk.



The report contains three tables:

- End-System Information
- Events
- Health

End-System Information

The table at the top of the report lists the end-systems that are affected as the result of unavailable devices.

ID
The identification number for the end-system. This column is hidden by default.

State
The end-system's connection state:

- Scan - The end-system is currently being scanned.
- Accept - The end-system is granted access with either the Accept policy or the policy returned from the RADIUS server in the filter-ID.
- Quarantine -The end-system is quarantined because the scanning test failed.
- Reject - The end-system was rejected because the assigned ExtremeControl profile was set to Reject, the MAC Locking test failed, or the RADIUS server was reachable but rejected the authentication request.
- Error - Indicates one of nine problems:
  - the MAC to IP resolution failed, if assessment is enabled
  - the MAC to IP resolution timed out, if assessment is enabled
  - all RADIUS servers are unreachable
  - the RADIUS request was non-compliant
  - all assessment servers are unavailable
  - the assessment server can't reach the end-system
  - no assessment servers are configured
  - the assessment server is not compatible with the current version of ExtremeCloud IQ Site Engine
  - the username and password configured in the Assessment Server section of the Access Control options (Administration > Options > Access Control) are incorrect for the assessment server

Last Seen
The last date and time the end-system was seen by the Access Control engine.

IP Address
The end-system's IP address.

OV MAC Key
: OV MAC Key. This column is hidden by default.

MAC Address
: The end-system's MAC address. MAC addresses are displayed as a full MAC address or with a MAC OUI (Organizational Unique Identifier) prefix, depending on the option you select the **Access Control Options** tab.

MAC OUI Vendor
: The vendor associated with the MAC OUI.

Host Name
: The end-system's host name.

Device Family
: The hardware family or the operating system family for the end-system.

Device Type
: The hardware type or the operating system type for the end-system.

User Name
: The User Name used for device access.

Switch IP
: The IP address of the switch to which the end-system is connected.

Switch Nickname
: The nickname defined for the switch to which the end-system is connected.

Switch Port
: The port alias (if defined) followed by the switch port number to which the end-system is connected.

Policy
: The policy role assigned to the end-system.

Authorization
: The Authorization granted to allow access to the end-system.

Risk Level
: The overall risk level assigned to the end-system based on the health result of the scan:

  - Red - High Risk
  - Orange - Medium Risk
  - Yellow - Low Risk
  - Green - No Risk
  - Gray - Unknown

Profile Name
: The name of the profile assigned to the end-system when it connected to the network.

Reason
: Provides additional information about the reasons why the end-system is in its particular connection state. It gives you an idea as to why a certain policy was applied to the end-system or why the end-system was rejected.

Authentication Type
: Identifies the latest authentication method used by the end-system to connect to the network.

State Description
: This column provides more details about the end-system state. For example, if the end-system's connection state is Reject, this column might list the RADIUS server (primary or secondary) that rejected the authentication request.

Extended State
: Provides additional information about the end-system's connection state.

Access Control Engine/Source IP
: The Engine to which the end-system is connecting.

Engine Group
: Displays what Engine group the ExtremeControl engine was in when the end-system event was generated. For example, if the Engine was in Engine group A when an end-system connected, but then later the Engine was moved to Engine group B, this column still list Engine group A for that end-system's entry.

RFC 3580 VLAN ID
: For end-systems connected to RFC 3580-enabled switches, this is the RFC3580 VLAN ID assigned to the end-system.

Warning Time
: Shows the time for warning. This column is hidden by default.

Last Quarantined
: The last date and time the end-system was quarantined. This column is hidden by default.

Score
: The total sum of the scores for all the health details that were included as part of the quarantine decision.

Top Score
: The highest score received for a health detail in the health result.

Actual
: The actual score is what the total score would be if all the health details including those marked Informational and Warning were included in the score.

Switch Port Index
: The switch port index to which the end-system connected.

Switch Location
: The physical location of the switch to which the end-system connected.

ELIN
: An extended set of data for an end-system based on a MAC address.

Port Info Raw
: Displays unformatted information as it is received from the port.

All Authentication Types
: This column displays all the authentication methods the end-system has used to authenticate.

Last Scan Result State
: The last scan result assigned to the end-system: Scan, Accept, Quarantine, Reject, Error. This is the state that was assigned to the end-system as a result of the last completed scan. This will typically match the end-system State if scanning is currently enabled and has been performed recently.

Last Scanned Time
: The last time an assessment (scan) was performed on the end-system.

First Seen Time
: he first time the end-system was seen by the ExtremeControl engine.

NAP Capable
: Indicates whether the end-system is Microsoft NAP (Network Access Protection) capable: **Yes** or **No**

Custom 1-4
: Use these column to add additional information that you would like displayed. You can add information for up to four Custom columns.

Registered User
: The registered username supplied by the end user during the registration process.

Registered Email
: The registered email address supplied by the end user during the registration process.

Registered Phone
: The registered phone number supplied by the end user during the registration process.

Sponsor
: The registered device's sponsor.

Registration 1-5
: The text from the Custom 1-5 registration fields supplied by the end user during the registration process.

Registration Description
: The device description supplied by the end user during the registration process.

Groups
: End-system groups are rule components that allow you to group together devices having similar network access requirements or restrictions.

Group 1-3
: Displays the names of up to three end-system groups.

Zone
: This field only displays if you have displayed the Zone column in the Access Control Configuration Rules table. Select the end-system zone assigned to any end-system matching this rule. See End-System Zones for more information.

Request Attributes
: Indicates if attributes have been requested

Registration Type
: Shows the type of registration

RADIUS Server IP
: The IP address of the RADIUS server with which the end-system is associated.

Source
: Displays the origin of the event:

  - Access Control engine — An Access Control engine.
  - Wireless Manager — An ExtremeWireless Controller or AP.
  - ExtremeXOS/Switch Engine ID Manager — An Extreme switch running ExtremeXOS/Switch Engine with the Identify Manager feature configured to send events to ExtremeCloud IQ Site Engine.
  - OneFabric Connect — An ExtremeConnect module (e.g. Solutions Architecture and Innovation (SAI) integration)
  - One Controller — The Extreme SDN Controller.

DCM
: Data Center Manager. This column is hidden by default.

TLS Client Certificate Expiration
: Expiration date of the TLS Client Certificate issued for 802.1x authentication.

TLS Client Certificate Issuer
: Name of the issuer of the TLS Client Certificate issued for 802.1x authentication.

Events Log

The Events table displays end-system events related to the unavailability of the site.

ID

The identification number for the end-system. This column is hidden by default.

State

The end-system's connection state:

- Scan - The end-system is currently being scanned.
- Accept - The end-system is granted access with either the Accept policy or the policy returned from the RADIUS server in the filter-ID.
- Quarantine -The end-system is quarantined because the scanning test failed.
- Reject - The end-system was rejected because the assigned ExtremeControl profile was set to Reject, the MAC Locking test failed, or the RADIUS server was reachable but rejected the authentication request.
- Error - Indicates one of nine problems:
  - the MAC to IP resolution failed, if assessment is enabled
  - the MAC to IP resolution timed out, if assessment is enabled
  - all RADIUS servers are unreachable
  - the RADIUS request was non-compliant
  - all assessment servers are unavailable
  - the assessment server can't reach the end-system
  - no assessment servers are configured
  - the assessment server is not compatible with the current version of NAC Manager
  - the username and password configured in the Assessment Server section of the Access Control options (Administration > Options > Assessment Server) are incorrect for the assessment server

Timestamp

Shows the date and time when an event occurred.

ExtremeControl engine / Source IP

The ExtremeControl engine to which the end-system is connecting.

Profile

The Profile assigned to the end-system in the ExtremeCloud IQ Site Engine database.

IP Address

The end-system's IP address.

MAC Address

The end-system's MAC address. MAC addresses are displayed as a full MAC address or with a MAC OUI (Organizational Unique Identifier) prefix, depending on the option you have selected

in the Display section of the Access Control Options (Administration > Options > Access Control).

User Name
The name of the user that triggered the event.

Host Name
The end-system's host name.

Device Family
The hardware family or the operating system family for the end-system.

Device Type
The hardware type or the operating system type for the end-system.

State Description
This column provides more details about the end-system's state. For example, if the end-system's connection state is Reject, this column might list the RADIUS server (primary or secondary) that rejected the authentication request.

Extended State
Provides additional information about the end-system's connection state.

Reason
Provides additional information about the reasons why the end-system is in its particular connection state. It gives you an idea as to why a certain policy was applied to the end-system or why the end-system was rejected.

Authorization
The attributes returned by the RADIUS server for this end-system. If the end-system is connected to a switch that supports multi-authentication, then this column may not reflect the actual active policy for the authenticated user. For Layer 3 Access Control Controller engines, this column displays the policy assigned to the end-system for its authorization.

Auth Type
Identifies the authentication method used by the end-system to connect to the network. For Layer 3 Access Control Controller engines, this column shows **IP**.

Switch IP
The IP address of the switch to which the end-system connected. If the end-system is connected to an Access Control Controller engine, this is the Access Control Controller PEP (Policy Enforcement Point) IP address..

Switch Nickname
The nickname defined for the switch to which the end-system is connected.

Switch Port Index
The switch port index to which the end-system is connected.

Switch Port
The switch port interface name to which the end-system is connected.

Switch Location
The physical location of the switch to which the end-system connected. If the end-system is connected to an Access Control Controller engine, this is the Access Control Controller PEP (Policy Enforcement Point) location.

ELIN
An extended set of data for an end-system based on a MAC address.

Port Info Raw
Displays unformatted information as it is received from the port.

Last Scan Time
The last time an assessment (scan) was performed on the end-system.

Zone
Displays the end-system zone to which the end-system is assigned.

Registration Type
The end-system type supplied by the end user during the registration process.

RADIUS Server IP
The IP address of the RADIUS server with which the end-system is associated.

Event Source
Displays the origin of the event:

- Access ControlEngine — A Access Controlengine.
- Wireless Manager — An ExtremeWireless Wireless Controller or AP.
- ExtremeXOS/Switch Engine ID Manager — An Extreme switch running ExtremeXOS/Switch Engine with the Identify Manager feature configured to send events to ExtremeCloud IQ Site Engine.
- OneFabric Connect — A custom project (e.g. Solutions Architecture and Innovation (SAI) integration)
- One Controller — The Extreme SDN Controller.

Health Log

This tab provides summary information on health results (assessment results) obtained for the end-system selected in the table above. You can specify the number of health result summaries displayed using the Health Result Persistence options in the Data Persistence Options.

Risk
The risk level assigned to the end-system based on the health result of the scan: High Risk, Medium Risk, Low Risk, or No Risk.

Name
This column lists the name of the test that is reported by the health result detail.

Test Case ID
The unique number assigned to the test case.

Score
The score assigned to the test case. The score is a value between 0.0 and 10.0. In the case of agent-based test cases, the score is either 0.0 for a passed test, or 10.0 for a failed test, unless specifically overwritten by the scoring override configuration.

Scoring Mode
The scoring mode that was used at the time the test was performed.

- Applied — The score returned by this test was included as part of the quarantine decision.
- Informational — The score returned by this test was reported, but did not apply toward a quarantine decision.
- Warning — The score returned by this test was only used to provide end user assessment warnings via the Notification portal web page.

CVE IDs
The CVE (Common Vulnerability and Exposures) ID assigned to the security vulnerability or exposure. For more information on CVE IDs, refer to the following URL: https://cve.mitre.org/.

Description
This column lists information about the health result detail.

Solution
This column lists a solution for the health result.

Port ID
The port on which the end-system the security risk was detected.

Protocol ID
The well-known number (ID) assigned to the IP Protocol Type.

Assessment
The list of test sets that were run during assessment, for example, Default Nessus, Default Agent-less, and Default Agent-based. Test sets are defined as part of the assessment configuration. If the end-system is NAP capable, then this column displays Microsoft NAP indicating that NAP performed the assessment.

Remediation
For agent-based assessment, this column lists the results of remediation attempts: Success, Failed, or Not Attempted.

Type

A "type" is assigned to each security risk found on a port during an assessment, and is used to determine whether to Quarantine an end-system. Types are configurable on the assessment agent. There are three types:

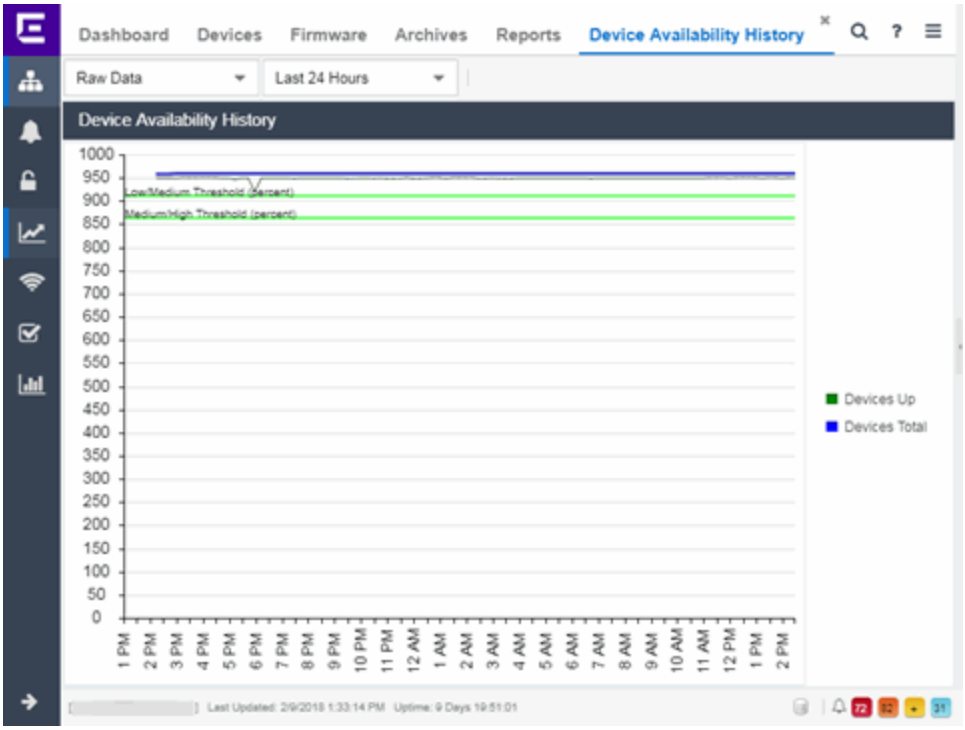
- Hole — The port is vulnerable to attack.
- Warning — The port may be vulnerable to attack.
- Note — There may be a security risk on the port.

Device Availability History Report

The Device Availability History report contains a graph that displays the number of devices with which ExtremeCloud IQ Site Engine can communicate (**Status** of **Up**) (green) and the total number of devices on your network (blue) for the duration you define. The values are the values displayed in the Device Availability ring chart over the time span you define.

Select the increment between which ExtremeCloud IQ Site Engine analyzes devices from the data drop-down list. Available options are **Raw**, **Hourly**, or **Daily** data.

Select the time span for which the report displays from the time span drop-down list. Available options are **Last 24 Hours**, **Yesterday**, **Last 3 Days**, **Last Week**, **Last 2 Weeks**, **Last Month**.



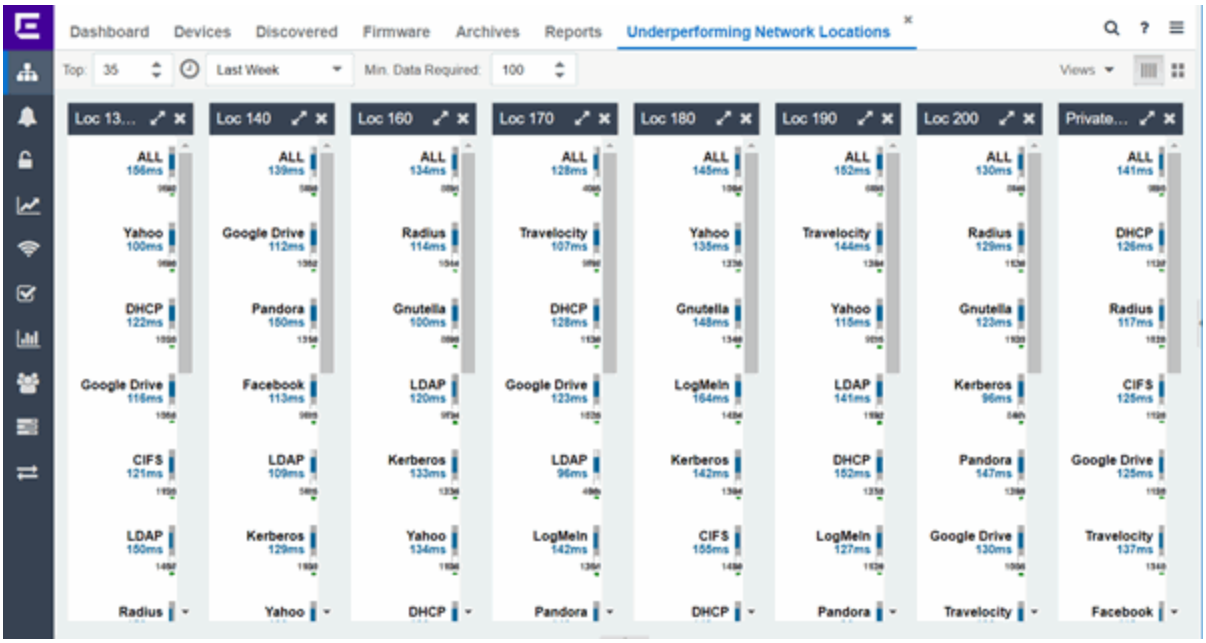
- Impact Analysis Dashboard Overview

Slow Locations Report

The Slow Locations report displays the tracked applications and network services that are experiencing slower-than-expected network response times for at least three consecutive minutes. Network response times that are slower-than-expected for less than three consecutive minutes are not displayed in the report.

In a network with two locations, a tracked application accessed at each location appears twice, one time for each location. Only affected applications for each site are displayed. If no applications have slower-than-expected network response times, the chart may display no data. The data in this report updates every 60 seconds.

NOTE: The graph displays network locations observed on all of your ExtremeAnalytics engines.



Use the menu at the top of the report to configure the information presented:

Top:
: Choose the number of locations in networks with the slowest response times to display response times in the chart.

Time Span
: Select the span of time for which network response times are displayed from the drop-down list. Available options are: **Custom**, **Today**, **Yesterday**, **Last 30 Minutes**, **Last Hour**, **Last 2 Hours**, **Last 6 Hours**, **Last 12 Hours**, **Last 24 Hours**, **Last 3 Days**, **Last Week**. The line graph displays detailed response time for each application over the length of time you define.

Min Data Required
Select the minimum number of response time data points required to display in the report.

Display Format
Select how data is displayed: Select ( ) to display the data in columns or ( ) to display the data in rows.

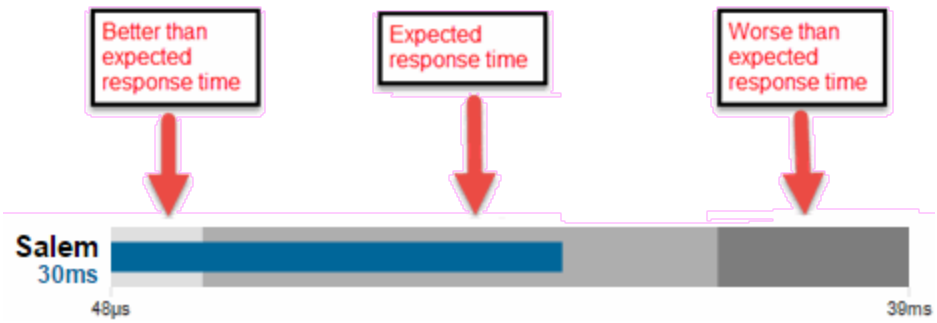
The report contains two types of graphs:

- Expected Response Time
- Historical Response Time

Expected Response Time

The Expected Response Time bar graph displays the range of network response times, the most recently measured network response time, and the expected network response time for an application a specific site (or all sites) during the date range you configure in the **Time Span** drop-down list. The value displayed on the far right of the graph is the slowest network response time observed during the selected time period. The vertical blue or red bar indicates the most recently observed network response time for the application.

NOTE: The values in this graph are an average of all response times observed every minute.



Hover over the Expected Response Time graph to display a pop-up with the most recent network response time for the site as well as the date and time the measurement occurred.

ExtremeCloud IQ Site Engine uses the standard deviation of the values gathered as network response times to determine the expected network response time for an application at a location. In the bar graph, the medium gray color indicates a network response time that falls within the "expected" range. This range is the average value of all observed network response times plus or minus two standard deviations, or about 95 percent of all response time values. A network response time in the light gray range is better than expected, while a network response time in the dark gray is worse than expected.

When a network response time is determined to be worse than expected, the location name and the network response time indicator turn red to flag the application.



Historical Response Time

The Historical Response Time line graph shows all of the network response times observed for the application at a location (or all locations).

NOTE: The values in this graph are an average of all response times observed every hour.



Hovering over a point in the graph causes a dot on the line graph to appear, indicating the point in the network response time at which you are looking. Additionally, a pop-up with the date, time, and network response time appears for that point.

This is the data set from which ExtremeCloud IQ Site Engine creates the Expected Response Time graph. The wider the expected network response time range in the Expected Response Time graph (indicated by the medium gray color), the greater the variance in the values in this graph.

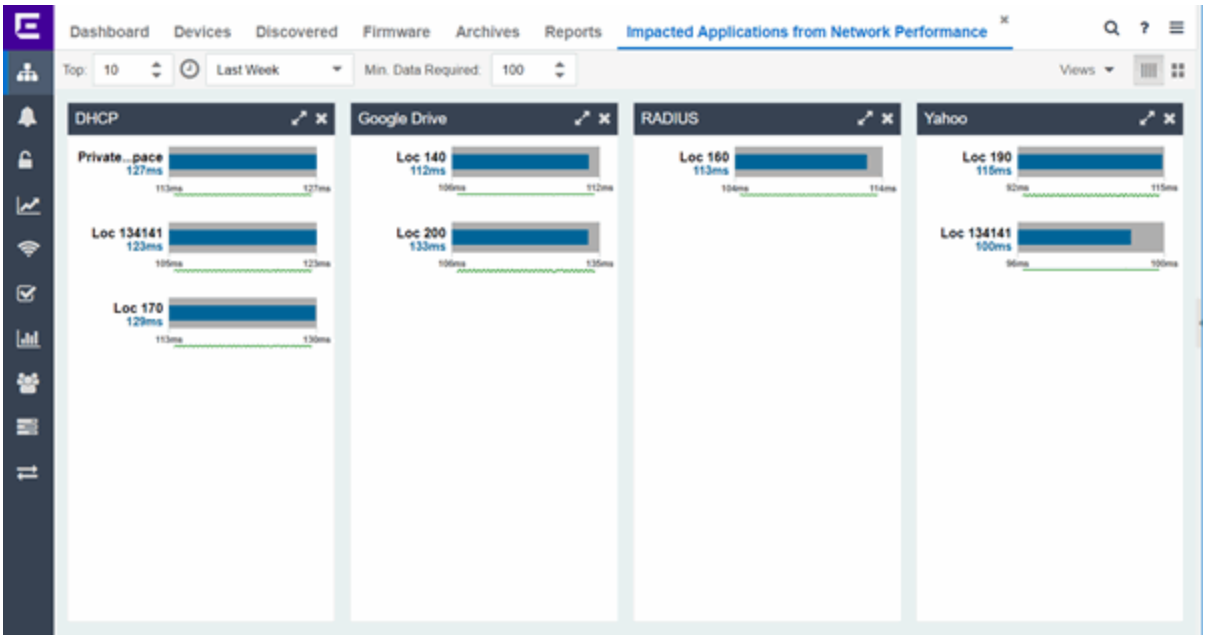
- Impact Analysis Dashboard Overview

Applications Impacted by Slow Locations Report

The Applications Impacted by Slow Locations report provides detailed information about tracked applications and network services that are experiencing slower-than-expected network response times for at least three consecutive minutes. Network response times that are slower-than-expected for less than three consecutive minutes are not displayed in the report.

In a network with two sites, a tracked application accessed at each site appears twice, one time for each site. Only affected applications for each location are displayed. If no applications have slower-than-expected network response times, the chart may display no data. The data in this report updates every 60 seconds.

NOTE: The graph displays network locations observed on all of your ExtremeAnalytics engines.



Use the menu at the top of the report to configure the information presented:

Top
: Select the number of sites to include in the report. The sites shown are those with the slowest network response times.

Time Span
: Select the span of time for which network response times for locations are displayed from the drop-down list. Available options are: **Custom**, **Today**, **Yesterday**, **Last 30 Minutes**, **Last Hour**, **Last 2 Hours**, **Last 6 Hours**, **Last 12 Hours**, **Last 24 Hours**, **Last 3 Days**, **Last Week**. The line graph displays detailed response time for each application at each location over the length of time you define.

Min Data Required
: Select the minimum number of response time data points required to display in the report.

Display Format
: Select how data is displayed: Select (▥) to display the data in columns or (▦) to display the data in rows.

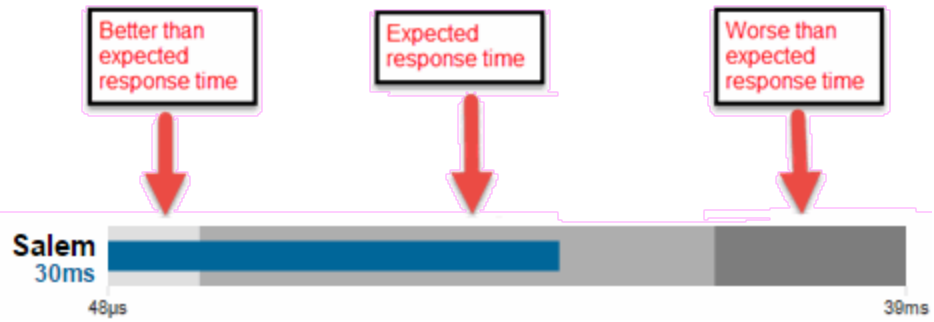
The report contains two graphs:

- Expected Response Time
- Historical Response Time

Expected Response Time

The Expected Response Time bar graph displays the range of network response times, the most recently measured network response time, and the expected network response time for an application a specific site (or all sites) during the date range you configure in the **Time Span** drop-down list. The value displayed on the far right of the graph is the slowest network response time observed during the selected time period. The vertical blue or red bar indicates the most recently observed network response time for the application.

NOTE: The values in this graph are an average of all network response times observed every minute.



Hover over the Expected Response Time graph to display a pop-up with the most recent network response time for the application, as well as the date and time the measurement occurred.

ExtremeCloud IQ Site Engine uses the standard deviation of the values gathered as network response times to determine the expected network response time for an application at a site. In the bar graph, the medium gray color indicates a network response time that falls within the "expected" range. This range is the average value of all observed network response times plus or minus two standard deviations, or about 95 percent of all network response time values. A network response time in the light gray range is better than expected, while a network response time in the dark gray is worse than expected.

When a network response time is determined to be worse than expected, the site name and the network response time indicator turn red to flag the application.



Historical Response Time

The Historical Response Time line graph shows all of the network response times observed for the application in the network (or all networks).

NOTE: The values in this graph are an average of all network response times observed every hour.



Hovering over a point in the graph causes a dot on the line graph to appear, indicating the point in the network response time at which you are looking. Additionally, a pop-up with the date, time, and network response time appears for that point.

This is the data set from which ExtremeCloud IQ Site Engine creates the Expected Response Time graph. The wider the expected network response time range in the Expected Response Time graph (indicated by the medium gray color), the greater the variance in the values in this graph.

- Impact Analysis Dashboard Overview

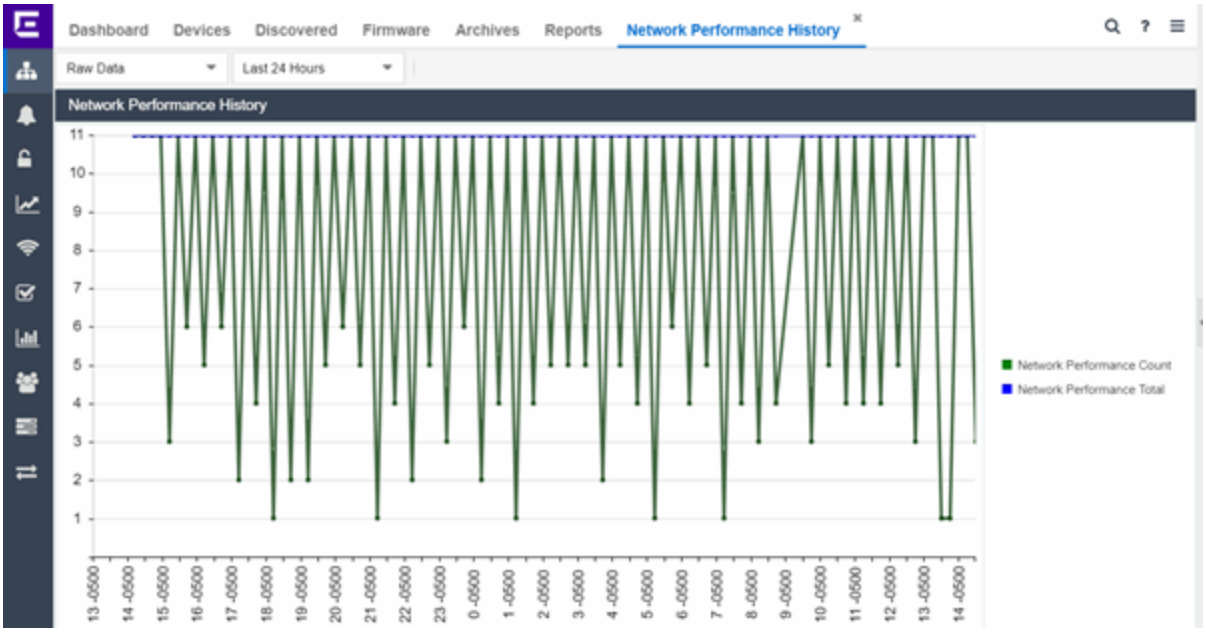
Network Performance History Report

The Network Performance History report contains a graph that displays the number of sites that have no tracked applications or network services with slower-than-expected network response times (green) and the total number of network locations (blue) for the duration you define. The values here are the values displayed in the Network Performance ring chart over the time span you define.

NOTE: The graph displays network locations observed on all of your ExtremeAnalytics engines.

Select the increment between which ExtremeCloud IQ Site Engine analyzes network locations from the data drop-down list. Available options are **Raw**, **Hourly**, or **Daily** data.

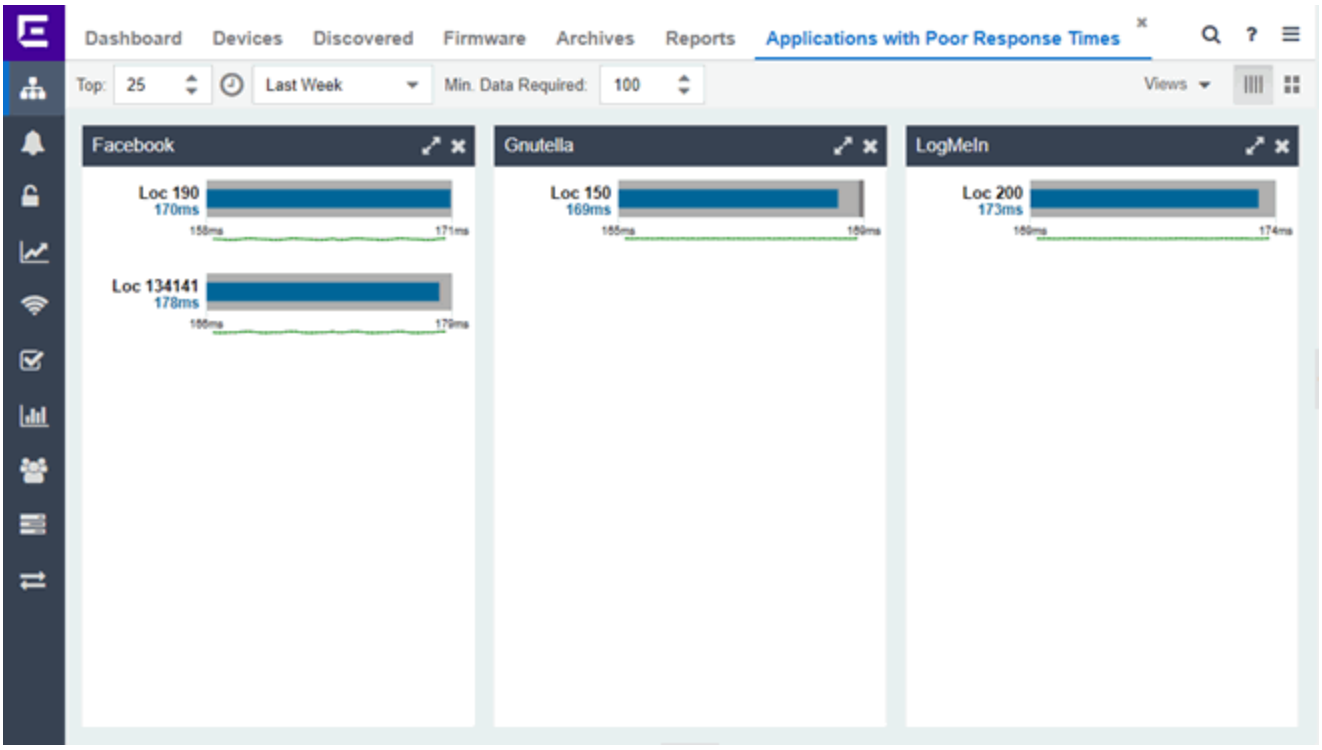
Select the time span for which the report displays from the time span drop-down list. Available options are **Last 24 Hours**, **Yesterday**, **Last 3 Days**, **Last Week**, **Last 2 Weeks**, **Last Month**.



- Impact Analysis Dashboard Overview

Slow Applications Report

The Slow Applications report displays the tracked applications and network services at sites with slower-than-expected application response times. In a network with two sites, a tracked application accessed at each site appears twice, one time for each site. Only affected applications for each site are displayed. If no applications have slower-than-expected application response times, the chart may display no data. The data in this report updates every 60 seconds.



Use the menu at the top of the report to configure the information presented:

Top:
: Choose the number of tracked applications and network services with slower-than-expected application response times to display application response times in the chart.

Time Span
: Select the span of time for which application response times are displayed from the drop-down list. Available options are: **Custom**, **Today**, **Yesterday**, **Last 30 Minutes**, **Last Hour**, **Last 2 Hours**, **Last 6 Hours**, **Last 12 Hours**, **Last 24 Hours**, **Last 3 Days**, **Last Week**. The line graph displays detailed response time for each application over the length of time you define.

Min Data Required
: Select the minimum number of response time data points required for a tracked application or network service to display in the report.

Display Format
: Select how data is displayed: Select (▥) to display the data in columns or (▦) to display the data in rows.

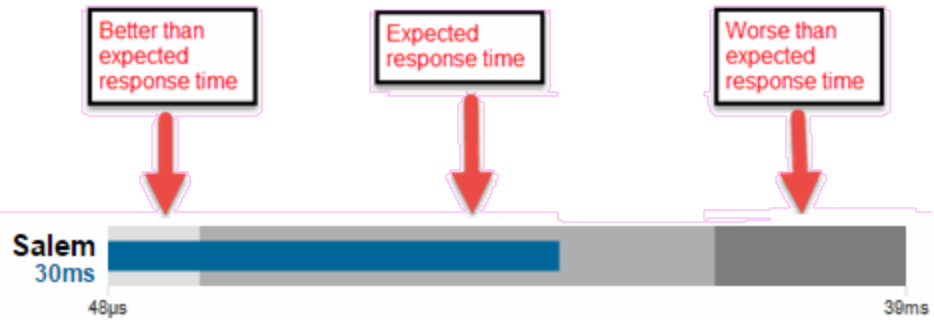
The report contains two types of graphs:

- Expected Response Time
- Historical Response Time

Expected Response Time

The Expected Response Time bar graph displays the range of application response times, the most recently measured response time, and the expected application response time for an application a specific site (or all sites) during the date range you configure in the **Time Span** drop-down list. The value displayed on the far right of the graph is the slowest application response time observed during the selected time period. The vertical blue or red bar indicates the most recently observed application response time for the application.

NOTE: The values in this graph are an average of all response times observed every minute.



Hover over the Expected Response Time graph to display a pop-up with the most recent application response time for the application as well as the date and time the measurement occurred.

ExtremeCloud IQ Site Engine uses the standard deviation of the values gathered as application response times to determine the expected application response time for an application at a site. In the bar graph, the medium gray color indicates an application response time that falls within the "expected" range. This range is the average value of all observed application response times plus or minus two standard deviations, or about 95 percent of all application response time values. An application response time in the light gray range is better than expected, while an application response time in the dark gray is worse than expected.

When an application response time is determined to be worse than expected, the site name and the application response time indicator turn red to flag the application.



Historical Response Time

The Historical Response Time line graph shows all of the application response times observed for the application at a site (or all sites).

NOTE: The values in this graph are an average of all response times observed every hour.



Hovering over a point in the graph causes a dot on the line graph to appear, indicating the point in the application response time at which you are looking. Additionally, a pop-up with the date, time, and an application response time appears for that point.

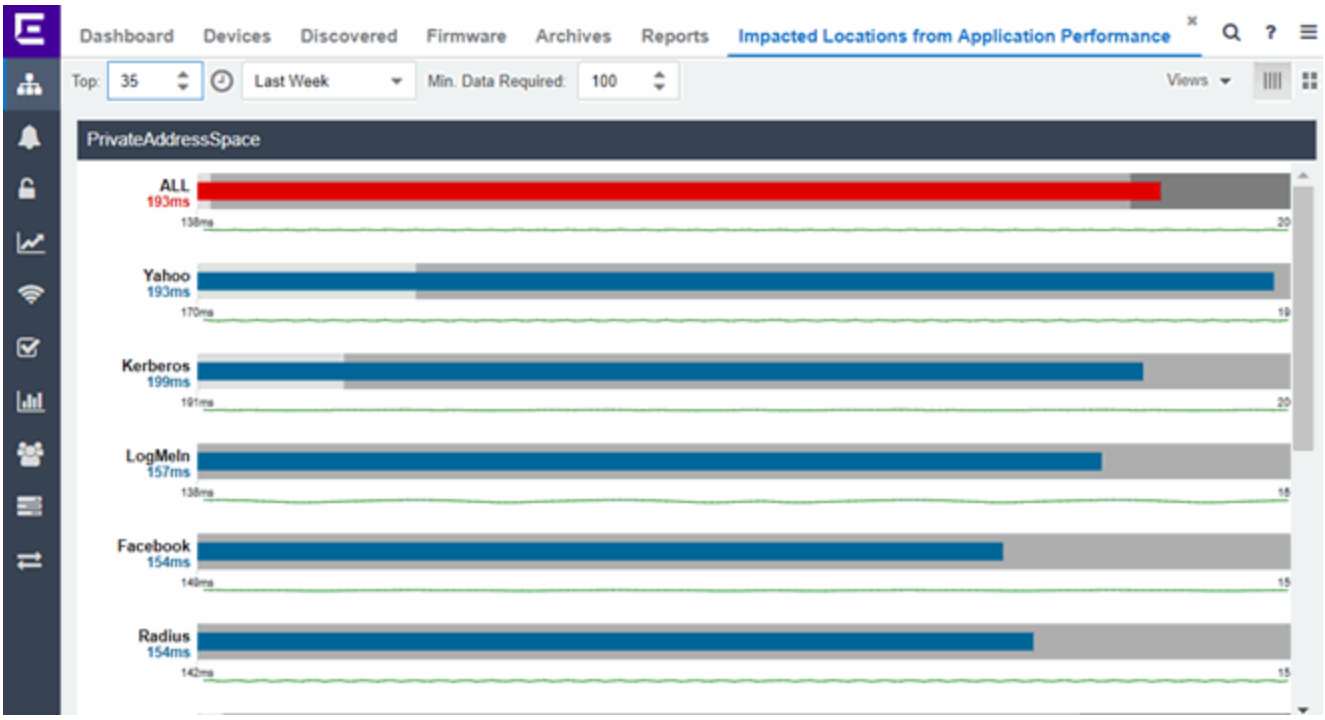
This is the data set from which ExtremeCloud IQ Site Engine creates the Expected Response Time graph. The wider the expected application response time range in the Expected Response Time graph (indicated by the medium gray color), the greater the variance in the values in this graph.

- Impact Analysis Dashboard Overview

Locations Impacted by Slow Applications

The Locations Impacted by Slow Applications report provides detailed information about sites with at least one application with a slower-than-expected application response time. All applications for each location are displayed, including those with better-than-expected or expected application response times. If no locations have applications with slower-than-expected application response times, the chart may display no data. The data in this report updates every 60 seconds.

NOTE: If you have multiple ExtremeAnalytics engines, you must select the engine for which you wish to display data.



Use the menu at the top of the report to configure the information presented:

Top
: Select the number of locations to include in the report. The locations shown are those with the slowest response times.

Time Span
: Select the span of time for which application response times for locations are displayed from the drop-down list. Available options are: **Custom**, **Today**, **Yesterday**, **Last 30 Minutes**, **Last Hour**, **Last 2 Hours**, **Last 6 Hours**, **Last 12 Hours**, **Last 24 Hours**, **Last 3 Days**, **Last Week**. The line graph displays detailed response time for each application at each location over the length of time you define.

Min Data Required
: Select the minimum number of response time data points required to display in the report.

Display Format
: Select how data is displayed: Select (▥) to display the data in columns or (▦) to display the data in rows.

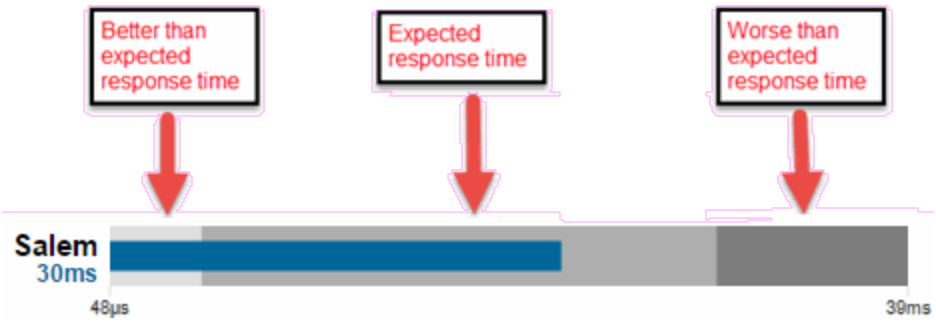
The report contains two types of graphs:

- Expected Response Time
- Historical Response Time

Expected Response Time

The Expected Response Time bar graph displays the range of application response times, the most recently measured application response time, and the expected application response time for an application at a specific location (or all locations) during the date range you configure in the **Time Span** drop-down list. The value displayed on the far right of the graph is the slowest application response time observed during the selected time period. The vertical blue or red bar indicates the most recently observed application response time for the application.

NOTE: The values in this graph are an average of all response times observed every minute.



Hover over the Expected Response Time graph to display a pop-up with the most recent application response time for the application, as well as the date and time the measurement occurred.

ExtremeCloud IQ Site Engine uses the standard deviation of the values gathered as application response times to determine the expected response time for an application at a location. In the bar graph, the medium gray color indicates a application response time that falls within the "expected" range. This range is the average value of all observed application response times plus or minus two standard deviations, or about 95 percent of all application response time values. An application response time in the light gray range is better than expected, while an application response time in the dark gray is worse than expected.

When an application response time is determined to be worse than expected, the location name and the application response time indicator turn red to flag the application.



Historical Response Time

The Historical Response Time line graph shows all of the application response times observed for the application at a location (or all locations).

NOTE: The values in this graph are an average of all response times observed every hour.



Hovering over a point in the graph causes a dot on the line graph to appear, indicating the point in the application response time at which you are looking. Additionally, a pop-up with the date, time, and application response time appears for that point.

This is the data set from which ExtremeCloud IQ Site Engine creates the Expected Response Time graph. The wider the expected application response time range in the Expected Response Time graph (indicated by the medium gray color), the greater the variance in the values in this graph.

- Impact Analysis Dashboard Overview

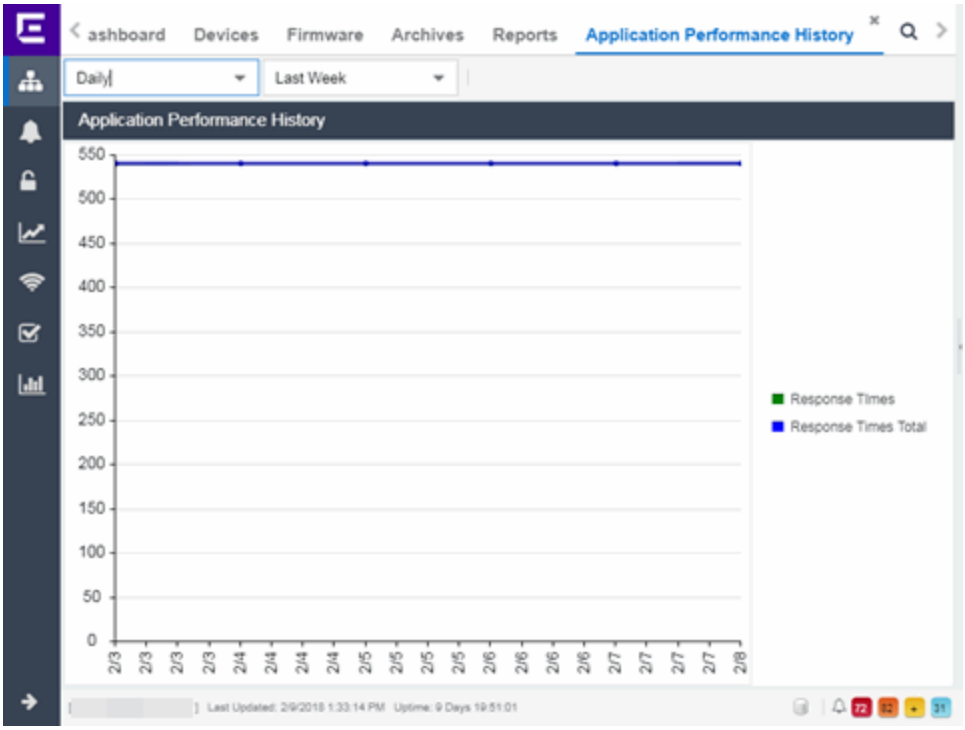
Application Performance History Report

The Application Performance History report contains a graph that provides the number of tracked applications and network services at all of your sites with an application response time within the expected range (green) and the total number of tracked applications and network services at all sites (blue) for the duration you define. If no sites have application response times within the expected range, the chart may not display data (green). In a network with two sites, a tracked application accessed at each site appears twice, one time for each site. The values here are the values displayed in the Application Performance ring chart over the time span you define.

NOTE: The graph displays tracked applications and network services observed on all of your ExtremeAnalytics engines.

Select the increment between which ExtremeCloud IQ Site Engine analyzes applications from the data drop-down list. Available options are **Raw**, **Hourly**, or **Daily** data.

Select the time span for which the report displays from the time span drop-down list. Available options are **Last 24 Hours**, **Yesterday**, **Last 3 Days**, **Last Week**, **Last 2 Weeks**, **Last Month**.

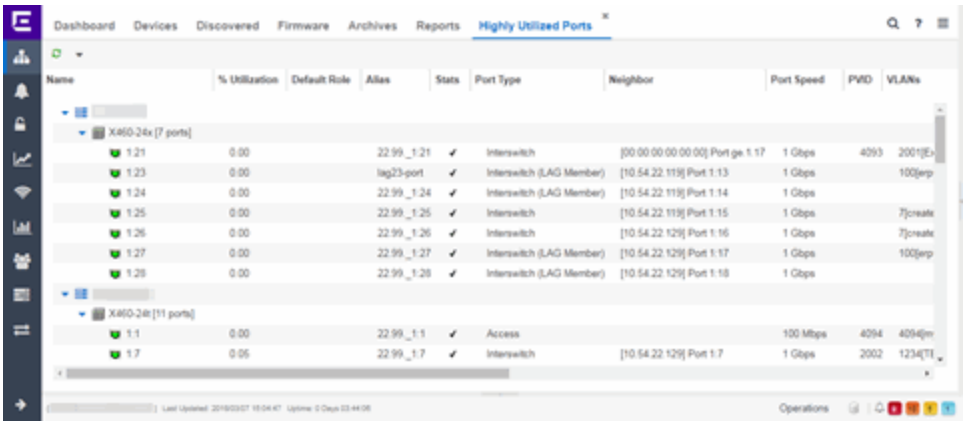


- Impact Analysis Dashboard Overview

Highly Utilized Ports Report

The Highly Utilized Ports report provides detailed information about the ports for which utilization statistics are above the threshold you configure. A port is displayed in the report if the port is up and historical data collection has been enabled on the device long enough for statistic collection.

NOTE: Use the Port Capacity Chart section of the Impact Analysis options to configure the threshold ExtremeCloud IQ Site Engine uses to determine port utilization.



The following columns are included in the report:

Name
The interface name for the port.

% Utilization
The percentage of utilization last reported for the port.

Default Role
If the end-user is unauthenticated, the port implements its default role. You can select to use the current default role on the device or set a default role. If there is no default role specified, there is no role on the port.

Alias
Shows the alias (ifAlias) for the interface, if one is assigned.

Stats
Displays information about the port, if configured in PortView.

Port Type
The type of port. Possible values include: Access, CDP, CDP FTM 1 Backplane, FTM 1 Backplane, and Logical.

Neighbor
The port to which the port is connected.

Port Speed
The speed of the port. Possible values include: 10/100, speed in megabits per second (for example, 800.0 Mbps), Unknown (displayed for logical ports).

PVID
Displays the VLAN ID of the VLAN assigned to the port. When you assign a VLAN to a port, that VLAN's ID (VID) becomes the Port VLAN ID (PVID) for the port.

VLANs
The VLANs to which the port is associated.

Description
A description of the port and the device.

Port Type Details
Additional information about the type of port.

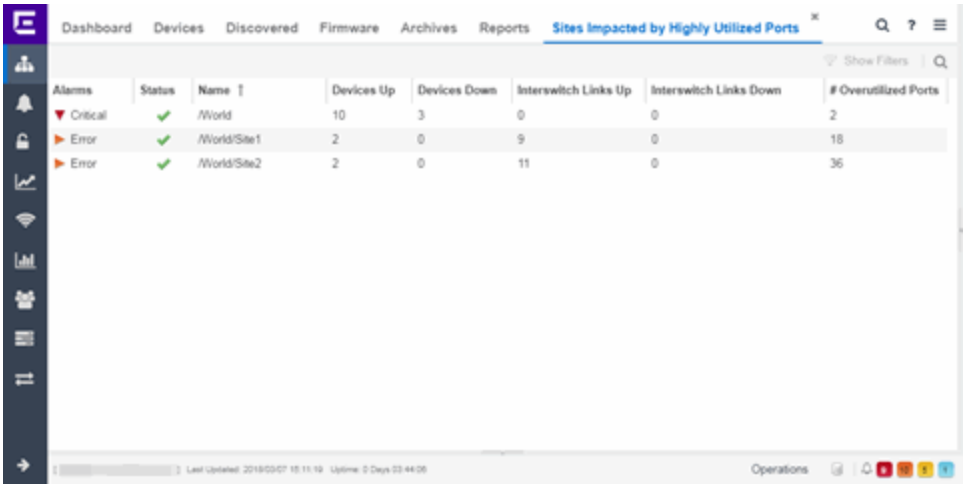
Serial Number
The serial number of the device.

- Impact Analysis Dashboard Overview

Sites Impacted by Highly Utilized Ports Report

The Sites Impacted by Highly Utilized Ports report detailed information about the ports for which utilization statistics are above the threshold you configure. A port is displayed in the report if the port is up and historical data collection has been enabled on the device long enough for statistic collection.

NOTE: Use the Port Capacity Chart section of the Impact Analysis options to configure the threshold ExtremeCloud IQ Site Engine uses to determine port utilization.



The following columns are included in the report:

Alarms

Shows the most severe alarm triggered by a device included in the site. The severity of the alarm is indicated by the following icons:

- Critical (▼) — A problem with significant implications.
- Error (▶) — A problem with limited implications.
- Warning (▲)— A condition that might lead to a problem.
- Info (■) — Information only; not a problem.
- None ( ) — No alarms on the device.

Status

Indicates whether the site is up or down, based on the percentage of devices in the site with which ExtremeCloud IQ Site Engine can communicate (**Status** of **Up**). A green check mark indicates the site is up, while a red X icon indicates the site is down.

Use the **Devices Up for Site Up (percent)** field on the **Impact Status Options** tab to configure the threshold ExtremeCloud IQ Site Engine uses to determine if a site is up. The

threshold is calculated as the ratio of devices in a site with a **Status** of **Up** to the total number of devices in the site.

Name
: The name of the site.

Devices Up
: This column indicates the number of devices with a **Status** of **Up** in the site.

Devices Down
: This column indicates the number of devices with a **Status** of **Down** in the site.

Interswitch Links Up
: This column indicates the number of Interswitch Links with a **Status** of **Up** in the site.

Interswitch Links Down
: This column indicates the number of Interswitch Links with a **Status** of **Down** in the site.

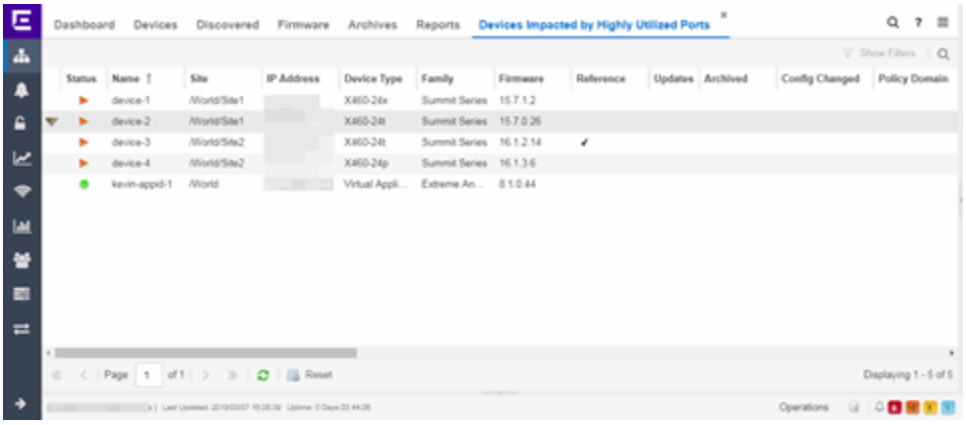
Overutilized Rate
: The number of ports with utilization percentage you configure as unacceptable in the Port Capacity Chart section of the Impact Analysis options

- Impact Analysis Dashboard Overview

Devices Impacted by Highly Utilized Ports Report

The Devices Impacted by Highly Utilized Ports report detailed information about the ports for which utilization statistics are above the threshold you configure. A port is displayed in the report if the port is up and historical data collection has been enabled on the device long enough for statistic collection.

NOTE: Use the Port Capacity Chart section of the Impact Analysis options to configure the threshold ExtremeCloud IQ Site Engine uses to determine port utilization.



The following columns are included in the report:

Device Status
: This column, hidden by default, indicates whether there is contact with the device. The color of the circle indicates the degree to which the device is communicating:

  - Green icon ( ) — Indicates ExtremeCloud IQ Site Engine is in contact with the device.
  - Yellow icon ( ) — Indicates ExtremeCloud IQ Site Engine has issues contacting the device.
  - Red icon ( ) — Indicates ExtremeCloud IQ Site Engine can not contact the device.

  Hover over the Device Status icon to view additional details about the status for that device.

Status
: Indicates the device/alarm status for the device. The icon indicates the severity of the most severe alarm on the device:

  - Red icon ( ) — A critical problem with significant implications.
  - Orange icon ( ) — An error with limited implications.
  - Yellow icon ( ) — A warning that might lead to a problem.
  - Blue icon ( ) — Information only; not a problem.
  - Green icon ( ) — ExtremeCloud IQ Site Engine can contact the device.

  Hover over the status icon to view the number of alarms. Select on the alarm/device status icon to open a new page with detailed information about the alarms for that device.

Device ID
: This column, hidden by default, displays a number that serves as a database identifier automatically created for the device. This number increments as you add additional devices.

Name
: The device name, nickname, or IP address.

Site
: The site in which the device is located.

Poll Type
: This column, hidden by default, indicates the poll type ExtremeCloud IQ Site Engine uses to discover devices: SNMP, Ping or Not Polled.

Poll Group Name
: This column, hidden by default, indicates the name of the Poll Group you define in the Poll Groups section of the Status Polling options.

Admin Profile
: This column, hidden by default, indicates the access Profile that gives ExtremeCloud IQ Site Engine administrative access to the device.

Client Profile
: This column, hidden by default, indicates the access Profile that gives ExtremeCloud IQ Site Engine client access to the device.

IP Address
: The device's IP address.

Context
: The Context column, hidden by default, displays a string that indicates how the device behaves, depending on whether the device is a router or a switch.

IP Context
: The IP Context column, hidden by default, displays a device's IP address with the context appended to the end of the address following a colon.

Trap Status
: Indicates whether a trap receiver is configured, not configured, or not supported for the device. This column is hidden by default.

Syslog Status
: Indicates whether the device is configured to send information to the syslog or if it is not supported for the device. This column is hidden by default.

Display Name
: The IP address of the device. This column is hidden by default.

Device Type
: The type of device.

Family
: The device product family.

Firmware
: The revision for the firmware running in the device.

Running Reference Firmware
: Indicates if the device's thresholds have been configured for Reference Firmware

Updates
: The firmware release status for the device according to the results from the latest Check for Firmware Updates operation. Place your cursor on the column to see a tooltip describing the status.

Archived
: Indicates if the device has been archived in the last 30 days.

Config Changed
: Indicates if the archived configuration for the device has changed in the last 30 days.

Policy Domain
: The policy domain assigned to the device.

Boot PROM
: The revision for the BootPROM installed on the device.

Base MAC
: The base MAC address for the device.

Serial Number
: The serial number for the device.

Stats
: Displays whether statistics collection is enabled or disabled on the device. A black check mark indicates that historical collection is enabled, a blue check mark indicates that threshold alarms collection (formerly monitor collection) is enabled.

Location
: The physical location of the device. You can set the location for one or more devices by selecting the devices in the table, right-clicking, and selecting Set Selected Location from the menu.

Contact
: The name of the responsible contact person. You can set the contact for one or more devices by selecting the devices in the table, right-clicking, and selecting Set Selected Contact from the menu.

System Name
: Hostname for the device taken from the **System Name** field on the **Device** tab of the **Configure Device** window. You can set the system name for a device by selecting the device in the table, right-clicking, and selecting **Device** > **Configure Device**.

Uptime
: The amount of time, in a days hh:mm:ss format, that the device has been running since the last start-up.

Nickname
: The user-defined nickname for the selected device.

Description
: A description of the unavailable device.

User Data 1-4, Notes
: These columns can provide additional information about the device.

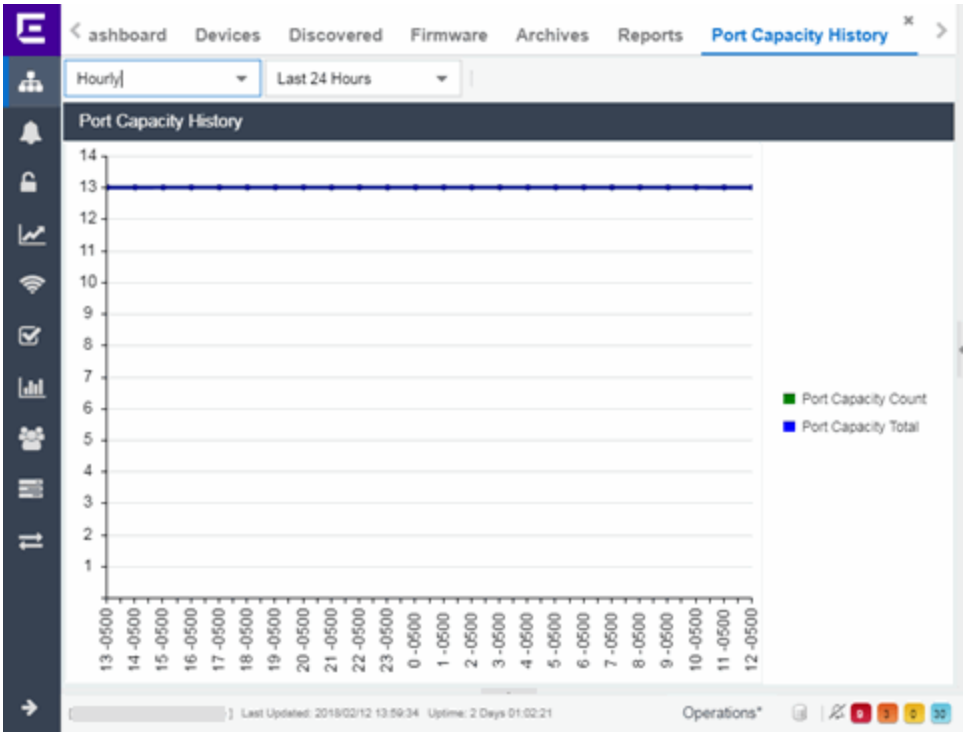
Asset Tag
: A unique asset number assigned to the module or component for inventory tracking purposes.

- Impact Analysis Dashboard Overview

Port Capacity History Report

The Port Capacity History report provides detailed information about the ports for which utilization statistics are above the threshold you configure (green) and the total number of ports (blue). A port is displayed in the report if the port is up and historical data collection has been enabled on the device long enough for statistic collection. The values here are the values displayed in the Port Capacity ring chart over the time span you define.

NOTE: Use the Port Capacity Chart section of the Impact Analysis options to configure the threshold ExtremeCloud IQ Site Engine uses to determine port utilization.



Select the increment between which ExtremeCloud IQ Site Engine analyzes ports from the data drop-down list. Available options are **Raw**, **Hourly**, or **Daily** data.

Select the time span for which the report displays from the time span drop-down list. Available options are **Last 24 Hours**, **Yesterday**, **Last 3 Days**, **Last Week**, **Last 2 Weeks**, **Last Month**.

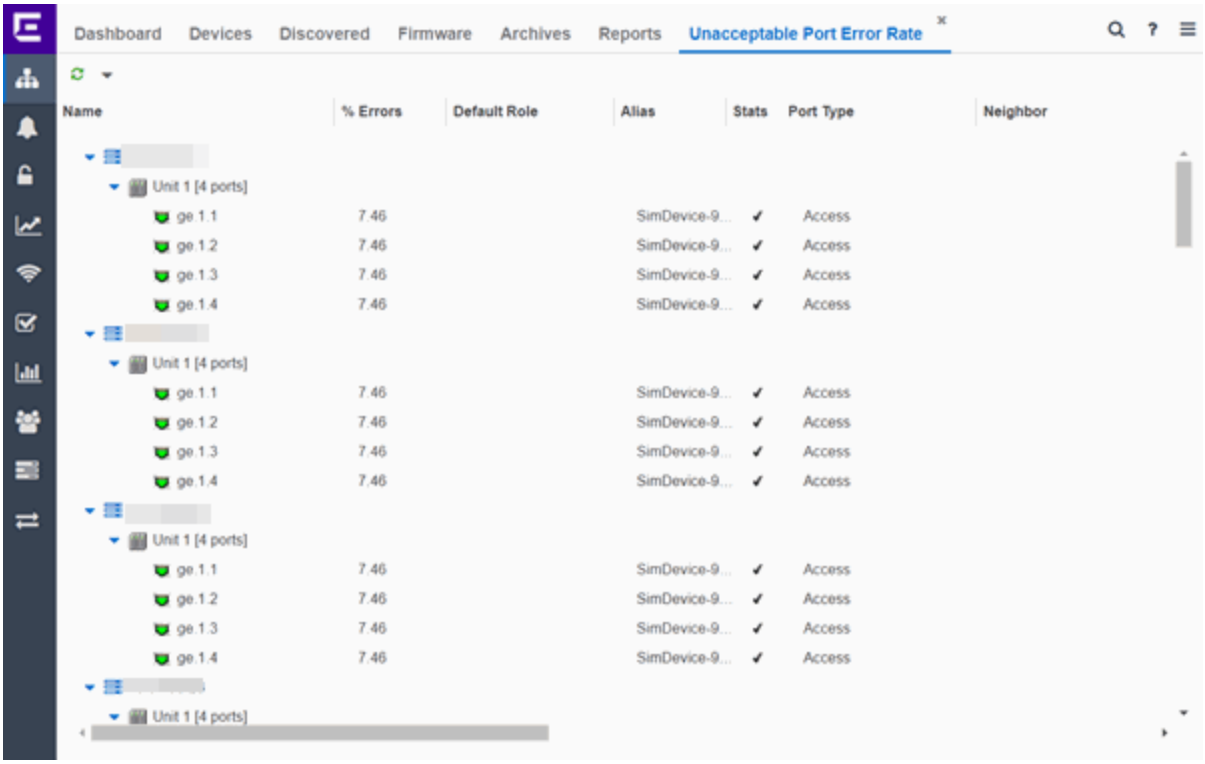
{img placeholder}

- Impact Analysis Dashboard Overview

High Error Ports Report

The High Error Ports report displays a list of ports for which error statistics are above the threshold you configure. A port is displayed in the report if the port is up and historical data collection has been enabled on the device long enough for statistic collection.

NOTE: Use the Port Health Chart section of the Impact Analysis options to configure the threshold ExtremeCloud IQ Site Engine uses to determine port error rates.



The following columns are included in the report:

Name
: The device or port interface name.

% Errors
: The percentage of errors (which is based on the Port Error Packets % statistic) as of the last report, in relation to the total number of ports indicated. The total errors indicated may include measurements of ifInDiscards, ifOutDiscards, IfInErrors, ifOutErrors, and ifInUnknownProtos. Other errors counters may be included if they are available on the device.

Default Role
: If the end user is unauthenticated, the port implements its default role. You can select to use

the current default role on the device or set a default role. If there is no default role specified, there is no role on the port.

Alias
: Shows the alias (ifAlias) for the interface, if one is assigned.

Stats
: Displays information about the port, if configured in PortView.

Port Type
: The type of port. Possible values include: Access, CDP, CDP FTM 1 Backplane, FTM 1 Backplane, and Logical.

Neighbor
: The port to which the port is connected.

Port Speed
: The speed of the port. Possible values include: 10/100, speed in megabits per second (for example, 800.0 Mbps), Unknown (displayed for logical ports).

PVID
: Displays the VLAN ID of the VLAN assigned to the port. When you assign a VLAN to a port, that VLAN's ID (VID) becomes the Port VLAN ID (PVID) for the port.

VLANs
: The VLANs to which the port is associated.

Description
: A description of the port and the device.

Port Type Details
: Additional information about the type of port.

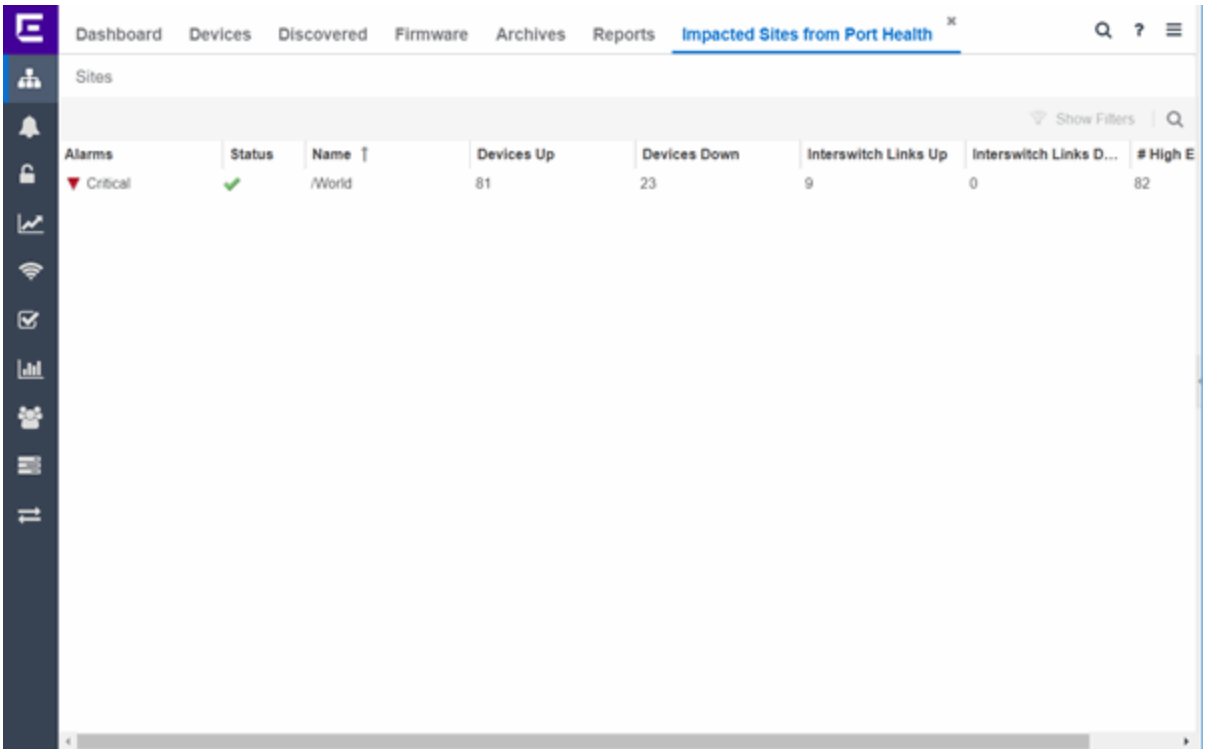
Serial Number
: The serial number of the device.

- Impact Analysis Dashboard Overview

Sites Impacted by High Error Ports Report

The Sites Impacted by High Error Ports report displays a list of devices with ports for which error statistics are above the threshold you configure. A port is displayed in the report if the port is up and historical data collection has been enabled on the device long enough for statistic collection.

NOTE: Use the Port Health Chart section of the Impact Analysis options to configure the threshold ExtremeCloud IQ Site Engine uses to determine port error rates.



The following columns are included in the report:

Alarms
: Shows the most severe alarm triggered by a device included in the site. The severity of the alarm is indicated by the following icons:

- Critical (▼) — A problem with significant implications.
- Error (▶) — A problem with limited implications.
- Warning (▲)— A condition that might lead to a problem.
- Info (■) — Information only; not a problem.
- None ( ) — No alarms on the device.

Status
: Indicates whether the site is up or down, based on the percentage of devices in the site with which ExtremeCloud IQ Site Engine can communicate (**Status** of **Up**). A green check mark indicates the site is up, while a red X icon indicates the site is down.

  Use the **Devices Up for Site Up (percent)** field on the **Impact Status Options** tab to configure the threshold ExtremeCloud IQ Site Engine uses to determine if a site is up. The threshold is calculated as the ratio of devices in a site with a **Status** of **Up** to the total number of devices in the site.

Name
: The name of the site.

Devices Up
: This column indicates the number of devices with a **Status** of **Up** in the site.

Devices Down
: This column indicates the number of devices with a **Status** of **Down** in the site.

Interswitch Links Up
: This column indicates the number of Interswitch Links with a **Status** of **Up** in the site.

Interswitch Links Down
: This column indicates the number of Interswitch Links with a **Status** of **Down** in the site.

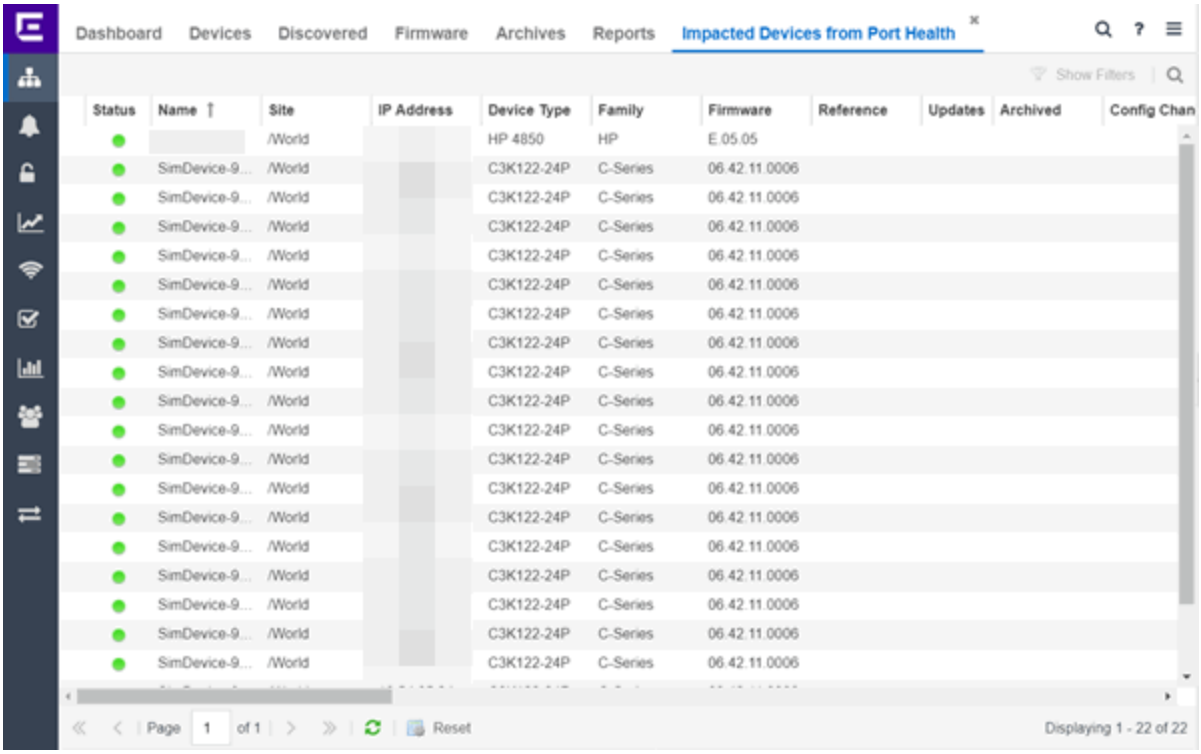
High Error Rate Ports
: The number of ports with tracking enabled in the site with an error rate above the value you configure as acceptable in the Port Health Chart section of the Impact Analysis options.

- Impact Analysis Dashboard Overview

Devices Impacted by High Error Ports Report

The Devices Impacted by High Error Ports report displays a list of devices with ports for which error statistics are above the threshold you configure.

NOTE: Use the Port Health Chart section of the Impact Analysis options to configure the threshold ExtremeCloud IQ Site Engine uses to determine port error rates.



The following columns are included in the report:

Device Status
: This column, hidden by default, indicates whether there is contact with the device. The color of the circle indicates the degree to which the device is communicating:

  - Green icon () — Indicates ExtremeCloud IQ Site Engine is in contact with the device.
  - Yellow icon () — Indicates ExtremeCloud IQ Site Engine has issues contacting the device.
  - Red icon () — Indicates ExtremeCloud IQ Site Engine can not contact the device.

  Hover over the Device Status icon to view additional details about the status for that device.

Status
: Indicates the device/alarm status for the device. The icon indicates the severity of the most severe alarm on the device:

  - Red icon () — A critical problem with significant implications.
  - Orange icon () — An error with limited implications.
  - Yellow icon () — A warning that might lead to a problem.
  - Blue icon () — Information only; not a problem.
  - Green icon () — ExtremeCloud IQ Site Engine can contact the device.

  Hover over the status icon to view the number of alarms. Select on the alarm/device status icon to open a new page with detailed information about the alarms for that device.

Device ID
: This column, hidden by default, displays a number that serves as a database identifier automatically created for the device. This number increments as you add additional devices.

Name
: The device name, nickname, or IP address.

Site
: The site in which the device is located.

Poll Type
: This column, hidden by default, indicates the poll type ExtremeCloud IQ Site Engine uses to discover devices: SNMP, Ping or Not Polled.

Poll Group Name
: This column, hidden by default, indicates the name of the Poll Group you define in the Poll Groups section of the Status Polling options.

Admin Profile
: This column, hidden by default, indicates the access Profile that gives ExtremeCloud IQ Site Engine administrative access to the device.

Client Profile
: This column, hidden by default, indicates the access Profile that gives ExtremeCloud IQ Site Engine client access to the device.

IP Address
: The device's IP address.

Context
: The Context column, hidden by default, displays a string that indicates how the device behaves, depending on whether the device is a router or a switch.

IP Context
: The IP Context column, hidden by default, displays a device's IP address with the context appended to the end of the address following a colon.

Trap Status
: Indicates whether a trap receiver is configured, not configured, or not supported for the device. This column is hidden by default.

Syslog Status
: Indicates whether the device is configured to send information to the syslog or if it is not supported for the device. This column is hidden by default.

Display Name
: The IP address of the device. This column is hidden by default.

Device Type
: The type of device.

Family
: The device product family.

Firmware
: The revision for the firmware running in the device.

Running Reference Firmware
: Indicates if the device is running reference firmware.

Updates
: The firmware release status for the device according to the results from the latest Check for Firmware Updates operation. Place your cursor on the column to see a tooltip describing the status.

Archived
: Indicates if the device has been archived in the last 30 days.

Config Changed
: Indicates if the archived configuration for the device has changed in the last 30 days.

Policy Domain
: The policy domain assigned to the device.

Boot PROM
: The revision for the BootPROM installed on the device.

Base MAC
: The base MAC address for the device.

Serial Number
: The serial number for the device.

Stats
: Displays whether statistics collection is enabled or disabled on the device. A black check mark indicates that historical collection is enabled, a blue check mark indicates that threshold alarms collection (formerly monitor collection) is enabled.

Location
: The physical location of the device. You can set the location for one or more devices by selecting the devices in the table, right-clicking, and selecting Set Selected Location from the menu.

Contact
: The name of the responsible contact person. You can set the contact for one or more devices by selecting the devices in the table, right-clicking, and selecting Set Selected Contact from the menu.

System Name
: Hostname for the device taken from the **System Name** field on the **Device** tab of the **Configure Device** window. You can set the system name for a device by selecting the device in the table, right-clicking, and selecting **Device** > **Configure Device**.

Uptime
: The amount of time, in a days hh:mm:ss format, that the device has been running since the last start-up.

Nickname
: The user-defined nickname for the selected device.

Description
: A description of the unavailable device.

User Data 1-4, Notes
: These columns can provide additional information about the device.

Asset Tag
: A unique asset number assigned to the module or component for inventory tracking purposes.

- Impact Analysis Dashboard Overview

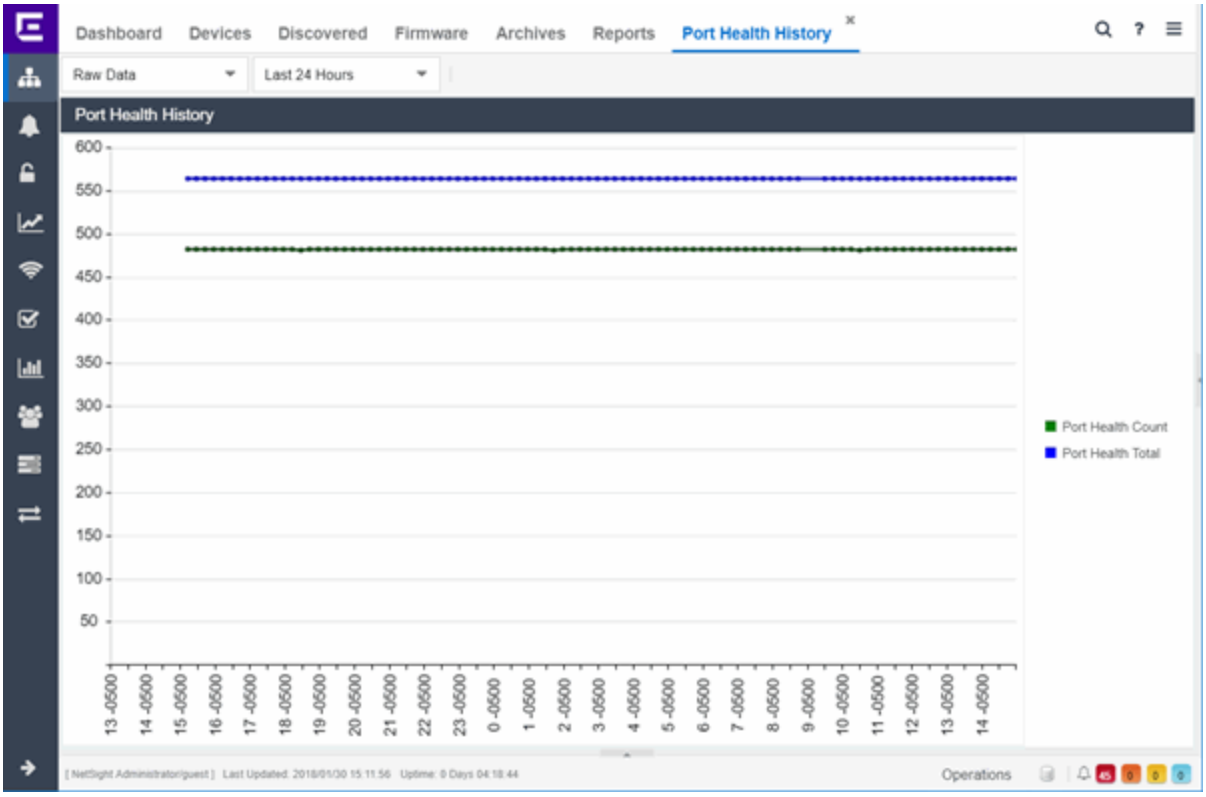
Port Health History Report

The Port Health History report provides detailed information about the ports for which error statistics are above the threshold you configure (green) and the total number of ports (blue). A port is displayed in the report if the port is up and historical data collection has been enabled on the device long enough for statistic collection. The values here are the values displayed in the Port Health ring chart over the time span you define.

NOTE: Use the Port Health Chart section of the Impact Analysis options to configure the threshold ExtremeCloud IQ Site Engine uses to determine port error rates.

Select the increment between which ExtremeCloud IQ Site Engine analyzes ports from the data drop-down list. Available options are **Raw**, **Hourly**, or **Daily** data.

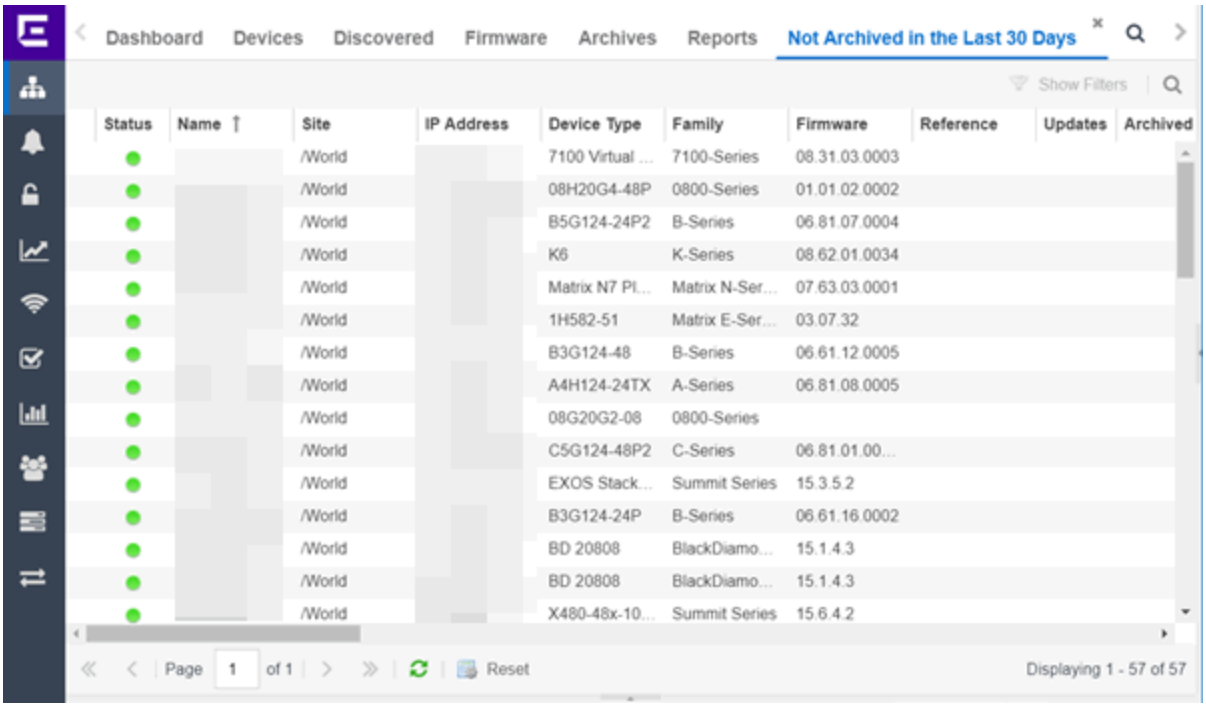
Select the time span for which the report displays from the time span drop-down list. Available options are **Last 24 Hours**, **Yesterday**, **Last 3 Days**, **Last Week**, **Last 2 Weeks**, **Last Month**.



- Impact Analysis Dashboard Overview

Unarchived Devices Report

The Unarchived Devices report displays a list of the devices not archived within the last 30 days and provides information about those devices. Devices listed in this report are capable of being archived; unarchivable devices are not included. You can create a new ExtremeCloud IQ Site Engine archive by right-clicking a device and selecting **More Actions** > **Backup Configuration**.



The following information is included in the report:

Device Status

This column, hidden by default, indicates whether there is contact with the device. The color of the circle indicates the degree to which the device is communicating:

- Green icon (●) — Indicates ExtremeCloud IQ Site Engine is in contact with the device.
- Yellow icon (●) — Indicates ExtremeCloud IQ Site Engine has issues contacting the device.
- Red icon (●) — Indicates ExtremeCloud IQ Site Engine can not contact the device.

Hover over the Device Status icon to view additional details about the status for that device.

Status

Indicates the device/alarm status for the device. The icon indicates the severity of the most severe alarm on the device:

- Red icon () — A critical problem with significant implications.
- Orange icon () — An error with limited implications.
- Yellow icon () — A warning that might lead to a problem.
- Blue icon () — Information only; not a problem.
- Green icon () — ExtremeCloud IQ Site Engine can contact the device.

Hover over the status icon to view the number of alarms. Select the alarm/device status icon to open a new page with detailed information about the alarms for that device.

Device ID
: This column, hidden by default, displays a number that serves as a database identifier automatically created for the device. This number increments as you add additional devices.

Name
: The device name, nickname, or IP address.

Site
: The site in which the device is located.

Poll Type
: This column, hidden by default, indicates the poll type ExtremeCloud IQ Site Engine uses to discover devices: SNMP, Ping or Not Polled.

Poll Group Name
: This column, hidden by default, indicates the name of the Poll Group you define in the Poll Groups section of the Status Polling options.

Admin Profile
: This column, hidden by default, indicates the access Profile that gives ExtremeCloud IQ Site Engine administrative access to the device.

Client Profile
: This column, hidden by default, indicates the access Profile that gives ExtremeCloud IQ Site Engine client access to the device.

IP Address
: The device's IP address.

Context:
: The Context column, hidden by default, displays a string that indicates how the device behaves, depending on whether the device is a router or a switch.

IP Context
: The IP Context column, hidden by default, displays a device's IP address with the context appended to the end of the address following a colon.

Trap Status
: Indicates whether a trap receiver is configured, not configured, or not supported for the device. This column is hidden by default.

Syslog Status
: Indicates whether the device is configured to send information to the syslog or if it is not supported for the device. This column is hidden by default.

Display Name
: The IP address of the device. This column is hidden by default.

Device Type
: The type of device.

Family
: The device product family.

Firmware
: The revision for the firmware running in the device.

Running Reference Firmware
: Indicates if the device's thresholds have been configured for Reference Firmware

Updates
: The firmware release status for the device according to the results from the latest Check for Firmware Updates operation. Place your cursor on the column to see a tooltip describing the status.

Archived
: Indicates if the device has been archived in the last 30 days.

Config Changed
: Indicates if the archived configuration for the device has changed in the last 30 days.

Policy Domain
: The policy domain assigned to the device.

Boot PROM
: The revision for the BootPROM installed on the device.

Base MAC
: The base MAC address for the device.

Serial Number
: The serial number for the device.

Stats
: Displays whether statistics collection is enabled or disabled on the device. A black check mark indicates that historical collection is enabled, a blue check mark indicates that threshold alarms collection (formerly monitor collection) is enabled.

Location
: The physical location of the device. You can set the location for one or more devices by selecting the devices in the table, right-clicking, and selecting Set Selected Location from the menu.

Contact
: The name of the responsible contact person. You can set the contact for one or more devices by selecting the devices in the table, right-clicking, and selecting Set Selected Contact from the menu.

System Name
: Hostname for the device taken from the **System Name** field on the **Device** tab of the **Configure Device** window. You can set the system name for a device by selecting the device in the table, right-clicking, and selecting **Device** > **Configure Device**.

Uptime
: The amount of time, in a days hh:mm:ss format, that the device has been running since the last start-up.

Nickname
: The user-defined nickname for the selected device.

Description
: A description of the unavailable device.

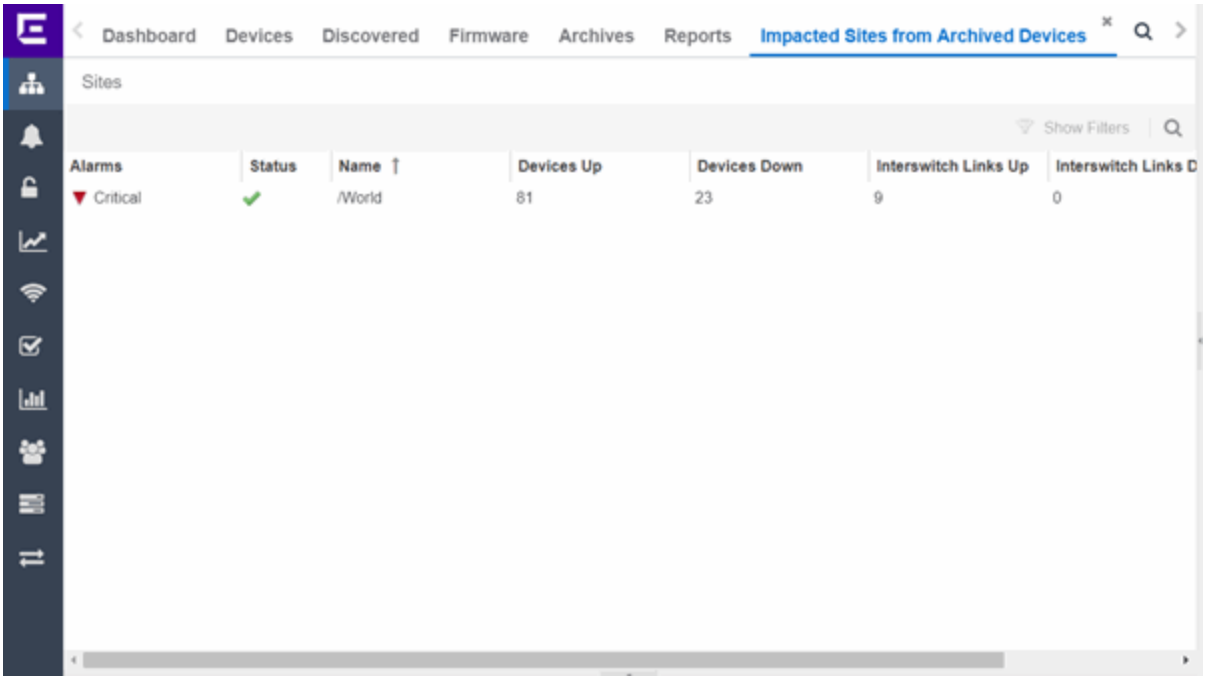
User Data 1-4, Notes
: These columns can provide additional information about the device.

Asset Tag
: A unique asset number assigned to the module or component for inventory tracking purposes.

- Impact Analysis Dashboard Overview

Sites Impacted by Unarchived Devices Report

The Sites Impacted by Unarchived Devices report provides detailed information about sites containing devices not archived in the past 30 days.



The following columns are included in the report:

Alarms
: Shows the most severe alarm triggered by a device included in the site. The severity of the alarm is indicated by the following icons:

  - Critical (▼) — A problem with significant implications.
  - Error (▶) — A problem with limited implications.
  - Warning (▲)— A condition that might lead to a problem.
  - Info (■) — Information only; not a problem.
  - None ( ) — No alarms on the device.

Status
: Indicates whether the site is up or down, based on the percentage of devices in the site with which ExtremeCloud IQ Site Engine can communicate (**Status** of **Up**). A green check mark indicates the site is up, while a red X icon indicates the site is down.

  Use the **Devices Up for Site Up (percent)** field on the to configure the threshold ExtremeCloud IQ Site Engine uses to determine if a site is up. The threshold is calculated as the ratio of devices in a site with a **Status** of **Up** to the total number of devices in the site.

Name
: The name of the site.

Devices Up
: This column indicates the number of devices with a **Status** of **Up** in the site.

Devices Down
: This column indicates the number of devices with a **Status** of **Down** in the site.

Interswitch Links Up
: This column indicates the number of Interswitch Links with a **Status** of **Up** in the site.

Interswitch Links Down
: This column indicates the number of Interswitch Links with a **Status** of **Down** in the site.

Unarchived Devices
: The number of devices not archived in the last 30 days in the site.

- Impact Analysis Dashboard Overview

Archived Devices History Report

The Archived Devices History report contains a graph that displays the number of devices archived within the last 30 days (green) and the total number of devices that can be archived (blue) for the duration you define. If no devices have been archived in the last 30 days, the chart may not display data (green). The values here are the values displayed in the Archived Devices ring chart over the time span you define.

Select the increment between which ExtremeCloud IQ Site Engine analyzes device archives from the data drop-down list. Available options are **Raw**, **Hourly**, or **Daily** data.

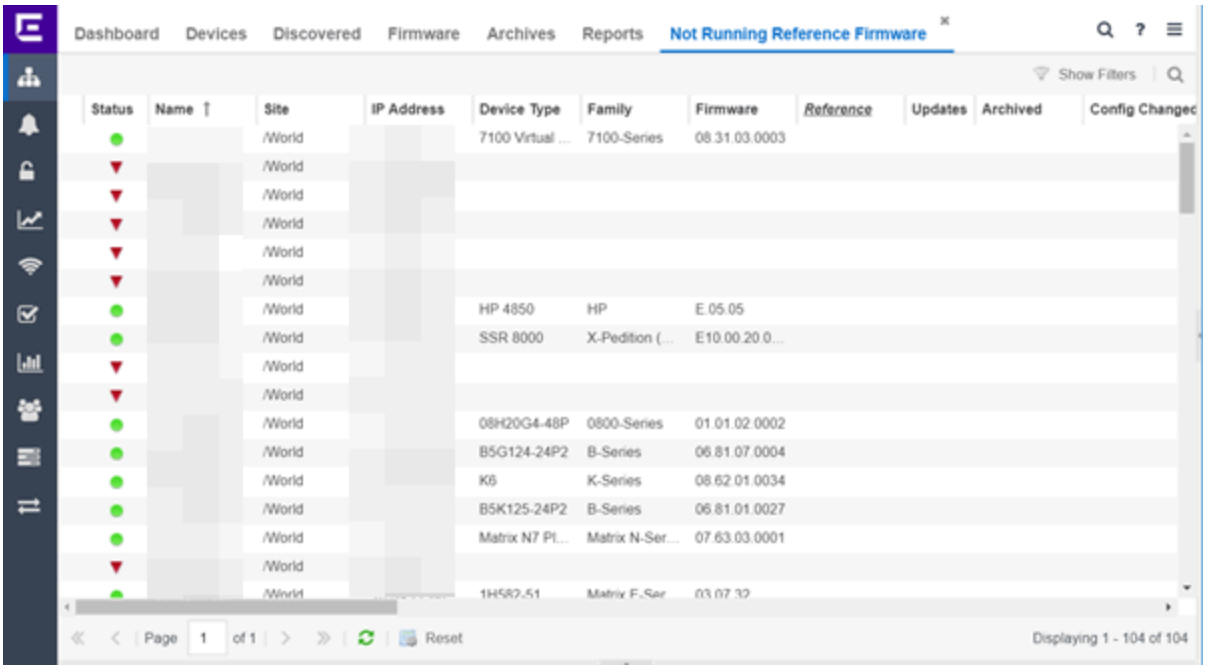
Select the time span for which the report displays from the time span drop-down list. Available options are **Last 24 Hours**, **Yesterday**, **Last 3 Days**, **Last Week**, **Last 2 Weeks**, **Last Month**.



- Impact Analysis Dashboard Overview

Devices Without Reference Firmware Report

The Devices Without Reference Firmware report provides detailed information about devices not running reference firmware.



The following columns are included in the report:

Device Status

This column, hidden by default, indicates whether there is contact with the device. The color of the circle indicates the degree to which the device is communicating:

- Green icon (●) — Indicates ExtremeCloud IQ Site Engine is in contact with the device.
- Yellow icon (●) — Indicates ExtremeCloud IQ Site Engine has issues contacting the device.
- Red icon (●) — Indicates ExtremeCloud IQ Site Engine can not contact the device.

Hover over the Device Status icon to view additional details about the status for that device.

Status

Indicates the device/alarm status for the device. The icon indicates the severity of the most severe alarm on the device:

- Red icon (▼) — A critical problem with significant implications.
- Orange icon (▶) — An error with limited implications.
- Yellow icon (▲) — A warning that might lead to a problem.
- Blue icon (■) — Information only; not a problem.
- Green icon (●) — ExtremeCloud IQ Site Engine can contact the device.

Hover over the status icon to view the number of alarms. Select the alarm/device status icon to open a new page with detailed information about the alarms for that device.

Device ID
: This column, hidden by default, displays a number that serves as a database identifier automatically created for the device. This number increments as you add additional devices.

Name
: The device name, nickname, or IP address.

Site
: The site in which the device is located.

Poll Type
: This column, hidden by default, indicates the poll type ExtremeCloud IQ Site Engine uses to discover devices: SNMP, Ping or Not Polled.

Poll Group Name
: This column, hidden by default, indicates the name of the Poll Group you define in the Poll Groups section of the Status Polling options.

Admin Profile
: This column, hidden by default, indicates the access Profile that gives ExtremeCloud IQ Site Engine administrative access to the device.

Client Profile
: This column, hidden by default, indicates the access Profile that gives ExtremeCloud IQ Site Engine client access to the device.

IP Address
: The device's IP address.

Context
: The Context column, hidden by default, displays a string that indicates how the device behaves, depending on whether the device is a router or a switch.

IP Context
: The IP Context column, hidden by default, displays a device's IP address with the context appended to the end of the address following a colon.

Trap Status
: Indicates whether a trap receiver is configured, not configured, or not supported for the device. This column is hidden by default.

Syslog Status
: Indicates whether the device is configured to send information to the syslog or if it is not supported for the device. This column is hidden by default.

Display Name
: The IP address of the device. This column is hidden by default.

Device Type
: The type of device.

Family
: The device product family.

Firmware
: The revision for the firmware running in the device.

Running Reference Firmware
: Indicates if the device's thresholds have been configured for Reference Firmware.

Updates
: The firmware release status for the device according to the results from the latest Check for Firmware Updates operation. Place your cursor on the column to see a tooltip describing the status.

Archived
: Indicates if the device has been archived in the last 30 days.

Config Changed
: Indicates if the archived configuration for the device has changed in the last 30 days.

Policy Domain
: The policy domain assigned to the device.

Boot PROM
: The revision for the BootPROM installed on the device.

Base MAC
: The base MAC address for the device.

Serial Number
: The serial number for the device.

Stats
: Displays whether statistics collection is enabled or disabled on the device. A black check mark indicates that historical collection is enabled, a blue check mark indicates that threshold alarms collection (formerly monitor collection) is enabled.

Location
: The physical location of the device. You can set the location for one or more devices by selecting the devices in the table, right-clicking, and selecting Set Selected Location from the menu.

Contact
: The name of the responsible contact person. You can set the contact for one or more devices by selecting the devices in the table, right-clicking, and selecting Set Selected Contact from the menu.

System Name
: Hostname for the device taken from the **System Name** field on the **Device** tab of the

Configure Device window. You can set the system name for a device by selecting the device in the table, right-clicking, and selecting **Device** > **Configure Device**.

Uptime
: The amount of time, in a days hh:mm:ss format, the device has been running since the last start-up.

Nickname
: The user-defined nickname for the selected device.

Description
: A description of the unavailable device.

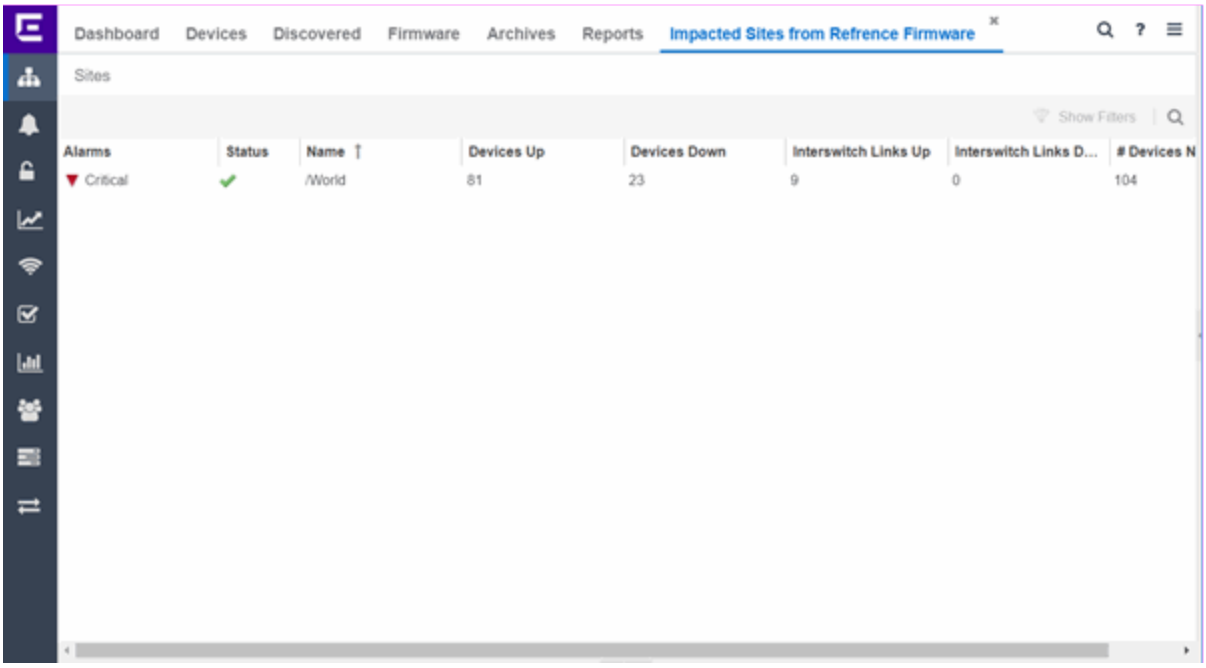
User Data 1-4, Notes
: These columns can provide additional information about the device.

Asset Tag
: A unique asset number assigned to the module or component for inventory tracking purposes.

- Impact Analysis Dashboard Overview

Sites Impacted by Devices Without Reference Firmware Report

This report provides a list of sites with devices not running reference firmware.



The following columns are included in the report:

Alarms
: Shows the most severe alarm triggered by a device included in the site. The severity of the alarm is indicated by the following icons:

  - Critical (▼) — A problem with significant implications.
  - Error (▶) — A problem with limited implications.
  - Warning (▲)— A condition that might lead to a problem.
  - Info (■) — Information only; not a problem.
  - None ( ) — No alarms on the device.

Status
: Indicates whether the site is up or down, based on the percentage of devices in the site with which ExtremeCloud IQ Site Engine can communicate (**Status** of **Up**). A green check mark indicates the site is up, while a red X icon indicates the site is down.

  Use the **Devices Up for Site Up (percent)** field on the **Impact Status Options** tab to configure the threshold ExtremeCloud IQ Site Engine uses to determine if a site is up. The threshold is calculated as the ratio of devices in a site with a **Status** of **Up** to the total number of devices in the site.

Name
: The name of the site.

Devices Up
: This column indicates the number of devices with a **Status** of **Up** in the site.

Devices Down
: This column indicates the number of devices with a **Status** of **Down** in the site.

Interswitch Links Up
: This column indicates the number of Interswitch Links with a **Status** of **Up** in the site.

Interswitch Links Down
: This column indicates the number of Interswitch Links with a **Status** of **Down** in the site.

Devices Not Running Reference Firmware
: The number of devices not running reference firmware in the site.

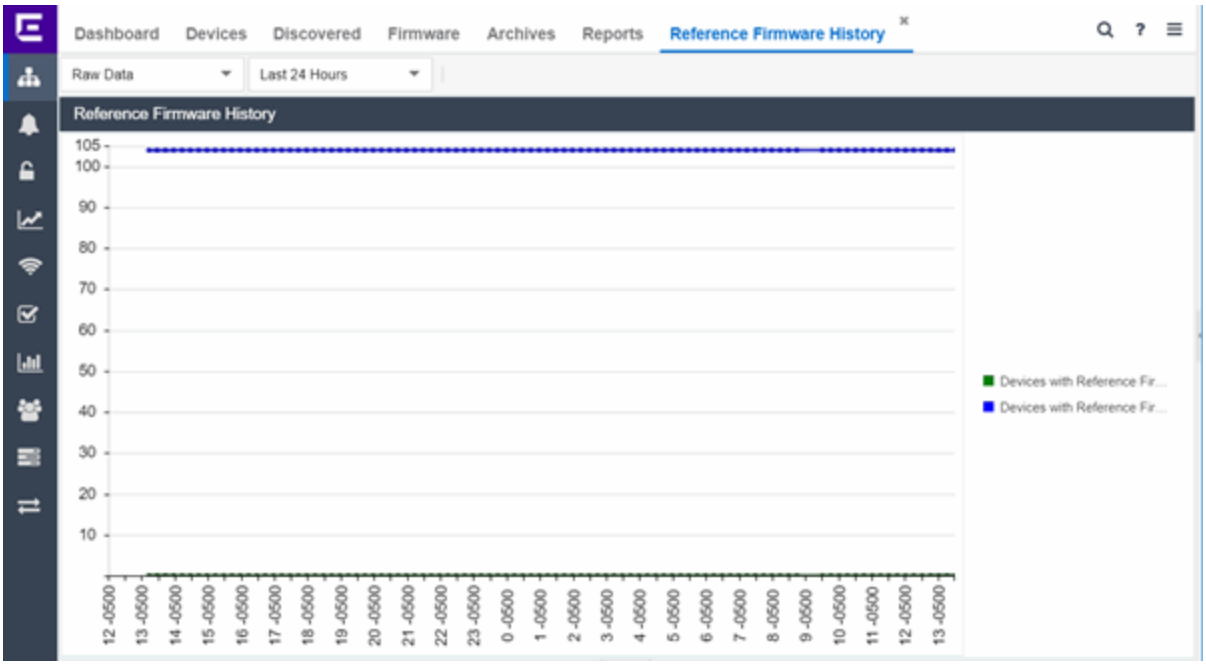
- Impact Analysis Dashboard Overview

Reference Firmware History Report

The Reference Firmware History Report displays the number of devices running reference firmware (green) and the total number of devices (blue) for the duration you define. If no devices are running reference firmware, the chart may not display data (green). The values here are the values displayed in the Devices with Reference Firmware ring chart over the time span you define.

Select the increment between which ExtremeCloud IQ Site Engine analyzes devices from the data drop-down list. Available options are **Raw**, **Hourly**, or **Daily** data.

Select the time span for which the report displays from the time span drop-down list. Available options are **Last 24 Hours**, **Yesterday**, **Last 3 Days**, **Last Week**, **Last 2 Weeks**, **Last Month**.



- Impact Analysis Dashboard Overview

Device Operations

This Help topic provides information on the following operations available from the **Network** > **Devices** tab:

Buttons

- Add Device
- Check for Firmware Updates
- Export to CSV

Menu Options

- Device View
- Terminal
- WebView
- FlexViews

- More Views
    - Port Tree
    - Interfaces
    - User Sessions
    - Fabric L2VSNs
    - SDWAN Appliance360
- Configure
- Compass Search
- Rediscover
- Clear Alarms
- Upgrade Firmware
- Add to Device Group
- More Actions
    - Restart Device
    - Set Device Profile
    - Set/Clear Frozen Ports
    - Import to Site
    - Import to Service Definition
    - View Available Firmware Releases
    - Run Site's Add Actions
    - Contact Device Using Group's Profile
    - Ping Device (ICMP)
    - Authentication Configuration
    - RADIUS Configuration
        - RADIUS Authentication
        - RADIUS Accounting
    - Delete Device
    - Overwrite Local Changes
    - Register Trap Receiver
    - Unregister Trap Receiver
    - Register SysLog Receiver
    - Unregister SysLog Receiver

    - Collect Device Statistics
    - Export Serial Numbers
    - Change Management Status
- Archives
    - Backup Configuration
    - Restore Configuration
    - Compare Last Configurations
    - Inventory Settings
- Tasks
    - CLI Commands
- Device Groups
- Maps
    - Add to Map
    - Create Map
    - Create Map for Locations
    - Search Maps
- Network
- Policy
- Fabric
- Working in the Devices Table
    - Table Column Definitions
    - Filtering
- Buttons, Search Field, and Paging Toolbar
- Local Settings

To view the **Devices** sub-tab on the **Network** tab, you must be a member of an authorization group assigned the OneView > Access OneView and the OneView > Events and Alarms > OneView Event Log Access capabilities.

Add Device

To add a new device to the Devices list, select the **Add Device** icon at the top of the tab. The Add Device window appears. Enter the information in the window and select **OK**.

AFter the device is added to the Devices list, it can be used in ExtremeCloud IQ Site Engine.

Check for Firmware Updates

To check for available firmware updates for the devices included in the Devices list, select the **Check for Firmware Updates** icon at the top of the Devices tab. Enter your ExtremeNetworks.com credentials to view available firmware updates.

To update the credentials used to access ExtremeNetworks.com, open the Administration > Options > ExtremeNetworks.com Updates tab and edit the values in the Update Credentials section.

Export to CSV

To export information from the Devices list, select the **Export to CSV** icon at the top of the tab. The **Devices** tab provides two methods of exporting the data in the table:

Export all rows
: Select to export all of the data in the table to a .CSV file. The exported data displays with any sorting, filtering, and searching applied.

Export selected rows
: Select to export the data in the currently selected row(s) in the table to a .CSV file. The exported data includes all columns in the table (including those not currently displayed).

Menu Options

Device View

Select the **Menu** icon (☰) or right-click in the Devices list to opens a Device View for the device in a separate tab.

Terminal

To open a terminal session to a device, select the **Menu** icon (☰) or right-click in the Devices list and select **Terminal**. The Extreme WebShell window opens a terminal session for the selected device.

You can copy and paste information to and from the terminal window. Additionally, you can also enable logging for device terminal sessions. To enable logging, access the **Administration** > **Diagnostics** tab and expand **Server** in the left-panel. Select **Server Diagnostics** and select the appropriate **Diagnostic Level** in the drop-down list for Extreme WebShell.

WebView

You can use the **Network** tab to access WebView web-based management, which lets you configure and manage certain Extreme Networks and Enterasys devices.

To open WebView, select a device in the Device list, select the **Menu** icon (☰) or right-click in the Devices list to select **WebView** from the menu.

The web-based management opens in a new browser window. If your authorization group has been assigned the capability for Suite > Device Local Management WebView, you can take advantage of the auto login feature for web local management of ExtremeControlengines and wireless controllers.

WebView is only available with certain Extreme Networks and Enterasys devices.

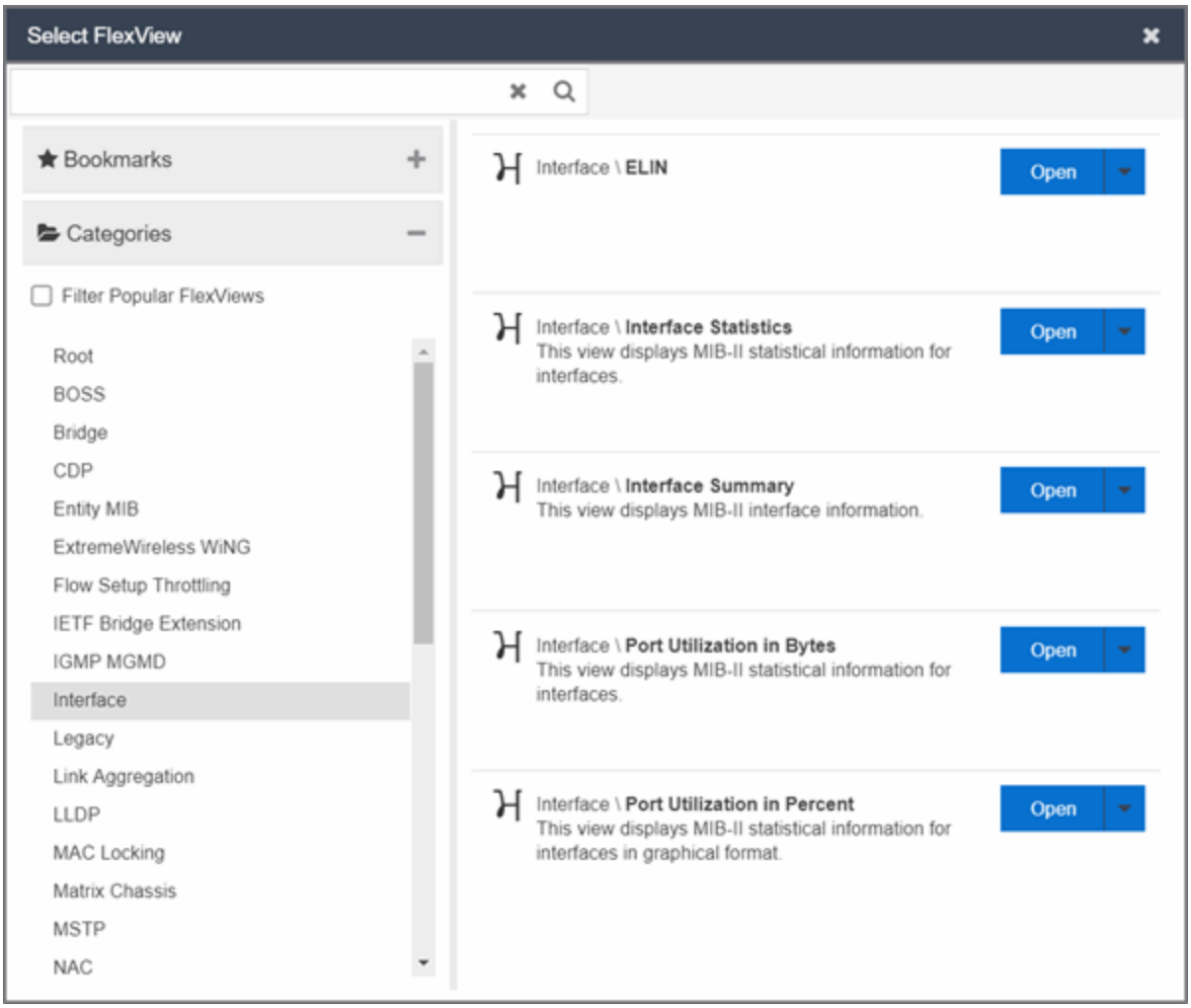
FlexViews

You can use the **Network** tab to access web-based FlexViews that provide a convenient way for Operations people to view FlexView data.

To launch a FlexView, you must be a member of an authorization group that has been assigned the OneView > FlexView > OneView FlexView Read Access capability. To launch and edit a web-based FlexView, you must be a member of an authorization group that has been assigned the OneView > FlexView > OneView FlexView Read/Write Access capability.

To launch a FlexView, select a device in the Device list, select the **Menu** icon (☰) or right-click in the Devices list and select **FlexView** from the menu. You can also right-click on a device and select **FlexView** from the menu.

The **Select FlexView** window opens.



Select a FlexView category from the left-panel and select the Open drop-down list. Select whether you want to open the FlexView in a new tab or window. The **Select FlexView** window displays only those FlexViews applicable to the device type selected.

For additional information about launching and using FlexViews from the **Network** tab, see Web-Based FlexViews.

More Views

Port Tree

The Port Tree displays interface information for a device.

To open the Port Tree:

1. Select a device in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.

3. Select **More Views** > **Port Tree.** The Port Tree opens in a new tab.
4. Expand the components to see the device's interfaces. Right-click on an interface to:
    - access PortView for that interface
    - view interface history including interface utilization, availability, and bandwidth/packets/flows statistics (Flow stats display only for S/K series and PF-FC-180 devices)
    - run scripts on the selected port
    - enable interface statistic collection
    - create policy profiles, called roles, that are assigned to the ports in your network.

In the Port Tree table, the Stats column displays whether statistics collection is enabled or disabled on the port. A black check indicates that historical collection is enabled, and a blue check indicates that threshold alarms collection (formerly monitor collection) is enabled. The Neighbor column displays neighbor details from CDP/EDP/LLDP. Hover your mouse over the column to see the protocol type.

Interfaces

Selecting **Interfaces** opens the Interface Summary, from which you can right-click on an interface to access PortView, view interface history, view current alarms and alarm history, enable interface statistic collection, and edit certain values for an interface.

To open the Interface Summary:

1. Select a device in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Views** > **Interfaces**.

    An Interface Summary FlexView opens for the device in a new tab.

User Sessions

Select User Sessions to view user sessions associated with the selected device.

To launch the user session, you must be a member of an authorization group that has been assigned the OneView > User Session > OneView User Session Read Access capability. To launch and edit a User Session , you must be a member of an authorization group that has been assigned the OneView > User Session > OneView User Session Read/Write Access capability.

To open a user session for a device:

1. Select a device in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Views** > **User Session**.

In the User Sessions window, you can view all users accessing the device selected.

For additional information about the User Sessions window, see User Sessions.

Fabric L2VSNs

Selecting **Fabric L2VSNs** opens the I-SID L2VSN and I-SID L2VSN interfaces with details about Fabric Connect L2 Services known to the device.

To open the Fabric L2VSNs:

1. Select a device in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Views** > **Fabric L2VSNs**.

   An Interface Fabric L2VSNs opens for the device in a new tab.

SDWAN Appliance360

Selecting **SDWAN Appliance360** opens the SDWAN Appliance360 in ExtremeCloud application. Additional authentication is required for the first time. This option is available only if there is an Extreme Networks SDWAN appliance connected to the selected Fabric Engine device.

To open the SDWAN Appliance360:

1. Select the Fabric Engine device with the Extreme SDWAN appliance connected in the device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Views** > **SDWAN Appliance360**.
4. If there are multiple Extreme SDWAN appliances connected, select the SDWAN appliance you want to manage.

   An SDWAN Appliance360 opens in a new tab.

Configure

To configure device information for an existing device:

1. Select the **Menu** icon (☰) or right-click in the Devices list.
2. Select **Configure**.

   The Configure Device window opens, which allows you to configure the device properties.

Compass Search

To open the Search window with Search with Compass selected for the selected devices:

1. Select the **Menu** icon (☰) or right-click in the Devices list.
2. Select **Device** > **Compass Search**.

   The **Search** window opens displaying the devices you selected with **Search with Compass** selected. Selecting a device group or site opens the **Search** window opens displaying the devices in the device group or site you selected with **Search with Compass** selected.

Rediscover

To refresh a device or multiple devices to update the information presented on the **Devices** tab:

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Rediscover Device**.

ExtremeCloud IQ Site Engine rediscovers the device and information about the device is refreshed.

Clear Alarms

To clear the alarms for a device or multiple devices in the Devices list:

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Clear Alarms**.

   A dialog box appears.
4. Select **Yes**.

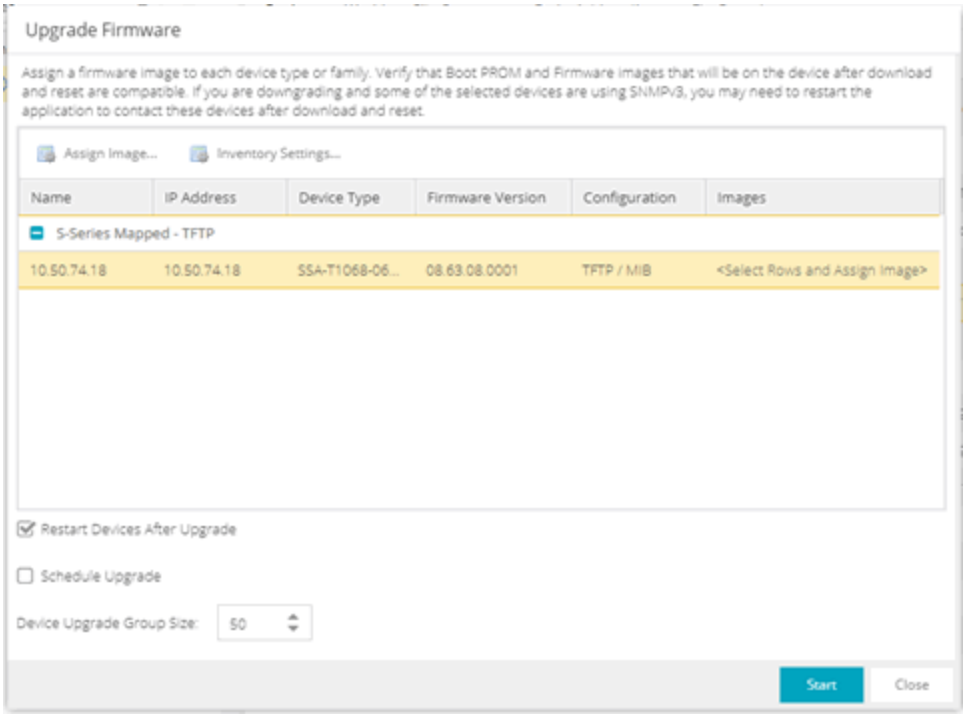
   The alarms on the selected devices clear.

Upgrade Firmware

To update devices in the ExtremeCloud IQ Site Engine database with the latest firmware releases:

1. Select the device or devices in the Devices list
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Upgrade Firmware**.

The results display in the Upgrade Firmware window with displaying information about the device and the available firmware versions. For additional information about upgrading device firmware, see How to Upgrade Firmware. Restart devices when the firmware is upgraded via the Restart Devices window by selecting **More Actions** > **Restart Device**.



Add to Device Group

The Add to Device Group menu option enables you to add devices or ports to a device group.

To add a device or multiple devices to a device group:

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Add to Device Group**.

   The Select Destination Group window displays, which allows you to select the device group to which the device or devices are added.
4. Select **OK** to add the devices to the group.

To add a port or multiple ports to a device group:

1. Select the port or port in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Add to Device Group**.

The Select Destination Group window displays, which allows you to select the device group to which the port or ports are added.

4. Select **OK** to add the ports to the group.

More Actions

Restart Device

To restart a device:

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Restart Device**.

   The Restart Devices window opens.
4. Select Start.

The devices are restarted.

Set Device Group's Profile

To change the profile settings for a device or multiple devices from the Devices list:

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Set Device Group's Profile**.

   The Set Device Group's Profile window appears.
4. Select a profile from the drop-down list to change the profile for the selected device or devices.
5. Select **OK**.

   A message appears confirming the device profile change.

NOTE: The access profile is changed for the user's group. To verify, check the Device Mapping.

Set/Clear Frozen Ports

To set or clear frozen ports on a device or multiple devices in the Devices list:

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions Set/Clear Frozen Ports**.
4. Select whether you want to freeze all ports, freeze the interswitch ports, or clear all frozen ports.
5. Select **Yes**. All ports are frozen, the interswitch ports are frozen, or all frozen ports are cleared, depending on what you select.

Import to Site

To import VLAN data from a device and save it to the site with which it is associated:

1. Select the device in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Import to Site**.
4. Select the **Overwrite VLAN Data** checkbox to remove all VLAN data from the site and copy the VLAN data from the device to the site.
   When this checkbox is not selected, the VLAN data from the device is added to the existing VLAN data on the device and only matching VLAN data is overwritten.
5. Select **Import** to import the VLAN data.

Import to Service Definition

To import data from a device and save it to a service definition:

1. Select the device in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Import to Service Definition**.

View Available Firmware Releases

To view all firmware releases available for a device:

1. Select the device in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **View Available Firmware Releases**.

Run Site's Add Actions

Select **Run Site's Add Actions** to run the actions configured for the site in which the device is contained:

1. Select the device in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Run Site's Add Actions**.

Contact Device Using Group's Profile

Select **Contact Device Using Group's Profile** to attempt to contact the selected devices via SNMP using the **Administration Profile** for a device, or the device's override profile configured on the Administration > Profiles > Device Mapping subtab.

1. Select the device in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Contact Device Using Group's Profile**.

Ping Device (ICMP)

Select Ping Device (ICMP) to determine if a device is having connectivity issues.

1. Select the device in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Ping Device (ICMP).**

> **NOTE:** After a request is sent, ExtremeCloud IQ Site Engine waits the specified amount of time configured on the Administration > Options > Status Polling tab to determine if the device is reachable or not reachable.

4. If contact with the device is successful, the message "Device with IP XX.XX.XX.XX is reachable" displays.
5. If contact with the device is not successful, the message "Device with IP XX.XX.XX.XX is not reachable" displays.

Authentication Configuration

Select Authentication Configuration to open the Authentication Configuration wizard, which allows you to configure the authentication used on a device or on the individual ports of a device.

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Authentication Configuration**.

RADIUS Configuration

RADIUS Authentication

Opens the **RADIUS Authentication** tab, which allows you to configure the RADIUS authorization servers and client settings used on a device.

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **RADIUS Authentication**.

RADIUS Accounting

Opens the **RADIUS Accounting** tab, which allows you to configure the RADIUS accounting servers and client settings used on a device.

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **RADIUS Accounting**.

Delete Device

To delete a device or multiple devices from the Devices list:

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Delete Device**. A Delete Confirmation window opens.
4. Select **Yes** to remove the device from ExtremeCloud IQ and any databases, maps, and ZTP+ configurations to which the device is added.

Overwrite Local Changes

Use this feature to modify the configuration of a device to replace any manual changes that were made directly (via the CLI) to the device with the values from the Device, VLAN and ports tabs of ExtremeCloud IQ Site Engine.

IMPORTANT: Local configuration changes that you make on ZTP+ managed switches may not be saved into the ExtremeCloud IQ Site Engine database. Any changes made locally that you can configure using ZTP+ will be removed the next time ExtremeCloud IQ Site Engine polls the ZTP+ device.

To alert you when ExtremeCloud IQ Site Engine detects that a ZTP+ managed device has Device, VLAN, or Port settings that are different from the configuration in ExtremeCloud IQ Site Engine, you can use the Alarm on Local Change option.

To overwrite local changes made to the device via the CLI and save the site configuration on a device or devices:

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Overwrite Local Changes**.

Register Trap Receiver

To receive trap information from the devices on your network, Select the **Menu** icon (☰) or right-click in the Devices list and select **More Actions** > **Register Trap Receiver** from the menu. Additionally, devices added to sites for which **Add Trap Receiver** is selected on the **Discovered Device Actions** tab automatically receive trap information. You can define the trap configuration details on the **Options** > **Trap** tab. Depending on the device, ExtremeCloud IQ Site Engine creates the trap configuration via SNMP or a script.

Unregister Trap Receiver

To stop receiving trap information from the devices on your network, Select the **Menu** icon (☰) or right-click in the Devices list and select **More Actions** > **Unregister Trap Receiver** from the menu.

Register SysLog Receiver

To receive syslog information from the devices on your network, select the **Menu** icon (☰) or right-click in the Devices list and select **More Actions** > **Register SysLog Receiver** from the menu. Additionally, devices added to sites for which **Add Syslog Receiver** is selected on the **Discovered Device Actions** tab automatically receive syslog information. You can define the syslog configuration details on the **Options** > **Syslog** tab. Depending on the device, ExtremeCloud IQ Site Engine creates the syslog configuration via SNMP or a script.

Unregister SysLog Receiver

To stop receiving syslog information from the devices on your network, select the **Menu** icon (☰) or right-click in the Devices list and select **More Actions** > **Unregister SysLog Receiver** from the menu.

Collect Device Statistics

The **Devices** tab provides the ability to start and stop device statistics collections for Extreme Networks and Enterasys devices, which allows the collection of data used in reports.

To collect device statistics:

1. Select one or more devices or wireless controllers in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Collect Device Statistics**.

   A window opens from which you can select your statistics collection criteria.

   - In **Historical mode**, device statistics are saved to the database and aggregated over time, for use in reports. The device statistics are also used for threshold alarms configured in the Console Alarms Manager. In the Active Threshold Alarm Summary box, you can see all active threshold alarms configured in the Console Alarms Manager that use these statistics.

     NOTE: Enabling Historical Device Statistics Collection may use substantial disk space.

   - In **Threshold Alarms (formerly Monitor) mode**, device statistics are saved for one hour and then dropped. You can use these statistics for threshold alarms, but not for ExtremeCloud IQ Site Engine reporting. In the Active Threshold Alarm Summary box, you can see all active threshold alarms configured in the **Alarms and Events** tab that use these statistics. (Note that you do not see the Threshold Alarms mode option if you have disabled threshold alarms collection in the OneView Collector Advanced Settings in **Administration** > **Options**.)
   - **Disable** — Select this check box to disable statistic collection mode.

If you are enabling statistics collection on an Access Control engine, ExtremeAnalytics engine, or ExtremeWireless Controller, read through the following notes:

- **ExtremeControl Engine** — When collecting statistics on an Access Control engine, the active engine must be added to ExtremeCloud IQ Site Engine to collect all appliance statistics. In addition, Threshold Alarms mode is not supported on Access Control engines.
- **ExtremeAnalytics Engine** — When collecting statistics on an ExtremeAnalytics engine, the engine must be added to the **Analytics** > **Configuration** > ExtremeAnalytics Engines table in order for ExtremeCloud IQ Site Engine to collect all Application Detection statistics. In addition, Threshold Alarms mode is not supported on ExtremeAnalytics engines.
- **ExtremeWireless Controller** — Wireless Controller statistics collection is configured separately from other devices. When you enable Wireless Controller statistics collection, it includes Wireless Controller, WLAN, Topology, and AP wired and wireless statistics, and you also have the option to collect wireless client statistics.

For additional information about collecting statistics, see Enable Report Data Collection.

Export Serial Numbers

To register or export serial numbers for your devices:

1. Select one or more devices in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Export Serial Numbers**.

   The **Export Serial Numbers** window opens.
4. Select **Export to File**

   Export to File collects all the serial numbers for the selected devices and downloads them to the browser in comma separated value (CSV) format. This function allows you to view the serial numbers before registering.

Change Management Status

When using ExtremeCloud IQ Site Engine in Air Gap mode, the **Change Management Status** sub-menu displays, enabling you to manually determine whether a device listed on the **Devices** tab is managed by ExtremeCloud IQ Site Engine. Unmanaged devices do not count against the license total in your license file.

To change the management status of a device:

1. Select one or more devices or wireless controllers in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Hover over **More Actions** > **Change Management Status**.
   a. Select **Manage Device(s)** to manage the devices you selected in the **Device** list using ExtremeCloud IQ Site Engine. The number of available licenses is reduced based on the number and size of devices you selected.
   b. Select **Unmanage Device(s)** if you no longer need to manage the selected devices in ExtremeCloud IQ Site Engine. All licenses consumed by the selected devices are returned to the available pool.

Archives

Backup Configuration

To back up (archive) your device configurations via the **Devices** tab:

1. Select one or more devices in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.

3. Select **Archives** > **Backup Configuration**.

Restore Configuration

To restore device configurations via the **Devices** tab:

1. Select one or more devices in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Archives** > **Restore Configuration**.

Compare Last Configurations

To compare two configuration files using the **Devices** tab:

1. Select one or more devices in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Archives** > **Compare Last Configurations**.

Inventory Settings

To configure the firmware, MIB, and script settings for a device:

1. Select one or more devices in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Archives** > **Inventory Settings**.

The Inventory Settings window opens, from which you can select the file transfer mode, firrmware download server, and MIB download settings.

Tasks

If you configure tasks or workflows to appear on devices, ports, or groups, you can use the **Devices** tab to run a task or workflow on a device, port, or group.

To run a task:

1. Select one or more devices or a device group in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Tasks** from the drop-down list.
4. Select **Config** to select the workflow you are running on the selected devices from within the **Tasks** menu.

> **NOTE:** For Fabric Engine devices, you can also select Config to disable or enable DvR (Direct Virtual Routing) leaf boot config flag.

5. Select **System** to select the script you are running on the selected devices from within the **Tasks** menu.

NOTE:

You can also access the **Tasks** menu from the left-panel menu by right-clicking an item. The items displayed in the left-panel depends on the criteria you select in the drop-down list.

- If the item in the left-panel is a device or contains devices, a **Device Tasks** submenu displays, containing those tasks specific to devices. To define a task as specific to devices, select **Device** on the **Menus** subtab for the script or workflow from which task is created.
- If the item in the left-panel is a port or contains ports, a **Port Tasks** submenu displays, containing those tasks specific to ports. To define a task as specific to ports, select **Port** on the **Menus** subtab for the script or workflow from which task is created.

6. Select **CLI Commands** to display CLI commands for the script or workflow you are running from within the **Tasks** menu.

CLI Commands

To run commands against multiple devices, use the Tasks > CLI Commands option:

1. Select the **Menu** icon (☰) or right-click in the Devices list.
2. Select **Tasks** > **CLI Commands**.

The Execute CLI Commands window opens, from which you can enter the commands and execute on the devices you select. Select the Launch link at the top of the window in the Terminal Window column to test the credentials and view the results in the Results tab at the bottom of the window.

NOTE: Commands you define are run on all of the devices displayed at the table at the top of the window.

Device Groups

Selecting the User Device Groups in the left-panel tree of the **Devices** tab enables you to create, delete, and rename device groups in your network, as well as remove a device from a device group, and remove a port from a device group.

Creating a Device Group

To create a device group:

1. Select **User Device Groups** in the left-panel tree on the **Devices** tab, or expand the User Device Groups list and select a device group.
2. Select the **Menu** icon (☰) or right-click on the device group you selected in the list.
3. Select **Device Groups** > **Create Device Group**.
4. The **Create Device Group** window opens. Enter a name for the new device group.

NOTE: Device Group names must be unique within the parent group.

Device Group names are case insensitive.

---

5. Select **OK**.

Deleting a Device Group

To delete a device group:

1. Select User Device Groups in the left-panel tree on the **Devices** tab.
2. Expand the User Device Group list and select a device group.
3. Select the **Menu** icon (☰) or right-click on the device group you selected.
4. Select **Device Groups** > **Delete Device Group**.
5. The **Confirm Delete** window opens. Select **Yes** to delete the device group.

Renaming a Device Group

To rename a device group:

1. Select User Device Groups in the left-panel tree on the **Devices** tab.
2. Expand the User Device Group list and select a device group.
3. Select the **Menu** icon (☰) or right-click on the device group you selected.
4. Select **Device Groups** > **Rename Device Group**.

5. The **Rename Device Group** window opens. Enter a new name for the device group.
6. Select **OK**.

Removing a Device from a Device Group

To remove a device from a device group:

1. Select **User Device Groups** in the left-panel tree on the **Devices** tab.
2. Expand the User Device Groups list and select a device.
3. Select the **Menu** icon (☰) or right-click on the device group you selected in the list.
4. Select **Remove from Device Group**.

NOTE: Devices contained in multiple nested device groups (for example, a device contained in a device group and also in a second device group nested in the "parent" device group) can be removed in multiple ways:

- Selecting a device in the left-panel tree, then right-clicking the device displays the option Remove from Device Group. The device is removed from the current device group, but no other device groups.
- Selecting a device group in the left-panel tree, then right-clicking a device in the right panel displays the option Remove from Device Groups. The device is removed from the current device group, as well as the nested "child" device groups.

Removing a Port from a Device Group

To remove a port from a device group:

1. Select **User Device Groups** in the left-panel tree on the **Devices** tab.
2. In the left-panel tree, expand the User Device Groups list and select a port.
3. Select the **Menu** icon (☰).
4. Select **Device Groups** > **Remove from Group**.

The port is removed from the currently selected device group.

Maps

Add to Map

To add a device to an existing map:

1. Select one or more devices in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.

3. Select **Maps** > **Add to Map**.

   For additional information, see Create and Edit Maps.

To add devices or APs to new maps:

1. Select one or more devices in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Maps** > **Create Maps For Locations**.

   For additional information, see Create and Edit Maps.

Create Map

Maps visually organize the devices on your network, based on their geographic location or based on the other devices to which they connect.

You can create a new map by either selecting the **Menu** icon (☰) or right-click in the World map navigation tree and selecting **Maps** > **Create Map**.

You can also create a map for a specific device or device group by selecting the device or device group in the Device Groups navigation tree in the Devices section of the window or in the Devices list and selecting **Maps** > **Create New Map**. For additional information, see Create and Edit Maps.

Create Map for Locations

You can create a new map based on the endpoint locations of the selected devices by either selecting the **Menu** icon (☰) or right-click in the World map navigation tree and selecting **Maps** > **Create Map for Locations**.

NOTE: The map is not created if the endpoint location matches a site that currently exists in ExtremeCloud IQ Site Engine.

For additional information, see Create and Edit Maps.

Search Maps

To search your existing maps to find a wired or wireless client or device:

1. Select one or more devices in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Maps** > **Search Maps**.

   If the search item is found, the map opens on a separate tab. For more information, see Maps Overview.

Network

The **Network** sub-menu allows you to view information about all of your network connections.

To open the Network sub-menu:

1. Select the **Menu** icon (☰) or right-click in the Devices list.
2. Select **Network**.
3. Select from **EAPS Summary**, **Link Summary**, **MLAG Summary**, **VLAN Summary**, or **VPLS Summary** to display a table with summary details for each network connection.

   NOTE: Network connection summaries are active only if the device supports the view. If the device does not support MLAG, for example, the MLAG Summary option will appear grey and inactive on this list.

   The tabs at the bottom of the window populate with information about the connection you select. All connections managed by ExtremeCloud IQ Site Engine are available. You can also view the Network Details for connections included in a specific Map by opening the Map and selecting one of the tabs in the Network Details section of the window. Selecting a connection listed on the tab highlights the connection on the map.

Policy

Use the **Policy** sub-menu to view and set policy for a device or port.

To view or set policy for a device:

1. Select one or more devices in the Devices table.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Open the **Policy** sub-menu to view the currently assigned domain, change domain assignment, set or clear the default role for all ports, or Enforce or Verify the domain.

To view or set policy for a port:

1. Select the **Menu** icon (☰) or right-click in the Devices list.
2. Select **More Views** > **Port Tree**.
3. Select one or more ports.
4. Right-click and use the Policy menu to view the currently assigned domain, set or clear the port default role, and see role details for the default role.

If the device doesn't support policy or isn't assigned to a domain, the Port Tree Policy menu options are grayed out and you see either "Policy Unsupported" or "Current Domain: Unassigned". If the domain is

unassigned, you must first assign the device to a domain before you can access Policy menu options in the Port Tree.

Fabric

The Fabric Topology selection on the Network tab displays your the fabric topologies you create for your devices.

To open the Fabric Connect tab for a site:

1. Open the **Network** > **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Right-click a site or select the **Menu** icon (☰) in the left panel.
4. Select **Maps/Sites** > **Fabric Topology**.

   The **Fabric Connect** tab opens.

NOTE: If a "503 Service Unavailable" error message displays when selecting Maps/Sites > Fabric Topology, open the Administration > Certificate tab, select the **Update Fabric Manager** button to open the Add Fabric Manager Certificate window, and select the **Generate Certificate** button.

Working in the Devices List

You can manipulate the Devices list data in several ways to customize the view for your own needs:

- Select the column headings to perform an ascending or descending sort on the column data.
- Hide or display different columns by selecting a column heading drop-down arrow and selecting the column options from the menu.
- Filter, export and search the data in each column in the table.

Devices List Column Definitions

- **Device View** — Place the cursor over the first column and select the icon to open a Device View that provides analysis and troubleshooting information for the selected device, including device summary, FlexView, and ExtremeCloud IQ Site Engine historical data. You must have historical statistic collection enabled for the device to see data for the full range of available reports. For more information, see Collect Device Statistics.
- **Device Status** — This column, hidden by default, indicates whether there is contact with the device. The color of the circle indicates the degree to which the device is communicating. A green icon indicates there is contact with the device. A yellow icon indicates there are issues

with contact to the device. A red icon indicates there is no contact with the device. Hover over the Device Status icon to view additional details about the status for that device.

- **Status** — Indicates the alarm/device status for the device.
  - (Green) Up — Up with no alarms.
  - (Red) Critical — Down or having alarms with significant implications.
  - (Orange) Error — A problem with limited implications.
  - (Yellow) Warning — Up, but with an alarm that might lead to a problem.
  - (Blue) Info — Information only; not a problem.

    Place the cursor over the status icon to view the number of alarms. Select the alarm/device status icon to open a new page with detailed information about the alarms for that device.
- **Device ID** — This column, hidden by default, displays a number that serves as a database identifier automatically created for the device. This number increments as you add additional devices.
- **Name** — The device name or nickname, or IP address. Select the link to open an Interface Summary FlexView for the device.
- **Site** — The site where the device is located.
- **Poll Type** — This column, hidden by default, indicates the poll type ExtremeCloud IQ Site Engine uses to discover devices: SNMP, Ping or Not Polled.
- **Poll Group Name** — This column, hidden by default, indicates the name of the Poll Group you define in the Poll Groups section of the Status Polling options.
- **Admin Profile** — This column, hidden by default, indicates the access Profile that gives ExtremeCloud IQ Site Engine administrative access to the device.
- **Client Profile** — This column, hidden by default, indicates the access Profile that gives ExtremeCloud IQ Site Engine client access to the device.
- **IP Address** — The device IP address. This column is hidden by default.
- **Context** — The Context column, hidden by default, displays a string that indicates how the device behaves, depending on whether the device is a router or a switch.
- **IP Context** — The IP Context column, hidden by default, displays a device's IP address with the context appended to the end of the address following a colon.
- **Trap Status** — Indicates whether a trap receiver is configured, not configured, or not supported for the device.
- **Syslog Status** — Indicates whether the device is configured to send information to the syslog or if it is not supported for the device.
- **Display Name** — The IP address of the device. This column is hidden by default.

- **Device Type** — The type of device.
- **Family** — The device product family.
- **Firmware** — The revision for the firmware running in the device.
- **Running Reference Firmware** — Indicates if the device's thresholds have been configured for Reference Firmware.
- **Updates** — The firmware release status for the device according to the results from the latest Check for Firmware Updates operation. Place your cursor on the column to see a tooltip describing the status.
    - Firmware Up To Date — The device is running the latest release of firmware.
    - New Firmware Release Available — There is a new release of firmware available for this device. Select the **Menu** icon (☰) or right-click the icon and select **More Actions** > **View Available Firmware Releases** to open a window listing the current firmware releases available with links to download the firmware.
    - Device does not support Firmware Updates feature — This device does not support the Check for Firmware Updates feature.
- **Archived** — Indicates if the device has been archived in the last 30 days.
- **Config Changed** — Indicates if the archived configuration for the device has changed in the last 30 days.
- **Connector** — Displays the connector version running on the ZTP+ device.
- **XIQ Onboarded** — Displays whether the device is onboarded to ExtremeCloud IQ to be locally managed by ExtremeCloud IQ Site Engine:
    a. Black check mark - Indicates that the device is onboarded to ExtremeCloud IQ..

    NOTES: Devices with IPv6 addresses in ExtremeCloud IQ Site Engine will not be onboarded as locally-managed devices in ExtremeCloud IQ. Only devices with IPv4 addresses qualify.

    b. Red X - Indicates the device is onboarded but Unmanaged, which means it is not using a license, it has read-only device-level support, and available features in ExtremeCloud IQ Site Engine are limited. Other functionality, including Status Polling, Historical Device + Port Statistics Collection, Existing Scheduled Tasks, and Archives, are supported for devices with Unmanaged status, but these devices cannot be configured for new tasks or new archives.

NOTES: In ExtremeCloud IQ Site Engine version 26.11.10, only use ExtremeCloud IQ to set an ExtremeCloud IQ Site Engine onboarded device to Unmanaged as a temporary measure while you obtain more licenses.

If you mark a device as Unmanaged so it does not trigger a license limit violation, you can then access ExtremeCloud IQ Site Engine and delete the device before the license violation occurs.

You can perform an enforce for an ExtremeControl engine with an Unmanaged status; however, if the device has an Unmanaged status, then the enforce does not reconfigure the device and changes are not written to the device.

When devices are marked as Unmanaged in ExtremeCloud IQ, they are also Unmanaged in ExtremeCloud IQ Site Engine.

In addition, existing ExtremeAnalytics functionality for devices with an Unmanaged status is still supported, but only with existing configuration.

c. Blank - Indicates the device is not successfully onboarded to ExtremeCloud IQ from the ExtremeCloud IQ Site Engine because either it is already onboarded to ExtremeCloud IQ (either from another ExtremeCloud IQ Site Engine or by using the IQ Agent to connect directly), or because ExtremeCloud IQ Site Engine lost its connection to ExtremeCloud IQ.

NOTE: If a device's status is Blank, it has limited features available in ExtremeCloud IQ Site Engine because management of the device is owned by ExtremeCloud IQ.

d. N/A - Indicates the device is not eligible to be onboarded to ExtremeCloud IQ because it does not have a valid serial number or MAC address, or Extreme does not yet offer onboarding support for the device.

NOTE: If ExtremeCloud IQ Site Engine does not recognize a device’s serial number or MAC address, right-click on the device and select Rediscover to attempt to discover the device’s serial number or MAC address. After the device's serial number or MAC address is discovered, it can be onboarded to ExtremeCloud IQ during the next onboarding cycle.

- **License** — Reflects the license of the device.
  - In Air Gap mode, this is the license type that ExtremeCloud IQ Site Engine is currently using for the device.

- In Connected mode, this is the license type that ExtremeCloud IQ Site Engine requested from ExtremeCloud IQ, not the license type that ExtremeCloud IQ could activate. For example, when ExtremeCloud IQ Site Engine onboards a device that requires a Navigator license, but ExtremeCloud IQ has no more Navigator licenses available, ExtremeCloud IQ activates a Pilot license for the device. However, ExtremeCloud IQ Site Engine will still show the required license type as Navigator.
- Values:
  - Not Licensed - The device was unmanaged by the system due to lack of licenses
  - Do Not Onboard - The device can't be onboarded to ExtremeCloud IQ
  - Navigator - See licensing
  - No Access - The device does not have an access profile assigned
  - Pending - The device is waiting for the license agreement
  - Pilot - See licensing
  - Ping Only - The device was added to the database with a Ping Only profile
  - Status Only - The device was added to the database as Monitor Status Only
  - Unmanaged - The device is unmanaged
  - Advanced - stack Advanced level - See licensing
  - Advanced Tier A - See licensing
  - Advanced Tier B - See licensing
  - Advanced Tier C - See licensing
  - Advanced Tier D - See licensing
  - Standard - stack Standard level - See licensing
  - Standard Tier A - See licensing
  - Standard Tier B - See licensing
  - Standard Tier C - See licensing
  - Standard Tier D - See licensing

- **Policy Domain** — The policy domain assigned to the device.
- **BootPROM** — The revision for the BootPROM installed on the device.
- **Base MAC** — The base MAC address for the device.
- **Serial Number** — The serial number for the device.
- **Stats** — Displays whether statistics collection is enabled or disabled on the device. A black check mark indicates that historical collection is enabled, a blue check mark indicates that threshold alarms collection (formerly monitor collection) is enabled.
- **Location** — The physical location of the device.

- **Contact** — The name of the responsible contact person.
- **System Name** — An administratively-assigned hostname for the device taken from the *sysName* MIB object.
- **Uptime** — The amount of time, in a days hh:mm:ss format, that the device has been running since the last start-up.
- **Nickname** — The user-defined nickname for the selected device. This is the name for this device that appears in the device tree in the left panel when the **Nickname** option is selected in the **Name Format** drop-down list in the ExtremeCloud IQ Site Engine tab options.
- **Description** — A description of the device.
- **SDWAN Neighbors** — The comma-separated list of SDWAN appliances neighboring the SNMP-managed Fabric Engine device. The list entry contains both IP address and S/N. The SDWAN appliance must be from Extreme Networks. This column is hidden by default.
- **User Data 1-4, Notes** — These columns can provide additional information about the device.
- **Asset Tag** — An asset tag is a unique asset number assigned to a device for inventory tracking purposes. This value is configured on the Device Annotation of the **Configure Device** window.
- **Network OS** — The Network Operating System installed on the device. This allows ExtremeCloud IQ Site Engine to display the appropriate scripts and workflows on a device's Tasks submenu when the device's Network OS matches one of the Network Operating Systems defined for the script or workflow.

Buttons, Search Field, and Paging Toolbar



Use the Filter function to view, modify, apply, or remove filters you add to a table column. You can filter multiple columns in a table. The filtered data is specific to the type of data presented in the column.

Search 

The search tool enables you to search for full or partial matches on fields in the table.

Paging Toolbar 

The paging toolbar provides four buttons that let you easily page through the table: first, previous, next, and last page.

Refresh 

Use the refresh button to update the data in the table.

Reset 

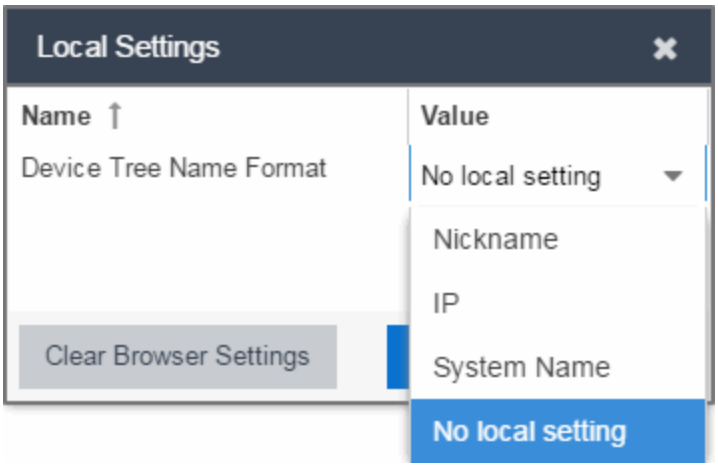
The reset button clears the search field and search results, clears all filters, and refreshes the table.

Bookmark

Use the bookmark button to save the search, sort, and filtering options you have currently set.

Local Settings

Selecting the Settings link in the top right of the **Network** tab opens the Local Settings window, shown below, from which you can select how the Device navigation tree displays the name of your devices using the Device Tree Name Format drop-down list.



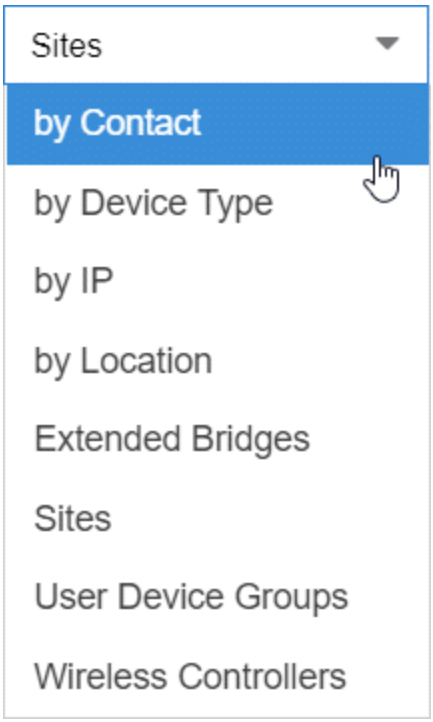
- **Nickname** — Displays device names in the Device navigation tree using the Nickname entered when you added the device.
- **IP** — Displays device names in the Device navigation tree using the IP address of the device.
- **System Name** — Displays device names in the Device navigation tree using the system name of the device.

Additionally, selecting the **Clear Browser Settings** button changes the ExtremeCloud IQ Site Engine settings back to the system default.

Devices Navigation

Filter by Criteria

The ExtremeCloud IQ Site Engine **Network** > **Devices** tab contains a left-panel drop-down list that allows you to filter for devices by specific criteria, view all devices on your network, or select maps or sites.



Selecting an item in the drop-down list filters the left-panel to display the devices, maps, or sites that apply to your selection.

by Contact

Select **by Contact** to organize devices based on the Contact you configure on the **Configure Device** window.

by Device Type

Select **by Device Type** to organize devices based on the type of device (for example, Summit Series).

by IP

Select **by IP** to organize devices based on the IP address of your devices (for example, all of the devices whose IP addresses begin with 10.20.30.x).

by Location

Select **by Location** to organize devices based on the Location you configure on the **Configure Device** window.

Extended Bridges

Select **Extended Bridges** to display all of the devices which control port extenders. Devices are organized by device type. Expand a controlling bridge to view the port extenders connected to that device.

Sites

Select **Sites** to display all of your sites in the left-panel in a Sites Tree View. A site is a group of devices that share a configuration. When a device is added to a site, ExtremeCloud IQ Site

Engine configures the device to match the configuration of the site. Sites can also contain maps, which display devices based on their geographical or topological location. Devices that share connections or are located in a particular location display in the same map.

User Device Groups

Select **User Device Groups** to display details about device groups you have created and organize devices into new device groups you create. You can also use this tab to delete or rename device groups.

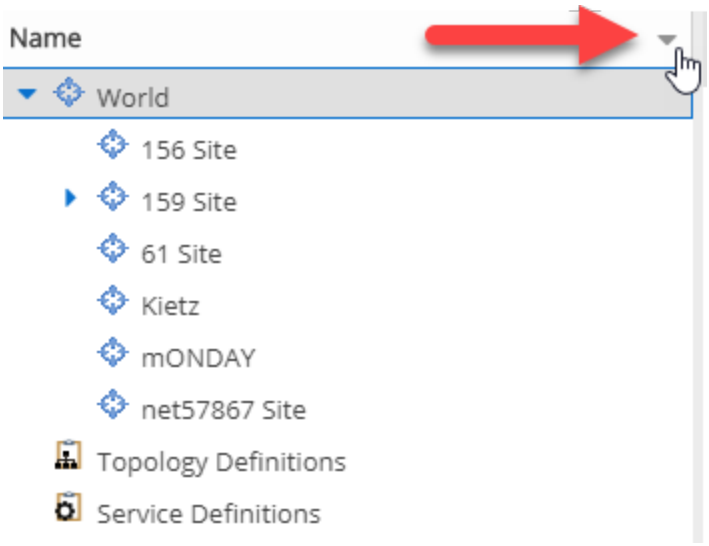
Wireless Controllers

Select **Wireless Controllers** to filter the left-panel to display wireless controllers in your network.

Once you select an item in the drop-down list, the Tree View refreshes to display the list by that criteria.

Sort Tree View

Sort the items displayed in the left panel by selecting the down arrow icon that appears when you hover your cursor over the right side of the **Name** heading row. An up arrow beside the Name title indicates the information listed in the left panel is sorted in descending order, while a down arrow beside the Name title indicates the left panel information is sorted in ascending order.



Sorting in ascending or descending order results in the following:

- **Sort Ascending** ( ) — Orders the information in the Tree View in the following order:
  - z-a (lower case)
  - Z-A (upper case)
  - 9-0 (numerical)

- **Sort Descending** ( ) — Orders the information in the Tree View in the following order:
  - 0-9 (numerical)
  - A-Z (upper case)
  - a-z (lower case)

NOTES: The World site, Topology Definitions section, and Service Definitions section do not change order when sorting.

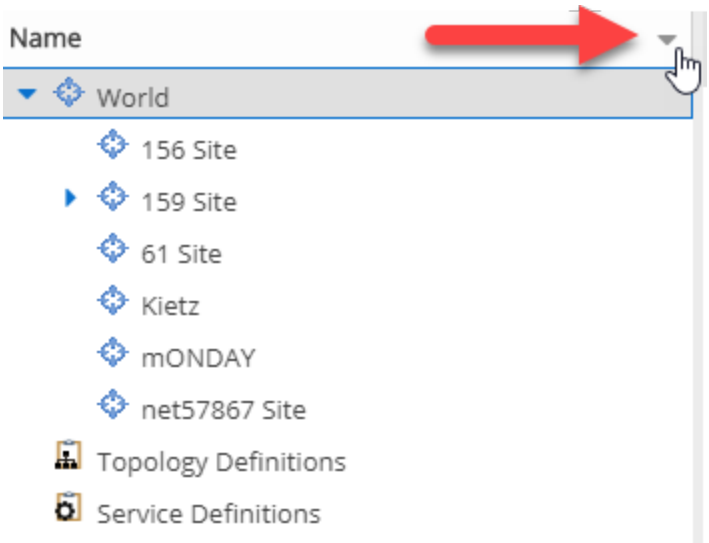
After adding or renaming a item, it may not move to the correct position in the Tree View. Refresh the window to update the items displayed.

Select a device, device group, map, or site in the left-panel and use the right-panel to perform a variety of device operations.

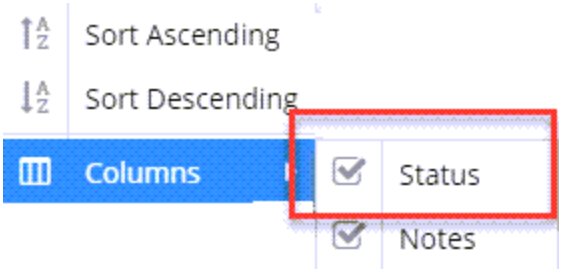
Status

The **Status** column displays in the left-panel and provides a description of the alarm status of the devices and whether the devices/ports included in each left-panel selection are reachable by ExtremeCloud IQ Site Engine.

Display the **Status** column by selecting the down arrow icon that appears when you hover your cursor over the right side of the left panel.



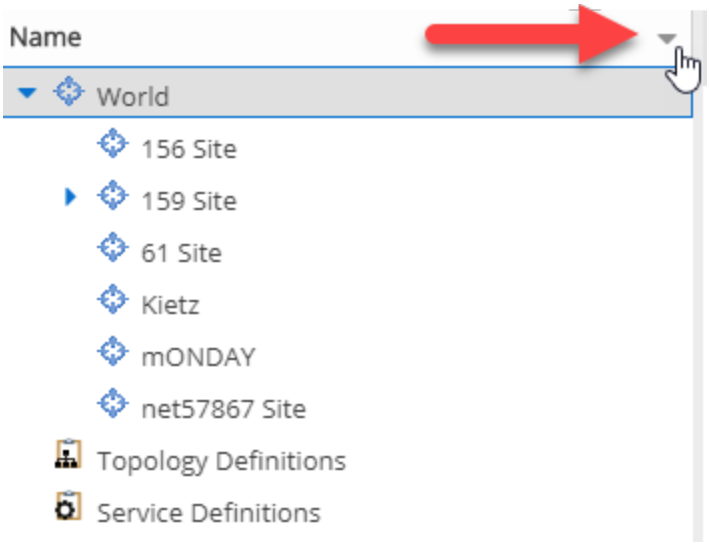
Select the **Columns** > **Status** checkbox from the menu.



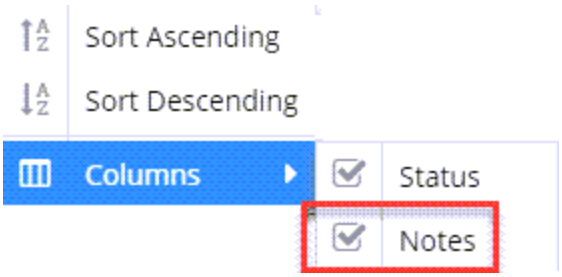
Notes

The **Notes** column displays in the left-panel and provides additional information about the devices included in each left-panel selection. The additional information for a device is user-defined and configured on the **Network** > **Devices** > **Configure Device** > Device Annotation tab.

Display the **Notes** column by selecting the down arrow icon that appears when you hover your cursor over the right side of the left panel.



Select the **Columns** > **Notes** checkbox from the menu.



For information on related topics:

- Devices
- Site
- Maps
- How to Create and Edit Maps
- Advanced Map Features

Device Operations

This Help topic provides information on the following operations available from the **Network** > **Devices** tab:

Buttons

- Add Device
- Check for Firmware Updates
- Export to CSV

Menu Options

- Device View
- Terminal
- WebView
- FlexViews
- More Views
    - Port Tree
    - Interfaces
    - User Sessions
    - Fabric L2VSNs
    - SDWAN Appliance360
- Configure
- Compass Search
- Rediscover
- Clear Alarms
- Upgrade Firmware
- Add to Device Group

- More Actions
    - Restart Device
    - Set Device Profile
    - Set/Clear Frozen Ports
    - Import to Site
    - Import to Service Definition
    - View Available Firmware Releases
    - Run Site's Add Actions
    - Contact Device Using Group's Profile
    - Ping Device (ICMP)
    - Authentication Configuration
    - RADIUS Configuration
        - RADIUS Authentication
        - RADIUS Accounting
    - Delete Device
    - Overwrite Local Changes
    - Register Trap Receiver
    - Unregister Trap Receiver
    - Register SysLog Receiver
    - Unregister SysLog Receiver
    - Collect Device Statistics
    - Export Serial Numbers
    - Change Management Status
- Archives
    - Backup Configuration
    - Restore Configuration
    - Compare Last Configurations
    - Inventory Settings
- Tasks
    - CLI Commands
- Device Groups

- Maps
    - Add to Map
    - Create Map
    - Create Map for Locations
    - Search Maps
- Network
- Policy
- Fabric
- Working in the Devices Table
    - Table Column Definitions
    - Filtering
- Buttons, Search Field, and Paging Toolbar
- Local Settings

To view the **Devices** sub-tab on the **Network** tab, you must be a member of an authorization group assigned the OneView > Access OneView and the OneView > Events and Alarms > OneView Event Log Access capabilities.

Add Device

To add a new device to the Devices list, select the **Add Device** icon at the top of the tab. The Add Device window appears. Enter the information in the window and select **OK**.

AFter the device is added to the Devices list, it can be used in ExtremeCloud IQ Site Engine.

Check for Firmware Updates

To check for available firmware updates for the devices included in the Devices list, select the **Check for Firmware Updates** icon at the top of the Devices tab. Enter your ExtremeNetworks.com credentials to view available firmware updates.

To update the credentials used to access ExtremeNetworks.com, open the Administration > Options > ExtremeNetworks.com Updates tab and edit the values in the Update Credentials section.

Export to CSV

To export information from the Devices list, select the **Export to CSV** icon at the top of the tab. The **Devices** tab provides two methods of exporting the data in the table:

Export all rows
Select to export all of the data in the table to a .CSV file. The exported data displays with any sorting, filtering, and searching applied.

Export selected rows
Select to export the data in the currently selected row(s) in the table to a .CSV file. The exported data includes all columns in the table (including those not currently displayed).

Menu Options

Device View

Select the **Menu** icon (☰) or right-click in the Devices list to opens a Device View for the device in a separate tab.

Terminal

To open a terminal session to a device, select the **Menu** icon (☰) or right-click in the Devices list and select **Terminal**. The Extreme WebShell window opens a terminal session for the selected device.

You can copy and paste information to and from the terminal window. Additionally, you can also enable logging for device terminal sessions. To enable logging, access the **Administration** > **Diagnostics** tab and expand **Server** in the left-panel. Select **Server Diagnostics** and select the appropriate **Diagnostic Level** in the drop-down list for Extreme WebShell.

WebView

You can use the **Network** tab to access WebView web-based management, which lets you configure and manage certain Extreme Networks and Enterasys devices.

To open WebView, select a device in the Device list, select the **Menu** icon (☰) or right-click in the Devices list to select **WebView** from the menu.

The web-based management opens in a new browser window. If your authorization group has been assigned the capability for Suite > Device Local Management WebView, you can take advantage of the auto login feature for web local management of ExtremeControlengines and wireless controllers.

WebView is only available with certain Extreme Networks and Enterasys devices.

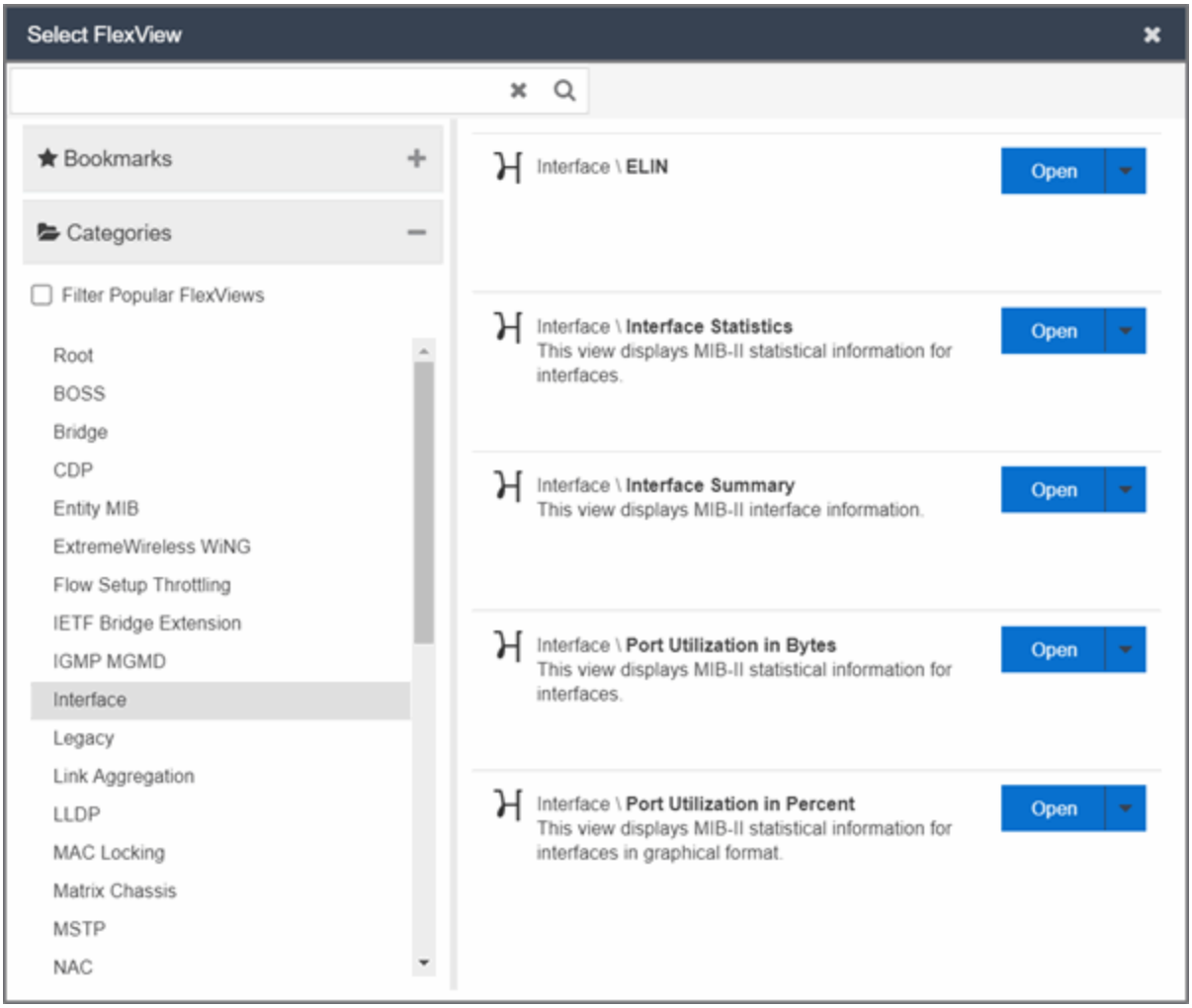
FlexViews

You can use the **Network** tab to access web-based FlexViews that provide a convenient way for Operations people to view FlexView data.

To launch a FlexView, you must be a member of an authorization group that has been assigned the OneView > FlexView > OneView FlexView Read Access capability. To launch and edit a web-based FlexView, you must be a member of an authorization group that has been assigned the OneView > FlexView > OneView FlexView Read/Write Access capability.

To launch a FlexView, select a device in the Device list, select the **Menu** icon (☰) or right-click in the Devices list and select **FlexView** from the menu. You can also right-click on a device and select **FlexView** from the menu.

The **Select FlexView** window opens.



Select a FlexView category from the left-panel and select the Open drop-down list. Select whether you want to open the FlexView in a new tab or window. The **Select FlexView** window displays only those FlexViews applicable to the device type selected.

For additional information about launching and using FlexViews from the **Network** tab, see Web-Based FlexViews.

More Views

Port Tree

The Port Tree displays interface information for a device.

To open the Port Tree:

1. Select a device in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Views** > **Port Tree.** The Port Tree opens in a new tab.
4. Expand the components to see the device's interfaces. Right-click on an interface to:
    - access PortView for that interface
    - view interface history including interface utilization, availability, and bandwidth/packets/flows statistics (Flow stats display only for S/K series and PF-FC-180 devices)
    - run scripts on the selected port
    - enable interface statistic collection
    - create policy profiles, called roles, that are assigned to the ports in your network.

In the Port Tree table, the Stats column displays whether statistics collection is enabled or disabled on the port. A black check indicates that historical collection is enabled, and a blue check indicates that threshold alarms collection (formerly monitor collection) is enabled. The Neighbor column displays neighbor details from CDP/EDP/LLDP. Hover your mouse over the column to see the protocol type.

Interfaces

Selecting **Interfaces** opens the Interface Summary, from which you can right-click on an interface to access PortView, view interface history, view current alarms and alarm history, enable interface statistic collection, and edit certain values for an interface.

To open the Interface Summary:

1. Select a device in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Views** > **Interfaces**.

    An Interface Summary FlexView opens for the device in a new tab.

User Sessions

Select User Sessions to view user sessions associated with the selected device.

To launch the user session, you must be a member of an authorization group that has been assigned the OneView > User Session > OneView User Session Read Access capability. To launch and edit a User Session , you must be a member of an authorization group that has been assigned the OneView > User Session > OneView User Session Read/Write Access capability.

To open a user session for a device:

1. Select a device in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Views** > **User Session**.

In the User Sessions window, you can view all users accessing the device selected.

For additional information about the User Sessions window, see User Sessions.

Fabric L2VSNs

Selecting **Fabric L2VSNs** opens the I-SID L2VSN and I-SID L2VSN interfaces with details about Fabric Connect L2 Services known to the device.

To open the Fabric L2VSNs:

1. Select a device in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Views** > **Fabric L2VSNs**.

   An Interface Fabric L2VSNs opens for the device in a new tab.

SDWAN Appliance360

Selecting **SDWAN Appliance360** opens the SDWAN Appliance360 in ExtremeCloud application. Additional authentication is required for the first time. This option is available only if there is an Extreme Networks SDWAN appliance connected to the selected Fabric Engine device.

To open the SDWAN Appliance360:

1. Select the Fabric Engine device with the Extreme SDWAN appliance connected in the device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Views** > **SDWAN Appliance360**.
4. If there are multiple Extreme SDWAN appliances connected, select the SDWAN appliance you want to manage.

   An SDWAN Appliance360 opens in a new tab.

Configure

To configure device information for an existing device:

1. Select the **Menu** icon (☰) or right-click in the Devices list.
2. Select **Configure**.

   The Configure Device window opens, which allows you to configure the device properties.

Compass Search

To open the Search window with Search with Compass selected for the selected devices:

1. Select the **Menu** icon (☰) or right-click in the Devices list.
2. Select **Device** > **Compass Search**.

   The **Search** window opens displaying the devices you selected with **Search with Compass** selected. Selecting a device group or site opens the **Search** window opens displaying the devices in the device group or site you selected with **Search with Compass** selected.

Rediscover

To refresh a device or multiple devices to update the information presented on the Devices tab:

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Rediscover Device**.

ExtremeCloud IQ Site Engine rediscovers the device and information about the device is refreshed.

Clear Alarms

To clear the alarms for a device or multiple devices in the Devices list:

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Clear Alarms**.

   A dialog box appears.
4. Select **Yes**.

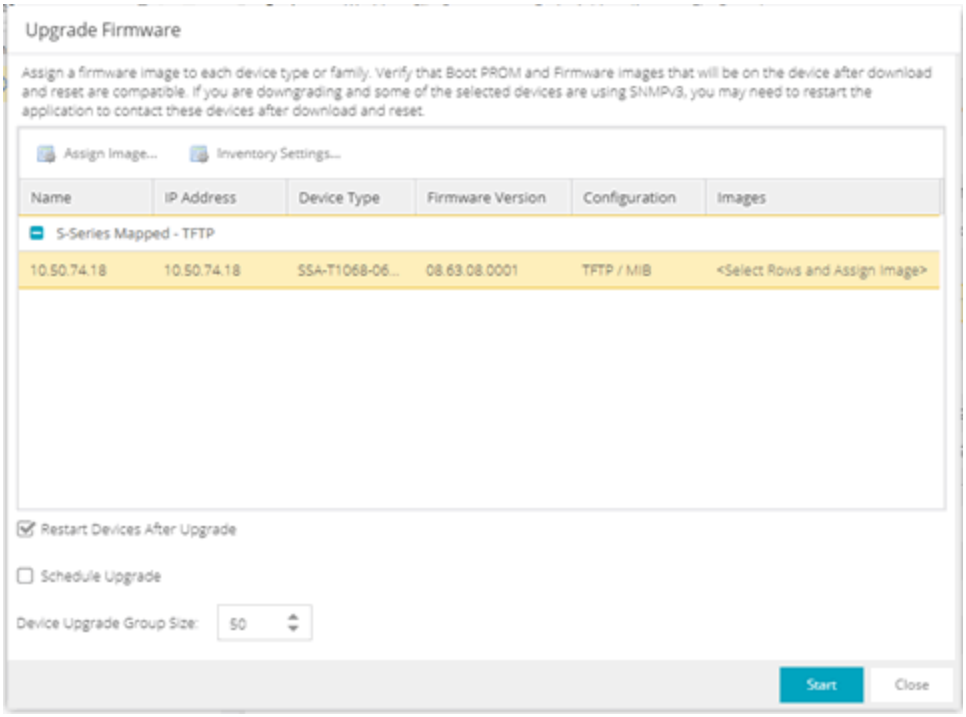
   The alarms on the selected devices clear.

Upgrade Firmware

To update devices in the ExtremeCloud IQ Site Engine database with the latest firmware releases:

1. Select the device or devices in the Devices list
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Upgrade Firmware**.

The results display in the Upgrade Firmware window with displaying information about the device and the available firmware versions. For additional information about upgrading device firmware, see How to Upgrade Firmware. Restart devices when the firmware is upgraded via the Restart Devices window by selecting More Actions > Restart Device.



Add to Device Group

The Add to Device Group menu option enables you to add devices or ports to a device group.

To add a device or multiple devices to a device group:

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Add to Device Group**.

   The Select Destination Group window displays, which allows you to select the device group to

which the device or devices are added.

4. Select **OK** to add the devices to the group.

To add a port or multiple ports to a device group:

1. Select the port or port in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Add to Device Group**.

   The Select Destination Group window displays, which allows you to select the device group to which the port or ports are added.
4. Select **OK** to add the ports to the group.

More Actions

Restart Device

To restart a device:

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Restart Device**.

   The Restart Devices window opens.
4. Select Start.

The devices are restarted.

Set Device Group's Profile

To change the profile settings for a device or multiple devices from the Devices list:

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Set Device Group's Profile**.

   The Set Device Group's Profile window appears.
4. Select a profile from the drop-down list to change the profile for the selected device or devices.
5. Select **OK**.

   A message appears confirming the device profile change.

NOTE: The access profile is changed for the user's group. To verify, check the Device Mapping.

Set/Clear Frozen Ports

To set or clear frozen ports on a device or multiple devices in the Devices list:

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions Set/Clear Frozen Ports**.
4. Select whether you want to freeze all ports, freeze the interswitch ports, or clear all frozen ports.
5. Select **Yes**. All ports are frozen, the interswitch ports are frozen, or all frozen ports are cleared, depending on what you select.

Import to Site

To import VLAN data from a device and save it to the site with which it is associated:

1. Select the device in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Import to Site**.
4. Select the **Overwrite VLAN Data** checkbox to remove all VLAN data from the site and copy the VLAN data from the device to the site.
   When this checkbox is not selected, the VLAN data from the device is added to the existing VLAN data on the device and only matching VLAN data is overwritten.
5. Select **Import** to import the VLAN data.

Import to Service Definition

To import data from a device and save it to a service definition:

1. Select the device in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Import to Service Definition**.

View Available Firmware Releases

To view all firmware releases available for a device:

1. Select the device in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.

3. Select **More Actions** > **View Available Firmware Releases**.

Run Site's Add Actions

Select **Run Site's Add Actions** to run the actions configured for the site in which the device is contained:

1. Select the device in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Run Site's Add Actions**.

Contact Device Using Group's Profile

Select **Contact Device Using Group's Profile** to attempt to contact the selected devices via SNMP using the **Administration Profile** for a device, or the device's override profile configured on the Administration > Profiles > Device Mapping subtab.

1. Select the device in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Contact Device Using Group's Profile**.

Ping Device (ICMP)

Select Ping Device (ICMP) to determine if a device is having connectivity issues.

1. Select the device in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Ping Device (ICMP).**

> **NOTE:** After a request is sent, ExtremeCloud IQ Site Engine waits the specified amount of time configured on the Administration > Options > Status Polling tab to determine if the device is reachable or not reachable.

4. If contact with the device is successful, the message "Device with IP XX.XX.XX.XX is reachable" displays.
5. If contact with the device is not successful, the message "Device with IP XX.XX.XX.XX is not reachable" displays.

Authentication Configuration

Select Authentication Configuration to open the Authentication Configuration wizard, which allows you to configure the authentication used on a device or on the individual ports of a device.

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.

3. Select **More Actions** > **Authentication Configuration**.

RADIUS Configuration

RADIUS Authentication

Opens the **RADIUS Authentication** tab, which allows you to configure the RADIUS authorization servers and client settings used on a device.

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **RADIUS Authentication**.

RADIUS Accounting

Opens the **RADIUS Accounting** tab, which allows you to configure the RADIUS accounting servers and client settings used on a device.

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **RADIUS Accounting**.

Delete Device

To delete a device or multiple devices from the Devices list:

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Delete Device**. A Delete Confirmation window opens.
4. Select **Yes** to remove the device from ExtremeCloud IQ and any databases, maps, and ZTP+ configurations to which the device is added.

Overwrite Local Changes

Use this feature to modify the configuration of a device to replace any manual changes that were made directly (via the CLI) to the device with the values from the Device, VLAN and ports tabs of ExtremeCloud IQ Site Engine.

IMPORTANT: Local configuration changes that you make on ZTP+ managed switches may not be saved into the ExtremeCloud IQ Site Engine database. Any changes made locally that you can configure using ZTP+ will be removed the next time ExtremeCloud IQ Site Engine polls the ZTP+ device.

To alert you when ExtremeCloud IQ Site Engine detects that a ZTP+ managed device has Device, VLAN, or Port settings that are different from the configuration in ExtremeCloud IQ Site Engine, you can use the Alarm on Local Change option.

To overwrite local changes made to the device via the CLI and save the site configuration on a device or devices:

1. Select the device or devices in the Devices list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Overwrite Local Changes**.

Register Trap Receiver

To receive trap information from the devices on your network, Select the **Menu** icon (☰) or right-click in the Devices list and select **More Actions** > **Register Trap Receiver** from the menu. Additionally, devices added to sites for which **Add Trap Receiver** is selected on the **Discovered Device Actions** tab automatically receive trap information. You can define the trap configuration details on the **Options** > **Trap** tab. Depending on the device, ExtremeCloud IQ Site Engine creates the trap configuration via SNMP or a script.

Unregister Trap Receiver

To stop receiving trap information from the devices on your network, Select the **Menu** icon (☰) or right-click in the Devices list and select **More Actions** > **Unregister Trap Receiver** from the menu.

Register SysLog Receiver

To receive syslog information from the devices on your network, select the **Menu** icon (☰) or right-click in the Devices list and select **More Actions** > **Register SysLog Receiver** from the menu. Additionally, devices added to sites for which **Add Syslog Receiver** is selected on the **Discovered Device Actions** tab automatically receive syslog information. You can define the syslog configuration details on the **Options** > **Syslog** tab. Depending on the device, ExtremeCloud IQ Site Engine creates the syslog configuration via SNMP or a script.

Unregister SysLog Receiver

To stop receiving syslog information from the devices on your network, select the **Menu** icon (☰) or right-click in the Devices list and select **More Actions** > **Unregister SysLog Receiver** from the menu.

Collect Device Statistics

The **Devices** tab provides the ability to start and stop device statistics collections for Extreme Networks and Enterasys devices, which allows the collection of data used in reports.

To collect device statistics:

1. Select one or more devices or wireless controllers in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Collect Device Statistics**.

   A window opens from which you can select your statistics collection criteria.

   - In **Historical mode**, device statistics are saved to the database and aggregated over time, for use in reports. The device statistics are also used for threshold alarms configured in the Console Alarms Manager. In the Active Threshold Alarm Summary box, you can see all active threshold alarms configured in the Console Alarms Manager that use these statistics.

     NOTE: Enabling Historical Device Statistics Collection may use substantial disk space.

   - In **Threshold Alarms (formerly Monitor) mode**, device statistics are saved for one hour and then dropped. You can use these statistics for threshold alarms, but not for ExtremeCloud IQ Site Engine reporting. In the Active Threshold Alarm Summary box, you can see all active threshold alarms configured in the **Alarms and Events** tab that use these statistics. (Note that you do not see the Threshold Alarms mode option if you have disabled threshold alarms collection in the OneView Collector Advanced Settings in **Administration** > **Options**.)
   - **Disable** — Select this check box to disable statistic collection mode.

If you are enabling statistics collection on an Access Control engine, ExtremeAnalytics engine, or ExtremeWireless Controller, read through the following notes:

- **ExtremeControl Engine** — When collecting statistics on an Access Control engine, the active engine must be added to ExtremeCloud IQ Site Engine to collect all appliance statistics. In addition, Threshold Alarms mode is not supported on Access Control engines.
- **ExtremeAnalytics Engine** — When collecting statistics on an ExtremeAnalytics engine, the engine must be added to the **Analytics** > **Configuration** > ExtremeAnalytics Engines table in order for ExtremeCloud IQ Site Engine to collect all Application Detection statistics. In addition, Threshold Alarms mode is not supported on ExtremeAnalytics engines.
- **ExtremeWireless Controller** — Wireless Controller statistics collection is configured separately from other devices. When you enable Wireless Controller statistics collection, it includes Wireless Controller, WLAN, Topology, and AP wired and wireless statistics, and you also have the option to collect wireless client statistics.

For additional information about collecting statistics, see Enable Report Data Collection.

Export Serial Numbers

To register or export serial numbers for your devices:

1. Select one or more devices in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **More Actions** > **Export Serial Numbers**.

   The **Export Serial Numbers** window opens.
4. Select **Export to File**

   Export to File collects all the serial numbers for the selected devices and downloads them to the browser in comma separated value (CSV) format. This function allows you to view the serial numbers before registering.

Change Management Status

When using ExtremeCloud IQ Site Engine in Air Gap mode, the **Change Management Status** sub-menu displays, enabling you to manually determine whether a device listed on the **Devices** tab is managed by ExtremeCloud IQ Site Engine. Unmanaged devices do not count against the license total in your license file.

To change the management status of a device:

1. Select one or more devices or wireless controllers in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Hover over **More Actions** > **Change Management Status**.
   a. Select **Manage Device(s)** to manage the devices you selected in the **Device** list using ExtremeCloud IQ Site Engine. The number of available licenses is reduced based on the number and size of devices you selected.
   b. Select **Unmanage Device(s)** if you no longer need to manage the selected devices in ExtremeCloud IQ Site Engine. All licenses consumed by the selected devices are returned to the available pool.

Archives

Backup Configuration

To back up (archive) your device configurations via the **Devices** tab:

1. Select one or more devices in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.

3. Select **Archives** > **Backup Configuration**.

Restore Configuration

To restore device configurations via the **Devices** tab:

1. Select one or more devices in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Archives** > **Restore Configuration**.

Compare Last Configurations

To compare two configuration files using the **Devices** tab:

1. Select one or more devices in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Archives** > **Compare Last Configurations**.

Inventory Settings

To configure the firmware, MIB, and script settings for a device:

1. Select one or more devices in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Archives** > **Inventory Settings**.

The Inventory Settings window opens, from which you can select the file transfer mode, firrmware download server, and MIB download settings.

Tasks

If you configure tasks or workflows to appear on devices, ports, or groups, you can use the **Devices** tab to run a task or workflow on a device, port, or group.

To run a task:

1. Select one or more devices or a device group in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Tasks** from the drop-down list.
4. Select **Config** to select the workflow you are running on the selected devices from within the **Tasks** menu.

> **NOTE:** For Fabric Engine devices, you can also select Config to disable or enable DvR (Direct Virtual Routing) leaf boot config flag.

5. Select **System** to select the script you are running on the selected devices from within the **Tasks** menu.

NOTE:

You can also access the **Tasks** menu from the left-panel menu by right-clicking an item. The items displayed in the left-panel depends on the criteria you select in the drop-down list.

- If the item in the left-panel is a device or contains devices, a **Device Tasks** submenu displays, containing those tasks specific to devices. To define a task as specific to devices, select **Device** on the **Menus** subtab for the script or workflow from which task is created.
- If the item in the left-panel is a port or contains ports, a **Port Tasks** submenu displays, containing those tasks specific to ports. To define a task as specific to ports, select **Port** on the **Menus** subtab for the script or workflow from which task is created.

6. Select **CLI Commands** to display CLI commands for the script or workflow you are running from within the **Tasks** menu.

CLI Commands

To run commands against multiple devices, use the Tasks > CLI Commands option:

1. Select the **Menu** icon (☰) or right-click in the Devices list.
2. Select **Tasks** > **CLI Commands**.

The Execute CLI Commands window opens, from which you can enter the commands and execute on the devices you select. Select the Launch link at the top of the window in the Terminal Window column to test the credentials and view the results in the Results tab at the bottom of the window.

NOTE: Commands you define are run on all of the devices displayed at the table at the top of the window.

Device Groups

Selecting the User Device Groups in the left-panel tree of the **Devices** tab enables you to create, delete, and rename device groups in your network, as well as remove a device from a device group, and remove a port from a device group.

Creating a Device Group

To create a device group:

1. Select **User Device Groups** in the left-panel tree on the **Devices** tab, or expand the User Device Groups list and select a device group.
2. Select the **Menu** icon (☰) or right-click on the device group you selected in the list.
3. Select **Device Groups** > **Create Device Group**.
4. The **Create Device Group** window opens. Enter a name for the new device group.

NOTE: Device Group names must be unique within the parent group.

Device Group names are case insensitive.

---

5. Select **OK**.

Deleting a Device Group

To delete a device group:

1. Select User Device Groups in the left-panel tree on the **Devices** tab.
2. Expand the User Device Group list and select a device group.
3. Select the **Menu** icon (☰) or right-click on the device group you selected.
4. Select **Device Groups** > **Delete Device Group**.
5. The **Confirm Delete** window opens. Select **Yes** to delete the device group.

Renaming a Device Group

To rename a device group:

1. Select User Device Groups in the left-panel tree on the **Devices** tab.
2. Expand the User Device Group list and select a device group.
3. Select the **Menu** icon (☰) or right-click on the device group you selected.
4. Select **Device Groups** > **Rename Device Group**.

5. The **Rename Device Group** window opens. Enter a new name for the device group.
6. Select **OK**.

Removing a Device from a Device Group

To remove a device from a device group:

1. Select **User Device Groups** in the left-panel tree on the **Devices** tab.
2. Expand the User Device Groups list and select a device.
3. Select the **Menu** icon (☰) or right-click on the device group you selected in the list.
4. Select **Remove from Device Group**.

NOTE: Devices contained in multiple nested device groups (for example, a device contained in a device group and also in a second device group nested in the "parent" device group) can be removed in multiple ways:

- Selecting a device in the left-panel tree, then right-clicking the device displays the option Remove from Device Group. The device is removed from the current device group, but no other device groups.
- Selecting a device group in the left-panel tree, then right-clicking a device in the right panel displays the option Remove from Device Groups. The device is removed from the current device group, as well as the nested "child" device groups.

Removing a Port from a Device Group

To remove a port from a device group:

1. Select **User Device Groups** in the left-panel tree on the **Devices** tab.
2. In the left-panel tree, expand the User Device Groups list and select a port.
3. Select the **Menu** icon (☰).
4. Select **Device Groups** > **Remove from Group**.

The port is removed from the currently selected device group.

Maps

Add to Map

To add a device to an existing map:

1. Select one or more devices in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.

3. Select **Maps** > **Add to Map**.

   For additional information, see Create and Edit Maps.

To add devices or APs to new maps:

1. Select one or more devices in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Maps** > **Create Maps For Locations**.

   For additional information, see Create and Edit Maps.

Create Map

Maps visually organize the devices on your network, based on their geographic location or based on the other devices to which they connect.

You can create a new map by either selecting the **Menu** icon (☰) or right-click in the World map navigation tree and selecting **Maps** > **Create Map**.

You can also create a map for a specific device or device group by selecting the device or device group in the Device Groups navigation tree in the Devices section of the window or in the Devices list and selecting **Maps** > **Create New Map**. For additional information, see Create and Edit Maps.

Create Map for Locations

You can create a new map based on the endpoint locations of the selected devices by either selecting the **Menu** icon (☰) or right-click in the World map navigation tree and selecting **Maps** > **Create Map for Locations**.

NOTE: The map is not created if the endpoint location matches a site that currently exists in ExtremeCloud IQ Site Engine.

For additional information, see Create and Edit Maps.

Search Maps

To search your existing maps to find a wired or wireless client or device:

1. Select one or more devices in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Maps** > **Search Maps**.

   If the search item is found, the map opens on a separate tab. For more information, see Maps Overview.

Network

The **Network** sub-menu allows you to view information about all of your network connections.

To open the Network sub-menu:

1. Select the **Menu** icon (☰) or right-click in the Devices list.
2. Select **Network**.
3. Select from **EAPS Summary**, **Link Summary**, **MLAG Summary**, **VLAN Summary**, or **VPLS Summary** to display a table with summary details for each network connection.

   NOTE: Network connection summaries are active only if the device supports the view. If the device does not support MLAG, for example, the MLAG Summary option will appear grey and inactive on this list.

   The tabs at the bottom of the window populate with information about the connection you select. All connections managed by ExtremeCloud IQ Site Engine are available. You can also view the Network Details for connections included in a specific Map by opening the Map and selecting one of the tabs in the Network Details section of the window. Selecting a connection listed on the tab highlights the connection on the map.

Policy

Use the **Policy** sub-menu to view and set policy for a device or port.

To view or set policy for a device:

1. Select one or more devices in the Devices table.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Open the **Policy** sub-menu to view the currently assigned domain, change domain assignment, set or clear the default role for all ports, or Enforce or Verify the domain.

To view or set policy for a port:

1. Select the **Menu** icon (☰) or right-click in the Devices list.
2. Select **More Views** > **Port Tree**.
3. Select one or more ports.
4. Right-click and use the Policy menu to view the currently assigned domain, set or clear the port default role, and see role details for the default role.

If the device doesn't support policy or isn't assigned to a domain, the Port Tree Policy menu options are grayed out and you see either "Policy Unsupported" or "Current Domain: Unassigned". If the domain is

unassigned, you must first assign the device to a domain before you can access Policy menu options in the Port Tree.

Fabric

The Fabric Topology selection on the Network tab displays your the fabric topologies you create for your devices.

To open the Fabric Connect tab for a site:

1. Open the **Network** > **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Right-click a site or select the **Menu** icon (☰) in the left panel.
4. Select **Maps/Sites** > **Fabric Topology**.

   The **Fabric Connect** tab opens.

NOTE: If a "503 Service Unavailable" error message displays when selecting Maps/Sites > Fabric Topology, open the Administration > Certificate tab, select the **Update Fabric Manager** button to open the Add Fabric Manager Certificate window, and select the **Generate Certificate** button.

Working in the Devices List

You can manipulate the Devices list data in several ways to customize the view for your own needs:

- Select the column headings to perform an ascending or descending sort on the column data.
- Hide or display different columns by selecting a column heading drop-down arrow and selecting the column options from the menu.
- Filter, export and search the data in each column in the table.

Devices List Column Definitions

- **Device View** — Place the cursor over the first column and select the icon to open a Device View that provides analysis and troubleshooting information for the selected device, including device summary, FlexView, and ExtremeCloud IQ Site Engine historical data. You must have historical statistic collection enabled for the device to see data for the full range of available reports. For more information, see Collect Device Statistics.
- **Device Status** — This column, hidden by default, indicates whether there is contact with the device. The color of the circle indicates the degree to which the device is communicating. A green icon indicates there is contact with the device. A yellow icon indicates there are issues

with contact to the device. A red icon indicates there is no contact with the device. Hover over the Device Status icon to view additional details about the status for that device.

- **Status** — Indicates the alarm/device status for the device.
  - (Green) Up — Up with no alarms.
  - (Red) Critical — Down or having alarms with significant implications.
  - (Orange) Error — A problem with limited implications.
  - (Yellow) Warning — Up, but with an alarm that might lead to a problem.
  - (Blue) Info — Information only; not a problem.

    Place the cursor over the status icon to view the number of alarms. Select the alarm/device status icon to open a new page with detailed information about the alarms for that device.
- **Device ID** — This column, hidden by default, displays a number that serves as a database identifier automatically created for the device. This number increments as you add additional devices.
- **Name** — The device name or nickname, or IP address. Select the link to open an Interface Summary FlexView for the device.
- **Site** — The site where the device is located.
- **Poll Type** — This column, hidden by default, indicates the poll type ExtremeCloud IQ Site Engine uses to discover devices: SNMP, Ping or Not Polled.
- **Poll Group Name** — This column, hidden by default, indicates the name of the Poll Group you define in the Poll Groups section of the Status Polling options.
- **Admin Profile** — This column, hidden by default, indicates the access Profile that gives ExtremeCloud IQ Site Engine administrative access to the device.
- **Client Profile** — This column, hidden by default, indicates the access Profile that gives ExtremeCloud IQ Site Engine client access to the device.
- **IP Address** — The device IP address. This column is hidden by default.
- **Context** — The Context column, hidden by default, displays a string that indicates how the device behaves, depending on whether the device is a router or a switch.
- **IP Context** — The IP Context column, hidden by default, displays a device's IP address with the context appended to the end of the address following a colon.
- **Trap Status** — Indicates whether a trap receiver is configured, not configured, or not supported for the device.
- **Syslog Status** — Indicates whether the device is configured to send information to the syslog or if it is not supported for the device.
- **Display Name** — The IP address of the device. This column is hidden by default.

- **Device Type** — The type of device.
- **Family** — The device product family.
- **Firmware** — The revision for the firmware running in the device.
- **Running Reference Firmware** — Indicates if the device's thresholds have been configured for Reference Firmware.
- **Updates** — The firmware release status for the device according to the results from the latest Check for Firmware Updates operation. Place your cursor on the column to see a tooltip describing the status.
    - Firmware Up To Date — The device is running the latest release of firmware.
    - New Firmware Release Available — There is a new release of firmware available for this device. Select the **Menu** icon (☰) or right-click the icon and select **More Actions** > **View Available Firmware Releases** to open a window listing the current firmware releases available with links to download the firmware.
    - Device does not support Firmware Updates feature — This device does not support the Check for Firmware Updates feature.
- **Archived** — Indicates if the device has been archived in the last 30 days.
- **Config Changed** — Indicates if the archived configuration for the device has changed in the last 30 days.
- **Connector** — Displays the connector version running on the ZTP+ device.
- **XIQ Onboarded** — Displays whether the device is onboarded to ExtremeCloud IQ to be locally managed by ExtremeCloud IQ Site Engine:
    a. Black check mark - Indicates that the device is onboarded to ExtremeCloud IQ..

    NOTES: Devices with IPv6 addresses in ExtremeCloud IQ Site Engine will not be onboarded as locally-managed devices in ExtremeCloud IQ. Only devices with IPv4 addresses qualify.

    b. Red X - Indicates the device is onboarded but Unmanaged, which means it is not using a license, it has read-only device-level support, and available features in ExtremeCloud IQ Site Engine are limited. Other functionality, including Status Polling, Historical Device + Port Statistics Collection, Existing Scheduled Tasks, and Archives, are supported for devices with Unmanaged status, but these devices cannot be configured for new tasks or new archives.

NOTES: In ExtremeCloud IQ Site Engine version 26.11.10, only use ExtremeCloud IQ to set an ExtremeCloud IQ Site Engine onboarded device to Unmanaged as a temporary measure while you obtain more licenses.

If you mark a device as Unmanaged so it does not trigger a license limit violation, you can then access ExtremeCloud IQ Site Engine and delete the device before the license violation occurs.

You can perform an enforce for an ExtremeControl engine with an Unmanaged status; however, if the device has an Unmanaged status, then the enforce does not reconfigure the device and changes are not written to the device.

When devices are marked as Unmanaged in ExtremeCloud IQ, they are also Unmanaged in ExtremeCloud IQ Site Engine.

In addition, existing ExtremeAnalytics functionality for devices with an Unmanaged status is still supported, but only with existing configuration.

c. Blank - Indicates the device is not successfully onboarded to ExtremeCloud IQ from the ExtremeCloud IQ Site Engine because either it is already onboarded to ExtremeCloud IQ (either from another ExtremeCloud IQ Site Engine or by using the IQ Agent to connect directly), or because ExtremeCloud IQ Site Engine lost its connection to ExtremeCloud IQ.

NOTE: If a device's status is Blank, it has limited features available in ExtremeCloud IQ Site Engine because management of the device is owned by ExtremeCloud IQ.

d. N/A - Indicates the device is not eligible to be onboarded to ExtremeCloud IQ because it does not have a valid serial number or MAC address, or Extreme does not yet offer onboarding support for the device.

NOTE: If ExtremeCloud IQ Site Engine does not recognize a device’s serial number or MAC address, right-click on the device and select Rediscover to attempt to discover the device’s serial number or MAC address. After the device's serial number or MAC address is discovered, it can be onboarded to ExtremeCloud IQ during the next onboarding cycle.

- **License** — Reflects the license of the device.
  - In Air Gap mode, this is the license type that ExtremeCloud IQ Site Engine is currently using for the device.

- In Connected mode, this is the license type that ExtremeCloud IQ Site Engine requested from ExtremeCloud IQ, not the license type that ExtremeCloud IQ could activate. For example, when ExtremeCloud IQ Site Engine onboards a device that requires a Navigator license, but ExtremeCloud IQ has no more Navigator licenses available, ExtremeCloud IQ activates a Pilot license for the device. However, ExtremeCloud IQ Site Engine will still show the required license type as Navigator.
- Values:
  - Not Licensed - The device was unmanaged by the system due to lack of licenses
  - Do Not Onboard - The device can't be onboarded to ExtremeCloud IQ
  - Navigator - See licensing
  - No Access - The device does not have an access profile assigned
  - Pending - The device is waiting for the license agreement
  - Pilot - See licensing
  - Ping Only - The device was added to the database with a Ping Only profile
  - Status Only - The device was added to the database as Monitor Status Only
  - Unmanaged - The device is unmanaged
  - Advanced - stack Advanced level - See licensing
  - Advanced Tier A - See licensing
  - Advanced Tier B - See licensing
  - Advanced Tier C - See licensing
  - Advanced Tier D - See licensing
  - Standard - stack Standard level - See licensing
  - Standard Tier A - See licensing
  - Standard Tier B - See licensing
  - Standard Tier C - See licensing
  - Standard Tier D - See licensing

- **Policy Domain** — The policy domain assigned to the device.
- **BootPROM** — The revision for the BootPROM installed on the device.
- **Base MAC** — The base MAC address for the device.
- **Serial Number** — The serial number for the device.
- **Stats** — Displays whether statistics collection is enabled or disabled on the device. A black check mark indicates that historical collection is enabled, a blue check mark indicates that threshold alarms collection (formerly monitor collection) is enabled.
- **Location** — The physical location of the device.

- **Contact** — The name of the responsible contact person.
- **System Name** — An administratively-assigned hostname for the device taken from the *sysName* MIB object.
- **Uptime** — The amount of time, in a days hh:mm:ss format, that the device has been running since the last start-up.
- **Nickname** — The user-defined nickname for the selected device. This is the name for this device that appears in the device tree in the left panel when the **Nickname** option is selected in the **Name Format** drop-down list in the ExtremeCloud IQ Site Engine tab options.
- **Description** — A description of the device.
- **SDWAN Neighbors** — The comma-separated list of SDWAN appliances neighboring the SNMP-managed Fabric Engine device. The list entry contains both IP address and S/N. The SDWAN appliance must be from Extreme Networks. This column is hidden by default.
- **User Data 1-4, Notes** — These columns can provide additional information about the device.
- **Asset Tag** — An asset tag is a unique asset number assigned to a device for inventory tracking purposes. This value is configured on the Device Annotation of the **Configure Device** window.
- **Network OS** — The Network Operating System installed on the device. This allows ExtremeCloud IQ Site Engine to display the appropriate scripts and workflows on a device's Tasks submenu when the device's Network OS matches one of the Network Operating Systems defined for the script or workflow.

Buttons, Search Field, and Paging Toolbar



Use the Filter function to view, modify, apply, or remove filters you add to a table column. You can filter multiple columns in a table. The filtered data is specific to the type of data presented in the column.

Search 

The search tool enables you to search for full or partial matches on fields in the table.

Paging Toolbar 

The paging toolbar provides four buttons that let you easily page through the table: first, previous, next, and last page.

Refresh 

Use the refresh button to update the data in the table.

Reset 

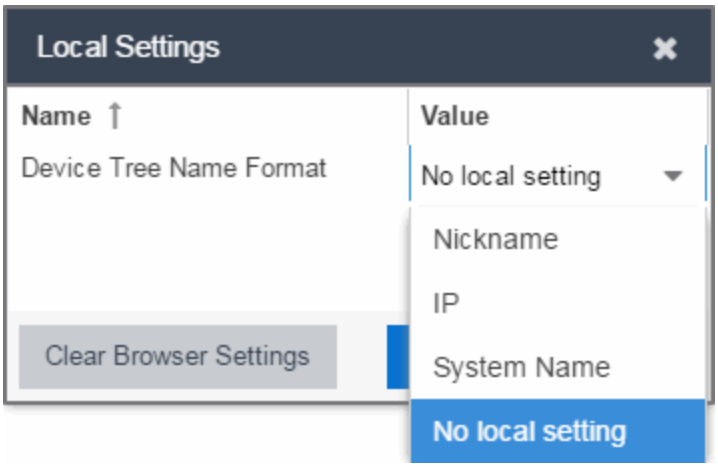
The reset button clears the search field and search results, clears all filters, and refreshes the table.

Bookmark

Use the bookmark button to save the search, sort, and filtering options you have currently set.

Local Settings

Selecting the Settings link in the top right of the **Network** tab opens the Local Settings window, shown below, from which you can select how the Device navigation tree displays the name of your devices using the Device Tree Name Format drop-down list.



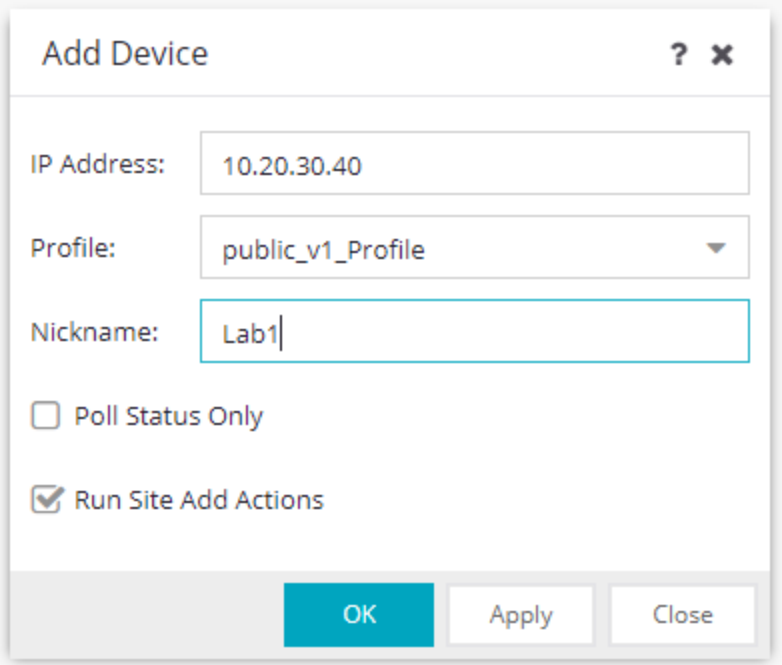
- **Nickname** — Displays device names in the Device navigation tree using the Nickname entered when you added the device.
- **IP** — Displays device names in the Device navigation tree using the IP address of the device.
- **System Name** — Displays device names in the Device navigation tree using the system name of the device.

Additionally, selecting the **Clear Browser Settings** button changes the ExtremeCloud IQ Site Engine settings back to the system default.

Add Device

Use this window to add a device to the ExtremeCloud IQ Site Engine database. From this window you can enter the device IP address, the device profile, and the device nickname.

This window is accessible by selecting the **Menu** icon (☰) and selecting **Device** > **Add Device** from the menu or by right-clicking an existing device and selecting **Device** > **Add Device** on the **Network** > **Devices** tab.



IP Address
The IP address of the device.

Profile
The access Profile used for the device. To create or edit a profile, open the **Administration** > **Profiles** tab.

Nickname
The name by which the device is known.

Poll Status Only
Select **Status Only** for devices for which you only need to monitor their status. The default polling interval for **Status Only** devices occurs every 12 hours and is configured in the **Status Only Poll Interval** field on the Administration > Options > **Status Polling** tab. **Status Only** devices do not support collection of statistics, FlexViews, Network Status Monitor, map links, or enforcement by ExtremeCloud IQ Site Engine. You can add a maximum of 10,000 **Status Only**

devices in ExtremeCloud IQ Site Engine, which do not count against your licensed device limit. The **Profile** determines the method by which the device is polled (SNMP or Ping).

Run Site's Add Actions

Run Site's Add Actions runs the actions configured for the site in which the device is contained. This function is active by default. Select the check box to disable this action. If you disable it, you can run this action manually, see Run Site's Add Actions in More Views.

NOTE:	To establish trust between ExtremeCloud IQ Site Engine and a 4000 series device you must have Cloud Connector and SSH enabled on the device.

OK

Select **OK** to add the device to ExtremeCloud IQ Site Engine and close the **Add Device** window.

Apply

Select **Apply** to add the device to ExtremeCloud IQ Site Engine and keep the **Add Device** window open to add additional devices.

Close

Select **Close** to close the **Add Device** window.

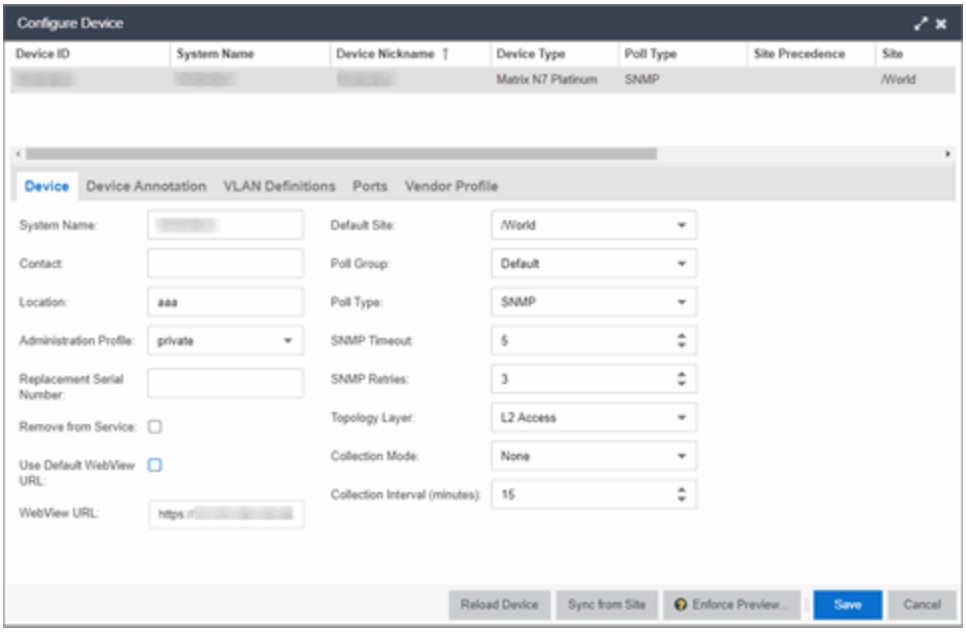
Configure Device

Use this window to configure information for an existing device. From this window you can edit basic information about the device, the device annotation, configure actions for the device, add or remove ports for the device, and configure VLANs for the device.

To access this window:

1. Open the **Network** > **Devices** tab.
2. Select the **Devices** sub-tab.
3. Select the **Menu** icon (☰) or right-click on a device.
4. Select **Device** > **Configure Device**.

This window is also accessible by selecting the Configure Device button on the Discovered and Site tabs.



When you first open the window, the **Device** tab opens.

The **Configure Device** window contains the following tabs:

- Device
- Device Annotation
- VRF Definition
- VLAN Definition
- CLIP Addresses
- Fabric Connect
- Services
- LAG
- Ports
- ZTP+ Device Settings
- Flow Sources
- Vendor Profile

Additionally, Buttons at the bottom of the window allow you to perform different actions.

Device

The **Device** tab displays basic information about the device.

System Name

The system name of the device. This is displayed in the **Network** > **Devices** tab tree when **Device Tree Name Format** is set to **System Name** in the **Local Settings** window.

Contact

Allows you to specify contact information for the person maintaining the device. Additionally, enter a backslash "/" between contacts to create a device group in a tiered tree structure. For example, to move the device into a device group called "John's Devices" within a device group called "Quality Assurance Testing", enter **Quality Assurance Testing/John's Devices** in this field.

Location

The physical location of the device. Additionally, enter a backslash "/" between locations to create a device group in a tiered tree structure. For example, to move the device into a device group called "London" within a device group called "Europe", enter **Europe/London** in this field.

Administration Profile

Use the drop-down list to select the access profile that gives the Discover tool administrative access to the devices you wish to discover. To create or edit a profile, use the **Profiles** tab.

Replacement Serial Number

Enter the number of the device replacing this device if **Remove from Service** is selected. When entered, ExtremeCloud IQ Site Engine restores the most recent archive of the device removed from service.

Remove from Service

Select this check box if the device is being removed from the network. ExtremeCloud IQ Site Engine will continue to monitor the device when Remove from Service is selected. When a replacement device is ready, continue the RMA process by adding the replacement device's serial number, shutting down the device to be removed, and starting the replacement device.

NOTE: A complete list of devices for which **Remove from Service** is selected is available via the Removed from Service Devices report on the **Reports** tab.

Use Default WebView URL

Select the check box to use the default WebView URL to access the device. The default WebView URL is provided by ExtremeCloud IQ Site Engine based on the vendor profile configured for the device.

WebView URL

Enter the WebView URL you want to use to access the device, if you do not want to use the default WebView URL.

NOTES: The option for editing the device Web View URL is available only after the device is onboarded to ExtremeCloud IQ Site Engine.

When modifying a device for the first time, the WebView URL is the default `http://%IP`. The `%IP` macro is replaced with the device's actual IP when Launch WebView is attempted.

If the `%IP` macro is present in the default WebView URL, it will be replaced with the device's actual IP Address when WebView is attempted.

For bulk edits on multiple devices, a valid WebView URL with the `%IP` macro is mandatory, so that `%IP` macro can be replaced with the actual IP Address of the device on which the WebView was attempted.

REST calls to the device will use the protocol (HTTP/HTTPS) and port configured in the WebView URL.

For ExtremeXOS/Switch Engine devices, the default WebView URL (`http://%IP%`) instructs ExtremeCloud IQ Site Engine to use HTTP to communicate with the device. You must override the default WebView URL to communicate with the device via HTTPS, and optionally include a non-standard port (for example, `https://%IP%:8443` - where 8443 is the non-standard port number in use).

Default Site

Use the drop-down list to select the map to which the device is associated. For additional information, see the Maps Overview topic.

Poll Group

Use the drop-down list to select a Poll Group for the discovered devices. ExtremeCloud IQ Site Engine provides three distinct poll groups (configured in the Status Polling view of the **Options** tab) that each specify a unique poll frequency. When you save newly discovered devices to the database, they are polled with the poll group specified here. If you save discovered devices that already exist in the database, the poll group specified here overwrites the poll group currently being used in the database.

NOTE: Poll Group is not used if you set the Poll Type to **Not Polled**. To use Poll Group, select a Poll Type other than Not Polled.

Poll Type

Use the drop-down list to select the Poll Type for devices:

- Select **Not Polled** if you do not want to poll the devices.
- Select **Ping** for the **Poll Type** if the **Profile** for the IP Range is also set to **Ping**.

  NOTE: On a Windows platform, device operational status cannot be determined for devices with their **Poll Type** set to **Ping** unless you are logged on and running ExtremeCloud IQ Site Engine as a user with Administrative privileges.

- Select **SNMP** to poll the device using SNMP. The SNMP version (SNMPv1 or SNMPv3) is determined by the Profile specified for the IP Range.
- Select **Maintenance** if you do not want to poll the devices temporarily. Using this **Poll Type** allows you to search for devices set to **Maintenance** to change them back to their regular **Poll Type** after maintenance on the device is complete.
- Select **ZTP+** for devices managed by ZTP+ and created through the ZTP+ process. When the **Poll Type** is **ZTP+**, ExtremeCloud IQ Site Engine does not initiate a poll, instead ExtremeCloud IQ Site Engine receives a message from the device or Fabric Manager messages to determine the status.

  For example, if ExtremeCloud IQ Site Engine does not receive a message from a device or Fabric Manager for three times the amount of time defined in the **Poll Interval** for the **Poll Group** of the device, then the **Status** is **Contact Lost**. When ExtremeCloud IQ Site Engine receives a message from the device, the **Device Status** is **Contact Established**.
- **Status Only** indicates a device for which you only need to monitor its status. This **Poll Type** is only displayed if the device was configured as **Status Only** when first added to ExtremeCloud IQ Site Engine.

  The default polling interval for **Status Only** devices occurs every 12 hours and is configured in the **Status Only Poll Interval** field on the Administration > Options > **Status Polling** tab. **Status Only** devices do not support check box of statistics, FlexViews, Network Status Monitor, or enforcement via ExtremeCloud IQ Site Engine. You can add a maximum of 10,000 **Status Only** devices in ExtremeCloud IQ Site Engine, which do not count against your licensed device limit.

  NOTE: You cannot change the **Poll Type** of an existing device to **Status Only**. To change the **Poll Type** of a device that currently exists in ExtremeCloud IQ Site Engine to **Status Only**, delete the device, add the device in ExtremeCloud IQ Site Engine via the **Add Devices** window, and select the **Poll Status Only** check box.

The options available in the Poll Type drop-down list vary depending on the method used to add the device:

- If device is added via ZTP+, **Not Polled**, **Ping**, **SNMP**, **Maintenance**, and **ZTP+** are available as **Poll Type** options. After changing the **Poll Type** to an option other than **ZTP+**, **ZTP+** is no longer be available. To select **ZTP+**, delete the device and add it via the ZTP+ process.
- If device is added using SNMP, **Not Polled**, **Ping**, **SNMP**, and **Maintenance** are available as **Poll Type** options.
- If device is added using **Ping**, **Not Polled**, **Ping**, **SNMP**, and **Maintenance** are available as **Poll Type** options.
- If device is added as **Status Only** (Ping or SNMP), then **Poll Group** and **Poll Type** options are not available.

Use Global SNMP Settings

Select the check box to use the global SNMP settings values from Administration > Options > SNMP > Configuration for the device.

When enabled, the SNMP Timeout and SNMP Retries fields and values are disabled.

SNMP Timeout

The amount of time that ExtremeCloud IQ Site Engine waits before re-trying to contact the device. The value for this setting must be between 1 and 60 seconds.

The **Use Global SNMP Settings** must be disabled for the SNMP Timeout value to apply to the device.

NOTE: When SNMP requests are redirected through the server, all SNMP timeouts are extended by a factor of four (timeout X 4) to allow for the delays incurred by redirecting requests through the server.

SNMP Retries

The number of attempts ExtremeCloud IQ Site Engine makes to contact a device after an attempt at contact fails. The value for this setting must be between 0 and 10 tries.

The **Use Global SNMP Settings** must be disabled for the SNMP Retries value to apply to the device.

Topology Layer

The layer and networking attributes for the device.

Collection Mode

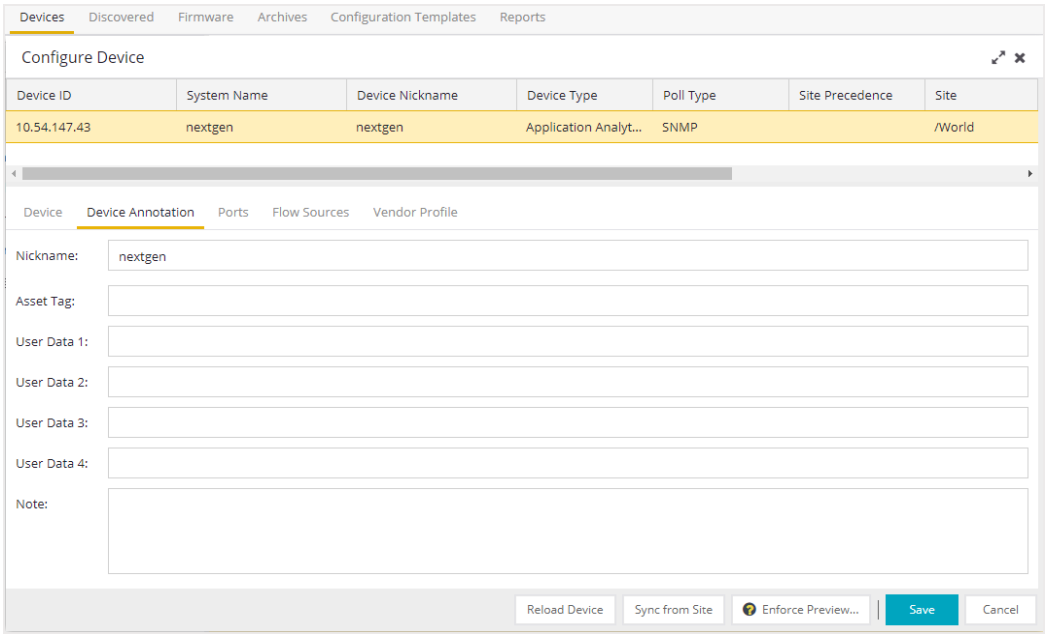
Select **None**, **Threshold Alarms**, or **Historical** from the check box Mode drop-down menu to indicate the mode to collect device statistics.

Collection Interval (minutes)

Select the interval at which device and statistics are collected. Extreme sets a minimum check box interval of five minutes and a maximum of 1440 minutes (24 hours).

Device Annotation

The **Device Annotation** tab allows you to add user-defined information about the device. Asset tag, User Data 1-4, and Device Note information saved on this tab is shared with ExtremeCloud IQ.



Nickname

The user-defined nickname for the selected device. The device nickname, which is used only by ExtremeCloud IQ Site Engine and is not stored on the device, displays when you select Nickname in the **Name Format** section on **Administration > Options tab**.

Asset Tag

A unique asset number assigned to a device for inventory tracking purposes.

User Data

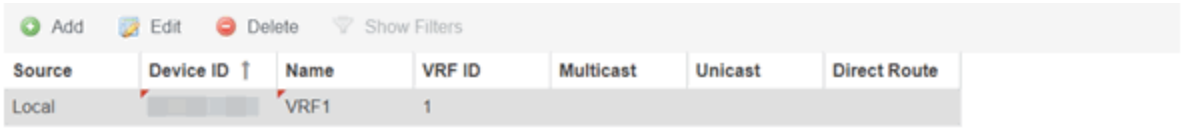
The user-defined information displayed in the devices table in the **User Data** columns. Additionally, enter a backslash "/" between user data to create a device group in a tiered tree structure. For example, to move the device into a device group called "Dorm 1" within a device group called "Campus", enter **Campus/Dorm 1** in this field.

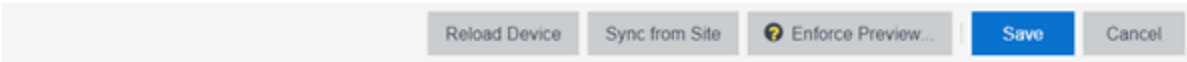
Notes

Additional user-defined information displayed in the devices table in the **Notes** column.

VRF Definition

The **VRF Definition** tab allows you to configure VRFs on the device. To add a VRF, select the **Add** button. You can remove a VRF by selecting the **Delete** button.





Source

Indicates the location from which the VRF is inherited. The VRF can be inherited from a site, locally configured on the device itself, or can be excluded.

NOTE: Selecting **Exclude** indicates you are excluding an inherited configuration. VRF configurations locally defined on the device and are not cannot be excluded. You can only select **Exclude** for configurations inherited from a Site (or a Service Application).

Device ID

Displays the IP address or name of the device.

Name

Displays the name of the VRF.

VRF ID

Displays the IP address or name of the device.

Multicast

Select to indicate the service sends IP packets to a group of hosts on the network.

Unicast

Select to indicate the service sends IP packets to a single recipient on the network.

Direct Route

Select to indicate the service sends IP packets directly to another device without going through a third device.

VLAN Definition

The **VLAN Definition** tab allows you to configure VLANs on the device.

The **VLAN Definition** tab also has the following buttons:

- **Add** - Use this button to add a VLAN.
- **Add Range** - Use this button to add VLANs in a group instead of manually adding and editing one entry at a time. For more information, see Fabric Assist.
- **Edit** - Use this button to you to change the configuration of a VLAN.
- **Delete** - Use this button to remove a VLAN.
- **Enable Pruning** - Use this button to prevent VLANs with no egress from being enforced to a device. For more information, see Fabric Assist.



Source

Indicates the location from which the VLAN is inherited. The VLAN can be inherited from a site, locally configured on the device itself, or can be excluded.

NOTE: Selecting **Exclude** indicates you are excluding an inherited configuration. VLAN configurations locally defined on the device and are not cannot be excluded. You can only select **Exclude** for configurations inherited from a Site (or a Service Application).

Name

Displays the name of the VLAN.

VID

Indicates the VLAN ID for the VLAN. A unique number between 1 and 4094 that identifies a particular VLAN. VID 1 is reserved for the Default VLAN.

VRF ID

Displays the ID number of the VRF associated with the VLAN.

IP Address

Indicates the IP address of the VLAN.

NOTE: IP Address provisioning is only supported on Fabric Engine devices.

Mask

Indicates the IP address mask.

Secondary IPs

Indicates the secondary IP addresses of the VLAN. Up to 32 secondary IPs are supported for each VLAN in the GRT or any VRF.

NOTE: Secondary IP Address provisioning is only supported on Fabric Engine devices.

Multicast
Select to indicate the service sends IP packets to a group of hosts on the network.

IGMP Version
Indicates which version of IGMP is utilized on the port (Version 1 or Version 2).

IGMP Querier
Indicates whether the device has sent IGMP queries to solicit VLAN membership information from other devices.

Querier Enable
Indicates whether an IGMP Query has been enabled.

Virtual Routing
Displays the version of VRRP the default gateway is using:

- **NONE** — Virtual routing is not configured on the VLAN.
- **VRRPv2** — VRRP version 2 is configured on the VLAN. VRRP version 2 only supports IP addresses in IPv4 format.
- **VRRPv3** — VRRP version 3 is configured on the VLAN. VRRP version 3 supports IP addresses in both IPv4 and IPv6 formats.
- **DvR** — DvR is configured on the VLAN. There are several requirements that must be met to configure DvR on a VLAN, including:
  - The VLAN must have an IP address and prefix.
  - The DvR IP address must be IPv4.
  - The DvR IP address must fall within the VLAN's subnet.
  - The DvR IP address cannot be reused across multiple VLANs on the device.
  - The VLAN must have an L2VSN associated with it.
  - If the VLAN is using on a non-zero VRF ID, the VLAN must also have:
    a. An L3VSN associated with the VRF.
    b. The VRF must have the unicast option enabled.
  - Devices participating in DvR as controllers must have non-zero IPv4 ISIS Source Addresses.
  - Devices participating in DvR must have IPv4 Shortcuts and Multicast enabled.
- **RSMLT** — Routing Redundancy Method is configured on the VLAN. RSMLT requires that a Virtual IST is configured. If the device is not configured as a vIST pair, **RSMLT** can be selected, but the feature is not active. Once the vIST is configured, RSMLT becomes active.

NOTES : Virtual Routing is only supported on Fabric Engine devices.

Fabric Engine devices support a new "dvr-one-ip" feature in the 8.2 release that allows you to share an IP address between a VLAN and its DvR interface. ExtremeCloud IQ Site Engine currently does not support the "dvr-one-ip" feature and cannot read or enforce configurations of this type. Configure Fabric Engine device IP addresses on VLANs and their DvR interfaces through the **VLAN Definitions** tab.

Virtual Routing Enable
Indicates whether virtual routing is enabled for the VLAN.

Virtual Routing Address
The IP address for the virtual routing interface. The Virtual Routing address must be in the same subnet as the VLAN subnet address.

VRRP ID
An identifier devices use to determine peer devices that participate in a VRRP (Virtual Routing Redundancy Protocol) virtual routing interface.

VRRP Priority
A value used by VRRP peers to determine the role of each of the devices in the VLAN. The default value is **100**. The device with the largest value is assigned the role of Controller. For example, in a VLAN with two routers, one with a **VRRP Priority** of **200** and one with a **VRRP Priority** of **100**, the router with a **VRRP Priority** of **200** becomes the Controller. In the event of identical priority numbers, the devices use the MAC address to determine priority.

VRRP Backup Master
This option determines if the backup router is able to forward traffic independently outside of the VLAN (enabled), or must forward the traffic to the Controller router before it is forwarded outside of the VLAN (disabled).

VRRP Advertisement Interval
Indicates frequency (in seconds) that protocol packets are sent from the virtual router in the VLAN.

VRRP Hold Down Timer
Indicates the amount of time (in hundredths of a second) that the backup router waits for the primary router to respond before it becomes the primary router.

DHCP Relay
Indicates whether a Dynamic Host Configuration Protocol relay server is enabled for the VLAN. A DHCP relay receives and converts a DHCP broadcast message to dynamically assign an IP address to a device on the network.

DHCP Relay Servers

The IP addresses of the DHCP relay servers for the VLAN.

NOTE: Select **Manage** to open the **Manage DHCP Relay Servers** window, where you can add or delete DHCP relay servers.

DHCP Snooping

Indicates whether DHCP snooping is enabled for the VLAN. DHCP Snooping is a Layer 2 security feature, that provides network security by filtering untrusted DHCP messages received from the external network causing traffic attacks within the network. DHCP Snooping is based on the concept of trusted versus untrusted switch ports. Switch ports configured as trusted can forward DHCP Replies, and the untrusted switch ports cannot. DHCP Snooping acts like a firewall between untrusted hosts and DHCP servers.

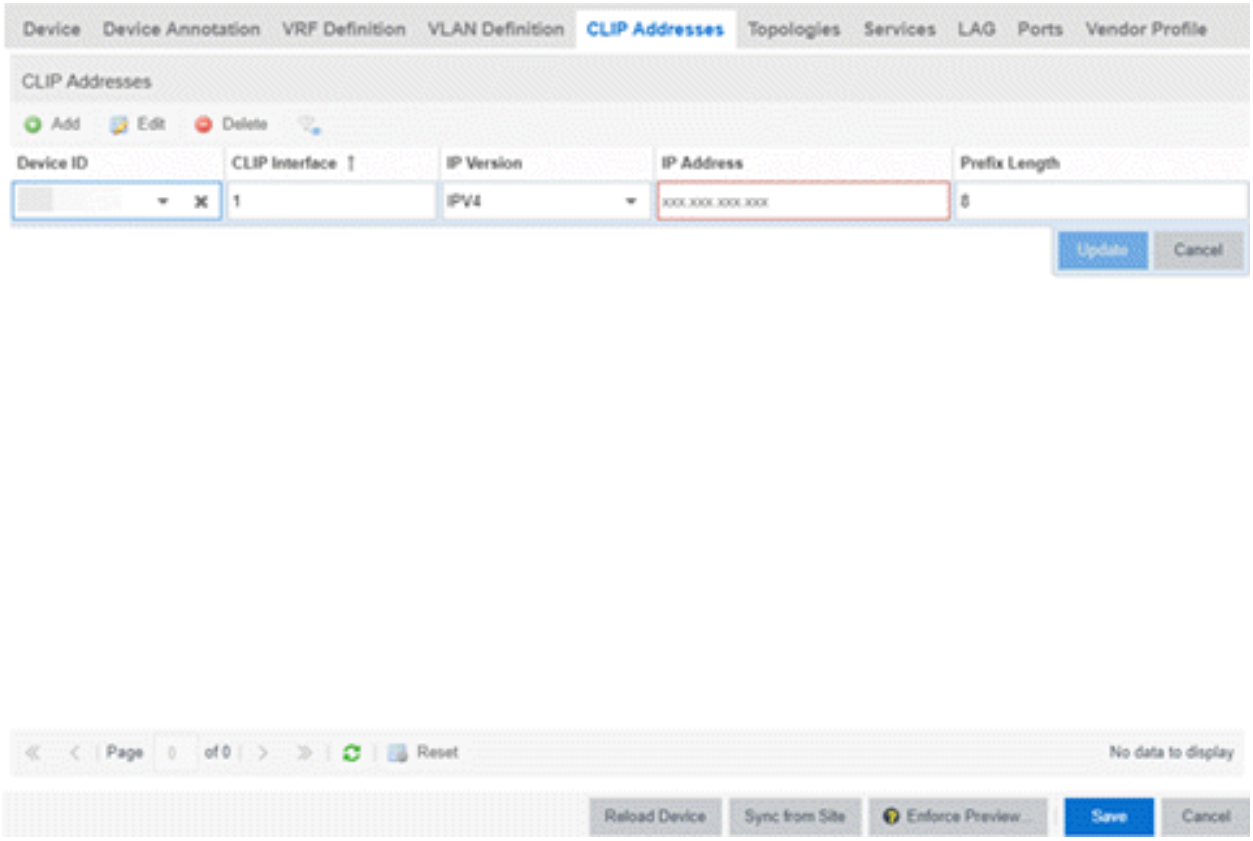
ARP Inspection

Indicates whether ARP inspection is enabled. Dynamic ARP Inspection (DAI) is a security feature that validates ARP packets in the network. Without DAI, a malicious user can attack hosts, switches, and routers connected to the Layer 2 network by poisoning the ARP caches of systems connected to the subnet, and intercepting traffic intended for other hosts on the subnet. DAI prevents these attacks by intercepting, logging, and discarding the ARP packets with invalid IP to MAC address bindings. The switch dynamically builds the address binding table from the information gathered from the DHCP requests and replies when DHCP Snooping is enabled. The switch pairs the MAC address from the DHCP request with the IP address from the DHCP reply to create an entry in the DHCP binding table. When you enable DAI, the switch filters ARP packets on untrusted ports based on the source MAC and IP addresses seen on the switch port. The switch forwards an ARP packet when the source MAC and IP address matches an entry in the address binding table. Otherwise, the switch drops the ARP packet.

NOTE: **DHCP Snooping** must be enabled to use **ARP Inspection**.

CLIP Addresses

Use the **CLIP Addresses** tab to add, edit or delete IPv4 and IPv6 CLIP Addresses to your device.



NOTE: To use the CLIP address on non-DVR Leaf the "IP Shortcuts" must be enabled.

To use the CLIP address on DVR Leaf the "IP Shortcuts" must be disabled.

"IP Shortcuts" can be enabled or disabled from the **Fabric Connect > Fabric Features** tab or the assigned Topology Definition.

VRF ID

The VRF for the CLIP address.

Device IP

The IP address of the device to which the CLIP address is assigned.

CLIP Interface

The interface ID for the CLIP address.

IP Version

Indicates the IP Address: IPv4 or IPv6

IP Address

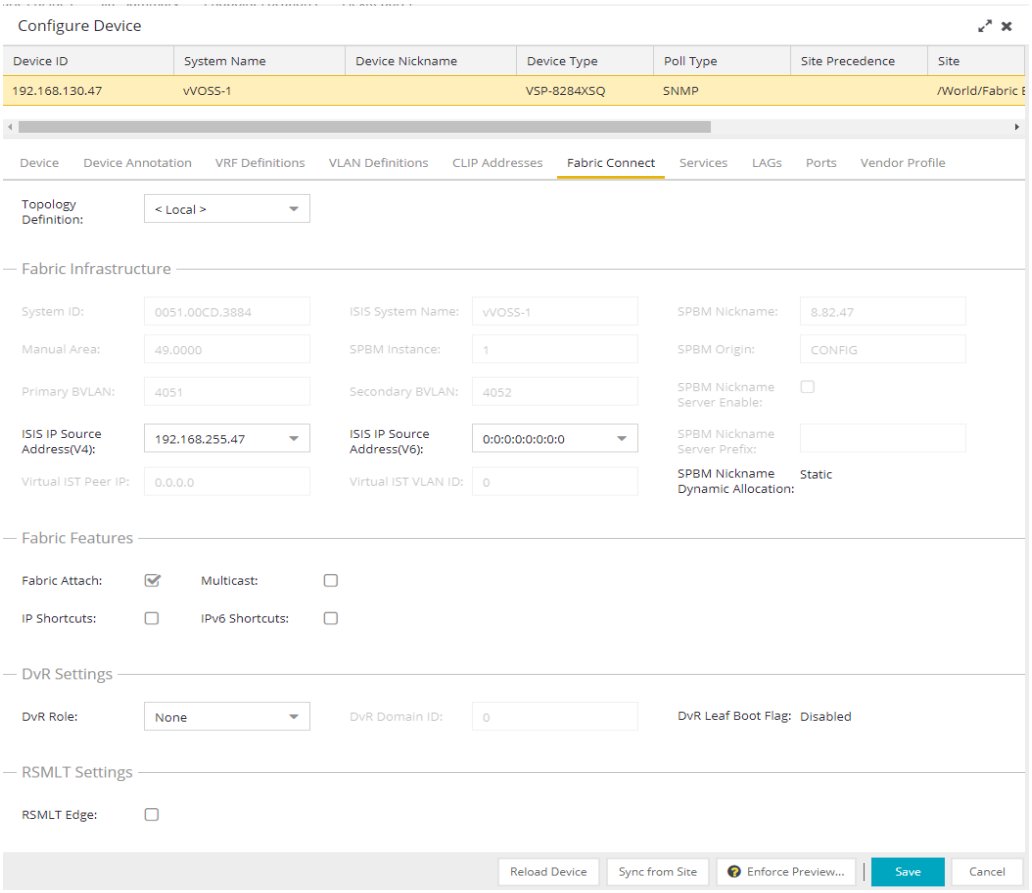
The IP address associated with the selected interface (VLAN, BROUTER or MGMT).

Prefix Length

Displays the number of digits that comprise the IP Address prefix. Prefix length for IPv4 Addresses is between 8 and 30 digits, and the prefix length for IPv6 addresses is between 8 and 128 digits.

Fabric Connect

The **Fabric Connect** tab allows you to select and configure Fabric Connect features to devices in your network.



Topology Definition

Select the Topology Definition that applies to the device. The Topology Definitions available in the drop-down list are configured in the **Topology Definition** tab.

- **None** – No Fabric Connect configuration on the device. If you select **None** for a device that is configured for Fabric Connect, that configuration is removed from ExtremeCloud IQ Site Engine when you select Save, and from the device when you enforce the change.
- **Local** – ExtremeCloud IQ Site Engine uses the Fabric Connect settings configured locally to enforce to the device.

- **Disabled** - The Fabric Connect configuration is applied to the device, but ISIS is disabled, which allows the user to take a device out of service without removing all its configuration.
- **Topology Definition** - The Topology Definition that has been specified for the site to which the device is assigned.

System ID

The system-defined fabric service identifier assigned to the device. The default is the MAC address for the device. This field is editable only if Topology Definition is disabled.

Manual Area

The IS-IS Manual Area in xx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx format (1-13 bytes). This information is configured on the **Sites > Topology Definition** tab. This field is editable only if Topology Definition is disabled.

Primary BVLAN

The Primary Backbone VLAN. This information is configured on the **Sites > Topology Definition** tab. This field is editable only if Topology Definition is disabled.

ISIS IP Source Address (V4)

The IPv4 address the device uses to transmit ISIS traffic to other fabric devices. The address must be unique within the fabric. This field is editable when **Topology Definition** is set to either Local or Disable, or a user-defined topologydefinition.

Virtual IST Peer IP

Virtual InterSwitch Trunk (IST) provides the ability to dual-home hosts, servers, and other network devices to a pair of Multi-Chassis Link Aggregation (MC-LAG) enabled devices. Virtual IST creates a virtualized channel through the SPBM cloud, and this channel connects two SMLT devices to form a virtualized cluster. The peer IP address identifies the other peers. It cannot be edited from this interface.

ISIS System Name

The system name of the device. This field is editable only if Topology Definition is disabled.

SPBM Instance

The system-defined identifier for the Fabric Connect configuration on the device. The default value is 1.

Secondary BVLAN

The Secondary Backbone VLAN. This information is configured on the **Sites > Topology Definition** tab. This field is editable only if Topology Definition is disabled.

ISIS IP Source Address (V6)

The IPv6 address the device uses to transmit ISIS traffic to other fabric devices. The address must be unique within the fabric. This field is editable when **Topology Definition** is set to either Local or Disable, or a user-defined Topology Definition.

Virtual IST VLAN ID

Virtual IST provides the ability to dual-home hosts, servers, and other network devices to a pair of MC-LAG enabled devices. Virtual IST creates a virtualized channel through the SPBM cloud, and this channel connects two SMLT devices to form a virtualized cluster. The VLAN ID identifies the communication channel between the peers. It cannot be edited from this interface.

SPBM Nickname

A value that other fabric devices use to identify the device. The SPBM Nickname must be unique within the fabric. This field is editable only if Topology Definition is disabled.

SPBM Origin

This field indicates the source of the SPBM configuration because it cannot be added from ExtremeCloud IQ Site Engine. If it is set to Config, it means the device is the source of the SPBM configuration. If it is set to Dynamic, it means that the SPBM configuration was provided via AutoSense.

SPBM Nickname Server Enable

This enables a Fabric Engine device to behave like a the Nickname Server. You can enable this function when **Topology Definition** is set to Local, Disable, or a user-defined topology definition, and **SPBM Nickname Dynamic Allocation** is set to Dynamic.

SPBM Nickname Server Prefix

Set the prefix for the Nickname Server. This is the 1-byte "x.y" portion of the larger "1.23.45" nickname format. This field can be edited when **SPBM Nickname Server Enable** is selected and the **Topology Definition** is Local, Disable, or a user-defined topology definition.

SPBM Nickname Dynamic Allocation

This field indicates where the device SPBM Nickname came from because it cannot be added from ExtremeCloud IQ Site Engine. Static means the **SPBM Nickname** was manually assigned by the user. Dynamic means the **SPBM Nickname** was allocated dynamically from another fabric node operating as an SPBM Nickname Server.

Fabric Attach

Select the check box to enable Fabric Attach server functions on a Fabric Connect device. Deselect the check box to disable Fabric Attach server functions.

NOTE: You can enable Fabric Attach on the following devices:

Fabric Engine, ERS 49xx v5.9.2 and later, ERS 4850 v5.9.2 and later, and ERS 59xx series devices

IP Shortcuts

Select the check box to enable IPv4 Shortcuts for the device.

Multicast

Select the check box to enable Multicast for the device.

IPv6 Shortcuts
Select the check box to enable IPv6 Shortcuts for the device.

DvR Role
Select the DvR Role from the drop-down list:

- None - DvR (Distributed Virtual Routing) is not configured on the device.
- Controller - Indicates the device is one of the main devices participating in the DvR virtual routing interface.
- Leaf - Indicates the device is one of several edge devices within the DvR domain. DvR Role as Leaf requires the DvR Leaf Boot Flag Enabled.
- Global Backbone - Indicates the device is a standard Fabric Connect device and does not run the DvR protocol, but learns routes from DvR controllers in the fabric.

DvR Domain ID
Displays the identifying number for the DvR domain.

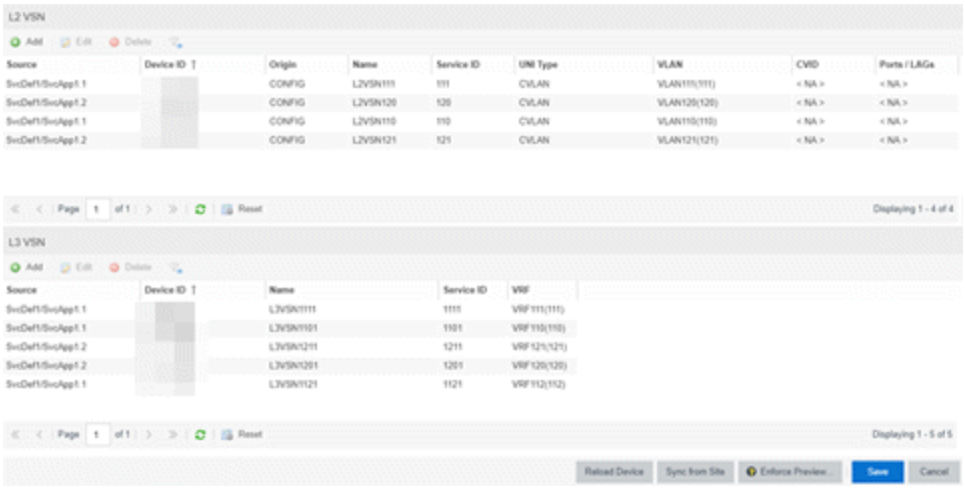
DvR Leaf Boot Flag
Indicates the DvR Leaf Boot Flag setting for the device. If the boot flag is Enabled, the DvR Role can be None or Leaf. If the boot flag is Disabled, the DvR Role can be None, Controller, or Global Backbone.

NOTE: You can use the system workflow to enable or disable the DvR Leaf Boot Flag for Fabric Engine Release 8.4 and earlier.

RSMLT Edge
Select this option to use the RSMLT Edge.

Services

The **Services** tab displays the services created within service applications and configured on the device. Use this tab to add new services to the device. Services may be inherited from a service definition or may be configured locally on the device.



L2 VSN

Source
The service application to which the Layer 2 service has been assigned.

Name
The name of the Layer 2 service.

UNI Type

The User-Network-Interface (UNI) of the fabric service. The following interface types are available:

- **Switched** — A VLAN-ID and a port (VID, port) mapped to a Layer 2 VSN I-SID. With UNI type, VLAN-IDs can be reused on other ports and mapped to different ISIDs.
- **Transparent** - A physical port maps to a Layer 2 VSN I-SID (all traffic through the port, 802.1Q tagged or untagged, ingress and egress maps to the I-SID).

  NOTE: All VLANs on a Transparent Port UNI interface now share the same single MAC learning table of the Transparent Port UNI I-SID.

- **CVLAN** — a platform customer VLAN-ID

VLAN
The customer VLAN-ID of the associated CVLAN UNI type

CVID
The customer VLAN-ID of the associated switched UNI port.

Management Service
Defines if the L2 VSN is used for switch management purposes.

AutoSense Service Type
Defines if the L2 VSN service is auto-assigned by the switch-level AutoSense detection. The following types are available:

- **AP Untagged** — If the AutoSense feature detects Access Point, then this service is automatically assigned to the port.
- **Camera Untagged** — If the AutoSense feature detects Camera then this service is automatically assigned to the port.
- **Voice Untagged** — If the AutoSense feature detects a VoIP device then this service is automatically assigned to the port.
- **Voice Tagged** — If the AutoSense feature detects a VoIP device then this service is automatically assigned to the port.

- **Proxy Switch Auth Tagged —** If the AutoSense feature detects a Fabric Attach switch capable of authenticating (ERS devices) then this service is automatically assigned to the port.
- **Proxy Switch No Auth Untagged —** If the AutoSense feature detects a Fabric Attach switch is not capable of authenticating (Switch Engine devices) then this service is automatically assigned to the port.
- **Proxy Switch Auth & Proxy Switch No Auth —** If the AutoSense feature detects any physical Fabric Attach switch (ERS/EXOS/Switch Engine device) then this service is automatically assigned to the port.
- **Data Untagged** — If the AutoSense feature does not detect a device type then this service is automatically assigned to the port.
- **None** — AutoSense is not related to this L2VSN service.

NOTE: Each AutoSense Service Type can only be used once on a switch. The switch cannot use two different service IDs with the same AutoSense Service Type.

AutoSense Service CVID

The AutoSense Service CVID value defines the 802.1q VLAN tag sent from the switch to the device. If the AutoSense Service Type is Voice Tagged or Proxy Switch Auth Tagged or Proxy Switch Auth & Proxy Switch No Auth then AutoSense Service CVID must be defined. The value range is 1-4094

Port Template

If the UNI Type is Switched or Transparent you can select from the Global Port templates to define the purpose of the port.

L3 VSN

Name

The name of the Layer 3 service.

Service ID

The ID number assigned to the service.

VRF

Select the virtual routing and forwarding definition included as part of the service.

Multi Cast

Select to indicate the service sends IP packets to a group of hosts on the network.

Unicast

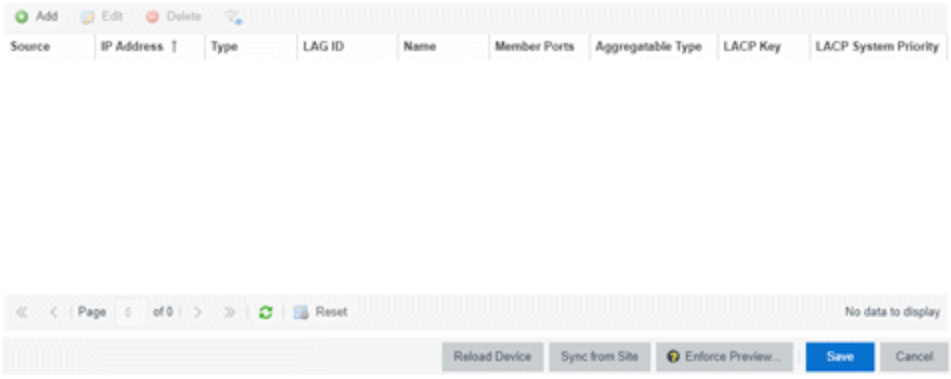
Select to indicate the service sends IP packets to a single recipient on the network.

Direct Route

Select to indicate the service sends IP packets directly to another device without going through a third device.

LAG

Use the **LAG** tab to configure LAGs and MLAGs (also known as MLTs and SMLTs, respectively). A LAG combines multiple network connections to increase the throughput beyond that of a single connection. An MLAG allows a device to send network traffic to two switches to improve network diversity, while only managing a single logical interface.



Source

Indicates the location from which the LAG is inherited. The LAG can be inherited from a site, locally configured on the device itself, or can be excluded.

NOTE: Selecting **Exclude** indicates you are excluding an inherited configuration. LAG configurations locally defined on the device and are not cannot be excluded. You can only select **Exclude** for configurations inherited from a Site (or a Service Application).

IP Address

Displays the IP address of the LAG.

Type

Displays the type of LAG, either LAG or MLAG.

LAG ID

Displays a system-defined ID number for the LAG.

Name

Displays a user-defined name for the LAG.

Member Ports

Displays the ports that are included in the LAG.

Aggregatable Type

Indicates whether the LAG is static or dynamic:

- Static — the LAG is static.
- LACP — the LAG is dynamic via LACP.

LACP Key

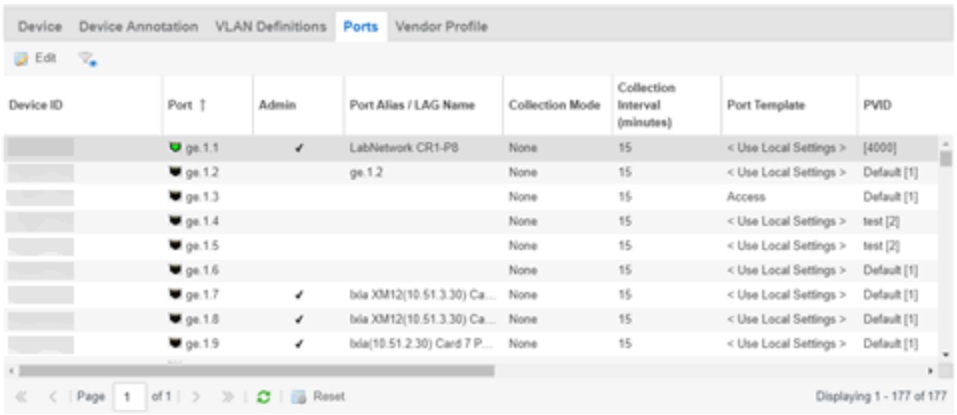
Displays the LACP key, which the LAG uses to ensure it only pairs with properly configured endpoints.

LACP System Priority

Displays the LACP priority, which ExtremeCloud IQ Site Engine uses to determine the probability network traffic uses the LAG. Valid values are between 1 and 65,535. The lower the value entered, the higher ExtremeCloud IQ Site Engine prioritizes the LAG.

Ports

The **Ports** tab allows you to edit information about the ports on a device.



Name

Enter the name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

Alias

Shows the alias (ifAlias) for the interface, if one is assigned.

Auto Negotiation

Displays whether auto negotiation is enabled or disabled on the port. If Auto Negotiation is enabled, multi-speed selections are enabled.

Speed

Displays the current speed of the selected port. Use the drop-down list to select the speed if auto negotiation is enabled on the port.

Duplex

Displays the current duplex mode for the selected port. Use the drop-down list to select the mode if auto negotiation is enabled on the port.

Collection Mode

Indicates the collection mode (Historical, Threshold Alarms, or None) which has been configured on the **Administration > Options > ExtremeCloud IQ Site Engine Collector > Port Collection** field, for port statistics collected for ports.

Collection Interval (minutes)

Indicates the frequency (in minutes) at which port statistics are collected. The poll interval is configured on the **Administration > Options > ExtremeCloud IQ Site Engine Collector > Port Collection** tab. The default poll interval set by ExtremeCloud IQ Site Engine is 15 minutes.

Port Template

Use the drop-down list to select a Port Template you define on the **Site** tab. Adding a device to a site allows you to select from the Port Templates defined for that site:

- **<Use Local Settings>** — Select this option if you do not want the port to inherit any settings from any defined Port Template.
- **Access** — Select this option if the port connects to user end-systems.
- **Interswitch** — You can also manually select this option if the port is used to connect to other switches. This option is selected by default if the port detects neighboring switches are configurable.
- **Management** — Select this option if the port is used to manage network traffic with ExtremeCloud IQ Site Engine.
- **AP** — Select this option if the port is used to connect with a networking device that allows a Wi-Fi device to connect to a wired network.
- **Phone** — Select this option if the port is used to connect to a telephone.
- **Router** — Select this option if the port is used to connect to a router.
- **Printer** — Select this option if the port is used to connect to a printer.
- **Security** — Select this option if the port is used to connect to a device or devices that have been configured with security or advanced security settings.
- **IoT** — Select this option if the port is used to connect to an additional wireless"smart" device.
- **Other** — Select this option if the port is used to connect to any other device.

PVID

Select the port's VLAN ID.

LAG

Select to indicate whether the port is part of an active link aggregation group (LAG).

LAG Details

Additional details about the LAG to which the port is assigned.

Authentication

Use the drop-down list to determine whether authentication is required to access the port:

- **None** — No authentication is required to access the port.
- **802.1X** — Select this option to require 802.1X authentication to access the port.
- **MAC Auth** — Select this option to require authentication based on the users MAC address.

VLAN Trunk

Automatically configures a port as a VLAN trunk when you check one box in the VLAN Trunk column. For more information, see Fabric Assist.

Tagged

Indicates the port's egress state is tagged. If you check the VLAN Trunk column, Fabric Assist automatically configures all the VLANs on the port as tagged. For more information, see Fabric Assist.

Fabric Enable

Indicates the fabric functionality is enabled on the port.

ExtremeCloud IQ Site Engine can extend FA functionality to ExtremeXOS/Switch Engine devices and provision them as FA Proxy devices. Select "Fabric Attach" or "" from the drop-down list to enable the port on a Fabric Engine device (acting as FA Server) to connect to an ExtremeXOS/Switch Engine device (acting as FA Proxy).

- **Fabric Attach** - Enable Fabric Attach server functionality on the port of a Fabric Engine device acting as a Fabric Attach server) to connect to an ExtremeXOS/Switch Engine device (acting as a Fabric Attach proxy).
- **Fabric Attach and Switched UNI** - Enable Fabric Attach server functionality on the port of a Fabric Engine device acting as a Fabric Attach server) to connect to an ExtremeXOS/Switch Engine device (acting as a Fabric Attach proxy). When selecting this option, the port is configured for both features, but only one feature is active at any one time.
- **Auto Sense** - Select **Auto Sense** on the port of a Fabric Engine device to enable the port to automatically sense and configure automatically sense and configure the appropriate Fabric settings for the port. These settings include the following:
  - PVID
  - VLAN Trunk
  - Tagged
  - Untagged
  - Fabric Mode

- Fabric Auth Type
- Fabric Auth Key
- Fabric Connect Drop STP-BPDU
- BPDU Guard
- Authentication

NOTE: If **Fabric Enable** is **Auto Sense** the Fabric settings listed above are not configurable.

Fabric Auth Type
Indicates the fabric authentication type used on the port.

Fabric Auth Key
Indicates the fabric authentication key used for the port.

Fabric Connect Drop STP-BPDU
Indicates the fabric-enabled port drops Spanning Tree Protocol BPDUs.

Policy
The policy assigned to the selected port.

Tagged
Select to indicate the port's egress state is tagged.

Untagged
Select to indicate the port's egress state is untagged.

Node Alias
Select to enable the node alias function on the port. The node alias settings are automatically enabled if Access Control is enabled on the device.

Span Guard
Select to enable Span Guard, which allows the device to shut down a network port if it receives a BPDU (bridge protocol data unit). Enable this feature on network edge ports to prevent rogue STA-aware devices from disrupting the existing Spanning Tree.

Loop Protect
Select to prevent loop formation in a network with redundant paths by requiring ports to receive type 2 BPDUs (RSTP/MSTP) on point-to-point interswitch links.

- If the ports receive the BPDUs, the link's State becomes Forwarding.
- If a BPDU timeout occurs on the ports, its state becomes listening until a BPDU is received.

MVRP
Indicates that the Multiple VLAN Registration Protocol (MVRP) has been enabled for the port. If

MVRP has been enabled globally, interswitch ports are automatically enabled and access ports default to disabled.

SLPP

Indicates Simple Loop Prevention Protocol (SLPP) is enabled on the port. SLPP provides active protection against Layer 2 network loops on a per-VLAN basis. If an SLPP packet is received, the port is disabled for the amount of time configured in the **SLPP Timer** field.

NOTE: If **SLPP** is enabled, **SLPP Guard** is not available.

SLPP Guard

Indicates whether SLPP Guard is enabled on the port. Use SLPP Guard to provide additional loop protection to protect wiring closets from erroneous connections. SLPP Guard requires **SLPP** to be enabled. SLPP detects loops in an SMLT network. Because SMLT networks disable Spanning Tree (STP), Rapid Spanning Tree (RSTP), or Multiple Spanning Tree Protocol (MSTP) for participating ports, SLPP Guard provides additional network loop protection, extending the loop detection to individual edge access ports. SLPP Guard can be configured on MLT or LAG ports. If the edge switch with SLPP Guard enabled receives an SLPP-PDU packet on a port, SLPP Guard operationally disables the port for the configured timeout interval in the **SLPP Guard Timer** field and appropriate log messages and SNMP traps are generated. If the disabled port does not receive any SLPP-PDU packets after the configured timeout interval expires, the port automatically re-enables and generates a local log message, a syslog message, and SNMP traps, if configured.

NOTE: If **SLPP Guard** is enabled, **SLPP** is not available

SLPP Guard Timer

Indicates the amount of time after receiving an SLPP packet before the port is re-enabled.

DHCP Snooping

Specifies the trust factor of the port for DHCP Snooping. The agent at the switch determines if DHCP reply packets are forwarded based on the DHCP Snooping mode of the VLAN and the trusted state of the port. If the value is "Trusted", the agent trusts the device on the port. If the value is "Untrusted", the agent does not trust the device on the port.

ARP Inspection

Dynamic ARP Inspection (DAI) is a security feature that validates ARP packets in the network. Without DAI, a malicious user can attack hosts, switches, and routers connected to the Layer 2 network by poisoning the ARP caches of systems connected to the subnet and intercepting traffic intended for other hosts on the subnet. DAI can prevent attacks by intercepting, logging, and discarding the ARP packets with invalid IP to MAC address bindings. The switch dynamically builds the address binding table from the information gathered from the DHCP requests and replies when DHCP Snooping is enabled. The switch pairs the MAC address from the DHCP request with the IP address from the DHCP reply to create an entry in the DHCP binding table. Values are "Trusted" and "Untrusted".

Source Guard

IP Source Guard (IPSG) is a Layer 2 port-to-port feature that works closely with DHCP Snooping. IPSG can prevent IP spoofing by allowing only IP addresses obtained using DHCP Snooping. When you enable IPSG on an untrusted port with DHCP Snooping enabled, an IP filter is automatically created or deleted for that port based on the information stored in the corresponding DHCP Snooping binding table entry. When a connecting client receives a valid IP address from the DHCP server, the filter installed on the port allows traffic only from that assigned IP address. If the value is "Disabled" the Source Guard is disabled. If the value is "IP" the IP Source Guard feature is enabled.

VPEX Type

Indicates how this port is used to connect a port extender to a controlling bridge or another port extender:

- **Cascade** — Traffic leaving this port is moving away from the controlling bridge.
- **Uplink** — Traffic leaving this port is moving toward the controlling bridge.
- **None** — The port is not included in connecting the extended bridge components.

NOTE: If the **VPEX Type** is **Cascade** or **Uplink**, you are unable to configure **PVID**, **Tagged** VLANs, and **Untagged** VLANs.

PoE Enable

Indicates that power over ethernet (PoE) is enabled for the port.

PoE Priority

Indicates the priority of PoE for the port; **LOW**, **HIGH**, or **CRITICAL**.

Update

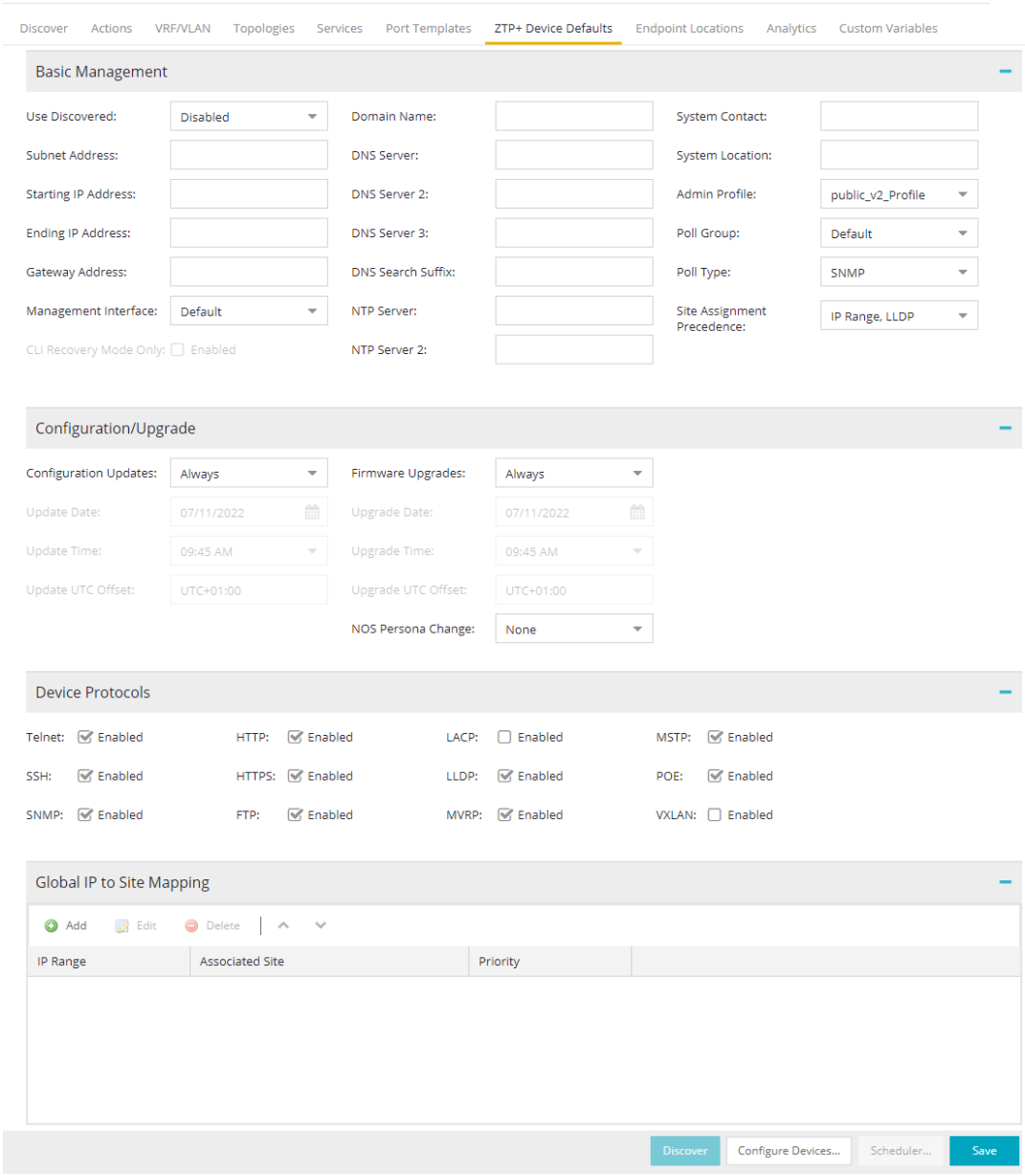
Select Update to save any changes made to the device configuration.

Cancel

Select Cancel to close the window and discard any changes.

ZTP+ Device Settings

The **ZTP+ Device Settings** tab contains basic information about an existing device AFTER the device was discovered by ExtremeCloud IQ Site Engine via ZTP+.



Basic Management

Serial Number

Enter the serial number assigned to the device.

Use Discovered

Use the drop-down list to select if ExtremeCloud IQ Site Engine assigns the IP address, IP address and Management Interface, or Management Interface to the ZTP+ device when it is discovered:

- **IP** — ExtremeCloud IQ Site Engine uses the **Discovered IP** assigned when the device was discovered. Select the **Management Interface** (the VLAN interface used to manage the device) manually.
- **IP and Management Interface** — ExtremeCloud IQ Site Engine uses the **Discovered IP** and the **Management Interface** that were assigned when the device was discovered.
- **Management Interface** — ExtremeCloud IQ Site Engine uses the **Management Interface** that was defined when the device was discovered. Enter the IP address and subnet, Gateway Address, Domain Name, and DNS Server in the tab (along with any of the optional fields) and then save.
- **Disabled** — Configure the IP address and subnet, Gateway Address, Domain Name and DNS Server in the tab (along with any of the optional fields) and then save.

IP Address / Subnet

Enter the **IP Address / Subnet** for the ZTP+ devices being discovered.

Gateway Address

Enter the **Gateway Address** for the ZTP+ devices being discovered.

Management Interface

Select the interface the device uses for Management and assigns the device IP to that interface. Options are: **VLAN, Out-Of-Band, Management Service, CLIP Address**. If the option **Management Service** is selected, then one of the L2 VSN services must have **Management Service** selected, and the management IP applied to the Management Service. If the option **CLIP Address** is selected, then during the ZTP+ onboarding you should define the CLIP address in the GlobalRouter VRF, and mark it as Address Type MGMT. Then the MGMT CLIP address will be used for the switch management.

CLI Recovery Mode Only

Select the check box to disable the CLI account while the device is able to communicate with ExtremeCloud IQ Site Engine. If connectivity between the device and ExtremeCloud IQ Site Engine is lost, the device enables the CLI account defined in the profile so the user can gain local access. When connectivity between the device and ExtremeCloud IQ Site Engine is reestablished, the CLI account is disabled again.

NOTE: Only devices managed using ZTP+ support this functionality.

Domain Name

Enter a value in the **Domain Name** field to configure the domain name on the ZTP+ devices being discovered.

DNS Server

The **DNS Server** field allows you to set the DNS server address on the ZTP+ devices associated with the site.

DNS Server 2

The **DNS Server 2** field allows you to set the secondary DNS server address on the ZTP+ devices associated with the site.

DNS Server 3

The **DNS Server 3** field allows you to set the tertiary DNS server address on the ZTP+ devices associated with the site.

DNS Search Suffix

The **DNS Search Suffix** field allows you add additional comma-separated entries to DNS search suffix list configured on the device. Support for the DNS search suffix is dependent on the device operating system and version. Refer to your device specifications to determine the maximum number of entries that you can add.

NTP Server

The **NTP Server** field allows you to set the NTP server address on the ZTP+ devices being discovered.

NTP Server 2

The **NTP Server 2** field allows you to set the secondary NTP server address on the ZTP+ devices associated with the site.

Configuration/Upgrade

Configuration Updates

Select the frequency for which ExtremeCloud IQ Site Engine checks for configuration updates for your ZTP+ enabled devices associated with the site.

Update Date

Select the date on which ExtremeCloud IQ Site Engine updates the configuration for your ZTP+ enabled devices associated with the site when you select **Scheduled** for **Configuration Updates**.

Update Time

Select the time at which ExtremeCloud IQ Site Engine updates the configuration for your ZTP+ enabled devices associated with the site when you select **Scheduled** for **Configuration Updates**.

Update UTC Offset

Select your time zone based on the number of hours you are offset from the Universal Time Coordinated.

Firmware Upgrades

Select the frequency for which ExtremeCloud IQ Site Engine checks for firmware upgrades for your ZTP+ enabled devices associated with the site.

Upgrade Date

Select the date on which ExtremeCloud IQ Site Engine upgrades the firmware for your ZTP+ enabled devices associated with the site when you select **Scheduled** for **Firmware Upgrades**.

Upgrade Time
Select the time at which ExtremeCloud IQ Site Engine upgrades the firmware for your ZTP+ enabled devices associated with the site when you select **Scheduled** for **Firmware Upgrades**.

Upgrade UTC Offset
Select your time zone based on the number of hours you are offset from the Universal Time Coordinated.

Device Protocols/Features

Telnet
Select the check box to enable Telnet access on the ZTP+ device.

SSH
Select the check box to enable SSH (Secure Shell) access on the ZTP+ device.

HTTP
Select the check box to enable HTTP (Hypertext Transfer Protocol) access on the ZTP+ device.

HTTPS
Select the check box to enable HTTPS (Hypertext Transfer Protocol Secure) access on the ZTP+ device.

NOTE: To enable HTTPS access, an SSL certificate must be configured on the device.

SNMP
Select the check box to enable SNMP (Simple Network Management Protocol) access on the ZTP+ device.

LACP
Select the check box to enable LACP (Link Aggregation Control Protocol) access on the ZTP+ device.

LLDP
Select the check box to enable LLDP (Link Layer Discovery Protocol) access on the ZTP+ device.

MSTP
Select the check box to enable MSTP (Multiple Spanning Tree Protocol) access on the ZTP+ device.

MVRP
Select the check box to enable MVRP (Multiple VLAN Registration Protocol) access on the ZTP+ device.

POE
Select the check box to indicate the ZTP+ devices being discovered for the site are electrically powered via the Ethernet cable.

VXLAN

Select the check box to indicate the ZTP+ devices being discovered for this site use VXLAN to tunnel Layer 2 traffic over a Layer 3 network.

NOTE: ZTP+ does not currently provision a Layer 3 network with which VXLAN operates. If your ZTP+ devices use VXLAN, the Layer 3 underlay network must be manually provisioned.

DvR Leaf

Select the check box to indicate the ZTP+ devices being discovered for the site operate in DvR Leaf mode. The DvR Leaf flag is enabled. Only devices running Fabric Engine support the DvR Leaf feature.

Flow Sources

The **Flow Sources** tab allows you to configure devices to act as flow sources for an ExtremeAnalytics engine.



Name

Displays the name of the flow source device.

IP

Displays the IP address of the flow source device.

Device Family

Displays the device family of the flow source device.

Port

Indicates the mirror port attached to the ExtremeAnalytics engine or used to create the GRE tunnel.

Source Ports

Displays the ports on which flow check box is enabled.

NOTE: Policy mirrors the first 15 packets of each flow received on the **Source Ports** to the ExtremeAnalyticsengine.

WLANs
Displays the WLANs of which the wireless controller being used as a flow source device is a member.

Tunnel
Indicates the device is configured to mirror flows using a GRE tunnel.

NOTE: If **Tunnel** is disabled, the ExtremeAnalytics engine must be directly attached to the flow source.

Tunnel IP
Displays the management IP address of the flow source device or the IP address of the loop-back interface on the device.

Add
Select **Add** to open a window from which you can select a device in ExtremeCloud IQ Site Engine to add as a flow source.

Remove
Select a flow source device in the table and select **Remove** to remove the device as a flow source.

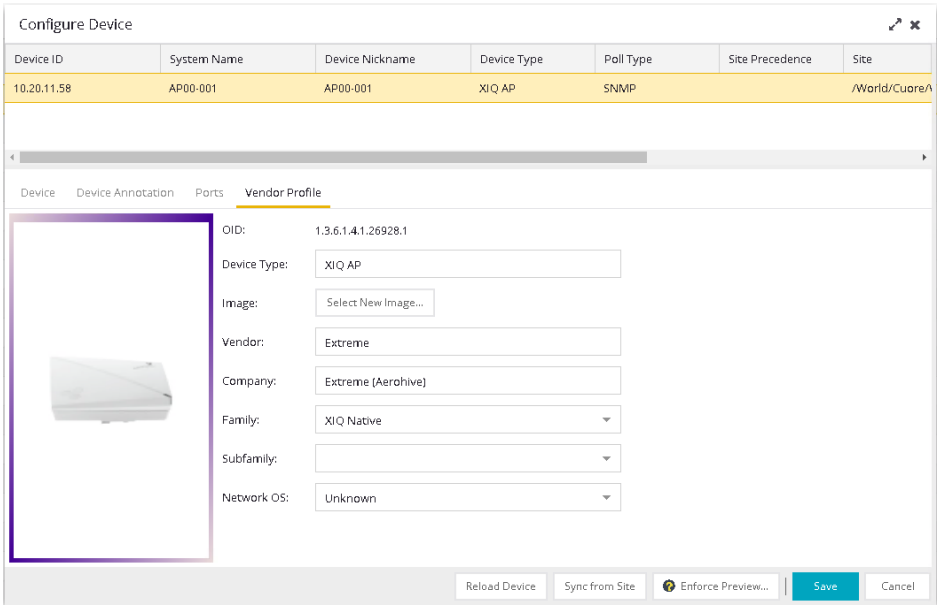
Edit
Select **Edit** to open a window from which you can change the configuration of a flow source device.

Test
Select **Test** to verify the GRE tunnel end-points can communicate.

NOTE: **Test** is only available if **Tunnel** is enabled.

Vendor Profile

Use the **Vendor Profile** tab to determine how devices are identified in ExtremeCloud IQ Site Engine.



OID

Displays the Object Identifier for the device.

Device Type

Displays the specific type of device.

NOTE: When **Device Type** is blank:

- ExtremeCloud IQ Site Engine cannot identify the device type, so the tab is named **New Vendor Profile** to allow you to optionally provide the device type details.
- If a device's **Vendor** is recognized, but ExtremeCloud IQ Site Engine does not have a profile for the device's unique **OID**, the **Device Type**, **Family** and **Subfamily** values are empty, but ExtremeCloud IQ Site Engine supplies the **Vendor** and **Company** values.
- If a **Device Type** is not recognized, and you leave the **Device Type** selection blank and subsequently upgrade to a version of ExtremeCloud IQ Site Engine with a Vendor Profile that recognizes the device type, ExtremeCloud IQ Site Engine supplies the properties of the Vendor Profile.
- If a Device Type is not recognized, and you customize the Device Type selection by entering the **Device Type, Image**, **Vendor**, **Company**, **Family**, **Subfamily**, and **Network OS** information, and subsequently upgrade to a version of ExtremeCloud IQ Site Engine with a Vendor Profile that recognizes the device type, the properties of the Vendor Profile are not updated and the customized device type data you entered is retained.

  To remove all user-defined Vendor Profile configurations and restore the default system configurations provided with the installed version of ExtremeCloud IQ Site Engine, select the **Restore to Defaults** button on the **Administration** > **Diagnostics** > **System** > **Vendor Profile Cache** tab. Selecting the **Restore to Defaults** button removes your customizations and any unknown device types and replaces them with the provided vendor profile data. If vendor profile mapping data still does not exist, selecting the **Restore to Defaults** button changes your customizations to "Unknown" and retains any unknown device types as "Unknown."
- You can use the drop-down menus to select the information or add it manually.
- You cannot use special characters when creating a new **Device Type**.

Image
Indicates the image used for the device in the Device View and Maps. Select the **Select New Image** icon to select a new image for the device type.

Vendor
Displays the vendor who sold the device.

Company
Displays the company that manufactures the device.

Family
Displays the group of devices to which the device belongs, known as the device family in ExtremeCloud IQ Site Engine.

Subfamily
Displays a smaller grouping to which the device belongs, if applicable.

Network OS
ExtremeCloud IQ Site Engine's classification of the Network Operating System installed on the device. This allows ExtremeCloud IQ Site Engine to provide the appropriate scripts and workflows on a device's Tasks submenu when the device's Network OS matches one of the Network Operating Systems defined for the script or workflow.

NOTE: ExtremeCloud IQ Site Engine displays **Unknown** for devices before their Network OS is determined via a script or workflow (for example, onboarding new devices or when Network OS Grouping has not been provided for the device type).

Buttons

Read Device
Select to read configuration information from the device to populate ExtremeCloud IQ Site Engine. **Read Device** reads the configuration (e.g. VLAN Definition, Ports, Port VLANs) from the device and reloads it in ExtremeCloud IQ Site Engine.

NOTE: Selecting **Read Device** removes all unsaved (or enforced) changes made in the **VLAN Definition** and **Ports** tabs and reloads the configuration from the device to those tabs.

Enforce Preview
Select to open the **Compare Device Configuration** window, from which you can view and compare your current configuration and the proposed new configuration. This window allows you to verify all of the changes you are making to your devices and then enforce those changes to the device. This button displays after making a change that affects the device.

Sync from Site
Select to copy the site's configuration from the site to ExtremeCloud IQ Site Engine's representation of the selected devices. The site's configuration will be applied to the device if

the device is assigned to the same site. The site's configuration settings that will override the device's settings are: device, device annotation, VRF definitions, VLAN definition, Fabric Connect, services, LAGs, and ports.

The Sync from Site feature applies the ZTP+ Device default settings (such as VRF definitions) if the ZTP+ Device confirmation dialog was set to **Yes** for the **Sync from Site** field.

You can use the **Enforce Preview** button to decide whether to save the settings to the device. (Some ExtremeCloud IQ Site Engine settings, like poll group and administration profile, will not be enforced to the device.)

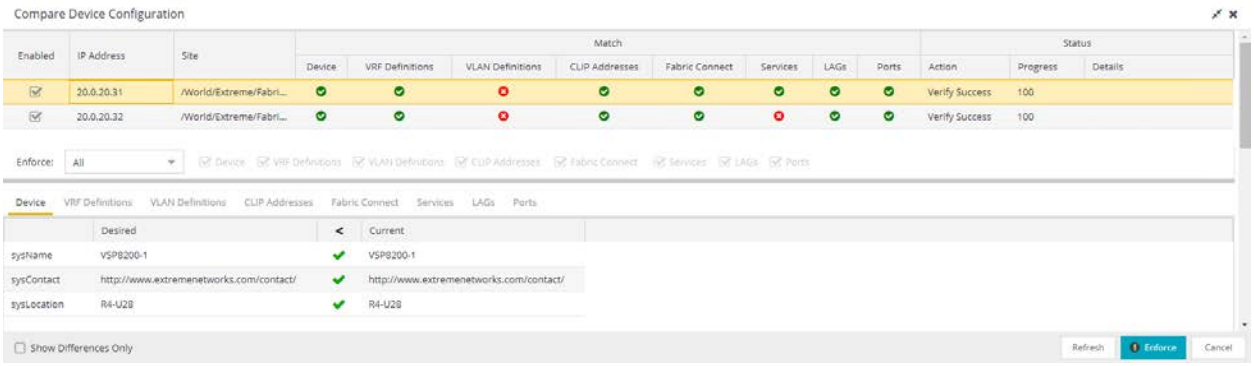
Save
Select to save any changes you make to a device in ExtremeCloud IQ Site Engine.

Cancel
Select to discard any unsaved changes and close the window.

Device Configuration Enforce Preview

This window allows you to preview changes you make to a device configuration and then enforce them to the device.

To access this window, select **Enforce Preview** in the **Configure Device** window.



The Compare Device Configuration window is divided into three sections:

- Device Details
- Enforce Options
- Device Configuration Detail Table

Device Details

The top of the window displays a list of the devices you selected to verify. Select a device in the table at the top of the window to display the configuration for that device in the Device Configuration Detail

table at the bottom of the window.

The data in this section is divided into **Match** and **Status** columns:

Match Column

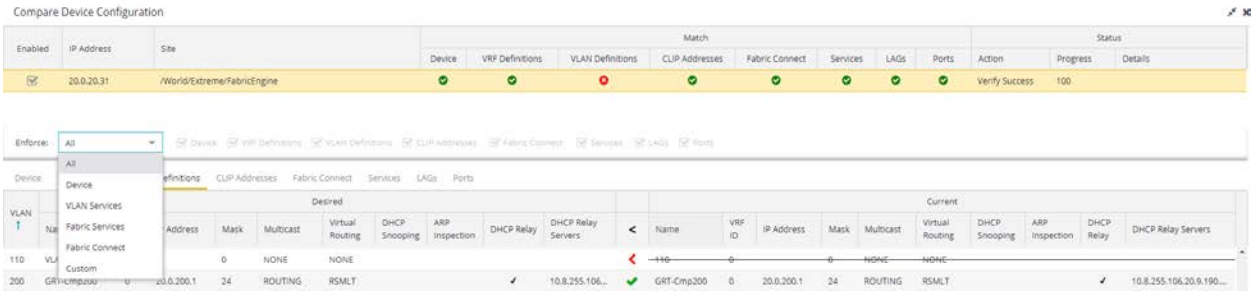
Devices on which the current configuration matches the desired configuration display a check icon (), while devices on which differences are detected display a red x ().

Status Column

The Status column displays the details of the status of the configuration matches in the Match column.

Enforce Options

The Enforce Options section of the window enables you to push the changes you made to the device, view and compare the changes to the current



Select an option from the **Enforce** drop-down list to push the changes you make to the device or the specific service you select. Your selection from the drop-down list displays the changes to the configurations that are being pushed to the device in the Device Configuration Detail Table at the bottom of the window.

NOTES: Device is the default option for the Enforce Options window.

Use Enforce to verify whether the settings you want to configure on the device require other settings to also be set on the device. The Enforce fails if the other required settings are not configured for the changes you want to make.

The following options are included in the **Enforce** drop-down list:

All

To push configuration changes to multiple components of the device, select **All**. The Device, VRF Definitions, VLAN Definitions, CLIP Address, Topology, Services, LAGs, and Ports tabs in the Device Configuration Detail table become available for you to view the changes and compare them to the current configuration.

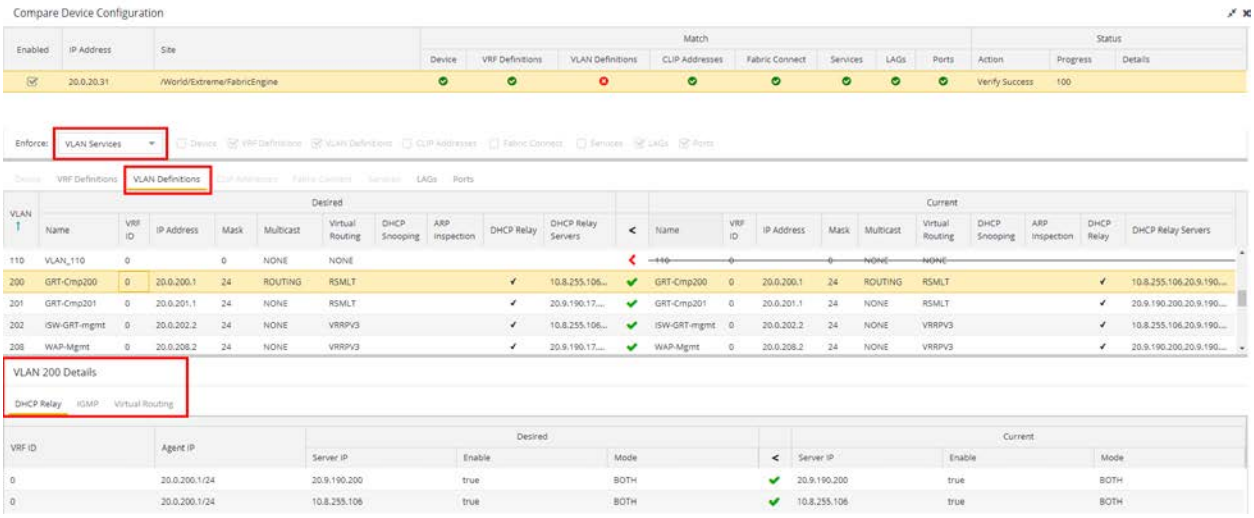
Device

To view configuration changes to the device, select **Device**. The Device tab in the Device Configuration Detail table becomes available for you to view the changes and compare them to the current configuration.

VLAN Services

To push configuration changes to the VLAN, select **VLAN Services**. The VRF Definitions, VLAN Definitions, LAGs, and Ports tabs in the Device Configuration Detail table become available for you to view the changes and compare them to the current configuration.

In addition, the VLAN Details grid opens at the bottom of the Device Configuration table. The grid provides additional details about the changes you made to the VLAN:



The VLAN Details grid includes the following tabs:

DHCP Relay

Displays details of changes you've made to the DHCP relay servers enabled for the VLAN.

IGMP

Displays changes you've made to the IGMP assigned to the VLAN.

VRRP

Displays changes to the state of the virtual router interfaces assigned to IPs in the VLAN.

Fabric Services

To push configuration changes to Fabric Services on the device, select **Fabric Services**. The VRF Definitions, VLAN Definitions, CLIP Addresses, Services, LAGs, and Ports tabs in the Device Configuration Detail table become available for you to view the changes and compare them to the current configuration.

Fabric Topology

To view the configuration changes to the fabric topology, select **Fabric Topology**. The Fabric Connect tab in the Device Configuration Detail table becomes available for you to view the changes and compare them to the current configuration.

Custom

The **Custom** option enables you to select which tabs to display in the Device Configuration Detail table. Use the check boxes to the right of the **Enforce** button to select the tabs you want to include in the table.

NOTE: Device is the default option for the Enforce Options window.

IMPORTANT: When performing an enforce on the following options, ExtremeCloud IQ Site Engine validates your changes:

- All
- VLAN Services
- Fabric Services
- Fabric Connect

An error displays if you are attempting to enforce changes that are not valid for the device.

Device Configuration Detail Table

The Device Configuration Detail table includes several tabs:

- Device
- VRF Definitions
- VLAN Definitions
- CLIP Addresses
- Fabric Connect
- Services
- LAGs
- Ports

The configurations are separated into two columns on each tab:

- The Desired column shows the configuration you are saving to the device on the next enforce.
- The Current column shows the configuration currently on the device.

A check mark between the columns (✔) indicates the Current configuration matches the Desired configuration.

A left arrow icon (◀) indicates the configurations do not match. Selecting it copies the Current configuration to the Desired configuration so no configuration change is made when enforcing the device.

Device

The **Device** tab displays any changes to basic information about the device.

sysName
The name by which the device is known.

sysContact
Allows you to specify contact information for the person maintaining the device.

sysLocation
The physical location of the device.

VRF Definitions

The **VRF Definitions** tab displays any changes to the configuration of VRFs on the device.

Name
Displays the name of the VRF.

Multicast
Select to indicate the service sends IP packets to a group of hosts on the network.

Unicast
Select to indicate the service sends IP packets to a single recipient on the network.

Direct Route
Select to indicate the service sends IP packets directly to another device without going through a third device.

Default Gateway
Enter the IP address of the switch's default gateway. If a device is ZTP+-enabled, the site's ZTP+ Device default gateway displays.

VLAN Definitions

The **VLAN Definitions tab** displays the changes to the configuration of VLANs on the device.

VLAN
A unique numerical identifier of the VLAN.

Name
Displays the name of the VLAN.

VRF ID
Displays the ID number of the VRF associated with the VLAN.

IP Address
Displays the IP address associated with the VLAN.

NOTE: IP Address provisioning is only supported on Fabric Engine devices.

Mask
Displays the IP/subnet mask.

Secondary IPs
Displays the secondary IP addresses associated with the VLAN.

NOTE: Secondary IP Address provisioning is only supported on Fabric Engine devices.

Multicast
Indicates the service sends IP packets to a group of hosts on the network.

IGMP Version
Indicates which version of IGMP is utilized on the port (Version 1 or Version 2).

IGMP Querier
The address of the IGMP Querier. This feature is used when there is no multicast router in the VLAN to originate the queries.

Querier Enable
Indicates whether an IGMP Query is enabled.

Virtual Routing
Displays the version of VRRP the default gateway is using:

- **NONE** — Virtual routing is not configured on the VLAN.
- **VRRPv2** — VRRP version 2 is configured on the virtual router. VRRP version 2 only supports IP addresses in IPv4 format.
- **VRRPv3** — VRRP version 3 is configured on the virtual router. VRRP version 3 supports IP addresses in both IPv4 and IPv6 formats.
- **DvR –**DvR is configured on the VLAN. There are several requirements that must be met to configure DvR on a VLAN, including:
  - The VLAN must have an IP address and prefix.
  - The DvR IP address must be IPv4.
  - The DvR IP address must fall within the VLAN's subnet.
  - The DvR IP address cannot be reused across multiple VLANs on the device.

- The VLAN must have an L2VSN associated with it.
- If the VLAN is using on a non-zero VRF ID, the VLAN must also have:
    a. An L3VSN associated with the VRF.
    b. The VRF must have the unicast option enabled.
- Devices participating in DvR as controllers must have non-zero IPv4 ISIS Source Addresses.
- Devices participating in DvR must have IPv4 Shortcuts and Multicast enabled.

- **RSMLT** — Routing Redundancy Method is configured on the VLAN. RSMLT requires that a Virtual IST is configured. If the device is not configured as a vIST pair, **RSMLT** can be selected, but the feature is not active. Once the vIST is configured, RSMLT becomes active.

NOTES:	Virtual Routing is only supported on Fabric Engine devices. Fabric Enginedevices support a new "dvr-one-ip" feature in the 8.2 release that allows you to share an IP address between a VLAN and its DvR interface. ExtremeCloud IQ Site Engine currently does not support the "dvr-one-ip" feature and cannot read or enforce configurations of this type. Configure Fabric Engine device IP addresses on VLANs and their DvR interfaces through the **VLAN Definitions** tab.

Virtual Routing Enable
Indicates whether virtual routing is enabled for the VLAN.

Virtual Routing Address
The IP address for the virtual router. The Virtual Routing address must be in the same subnet as the VLAN subnet address.

VRRP ID
An identifier devices use to determine peer devices that participate in a VRRP (Virtual Routing Redundancy Protocol) virtual routing interface.

VRRP Priority
A value used by VRRP peers to determine the role of each of the devices in the VLAN. The default value is **100**. The device with the largest value is assigned the role of Controller. For example, in a VLAN with two routers, one with a **VRRP Priority** of **200** and one with a **VRRP Priority** of **100**, the router with a **VRRP Priority** of **200** becomes the Controller. In the event of identical priority numbers, the devices use the MAC address to determine priority.

VRRP Backup Master
This option determines if the backup router is able to forward traffic independently outside of the VLAN (enabled), or must forward the traffic to the Controller router before it is forwarded outside of the VLAN (disabled).

VRRP Advertisement Interval

Indicates frequency (in seconds) that protocol packets are sent from the virtual router in the VLAN.

VRRP Hold Down Timer

Indicates the amount of time (in hundredths of a second) that the backup router waits for the primary router to respond before it becomes the primary router.

DHCP Snooping

Indicates whether DHCP snooping is enabled for the VLAN. DHCP Snooping is a Layer 2 security feature, that provides network security by filtering untrusted DHCP messages received from the external network causing traffic attacks within the network. DHCP Snooping is based on the concept of trusted versus untrusted switch ports. Switch ports configured as trusted can forward DHCP Replies, and the untrusted switch ports cannot. DHCP Snooping acts like a firewall between untrusted hosts and DHCP servers.

ARP Inspection

Indicates whether ARP inspection is enabled. Dynamic ARP Inspection (DAI) is a security feature that validates ARP packets in the network. Without DAI, a malicious user can attack hosts, switches, and routers connected to the Layer 2 network by poisoning the ARP caches of systems connected to the subnet, and intercepting traffic intended for other hosts on the subnet. DAI prevents these attacks by intercepting, logging, and discarding the ARP packets with invalid IP to MAC address bindings. The switch dynamically builds the address binding table from the information gathered from the DHCP requests and replies when DHCP Snooping is enabled. The switch pairs the MAC address from the DHCP request with the IP address from the DHCP reply to create an entry in the DHCP binding table. When you enable DAI, the switch filters ARP packets on untrusted ports based on the source MAC and IP addresses seen on the switch port. The switch forwards an ARP packet when the source MAC and IP address matches an entry in the address binding table. Otherwise, the switch drops the ARP packet.

NOTE: **DHCP Snooping** must be enabled to use **ARP Inspection**.

DHCP Relay

Indicates whether a Dynamic Host Configuration Protocol relay server is enabled for the VLAN. A DHCP relay receives and converts a DHCP broadcast message to dynamically assign an IP address to a device on the network.

DHCP Relay Servers

The IP addresses of the DHCP relay servers for the VLAN.

NOTE: Select **Manage** to open the **Manage DHCP Relay Servers** window, where you can add or delete DHCP relay servers.

CLIP Addresses

Use the **CLIP Addresses** tab to view changes to IPv4 and IPv6 CLIP Addresses on your device.

Device ID
The ID address of the device to which the CLIP address is assigned.

CLIP Interface
The interface ID for the CLIP address.

IP Version
Indicates the IP Address: IPv4 or IPv6

IP Address
The IP address associated with the selected interface (VLAN, BROUTER or MGMT).

Prefix Length
Displays the number of digits that comprise the IP Address prefix. Prefix length for IPv4 Addresses is between 8 and 30 digits, and the prefix length for IPv6 addresses is between 8 and 128 digits

Fabric Connect

The **Fabric Connect** tab displays changes to the Fabric Connect features to devices in your network.

Topology Definition
Displays the Topology Definition that applies to the device. The Topology Definitions available in the drop-down list are configured in the **Topology Definition** tab.

- **None** - No Fabric Connect configuration on the device. If you select **None** for a device that is configured for Fabric Connect, that configuration is removed.
- **Local** - The Fabric Connect configuration is configured locally and not by ExtremeCloud IQ Site Engine.
- **Disabled** - The Fabric Connect configuration is applied to the device, but ISIS is disabled, which allows the user to take a device out of service without removing all its configuration.
- **Service Definition** - The Service Definition that has been applied to the site to which the device is assigned.

SPBM Instance
The system-defined identifier for the Fabric Connect configuration on the device. The default value is 1.

Secondary BVLAN
The Secondary Backbone VLAN. This information is configured on the **Sites > Topology Definition** tab.

Primary BVLAN
The Primary Backbone VLAN. This information is configured on the **Sites > Topology Definition** tab.

Nickname Server Prefix
: This is the 1-byte "x.y" portion of the larger "1.23.45" nickname format. This field can be edited when **Nickname Server Enable** is selected and the **Topology Definition** is Local, Disable, or a user-defined topology definition.

Nickname Server Enable
: This enables the Nickname Server on a Fabric Engine device. You can enable this function when **Topology Definition** is set to Local, Disable, or a user-defined topology definition, and **SPBM Nickname Dynamic Allocation** is set to Dynamic.

Nickname
: A value that other fabric devices use to identify the device. The SPBM nickname must be unique within the fabric.

Multicast Enable
: The check box is selected if Multicast is enabled for the device.

ISIS System Name
: The system name of the device.

ISIS System ID
: The system-defined fabric service identifier assigned to the device. The default is the MAC address for the device.

ISIS IP Source Address (V6)
: The IPv6 address the device uses to transmit ISIS traffic to other fabric devices. The address must be unique within the fabric.

ISIS IP Source Address
: The IPv4 address the device uses to transmit ISIS traffic to other fabric devices. The address must be unique within the fabric.

ISIS Manual Area
: The IS-IS Manual Area in xx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx format (1-13 bytes). This information is configured on the **Sites > Topology Definition** tab.

IPv6 Shortcuts
: The check box is selected if IPv6 Shortcuts are enabled for the device.

IPv4 Shortcuts
: The check box is selected if IPv4 Shortcuts are enabled for the device.

Enable RSMLT Edge Support
: Select this option to use the RSMLT Edge.

Enable Fabric Attach
: The check box is selected if Fabric Attach functionality is supported.

Enable Fabric
: Select this option to use the SPBM fabric.

DvR Role

Displays the DvR Role from the drop-down list:

- None - DvR (Distributed Virtual Routing) is not configured on the device.
- Controller - Indicates the device is one of the main devices participating in the DvR virtual routing interface.
- Leaf - Indicates the device is one of several edge devices within the DvR domain.
- Global Backbone - Indicates the device is a standard Fabric Connect device that and does not run the DvR protocol, but will learn routes from DvR controllers in the fabric.

DvR Domain ID

Displays the identifying number for the DvR domain.

Services

The **Services** tab displays the services created within service applications and configured on the device. Use this tab to add new services to the device. Services may be inherited from a service definition or may be configured locally on the device.

L2 VSN

Source

Indicates the service definition and service application from which the service is inherited.

Device ID

Indicates the IP address of the device on which the service is used.

Origin

Indicates how the service is created.

Name

The name of the Layer 2 service.

Service ID

The ID number of the fabric service.

VLAN

The VLAN to which the fabric service is associated.

L3 VSN

Source

Indicates the service definition from which the service is inherited.

Name

The name of the Layer 3 service.

Service ID
The ID number assigned to the service.

VRF
Select the VRF to which the service is associated.

LAGs

Use the **LAG** tab to configuration changes to LAGs and MLAGs (also known as MLTs and SMLTs, respectively). A LAG combines multiple network connections to increase the throughput beyond that of a single connection. An MLAG allows a device to send network traffic to two switches to improve network diversity, while only managing a single logical interface.

Source
Indicates the location from which the LAG is inherited. The LAG can be inherited from a site, locally configured on the device itself, or can be excluded.

NOTE: Selecting **Exclude** indicates you are excluding an inherited configuration. LAG configurations locally defined on the device and are not cannot be excluded. You can only select **Exclude** for configurations inherited from a Site (or a Service Application).

IP Address
Displays the IP address of the LAG.

Type
Displays the type of LAG, either LAG or MLAG.

LAG ID
Displays a system-defined ID number for the LAG.

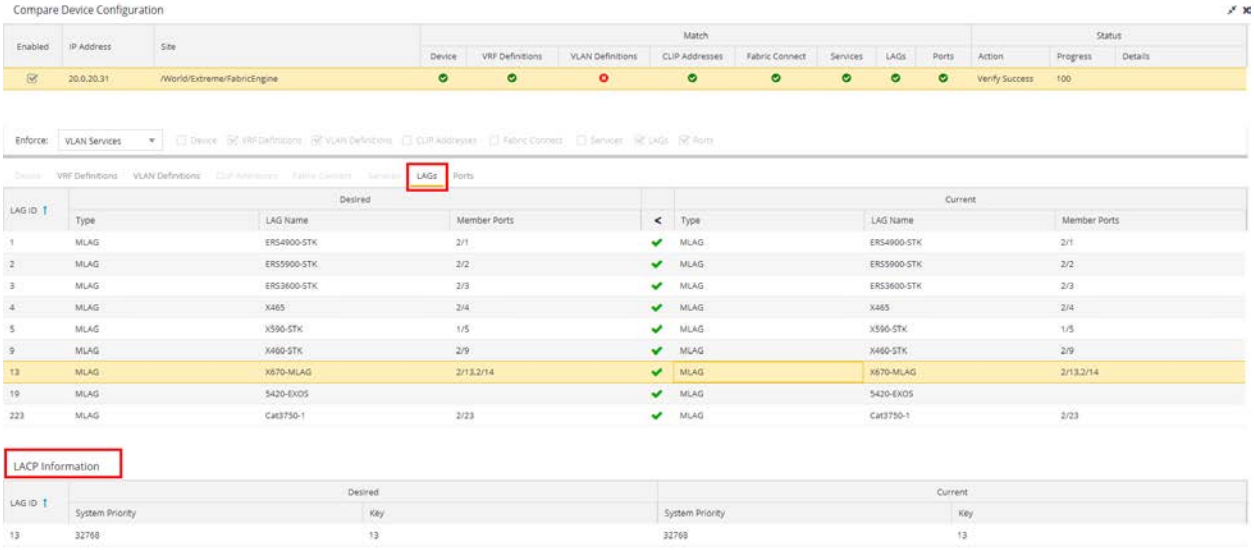
Name
Displays a user-defined name for the LAG.

Member Ports
Displays the ports that are included in the LAG.

Aggregatable Type
Indicates whether the LAG is static or dynamic:

- Static — the LAG is static.
- LACP — the LAG is dynamic via LACP.

The LACP Information grid opens at the bottom of the Device Configuration table:



The LACP Information grid displays the following tabs, separated into Desired and Current columns:

System Priority

Displays the LACP priority, which ExtremeCloud IQ Site Engine uses to determine the probability network traffic uses the LAG. Valid values are between 1 and 65,535. The lower the value entered, the higher ExtremeCloud IQ Site Engine prioritizes the LAG.

Key

Displays the LACP key, which the LAG uses to ensure it only pairs with properly configured endpoints.

Ports

The **Ports** tab displays any changes to the configuration of ports on the device.

Port

The name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

Alias

Displays the alias for the port, if one is assigned.

PVID

The port's VLAN assignment. Possible values are 1 through 4094.

Tagged

The port is added to the list with the egress state set to Tagged (frames are forwarded as tagged).

Untagged

The port is added to the list with the egress state set to Untagged (frames are forwarded as untagged).

Fabric Enable

Indicates the fabric functionality is enabled on the port.

ExtremeCloud IQ Site Engine can extend FA functionality to ExtremeXOS/Switch Engine devices and provision them as FA Proxy devices. Select "Fabric Attach" or "" from the drop-down list to enable the port on a Fabric Engine device (acting as FA Server) to connect to an ExtremeXOS/Switch Engine device (acting as FA Proxy).

- **Fabric Attach** - Enable Fabric Attach server functionality on the port of a Fabric Engine device acting as a Fabric Attach server) to connect to an ExtremeXOS/Switch Engine device (acting as a Fabric Attach proxy).
- **Fabric Attach and Switched UNI** - Enable Fabric Attach server functionality on the port of a Fabric Engine device acting as a Fabric Attach server) to connect to an ExtremeXOS/Switch Engine device (acting as a Fabric Attach proxy). When selecting this option, the port is configured for both features, but only one feature is active at any one time.
- **Auto Sense** - Select **Auto Sense** on the port of a Fabric Engine device to enable the port to automatically sense and configure automatically sense and configure the appropriate Fabric settings for the port. These settings include the following:
  - PVID
  - VLAN Trunk
  - Tagged
  - Untagged
  - Fabric Mode
  - Fabric Auth Type
  - Fabric Auth Key
  - Fabric Connect Drop STP-BPDU
  - BPDU Guard
  - Authentication

NOTE: If **Fabric Enable** is **Auto Sense** the Fabric settings listed above are not configurable.

Fabric Auth Type

If **Fabric Enable** is **Fabric Attach** or **NNI**, this defines the type of authentication the device uses for the port to communicate with the other ISIS devices to secure those services.

Fabric Auth Key

Indicates the fabric authentication key used for the port.

Span Guard

Select to enable Span Guard, which allows the device to shut down a network port if it receives a BPDU (bridge protocol data unit). Enable this feature on network edge ports to prevent rogue STA-aware devices from disrupting the existing Spanning Tree.

SLPP

Indicates Simple Loop Prevention Protocol (SLPP) is enabled on the port. SLPP provides active protection against Layer 2 network loops on a per-VLAN basis. If an SLPP packet is received, the port is disabled for the amount of time configured in the **SLPP Timer** field.

NOTE: If **SLPP** is enabled, **SLPP Guard** is not available.

SLPP Guard

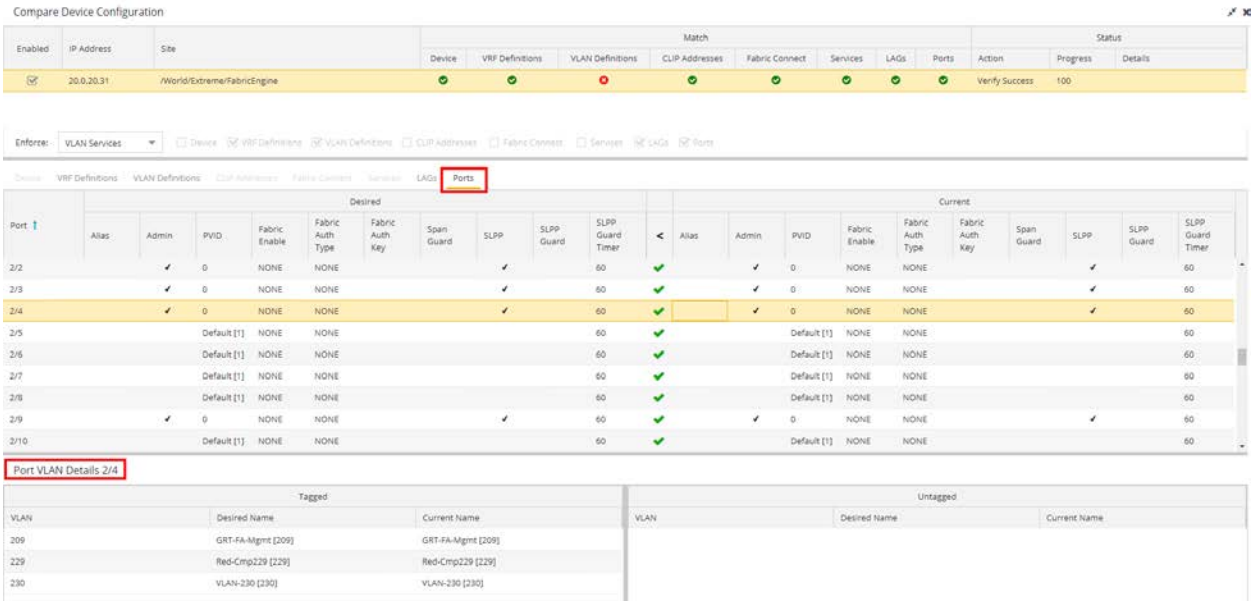
Indicates whether SLPP Guard is enabled on the port. Use SLPP Guard to provide additional loop protection to protect wiring closets from erroneous connections. SLPP Guard requires **SLPP** to be enabled. SLPP detects loops in an SMLT network. Because SMLT networks disable Spanning Tree (STP), Rapid Spanning Tree (RSTP), or Multiple Spanning Tree Protocol (MSTP) for participating ports, SLPP Guard provides additional network loop protection, extending the loop detection to individual edge access ports. SLPP Guard can be configured on MLT or LAG ports. If the edge switch with SLPP Guard enabled receives an SLPP-PDU packet on a port, SLPP Guard operationally disables the port for the configured timeout interval in the **SLPP Guard Timer** field and appropriate log messages and SNMP traps are generated. If the disabled port does not receive any SLPP-PDU packets after the configured timeout interval expires, the port automatically re-enables and generates a local log message, a syslog message, and SNMP traps, if configured.

NOTE: If **SLPP Guard** is enabled, **SLPP** is not available

SLPP Guard Timer

Indicates the amount of time after receiving an SLPP packet before the port is re-enabled.

The Port VLAN Details grid opens at the bottom of the Device Configuration table:



The Port VLAN Details grid displays desired and current ports, separated into **Tagged** and **Untagged** columns.

Select **Enforce** to save your changes to the device.

How to Change the Configuration of a Device Included Site

Sites allow you to select the default configuration for devices you add to your network via a device discover or using ZTP+ functionality.

In some instances, a device in a site may need to be configured slightly differently than the other devices in the site.

To change the configuration of a device included in a site:

1. Open the **Network** > **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Select the site that includes the device for which you are changing the configuration.
4. In the right-panel, select the **Devices** tab.
5. Right-click the device and select **Device** > **Configure Device**.
   The **Configure Device** window opens.
6. Make the necessary changes and select **Save**.

For information on related topics:

- Sites
- How to Discover Devices in ExtremeCloud IQ Site Engine
- Devices

Sites

Use the **Sites tab** to define configuration templates. ExtremeCloud IQ Site Engine applies these configuration templates to devices you add to a site in your network. You can also use the tab to discover new devices in the site via device discovery or by using ZTP+ functionality.

NOTE: When adding an ExtremeXOS/Switch Engine device in ExtremeCloud IQ Site Engine, enter the following commands in the device CLI:

```
configure snmpv3 add community "private" name "private" user "v1v2c_rw"
configure snmpv3 add community "public" name "public" user "v1v2c_rw"
enable snmp access
enable snmp access snmp-v1v2c
disable snmp access snmpv3
```

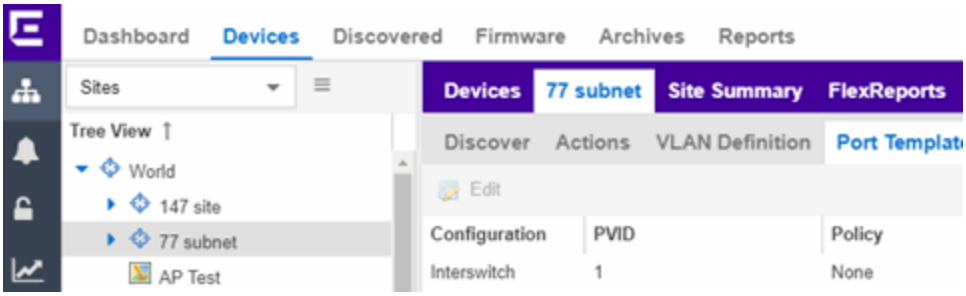
The **Sites tab** is divided into multiple sections, which you can expand to display more information.

NOTE: To save your changes and other additional functions for a device included in the site, right-click on the device and select **Configure Device** from the drop-down list. The **Configure Device** window opens. Use the buttons at the bottom of the **Configure Device** window to save, sync settings from the site to the device's configuration, enforce changes to the device, and more.

Access **Network** > Devices and select **Sites** from the left-panel drop-down list. The Sites Tree View opens, which includes the sites in your network, as well as **Topology Definitions** and **Service Definitions** tabs.

Right-click the Topology Definitions tab to create topology or LAG (link aggregation group) topology definitions. Right-click the Service Definitions tab to create service definitions. The topology, LAG and service definitions are used to create the templates that build Fabric technology.

Select a site from the left-panel Sites Tree View. A tab in the **Devices** window opens with the name of the site you selected. To create a new site, click the menu icon in the left-panel and select **Maps/Sites** > **Create Site**.



The **Site Name** tab contains the following tabs:

- Discover
- Actions
- VRF/VLAN
- Fabric Connect
- Services
- LAG Topologies
- Port Templates
- ZTP+ Device Defaults
- Endpoint Locations
- Analytics
- Custom Variables
- XIQ Location

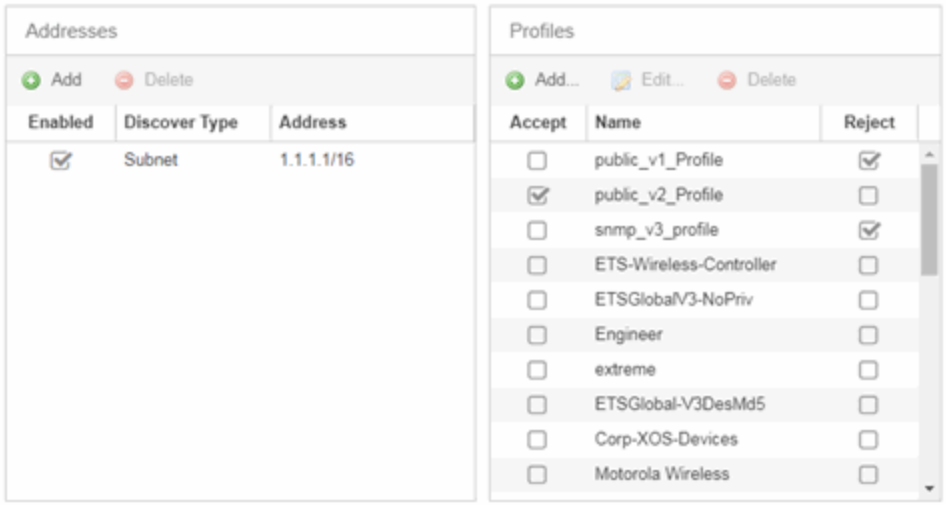
Additionally, the bottom of the tab contains buttons to save your configurations in ExtremeCloud IQ Site Engine and on the devices included in the site.

Discover

The **Discover** tab allows you to enter address information for new devices on your network, which adds them to the ExtremeCloud IQ Site Engine database in the current Site. You can perform a CDP (Cabletron Discovery Protocol) discover for CDP-compliant devices, an LLDP (Link Layer Discovery Protocol) discover for LLDP-compliant devices, and an EDP (Extreme Discovery Protocol) discover for EDP-compliant devices. Additionally, you can discover new devices based on subnets or IP address ranges. When discovering devices, you can choose to accept or reject devices based on the profile type using the respective checkboxes in the Profiles section.

NOTES: ExtremeCloud IQ Site Engine only allows a subnet search of a 16-bit mask or higher when discovering devices.

Discovering devices via the **Site** tab using a **Range**, **Subnet**, or **Seed** discover may not successfully add all expected devices. To correct the issue, increase the **Length of SNMP Timeout** value on the Administration > Options > Site tab in the Discover First SNMP Request section.



Addresses

Click the **Add** button in the Addresses list to allow you to add devices by seed address, subnet, or address range. Selecting **Seed Address** allows you to perform a discover for CDP, LLDP, SONMP, or EDP-compliant devices.

NOTE: The protocols for seed discovery are specified on the Administration tab.

Click the **Discover** button at the bottom of the tab to begin the device discover. The results of the Discover process are displayed in the left-panel tree when added to the ExtremeCloud IQ Site Engine database.

Profiles

Select the access Profile(s) that give you the access you need (for example, Read, or Read/Write) to the devices you wish to discover by selecting the **Accept** checkbox. Select the Profiles that are not valid on the device being discovered by selecting the **Reject** checkbox. To create a profile, click the **Add** button or edit a profile by selecting the **Edit** button. If you discover an existing device using a different profile than the device is already using in the database, click **Save** to overwrite the profile currently being used in the database.

Actions

The **Actions** tab contains basic information about the device being discovered.

Automatically Add Devices

Selecting the **Automatically Add Devices** checkbox causes ExtremeCloud IQ Site Engine to automatically add devices to the database that match the address information you entered in the Discover section of the tab. If a device is discovered with more than one profile, the device is listed on the **Network** > **Discovered** tab, where you can decide which profile you want to add. When this box is NOT selected and a discover occurs, devices are added to the **Network** > **Discovered** tab, where they can be configured prior to being added to the database.

Add Trap Receiver

Select this checkbox to configure devices added to the site to send trap information to ExtremeCloud IQ Site Engine. You can define the trap configuration details on the **Options** > **Trap** tab. Depending on the device, ExtremeCloud IQ Site Engine creates the trap configuration via SNMP or a script.

Add Syslog Receiver

Select this checkbox to configure the devices added to the site to send syslog information to ExtremeCloud IQ Site Engine. You can define the syslog configuration details on the **Options** > **Syslog** tab. Depending on the device, ExtremeCloud IQ Site Engine creates the syslog configuration via SNMP or a script.

Collection Mode

Select **None**, **Threshold Alarms**, or **Historical** from the Collection Mode drop-down menu to indicate the mode used to collect device statistics on devices being discovered. ExtremeCloud IQ Site Engine uses the device and physical port statistics in reports.

Collection Interval (minutes)

Select the interval at which device and statistics (for devices being discovered) are collected. Extreme sets a minimum collection interval of five minutes and a maximum of 1440 minutes (24 hours).

Add to Archive

Select this checkbox to create an archive, which saves the configurations of the devices being discovered in the **Network** > **Archives** tab.

Add to Map

Select this checkbox to add the devices being discovered in the site to a map. To add a device to multiple maps, add it via this drop-down list and then manually add it via the **Maps** > **Add to Map** on the **Devices** tab.

Custom Configuration

Click the **Add** button to configure ExtremeCloud IQ Site Engine to automatically run a task (a script or workflow) when discovering a device in a particular device family that also matches the **Topology** you select.

CAUTION: If the script or workflow task selected for the Custom Configuration restarts the device, other actions selected to execute during discovery might not execute (for example, Add Trap Receiver).

NOTE: Selecting a **Topology** of **Any** runs the task on all devices in a device family, regardless of the **Topology** configuration.

Policy

Add Device to Policy Domain

Select this checkbox to add the device to a policy domain you create on the **Policy** tab. When the checkbox is selected, use the **Policy Domain** drop-down list to select the policy domain to which the device is added. ExtremeCloud IQ Site Engine enforces are done automatically when a newly added device is discovered and added.

Click the **Import VLANs** button to import the VLAN definitions from the policy selected in the Policy Domain drop-down list.

Access Control

Add Device to Access Control Engine Group

Select this checkbox to add the device to an Access Control Engine Group you create on the **Access Control** tab. When the checkbox is selected, use the Access Control **Engine Group** drop-down list to select the engine group to which the device is added.

- If the device is an Access Control engine, ExtremeCloud IQ Site Engine adds it as an engine to the engine group.
- If the device is not an engine, ExtremeCloud IQ Site Engine adds it as a switch to up to two engines in the engine group. ExtremeCloud IQ Site Engine runs an enforce against the engine group if a switch is added.
    - Enable RADIUS Accounting - defines if the RADIUS Accounting is enabled or disabled. If Enable RADIUS Accounting is checked and the "Authentication Access Type" is " Manual RADIUS Configuration" then the Access Control Engine accepts RADIUS Accounting packets from that device. If Enable RADIUS Accounting is checked and "Authentication Access Type" is not "Manual RADIUS Configuration" then Access Control Engine enables RADIUS Accounting on the device and accepts RADIUS Accounting packets from that device.
    - Message-Authenticator Attribute - defines if the Access-Request must contain the Message-Authenticator attribute in the RADIUS communication with this device. Not every RADIUS client supports this attribute, but the security best practice is to require the Message-Authenticator attribute. If set to "Required", then RADIUS

packets without the Message-Authenticator attribute are dropped.

- **Authentication Access Type** - defines if the device is configured to use "Network Access" or "Management Access" or "Any Access" or the "Manual RADIUS Configuration".
- **Override RADIUS Attributes to Send** - if checked then you can define what "RADIUS Attributes to Send" will be used. If unchecked then default "RADIUS Attributes to Send" will be used. The default is:
  - If the device is running the Fabric Engine operating system and the policy domain is specified, then Per-User ACLs RADIUS attributes are used.
  - If the device is running Fabric Engine operating system and the policy domain is not specified, the Fabric Attach RADIUS attributes are used.
  - If the device is running a policy capable operating system, for example, ExtremeXOS, then Extreme Policy RADIUS attributes are used.
- For more details, see Add Switches to Access Control Engine Group.

Enable Authentication Using Port Template

Select this checkbox to allow users to authenticate to the device using a port template. Configure Port Templates in the Port Templates section of the tab.

ExtremeAnalytics

Add as Flow/Telemetry Source to Home Engine using Management IP

Select this checkbox to add application telemetry to the ExtremeAnalytics engine configured as the site's home engine. Flow Source is preferred if the device can be added as Flow Source and Telemetry Source.

ERSPAN VLAN

Enter the Encapsulated Remote Switch Port Analyzer (ERSPAN) VLAN to add to devices added to the site.

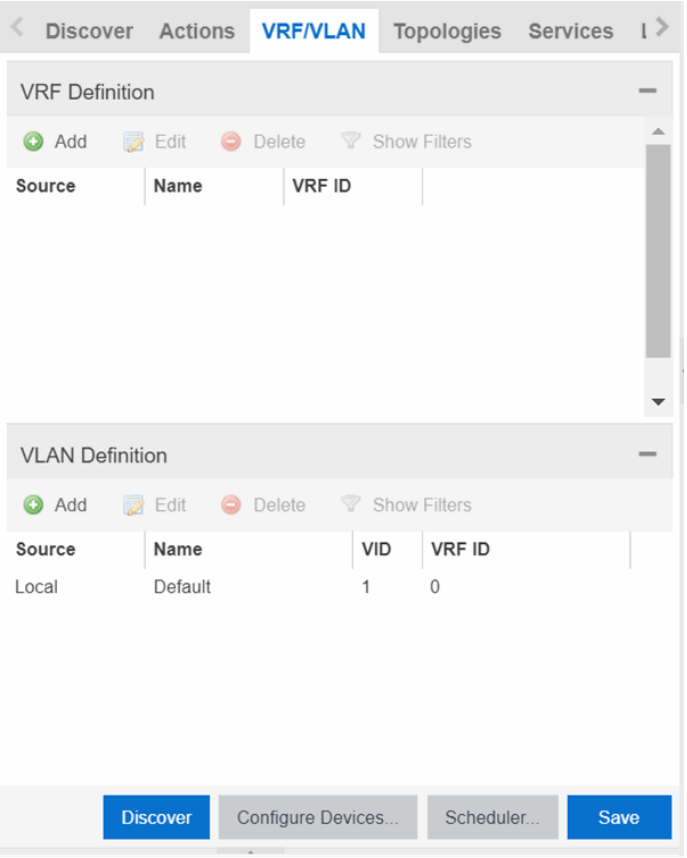
Sample Rate

Enter the rate of traffic ExtremeAnalytics samples to determine application information.

VRF/VLAN

The **VRF/VLAN** tab allows you to configure and manage virtual routing and forwarding (VRF), VLANs on the devices included in the site. Add a VRF or VLAN definition by selecting **Add** in the VRF Definition or VLAN Definition table, respectively. Edit an existing VRF or VLAN definition by selecting a VRF/VLAN and selecting **Edit**, or remove a VRF or VLAN definition by selecting a VRF/VLAN and selecting **Delete**.

NOTE: You must have a Fabric Manager license to configure VRFs. If you do not have one, this tab is just called VLAN.



VRF Definition

Source

The **Source** represents the Site where the VRF settings were created. **Local** indicates the VRF was created in the selected site. When a VRF is created for a Site, any Sites created nested within that Site inherit the VRF settings from the Site. Changes or Deletions can only be made to the VRF in the site in which it was created (**Source** is **Local**).

Name

Displays the name of the VRF definition.

VRF ID

The ID number assigned to the VRF definition.

Multicast

Select to indicate the service sends IP packets to a group of recipients on the network.

Unicast

Select to indicate the service sends IP packets to a single recipient on the network.

Direct Route

Select to indicate the service sends IP packets directly to a another device without going through a third device.

VLAN Definition

Source

The **Source** represents the Site where the VLAN settings were created. **Local** indicates the VLAN was created in the selected site. When a VLAN is created for a Site, any Sites created nested within that Site inherit the VLAN settings from the Site. Changes or Deletions can only be made to the VLAN in the site in which it was created (**Source** is **Local**).

Name

Displays the name of the VLAN.

VID

Indicates the VLAN ID for the VLAN. A unique number between 1 and 4094 that identifies a particular VLAN. VID 1 is reserved for the Default VLAN.

VRF ID

The VRF ID associated with the VLAN definition.

Multicast

Select to configure the service to distribute data to multiple recipients. Using multicast, a source can send a single copy of data to a single multicast address, which is then distributed to an entire group of recipients.

IGMP Version

Indicates which version of IGMP is utilized (Version 1 or Version 2).

IGMP Querier

Enter the address of the IGMP Querier. Use this feature when there is no multicast router in the VLAN to originate the queries.

Querier Enable

Indicates whether an IGMP Query is enabled.

Virtual Routing

Displays the version of VRRP the default gateway is using:

- **NONE** — Virtual routing is not configured on the VLAN.
- **DvR** - DvR (Direct Virtual Routing) is configured.
- **VRRPv2** — VRRP version 2 is configured on the virtual router. VRRP version 2 only supports IP addresses in IPv4 format.
- **VRRPv3** — VRRP version 3 is configured on the virtual router. VRRP version 3 supports IP addresses in both IPv4 and IPv6 formats.
- **RSMLT** — Routing Redundancy Method is configured on the VLAN. RSMLT requires that a Virtual IST is configured. If the device is not configured as a vIST pair, **RSMLT** can be selected, but the feature is not active. Once the vIST is configured, RSMLT becomes active.

NOTE: Virtual Routing is only supported on Fabric Engine devices.

Virtual Routing Enable
Indicates whether virtual routing (DvR or VRRPs) is enabled for the VLAN.

Virtual Routing Address
The IP address for the virtual routing interface for either DvR or VRRP. The Virtual Routing address must be in the same subnet as the VLAN subnet address.

VRRP ID
An identifier devices use to determine peer devices that participate in a virtual routing interface.

VRRP Priority
A value used by VRRP peers to determine the role of each of the devices in the VLAN. The default value is **100**. The device with the largest value is assigned the role of Controller. For example, in a VLAN with two routers, one with a **VRRP Priority** of **200** and one with a **VRRP Priority** of **100**, the router with a **VRRP Priority** of **200** becomes the Controller. In the event of identical priority numbers, the devices use the MAC address to determine priority.

VRRP Backup Master
This option determines if the backup router is able to forward traffic independently outside of the VLAN (enabled), or must forward the traffic to the Controller router before it is forwarded outside of the VLAN (disabled).

VRRP Advertisement Interval
Indicates frequency (in seconds) that protocol packets are sent from the virtual router in the VLAN.

VRRP Hold Down Timer
Indicates the amount of time (in hundredths of a second) that the backup router waits for the primary router to respond before it becomes the primary router.

DHCP Relay
Indicates whether a Dynamic Host Configuration Protocol relay server is enabled for the VLAN. A DHCP relay receives and converts a DHCP broadcast message to dynamically assign an IP address to a device on the network.

DHCP Relay Servers
The IP addresses of the DHCP relay servers for the VLAN.

DHCP Snooping
Indicates whether DHCP snooping is enabled for the VLAN. DHCP Snooping is a Layer 2 security feature, that provides network security by filtering untrusted DHCP messages received from the external network causing traffic attacks within the network. DHCP Snooping is based on the concept of trusted versus untrusted switch ports. Switch ports configured as

trusted can forward DHCP Replies, and the untrusted switch ports cannot. DHCP Snooping acts like a firewall between untrusted hosts and DHCP servers.

ARP Inspection

Indicates whether ARP inspection is enabled. Dynamic ARP Inspection (DAI) is a security feature that validates ARP packets in the network. Without DAI, a malicious user can attack hosts, switches, and routers connected to the Layer 2 network by poisoning the ARP caches of systems connected to the subnet, and intercepting traffic intended for other hosts on the subnet. DAI prevents these attacks by intercepting, logging, and discarding the ARP packets with invalid IP to MAC address bindings. The switch dynamically builds the address binding table from the information gathered from the DHCP requests and replies when DHCP Snooping is enabled. The switch pairs the MAC address from the DHCP request with the IP address from the DHCP reply to create an entry in the DHCP binding table. When you enable DAI, the switch filters ARP packets on untrusted ports based on the source MAC and IP addresses seen on the switch port. The switch forwards an ARP packet when the source MAC and IP address matches an entry in the address binding table. Otherwise, the switch drops the ARP packet.

NOTE: **DHCP Snooping** must be enabled to use **ARP Inspection**.

DHCP Relay Servers

Source

Indicates the site from which the DHCP Relay Server is inherited. Currently, the VLAN definition Source can only be **Local**, indicating the DHCP Relay Server is configured in the current site.

Server IP

The IP address of the DHCP server.

Fabric Connect

The **Fabric Connect** tab allows you to select the topology definition. Use this tab to apply the fabric topology features you configure to a site.

Topology Definition

Select the Topology Definition that applies to the site. The Topology Definitions available in the drop-down list are configured in the **Topology Definition** tab.

DvR Domain ID

Select the DvR Domain ID that applies to the site. The DvR Domain IDs available in the drop-down list are configured in the **Topology Definition** tab.

Services

Select to configure the services configured in your virtual services network. Use this tab to select a service definition you create by configuring services on the Services tab to add to the site.

The **Services** tab displays all of the services included in a service application or all of the services included in a service definition, depending if you select a service application or a service definition in the left-panel, respectively. The Services tab is included in the **Sites** tab.

Services are created within service applications. You can include multiple services within an application. Service applications are then included within service definitions. You can also include multiple service applications within a service definition. A service definition that includes a complete set of services is then assigned to a site, which configures the fabric-enabled devices within that site.

Select the Service Definition assigned to the site from the Service Definition drop-down list. Select **NONE** if the services you configure are not assigned to a service definition.

NOTE: When services have been assigned to a site, they cannot be deleted; however, services not assigned to a service definition (where NONE has been selected) can be deleted from a site after they have been assigned to that site.

L2 VSN

Source
The service application to which the Layer 2 service has been assigned.

Name
The name of the Layer 2 service.

Service ID
The ID number of the fabric service.

UNI Type
The User-Network-Interface (UNI) of the fabric service. The following interface types are available:

- **Switched** — A VLAN-ID and a port (VID, port) mapped to a Layer 2 VSN I-SID. With UNI type, VLAN-IDs can be reused on other ports and mapped to different ISIDs.
- **Transparent** - A physical port maps to a Layer 2 VSN I-SID (all traffic through the port, 802.1Q tagged or untagged, ingress and egress maps to the I-SID).

  NOTE: All VLANs on a Transparent Port UNI interface now share the same single MAC learning table of the Transparent Port UNI I-SID.

- **CVLAN** — a platform customer VLAN-ID.

VLAN
The customer VLAN-ID of the associated CVLAN UNI type.

CVID
The customer VLAN-ID of the associated switched UNI port.

Management Service

Defines if the L2 VSN is used for switch management purposes.

AutoSense Service Type

Defines if the L2 VSN service is auto-assigned by the switch-level AutoSense detection. The following types are available:

- **AP Untagged** — If the AutoSense feature detects Access Point, then this service is automatically assigned to the port.
- **Camera Untagged** — If the AutoSense feature detects Camera then this service is automatically assigned to the port.
- **Voice Untagged** — If the AutoSense feature detects a VoIP device then this service is automatically assigned to the port.
- **Voice Tagged** — If the AutoSense feature detects a VoIP device then this service is automatically assigned to the port.
- **Proxy Switch Auth Tagged —** If the AutoSense feature detects a Fabric Attach switch capable of authenticating (ERS devices) then this service is automatically assigned to the port.
- **Proxy Switch No Auth Untagged —** If the AutoSense feature detects a Fabric Attach switch is not capable of authenticating (Switch Engine devices) then this service is automatically assigned to the port.
- **Proxy Switch Auth & Proxy Switch No Auth —** If the AutoSense feature detects any physical Fabric Attach switch (ERS/EXOS/Switch Engine device) then this service is automatically assigned to the port.
- **Data Untagged** — If the AutoSense feature does not detect a device type then this service is automatically assigned to the port.
- **None** — AutoSense is not related to this L2VSN service.

NOTE: Each AutoSense Service Type can only be used once on a switch. The switch cannot use two different service IDs with the same AutoSense Service Type.

AutoSense Service CVID

The AutoSense Service CVID value defines the 802.1q VLAN tag sent from the switch to the device. If the **AutoSense Service Type** is **Voice Tagged** or **Proxy Switch Auth Tagged** or **Proxy Switch Auth & Proxy Switch No Auth** then AutoSense Service CVID must be defined. The value range is 1-4094.

Port Template

If the **UNI Type** is **Switched** or **Transparent** you can select from the Global Port templates to define the purpose of the port.

L3 VSN

Name
The name of the Layer 3 service.

Service ID
The ID number assigned to the service.

VRF
Select the virtual routing and forwarding definition included as part of the service.

Multi Cast
Select to indicate the service sends IP packets to a group of hosts on the network.

Unicast
Select to indicate the service sends IP packets to a single recipient on the network.

Direct Route
Select to indicate the service sends IP packets directly to another device without going through a third device.

LAG Topologies

The LAG Topologies tab allows you to configure link aggregation group topologies you include on devices in the site.

Name
Displays the name of the LAG.

Topology Type
Select the type of LAG topology for the site.

Topology Definition
Select the Topology Definition for the LAG in the drop-down list.

Device 1/Cluster 1
Select the first device or cluster included in the LAG.

Device 2/Cluster 2
Select the second device or cluster included in the LAG.

Device 1 VLAN IP Address/Mask
Enter IP address and mask for the first device or cluster included in the LAG.

Device 2 VLAN IP Address/Mask
Enter IP address and mask for the second device or cluster included in the LAG.

LACP MAC
Enter the MAC address for the device located between two devices designed to detect when a link is down, if you use link aggregation control protocol (LACP).

MLAG ID
The ID number of the MLAG configured for the LAG topology.

L2 ISID
The service instance identifier.

vIST
Select the Virtual IST (vIST) type. vIST provides the ability to dual-home hosts, servers and other network devices to a pair of Multi-Chassis Link Aggregation (MLAG) enabled devices.

Port Templates

The **Port Templates** tab has two panels. The top panel displays information about user-defined port templates. For more information, see Port Templates Panel.

The bottom panel displays information about automated port templates. For more information, see ZTP+ Automated Templates Panel.

Port Templates Panel

The **Port Templates** panel displays port information for those devices discovered in a site. The port templates you configure in this table are available for the devices included in this site in the **Configure Device** window.

Click the **Add** (Add) button to add a port template to the table.

Select a port template and select the **Edit** (Edit) button to make changes to the selected port template.

Select a user-created port template and select the **Delete** (Delete) button to delete it from the table. You can not delete system-defined port templates.

Select the **Local Only** button as a toggle button to display local templates only and, alternately, to display all templates.

Click **Save** to save your additions or changes.

The following columns are included on the **Ports Templates** panel:

Source
Indicates the site which defines the values used for the Port Template.

- Port templates with a **Source** of **Global** can only be edited in the /World site.
- A **Source** of **Local** indicates that the values are coming from the currently selected site. In order to change the value of a Port Template, select the **Port Templates** tab for the site that shows the **Source** as **Local**. When creating a new site, the values of the new site's Port Templates are inherited from the parent site.

  When you create port template after creating a new site, the new port template is also

created in the /World site. All port templates in the /World site display a **Local** for **Source**. You can modify the values of the port template in both the /World site and in the site where the port template was created. Sites that are the children of the /World site display the **Source** for the port template values as /World. Sites that are the children of the site in which the port template was created display the **Source** for the port template values as the site where the port template was created.

When the **Source** is not **Local**, the port template values act like default values for the site. Editing the port template in the site and changing the **Source** to **Local** allows you to edit the port template for the current site and the sites that are children of that site.

Configuration

Indicates the purpose of a port. Defines the behavior of ports on devices in a site, based on the role of that port. After you configure your port templates in this table, select the **Configuration** for devices in the site in the **Configure Device** window. The configuration of the port is initially discovered by ExtremeCloud IQ Site Engine during discovery or during a ZTP+ process, but can be changed to meet the needs of the devices in your site. The following port types are included:

- **Access**
  Applies access port template settings to the device in the site.
- **Interswitch**
  Applies interswitch port template settings to the device in the site.
- **Management**
  Applies management port template settings to the device in the site.
- **AP**
  Applies AP port template settings to the device in the site.
- **Phone**
  Applies phone port template settings to the device in the site.
- **Router**
  Applies router port template settings to the device in the site.
- **Printer**
  Applies printer port template settings to the device in the site.
- **Security**
  Applies security port template settings to the device in the site.
- **IoT**
  Applies guest or external device port template settings to the device in the site.
- **vSwitch**

Applies virtual switch port template settings to the device in the site.

- **Other**

PVID

The port's VLAN ID.

The PVID value "None [0]" means incoming untagged traffic is not assigned to any VLAN. The value "None [0]" is compatible with Switch Engine persona devices.

Default Role

The policy role assigned to the selected port. To assign policy to the selected port, select **Add Device to Policy Domain** and select a **Policy Domain** from the drop-down list in the **Actions** tab. ExtremeCloud IQ Site Engine assigns policy to the port after a successful policy domain enforce.

Authentication

Use the drop-down list to determine whether authentication is configured to the port:

- **None** — No authentication is required to access the port.
- **802.1X** — Select this option to enable 802.1X authentication to the port.
- **MAC Auth** — Select this option to enable authentication based on the users MAC address.

WARNING: Configuring the authentication could affect communication to a device and result in loss of connectivity through the interswitch link ports if not detected or configured properly during the discovery process. If you are configuring the policy and authentication on the interswitch link, it's strongly recommended to ensure neighbor discovery protocols such as LLDP, EDP, and CDP are enabled before enabling the authentication using port templates.

VLAN Trunk

Automatically configures a port as a VLAN trunk when you check one box in the VLAN Trunk column. For more information, see Fabric Assist.

Tagged

Indicates the port's egress state is tagged. If you check the VLAN Trunk column, Fabric Assist automatically configures all the VLANs on the port as tagged. For more information, see Fabric Assist.

Fabric Enable

Indicates the fabric functionality is enabled on the port.

NOTE: **Fabric Enable** options are only configurable for Global port templates. You can create a global port template on the World site level.

ExtremeCloud IQ Site Engine can extend FA functionality to ExtremeXOS/Switch Engine devices and provision them as FA Proxy devices. Select **Fabric Attach** or **Fabric Attach and Switched UNI** or **Auto Sense** from the drop-down list to enable the port on a Fabric Engine device (acting as FA Server) to connect to an ExtremeXOS/Switch Engine device (acting as FA Proxy).

- **Fabric Attach** - Enable Fabric Attach server functionality on the port of a Fabric Engine device acting as a Fabric Attach server) to connect to an ExtremeXOS/Switch Engine device (acting as a Fabric Attach proxy).
- **Fabric Attach and Switched UNI** - Enable Fabric Attach server functionality on the port of a Fabric Engine device acting as a Fabric Attach server) to connect to an ExtremeXOS/Switch Engine device (acting as a Fabric Attach proxy). When selecting this option, the port is configured for both features, but only one feature is active at any one time.
- **Auto Sense** - Select **Auto Sense** on the port of a Fabric Engine device to enable the port to automatically sense and configure automatically sense and configure the appropriate Fabric settings for the port. These settings include the following:
  - PVID
  - VLAN Trunk
  - Tagged
  - Untagged
  - Fabric Mode
  - Fabric Auth Type
  - Fabric Auth Key
  - Fabric Connect Drop STP-BPDU
  - BPDU Guard
  - Authentication

  NOTE: If **Fabric Enable** is **Auto Sense** the Fabric settings listed above are not configurable.

Fabric Auth Type
Indicates the fabric authentication type used on the port.

Fabric Auth Key
Indicates the fabric authentication key used for the port.

Fabric Connect Drop STP-BPDU
Indicates the fabric-enabled port drops Spanning Tree Protocol BPDUs.

Untagged
Indicates the port's egress state is untagged.

Node Alias
Select to enable the node alias function on the port. The node alias settings are automatically enabled if Access Control is enabled on the device.

Span Guard
Select to enable Span Guard, which allows the device to shut down a network port if it receives a BPDU (bridge protocol data unit). Enable this feature on network edge ports to prevent rogue STA-aware devices from disrupting the existing Spanning Tree.

Loop Protect
Select to prevent loop formation in a network with redundant paths by requiring ports to receive type 2 BPDUs (RSTP/MSTP) on point-to-point interswitch links.

- If the ports receive the BPDUs, the link's **State** becomes **Forwarding**.
- If a BPDU timeout occurs on the ports, its **State** becomes **Listening** until a BPDU is received.

MVRP
Indicates that the Multiple VLAN Registration Protocol (MVRP) is enabled for the port. If MVRP has been enabled globally, interswitch ports are automatically enabled and access ports default to disabled.

SLPP
Indicates Simple Loop Prevention Protocol (SLPP) is enabled on the port. SLPP provides active protection against Layer 2 network loops on a per-VLAN basis. If an SLPP packet is received, the port is disabled for the amount of time configured in the **SLPP Timer** field.

NOTE: If **SLPP** is enabled, **SLPP Guard** is not available.

SLPP Guard
Indicates whether SLPP Guard is enabled on the port. Use SLPP Guard to provide additional loop protection to protect wiring closets from erroneous connections. SLPP Guard requires **SLPP** to be enabled. SLPP detects loops in an SMLT network. Because SMLT networks disable Spanning Tree (STP), Rapid Spanning Tree (RSTP), or Multiple Spanning Tree Protocol (MSTP) for participating ports, SLPP Guard provides additional network loop protection, extending the loop detection to individual edge access ports. SLPP Guard can be configured on MLT or LAG ports. If the edge switch with SLPP Guard enabled receives an SLPP-PDU packet on a port, SLPP Guard operationally disables the port for the configured timeout interval in the **SLPP Guard Timer** field and appropriate log messages and SNMP traps are generated. If the disabled port does not receive any SLPP-PDU packets after the configured timeout interval expires, the port automatically reenables and generates a local log message, a syslog message, and SNMP traps, if configured.

NOTE: If **SLPP Guard** is enabled, **SLPP** is not available

SLPP Guard Timer
Indicates the amount of time after receiving an SLPP packet before the port is reenabled.

DHCP Snooping
Specifies the trust factor of the port for DHCP Snooping. The agent at the switch determines if DHCP reply packets are forwarded based on the DHCP Snooping mode of the VLAN and the trusted state of the port. If the value is "Trusted", the agent trusts the device on the port. If the value is "Untrusted", the agent does not trust the device on the port.

ARP Inspection
Dynamic ARP Inspection (DAI) is a security feature that validates ARP packets in the network. Without DAI, a malicious user can attack hosts, switches, and routers connected to the Layer 2 network by poisoning the ARP caches of systems connected to the subnet and intercepting traffic intended for other hosts on the subnet. DAI can prevent attacks by intercepting, logging, and discarding the ARP packets with invalid IP to MAC address bindings. The switch dynamically builds the address binding table from the information gathered from the DHCP requests and replies when DHCP Snooping is enabled. The switch pairs the MAC address from the DHCP request with the IP address from the DHCP reply to create an entry in the DHCP binding table. Values are "Trusted" and "Untrusted".

Source Guard
IP Source Guard (IPSG) is a Layer 2 port-to-port feature that works closely with DHCP Snooping. IPSG can prevent IP spoofing by allowing only IP addresses obtained using DHCP Snooping. When you enable IPSG on an untrusted port with DHCP Snooping enabled, an IP filter is automatically created or deleted for that port based on the information stored in the corresponding DHCP Snooping binding table entry. When a connecting client receives a valid IP address from the DHCP server, the filter installed on the port allows traffic only from that assigned IP address. If the value is "Disabled" the Source Guard is disabled. If the value is "IP" the IP Source Guard feature is enabled.

PoE Enable
Indicates that power over ethernet (PoE) is enabled for the port.

PoE Priority
Indicates the priority of PoE for the port; **LOW**, **HIGH**, or **CRITICAL**.

Collection Mode
Indicates the mode to collect port statistics.

Collection Interval (minutes)
Indicates the interval (in minutes) at which port statistics are collected.

ZTP+ Automated Templates

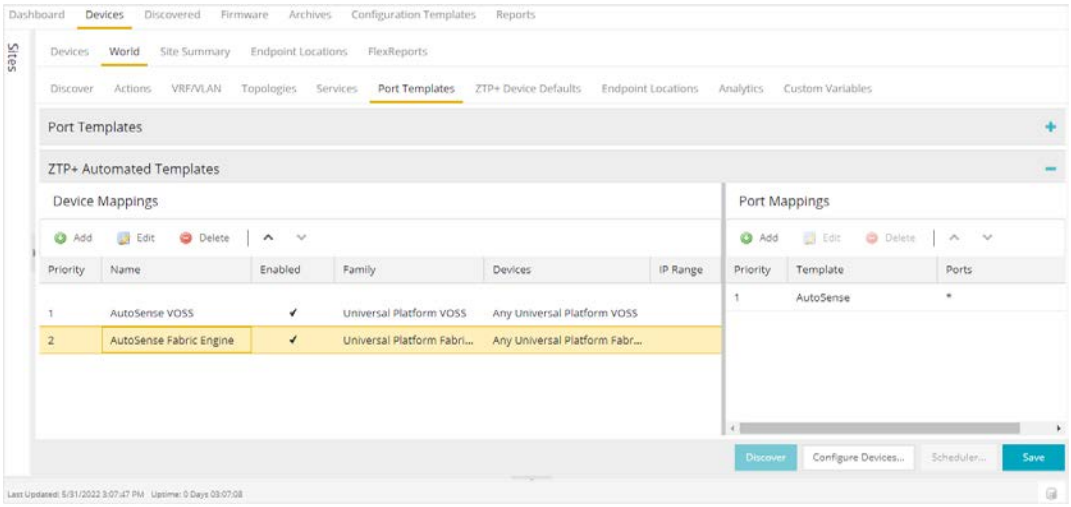
The **ZTP+ Automated Templates** displays information about templates configured by family. These templates are listed in priority order, which means they are evaluated in the order they are displayed. You can change the order by using the priority arrows in the toolbar or dragging and dropping a template.

NOTE: ExtremeCloud IQ Site Engine supports automated port templates for ZTP+ devices only.

The automated port templates panel has two sections: Device Mappings on the left and Port Mappings on the right.

On the left side, specify the name for the Device Mapping and then select the family and devices you want to apply the template to. Optionally, you can also match based on an IP range.

The right side displays the port mappings associated with the device mapping that you selected on the left side. The bindings are in priority order, and the template matches the ports in the order they are listed. You can change the order by using the priority arrows in the toolbar or dragging and dropping a template.



Click **Add** (Add) to add a device mapping to the table.

Select a device mapping and select **Edit** (Edit) to make changes.

Select a device mapping and select **Delete** (Delete) to delete it from the table.

Click **Save** to save your changes.

The following columns are included on the **Device Mappings** panel:

Priority
Displays the order in which device mappings are evaluated.

Name
The name of the device mapping.

Enabled
Indicates whether the device mapping is enabled or disabled.

Family
Specifies the family of devices to which the device mapping applies.

Devices
Specifies which device within the family to which the template applies.

IP Range
Specifies a single IP address or a range of addresses in the following formats:

- 1.2.3.4 (v4)
- 1111:2222::3333:4444 (v6)
- 1.2.3.4/24 (v4 with mask)
- ::1/64 (v6 with mask)
- 1.2.3.4-2.3.4.5 (range)
- 1::1-1::2 (range)

The following columns are included in the **Port Templates** panel:

Priority
Displays the order in which port templates are evaluated.

Template
Displays the list of available automated port templates.

Port Binding accepts any of the following formats (device dependent):

- 1 (single port)
- 1-5 (port range)
- 1,3,5 (comma separated ports)
- 1-3,5-7 (comma separated port ranges)
- * (wildcard)

Ports
Displays the list of configured ports next to their associated template. For devices that require slot and port numbers, use the appropriate format for the device:

- Single Port:
  - 210-Series: "1/1" or "1/1, 1/3, 1/5, 1/7"
  - 220-Series: "1/0/1" or "1/0/1, 1/0/3, 1/0/5, 1/0/7"
  - ERS: "1/1" or "1/1, 1/3, 1/5, 1/7"
  - ExtremeXOS/Switch Engine: "1:1" or "1:1,1:3,1:5,1:7"

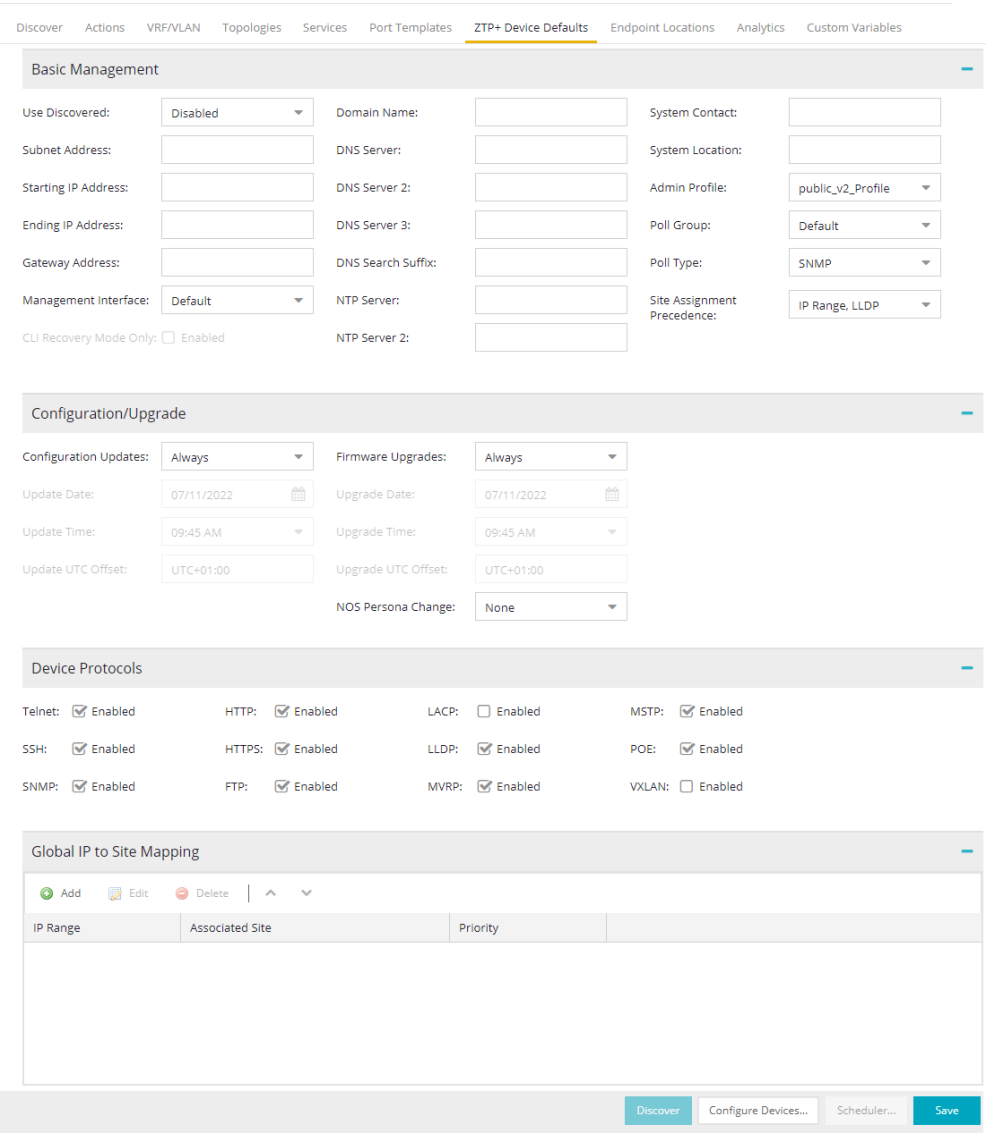
        - ExtremeXOS/Switch Engine Stack/VPEX: "1:1" or "1:1, 1:3, 1:5, 1:7"
        - SLX: "Ethernet 0/1" or "Ethernet 0/1, Ethernet 0/3"
    - Port Ranges:
        - 210-Series: "1/5-1/7" or "100/5-100/7, 111/9-111/12, 113/15-113/19"
        - 220-Series: "1/0/1-1/0/5" or "1/0/1, 1/0/3, 1/0/5, 1/0/7"
        - ERS: "1/5 - 1/7" or "100/5-100/7, 111/9-111/12, 113/15-113/19"
        - ExtremeXOS/Switch Engine: "1:5-1:7" or "1:5-1:7, 1:9-1:12, 1:15-1:19"
        - ExtremeXOS/Switch Engine Stack: "1:5-1:7" or "1:5-1:7, 2:9-2:12, 3:15-3:19"
        - ExtremeXOS/Switch Engine channelized ports are included in the master port: "1:24" is equal to "1:24:1,1:24:2,1:24:3,1:24:4"
        - SLX: "Ethernet 0/1-Ethernet 0/4" or "Ethernet 0/1-Ethernet 0/5, Ethernet 0/8-Ethernet 0/15"
    - Wildcarding:
        - "*" is always allowed, matches anything, useful as default rule at the end of a set of bindings
        - In a single port scenario, the wildcard may be applied as the slot or port value:
            - 210-Series: "*/1" or "1/*"
            - 220-Series: "*/0/1" or "1/0/*"
            - ERS: "*/1" or "1/*"
            - ExtremeXOS/Switch Engine: "*"
            - ExtremeXOS/Switch Engine Stack/VPEX: "*:1" or "1:*"
            - SLX: "Ethernet 0/*" or "Ethernet */3,Ethernet */5"
    - Port ranges support limited use of wildcards: for port ranges in the slot/port or slot/unit/port format, use the wildcard on the same item.

To refresh the port templates, go the **Devices** view and select one or more port templates. Then, right-click **More Actions > Refresh ZTP+ Automated Templates**. This updates the port template settings on all selected devices based on the configured automated port templates. This action also creates an operation in the Operations view and generates an event detailing the results.

After configuring the automated port templates, when ExtremeCloud IQ Site Engine discovers devices via ZTP+ and asks for configuration, the automated port templates are automatically assigned to the ports on the device.

ZTP+ Device Defaults

The **ZTP+ Device Defaults** tab contains information about a device with ZTP+ (Zero Touch Provisioning Plus) enabled. Use the following dialog to specify the parameters that should be used during the process of learning about a ZTP+ device. ExtremeCloud IQ Site Engine then applies these configuration templates to devices that you add to a site in your network.



Basic Management

Use Discovered

Use the drop-down list to select if ExtremeCloud IQ Site Engine assigns the IP address, IP address and Management Interface, or Management Interface to the ZTP+ device when it is discovered:

- **IP** — ExtremeCloud IQ Site Engine uses the **Discovered IP** assigned when the device was discovered. Select the **Management Interface** (the VLAN interface used to manage the device) manually.
- **IP and Management Interface** — ExtremeCloud IQ Site Engine uses the **Discovered IP** and the **Management Interface** that were assigned when the device was discovered.
- **Management Interface** — ExtremeCloud IQ Site Engine uses the **Management Interface** that was defined when the device was discovered. Enter the IP address and subnet, Gateway Address, Domain Name, and DNS Server in the tab (along with any of the optional fields) and then save.
- **Disabled** — Configure the IP address and subnet, Gateway Address, Domain Name and DNS Server in the tab (along with any of the optional fields) and then save.

Subnet Address

Enter the **Subnet Address** for the ZTP+ devices associated with the site.

Starting IP Address

The **Starting IP Address** field allows you to set the starting IP address of the IP address range for the ZTP+ devices associated with the site.

Ending IP Address

The **Ending IP Address** field allows you to set the ending IP address of the IP address range for the ZTP+ devices associated with the site.

Gateway Address

Enter the **Gateway Address** for the ZTP+ devices associated with the site.

Management Interface

Select the interface that the device uses for Management and assign the device IP to that interface.

CLI Recovery Mode Only

Select the checkbox to disable the CLI account while the device is able to communicate with ExtremeCloud IQ Site Engine. If connectivity between the device and ExtremeCloud IQ Site Engine is lost, the device enables the CLI account defined in the profile so the user can gain local access. When connectivity between the device and ExtremeCloud IQ Site Engine is re-established, the CLI account is disabled again.

NOTE: Only devices managed using ZTP+ support this functionality.

Domain Name

Enter a value in the **Domain Name** field to configure the domain name on the ZTP+ devices associated with the site.

DNS Server

The **DNS Server** field allows you to set the DNS server address on the ZTP+ devices associated with the site.

DNS Server 2

The **DNS Server 2** field allows you to set the secondary DNS server address on the ZTP+ devices associated with the site.

DNS Server 3

The **DNS Server 3** field allows you to set the tertiary DNS server address on the ZTP+ devices associated with the site.

DNS Search Suffix

The **DNS Search Suffix** field allows you add additional comma-separated entries to DNS search suffix list configured on the device. Support for the DNS search suffix is dependent on the device operating system and version. Refer to your device specifications to determine the maximum number of entries that you can add.

NTP Server

The **NTP Server** field allows you to set the NTP server address on the ZTP+ devices being discovered.

NTP Server 2

The **NTP Server 2** field allows you to set the secondary NTP server address on the ZTP+ devices associated with the site.

System Contact

Allows you to specify contact information for the person maintaining the device. Additionally, enter a backslash "\" between contacts to create a device group in a tiered tree structure. For example, to move the device into a device group called "John's Devices" within a device group called "Quality Assurance Testing", enter **Quality Assurance Testing\John's Devices** in this field.

System Location

A description of the location of the ZTP+ devices associated with the site.

Admin Profile

Use the drop-down list to select the access Profile that gives ExtremeCloud IQ Site Engine administrative access to the ZTP+ devices associated with the site. Use the Profiles list in the Discover section of the **Site** tab to create or edit a profile. If you discover an existing device using a different profile than the device is already using in the database, click **Save** to overwrite the device profile currently being used in the database.

Poll Group

Use the drop-down list to select a Poll Group for the discovered ZTP+ devices. ExtremeCloud IQ Site Engine provides three distinct poll groups (defined in the Status Polling options (**Administration** > **Options**) that each specify a unique poll frequency. When you save newly discovered devices to the database, they are polled with the poll group specified here. If you save discovered devices that already exist in the database, the poll group specified here overwrites the poll group currently being used in the database.

NOTE: If you select **Not Polled**, the **Poll Group** is only used if/when the **Poll Type** is changed to **SNMP** or **Ping**.

Poll Type

Use the drop-down list to select the Poll Type for devices included in the site:

- Select **Not Polled** if you do not want to poll the devices.
- Select **Ping** for the **Poll Type** if the **Profile** for the IP Range is also set to **Ping**.
- Select **SNMP** to poll the device using SNMP. The SNMP version (SNMPv1 or SNMPv3) is determined by the Profile specified for the IP Range.
- Select **Maintenance** if you do not want to poll the devices temporarily. Using this **Poll Type** allows you to search for devices set to **Maintenance** to change them back to their regular **Poll Type** when maintenance on the device is complete.
- Select **ZTP+** for devices managed by ZTP+ and created through the ZTP+ process. When the **Poll Type** is **ZTP+** the ExtremeCloud IQ Site Engine does not initiate a poll, instead the ExtremeCloud IQ Site Engine receives a message from the device to determine the status. The ZTP+ Poll Type is incompatible with Switch Engine devices running with FIPS mode enabled.

  For example, if ExtremeCloud IQ Site Engine does not receive a message from a device or Fabric Manager for three times the amount of time defined in the **Poll Interval** for the **Poll Group** of the device, then the **Status** is **Contact Lost**. When ExtremeCloud IQ Site Engine receives a message from the device, the **Device Status** is **Contact Established**.

Site Assignment Precedence

Set the precedence by which ZTP+ devices will be assigned to the site. This field is used in conjunction with the Global IP to Site Mapping settings in determining the site assignment. For example, during the device configuration, if the precedence is set to IP range only, the device will try to match any of the single IP addresses or fit within a range. If an IP does not match any value in the table then it will default to /World.

The following values can be configured:

- **IP Range, LLDP:** Uses IP range first. If no IP range is set, uses LLDP instead.
- **LLDP, IP Range:** Uses LLDP first. If LLDP is not available, uses IP range instead.
- **LLDP Only:** Uses LLDP only.
- **IP Range Only**: Uses IP range only.
- **None:** Uses neither LLDP or IP range.

All discovered ZTP+ devices are assigned to the site based on the this value. However, you can manually change the value for individual devices in the device configuration.

If there are multiple IP ranges that match the site, the device will use the mapping that has the highest priority.

Configuration/Upgrade

Configuration Updates

Select the frequency for which ExtremeCloud IQ Site Engine checks for configuration updates for devices with a **Poll Type** as **ZTP+** associated with the site.

The following values can be configured:

- **Always:** Operations are checked on every ZTP+ check-in.
- **Never:** Operations are skipped for every ZTP+ check-in.
- **Scheduled:** The operation only occurs after the selected date or time, then reverts to Never.
- **Suspend:** The operation is skipped until the selected date or time, then reverts to Always.

NOS Persona Change

Select To Fabric Engine to change the Network Operating System (NOS) of a universal switch currently running Switch Engine to Fabric Engine. The NOS Persona Change field has values of None and To Fabric Engine. The persona change to Fabric Engine requires a Fabric Engine firmware in Set as Reference image,

When the switch completes the persona change from Switch Engine to Fabric Engine, all previous Switch Engine references for the switch are removed from ExtremeCloud IQ Site Engine. Including but not limited to the Discovered panel, and the Device Tree. You must now stage configuration for the 'new' Fabric Engine switch in ExtremeCloud IQ Site Engine.

IMPORTANT:

The NOS persona change **To Fabric Engine** is ignored if:

- The universal switch is running EXOS (Upgrade to Switch Engine before changing persona)
- The non-universal switch is running EXOS (A firmware upgrade for EXOS occurs if the EXOS image is set as reference image)
- You did not specify a Fabric Engine reference image (The destination firmware must be a Fabric Engine firmware set as reference image)

A Switch Engine reference image is not required. If you only specify a Fabric Engine firmware in **Set as Reference Image**, then only one firmware upgrade occurs on the switch during the change from Switch Engine to Fabric Engine, which increases the persona change speed.

Upload the Fabric Engine firmware to both of the TFTP and SFTP directories (Network > Firmware > Upload...). You must specify the Fabric Engine firmware located in the SFTP directory as a reference image.

NOTE:

You can specify one reference image for upgrading EXOS to Switch Engine, and another reference image for a persona change from Switch Engine to Fabric Engine.

If you specify reference images for Switch Engine and for Fabric Engine and the universal switch is not currently running the Switch Engine reference image, a firmware upgrade for Switch Engine occurs before the persona change to Fabric Engine.

Update Date

Select the date on which ExtremeCloud IQ Site Engine updates the configuration for your devices with a **Poll Type** as **ZTP+** associated with the site when you select **Scheduled** for **Configuration Updates**.

Update Time

Select the time at which ExtremeCloud IQ Site Engine updates the configuration for your devices with a **Poll Type** as **ZTP+** associated with the site when you select **Scheduled** for **Configuration Updates**.

Update UTC Offset

Select your time zone based on the number of hours you are offset from the Universal Time Coordinated.

Firmware Upgrades

Select the frequency for which ExtremeCloud IQ Site Engine checks for firmware upgrades for your devices with a **Poll Type** as **ZTP+** associated with the site.

Upgrade Date
Select the date on which ExtremeCloud IQ Site Engine upgrades the firmware for your devices with a **Poll Type** as **ZTP+** associated with the site when you select **Scheduled** for **Firmware Upgrades**.

Upgrade Time
Select the time at which ExtremeCloud IQ Site Engine upgrades the firmware for your devices with a **Poll Type** as **ZTP+** associated with the site when you select **Scheduled** for **Firmware Upgrades**.

Upgrade UTC Offset
Select your time zone based on the number of hours you are offset from the Universal Time Coordinated.

Device Protocols/Features

Telnet
Select the checkbox to enable Telnet access on the ZTP+ device.

SSH
Select the checkbox to enable SSH (Secure Shell) access on the ZTP+ device.

HTTP
Select the checkbox to enable HTTP (Hypertext Transfer Protocol) access on the ZTP+ device.

HTTPS
Select the checkbox to enable HTTPS (Hypertext Transfer Protocol Secure) access on the ZTP+ device.

NOTE: To enable HTTPS access, an SSL certificate must be configured on the device.

SNMP
Select the checkbox to enable SNMP (Simple Network Management Protocol) access on the ZTP+ device.

LACP
Select the checkbox to enable LACP (Link Aggregation Control Protocol) access on the ZTP+ device.

LLDP
Select the checkbox to enable LLDP (Link Layer Discovery Protocol) access on the ZTP+ device.

MSTP
Select the checkbox to enable MSTP (Multiple Spanning Tree Protocol) access on the ZTP+ device.

MVRP
Select the checkbox to enable MVRP (Multiple VLAN Registration Protocol) access on the ZTP+ device.

POE
Select the checkbox to indicate the ZTP+ devices being discovered for the site are electrically powered by Ethernet cable.

VXLAN
Select the checkbox to indicate the ZTP+ devices being discovered for this site use VXLAN to tunnel Layer 2 traffic over a Layer 3 network.

NOTE: ZTP+ does not currently provision a Layer 3 network with which VXLAN operates. If your ZTP+ devices use VXLAN, the Layer 3 underlay network must be manually provisioned.

DvR Leaf
Select the checkbox to indicate the ZTP+ devices being discovered for the site operate in DvR Leaf mode. The DvR Leaf flag is enabled. Only devices running Fabric Engine support the DvR Leaf feature.

Global IP To Site Mapping

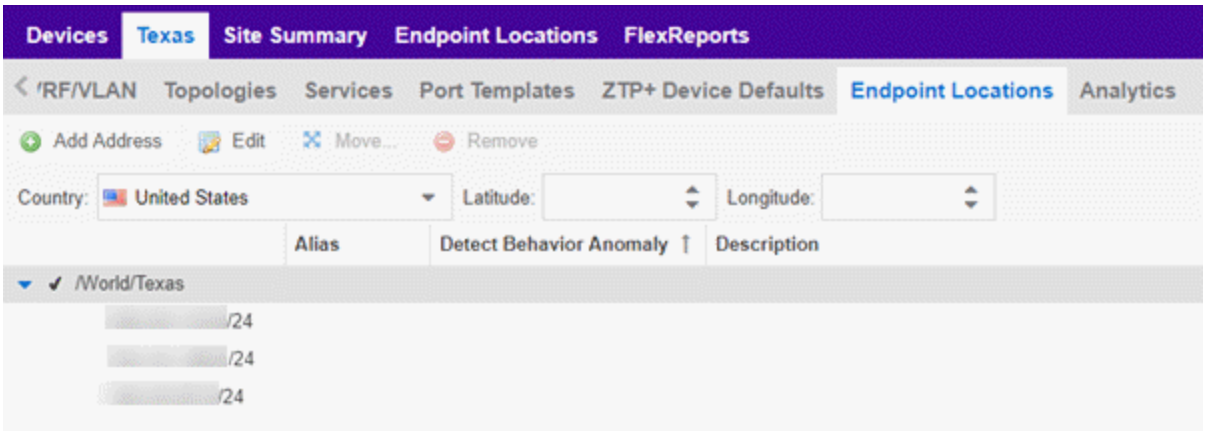
IP Range
Select **Add** or **Edit** to enter a single IP address or an IP range.

Associated Site
Select a site from the drop-down list that the discovered ZTP+ devices will be associated with when the devices are discovered.

Endpoint Locations

Use the **Endpoint Locations** tab to define the geographical location of the site and addresses in it. After the geographical locations are defined for your devices, flows on the Application Flows tab display geographical information depending on the device on which the flow is observed.

Select the **Add Address** button at the top of the table to add an additional address to the table. Select the **Edit** button to modify the site or selected address of the site. The **Move** button allows you to move an address to a different site in the drop-down list. Select the **Remove** button to delete a selected address from the table. These options are also accessible when you right-click an address in the table.



Use the Country, Latitude, and Longitude drop-down lists to configure or change the following information for the site:

Country
: Select the country in which the site is located.

Latitude
: Enter the site's latitude location in decimal degrees.

Longitude
: Enter the site's longitude location in decimal degrees.

The following columns are displayed in the Endpoint Locations table:

Tracked
: This column displays the name of the site or the IP Address/Mask of the devices on the site. A check mark to the left of the site name indicates it is a Tracked Site. Right-click any site to either add or remove the site from your Tracked Sites list.

Alias
: An alternate name for the site, or a specific subnet of the site.

Description
: A description of the site location.

Analytics

The **Analytics** tab allows you to configure the default ExtremeAnalytics functionality for the devices in the site.

Analytics Role
: Allows you to indicate the purpose of the devices added to the site: **Access**, **Core**, **Data Center**, **DMZ**. This field is informational only.

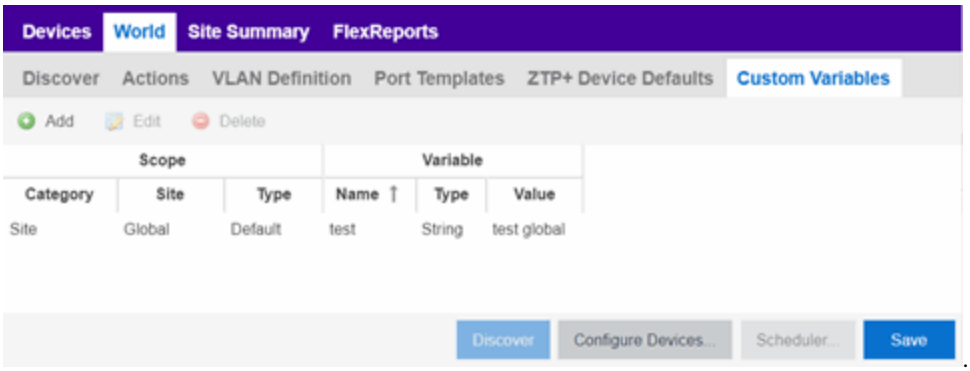
Analytics Home Engine
: Displays the ExtremeAnalytics engine located with the devices associated with the site.

Custom Variables

The **Custom Variables** tab allows you to add, edit, or delete variables used in ExtremeCloud IQ Site Engine.

Variables you create serve as a placeholder for a specific value. The fields included in the **Scope** section determine where the variable is used in ExtremeCloud IQ Site Engine, while the fields in the **Variable** section allow you to define a value for the variable. After you create a variable, ExtremeCloud IQ Site Engine automatically substitutes the **Value** you define in the appropriate feature of ExtremeCloud IQ Site Engine when the criteria specified in the **Scope** section is met. Variables you create on the **Site** tab can then be used in a configuration template, script or workflow, in a CLI command, or in a third-party application via the Northbound Interface.

NOTE: Custom variables you create are not displayed in ExtremeCloud IQ Site Engine. To view and reference the variables, use the Northbound Interface functionality in the **Diagnostics** tab.



Scope

Category

Displays where the variable is used in ExtremeCloud IQ Site Engine. Select **Port Template**, **Site**, or **Topology** from the drop-down list, depending on the purpose of the variable.

Site

Defines the site in which the variable is used.

- **Global** indicates ExtremeCloud IQ Site Engine uses the variable for all sites.
- Selecting **/World** indicates ExtremeCloud IQ Site Engine uses the variable for all devices added to the /World site. Devices added to a site other than /World do not use the variable.
- Selecting the current site also creates an additional variable with a **Site** of **Global**. This allows you to use the variable in workflows run on devices not included in the current site.

Type
Defines the type of Port Template or Topology for which the variable applies. The values in this drop-down list change depending on what **Category** you select.

- Port Template — Indicates the Port Configuration for which the variable is used by ExtremeCloud IQ Site Engine.
- Topology — Displays the type of network topology for which the variable is used by ExtremeCloud IQ Site Engine.

Variable

Name
Displays the name of the variable.

Type
Defines the type of information the variable is substituting. Select **Boolean**, **IP**, **MAC Address**, **Number**, **String**, or **Subnet** from the drop-down list.

Value
Displays the value ExtremeCloud IQ Site Engine uses when substituting the variable. Enter a value associated with the variable type you define. For example, if the variable type is **Boolean**, choose **True** or **False**; if the attribute type is **IP**, enter the IP Address of the variable).

Add
Click the button to add a row to the table where you can create a new custom variable.

Edit
Select a variable in the table and select **Edit** to make changes to a custom variable.

Delete
Select a variable in the table and select **Delete** to remove a custom variable from the table.

Update
Click the **Update** button when you finish adding a new or editing an existing custom variable.

Cancel
Click the **Cancel** button to cancel the new variable or the changes you made to an existing variable.

XIQ Location

Devices assigned to the site are automatically mapped to the specified locations in ExtremeCloud IQ, and the XIQ location is assigned on the site level. Values in the drop down are obtained from ExtremeCloud IQ. The assignment of the device to the XIQ location is configurable in the ExtremeCloud IQ Site Engine, but not in ExtremeCloud IQ.

NOTE: The XIQ Location tab is only displayed in connected deployment mode.

Buttons

Edit Devices

Clicking **Configure Devices** opens the **Configure Device** window for all of the devices added to the site. This allows you to change the configuration of a single device or a subset of devices within the site.

Save

Clicking **Save** saves any changes you make to a site. This button displays after making a change to the tab.

Cancel

Clicking **Cancel** discards any changes you make to a site. This button displays after making a change to the tab.

Discover

Clicking **Discover** adds to the site any new devices that match the criteria entered in the Discover section of the window. This button displays after selecting **Create** or **Save**.

Scheduler

Clicking **Scheduler** opens the **Add Scheduled Task** window, where you can create a new task that automatically adds devices matching the criteria entered in the Discover section of the **Site** tab to the site. This button displays after selecting **Create** or **Save**.

NOTE: After you create a scheduled task to discover devices, edit or delete the task on the **Scheduled Tasks** tab.

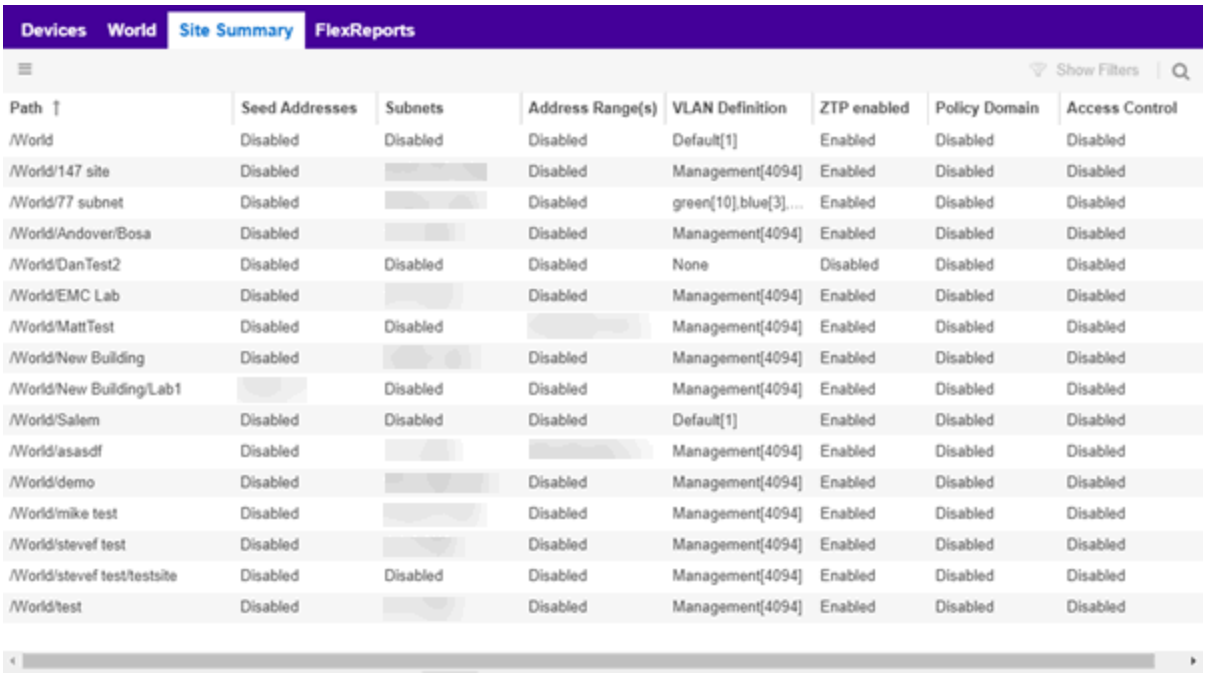
For information on related topics:

- How to Discover Devices in ExtremeCloud IQ Site Engine
- Devices
- Maps
- How to Create and Edit Maps
- Advanced Map Features

Site Summary

The **Site Summary** tab contains a table that lists all of the Sites created on your network.

Access the **Site Summary** tab by opening the **Devices** tab and selecting the **Site Summary** tab in the right-panel.



Path	Seed Addresses	Subnets	Address Range(s)	VLAN Definition	ZTP enabled	Policy Domain	Access Control
/World	Disabled	Disabled	Disabled	Default[1]	Enabled	Disabled	Disabled
/World/147 site	Disabled		Disabled	Management[4094]	Enabled	Disabled	Disabled
/World/77 subnet	Disabled		Disabled	green[10],blue[3],...	Enabled	Disabled	Disabled
/World/Andover/Bosa	Disabled		Disabled	Management[4094]	Enabled	Disabled	Disabled
/World/DanTest2	Disabled	Disabled	Disabled	None	Disabled	Disabled	Disabled
/World/EMC Lab	Disabled		Disabled	Management[4094]	Enabled	Disabled	Disabled
/World/MattTest	Disabled	Disabled		Management[4094]	Enabled	Disabled	Disabled
/World/New Building	Disabled		Disabled	Management[4094]	Enabled	Disabled	Disabled
/World/New Building/Lab1		Disabled	Disabled	Management[4094]	Enabled	Disabled	Disabled
/World/Salem	Disabled	Disabled	Disabled	Default[1]	Enabled	Disabled	Disabled
/World/asasdf	Disabled			Management[4094]	Enabled	Disabled	Disabled
/World/demo	Disabled		Disabled	Management[4094]	Enabled	Disabled	Disabled
/World/mike test	Disabled		Disabled	Management[4094]	Enabled	Disabled	Disabled
/World/stevef test	Disabled		Disabled	Management[4094]	Enabled	Disabled	Disabled
/World/stevef test/testsite	Disabled	Disabled	Disabled	Management[4094]	Enabled	Disabled	Disabled
/World/test	Disabled		Disabled	Management[4094]	Enabled	Disabled	Disabled

You can edit a site within the table by selecting the site row, selecting the **Menu** (☰) button, and selecting **Edit** ( ). The Site tab opens for the site you selected, which allows you to configure devices included in the site.

The following columns are included on the **Site Summary** tab:

Path
The full path of the site.

Seed Addresses
Any Seed Address Discover Types that are configured for the site.

Subnets
Any Subnets Discover Types that are configured for the site.

Address Range(s)
Any Address Range Discover Types that are configured for the site.

VLAN Definition
The VLAN Definition for the site.

ZTP
Indicates whether ZTP+ (Zero Touch Provisioning Plus) is enabled for the site.

Policy Domain
Displays the policy domain to which devices added to the site are assigned.

Access Control
Displays the Access Control's engine group to which devices added to the site are assigned.

Analytics Role
Displays the purpose of the devices added to the site: **Access**, **Core**, **Data Center**, **DMZ**.

Analytics Home Engine
Displays the ExtremeAnalytics engine located with the devices associated with the site.

XIQ Location
Indicates whether devices assigned to the site are mapped to the specific locations in ExtremeCloud IQ. The XIQ Location is assigned on the site level and values are only present in ExtremeCloud IQ Site Engine deployments in connected mode.

For information on related topics:

- Devices
- Site
- Maps

Compare Device Configurations

You can compare archived device configurations in ExtremeCloud IQ Site Engine by using either the **Network** > **Devices** tab or the Archive Details Report available in the **Network** > **Reports** tab.

In order to perform the compare configuration operation, you must be a member of an authorization group with the Inventory Manager > Configuration Archive Management > View/Compare Configurations capability.

This Help topic provides the following information:

- Selecting the Files to Compare
- Comparing the Files

Selecting the Files to Compare

Select the files to compare using either the **Network** tab or the **Reports** tab.

From the Network tab:

Use the **Network** tab to compare the last two archived configuration files for a device.

Select a device in the table and use either the **Menu** icon (☰) or the right-click menu off the device to select **More Actions** > **Compare Last Configurations**.

From the Reports tab:

Use the **Reports** tab to compare two configuration files selected from all archived files for the device.

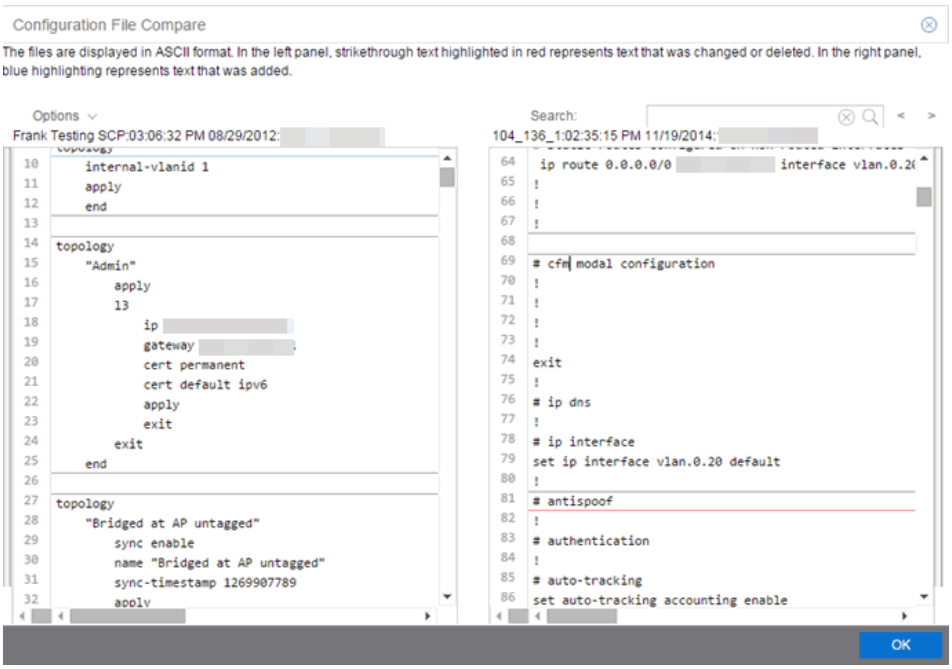
Select the Device > Device Archives report. Select the **Archive Details** tab in the right panel and then select the **Archives by Device** sub-tab.

The tab displays all the ExtremeCloud IQ Site Engine archives by device IP address. Select two files to compare and select **Compare Configuration**.

Comparing the Files

The Configuration File Compare window displays the files in two panels. Titles over each file show the archive name that contains the configuration file, the date, and the IP address of the device from which you create the configuration file.

Scroll through the two files to view file differences. Typically, the newer file displays in the right panel. You can use the "Swap sides" option to swap the files. In the left panel, strikethrough text highlighted in red represents text that is changed or deleted. In the right panel, blue highlighting represents text that is added.



Use the toolbar Options menu to control the look of the display window:

- Enable line numbers displays line numbers alongside the text.
- Wrap lines shows all the text in the column and removes the horizontal scroll bars.
- Enable side bars shows where the text differences are in the whole file.
- Swap sides swaps the files contained in the left and right panels.

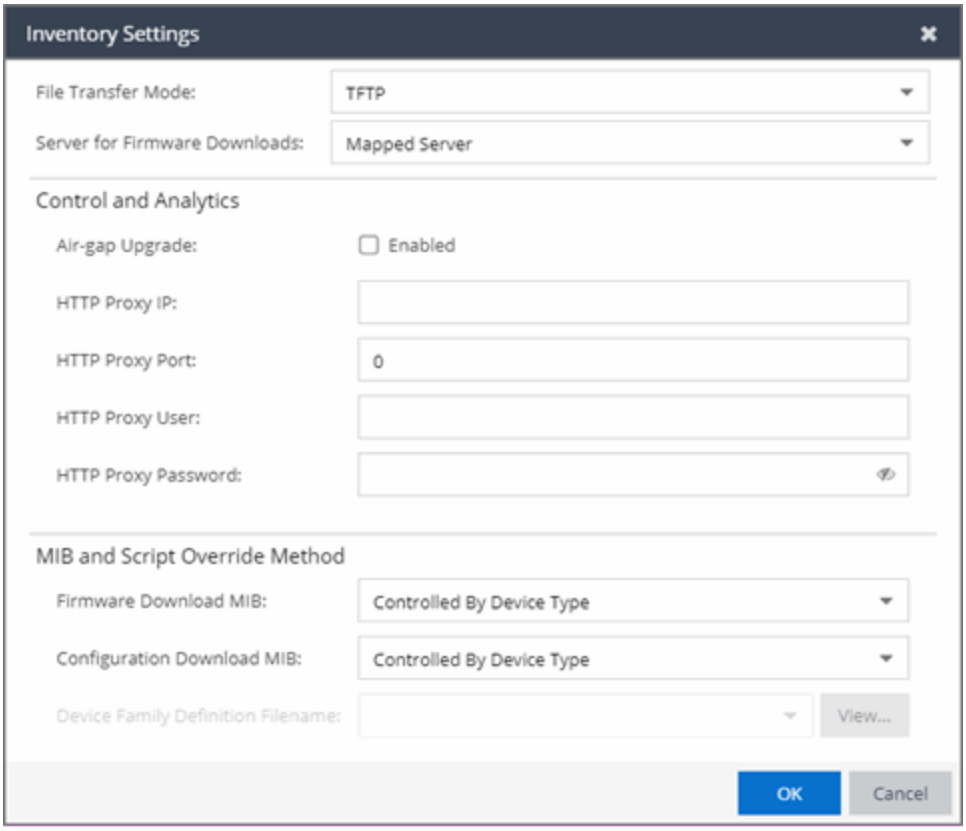
TIP: Removing line numbers and side bars may speed up the display of larger files.

Use the **Search** field in the toolbar to perform a search in the panel side that is selected by the cursor. Use the forward and back arrows to search for the next or previous instance of the search term.

Inventory Settings

Use this window to configure the file transfer method as well as the firmware and MIB download settings for a device.

This window is accessible by selecting a device and selecting the **Menu** icon (☰) and selecting **Archives** > **Inventory Settings** from the menu or by right-clicking a device and selecting **Archives** > **Inventory Settings** on the **Network** > **Devices** tab.



File Transfer Mode

The file transfer method used by the device.

Valid file transfer methods are:

- TFTP
- FTP
- SCP
- SFTP

Server for Firmware Downloads

The server from which devices access new firmware images during upgrades. Selecting the default **Mapped Server** indicates the firmware downloads use the server IP addresses you define in the Inventory Manager options.

Air-gap Upgrade

Select the checkbox if ExtremeCloud IQ Site Engine can upgrade the ExtremeControl and ExtremeAnalytics engines without an internet connection.

NOTE: License upgrade without an internet connection (Air Gap mode licensing) is not available in this release.

HTTP Proxy IP

Enter the HTTP proxy IP address ExtremeCloud IQ Site Engine uses to upgrade the ExtremeControl and ExtremeAnalytics engines.

HTTP Proxy Port

Enter the HTTP proxy port ExtremeCloud IQ Site Engine uses to upgrade the ExtremeControl and ExtremeAnalytics engines.

HTTP Proxy User

Enter the username with permission to access the IP address defined in the **HTTP Proxy IP** field.

HTTP Proxy Password

Enter the password for the user defined in the **HTTP Proxy User** field.

Firmware Download MIB

The Firmware Download MIB supported by this device type. If the device type supports more than one Firmware Download MIB, use the drop-down list to select the desired MIB. In addition to a list of MIBs, other menu options include:

- **Controlled by Device Type** — ExtremeCloud IQ Site Engine reads the **Firmware Download MIB** on the first device of this device type that you add or import, and displays it here. ExtremeCloud IQ Site Engine uses that MIB to perform firmware and boot PROM downloads on all devices of this device type.
- **Disabled** — Firmware download functionality is not allowed for this device type.
- **Script** — Allows the firmware download function to be executed through the use of a script. Use this option when upgrading the ExtremeControl and ExtremeAnalytics engines as well as for third-party devices that do not support the required SNMP MIBs.

Configuration Download MIB

The Configuration Download MIB supported by this device type. If the device type supports more than one Configuration Download MIB, use the drop-down list to select the desired MIB. In addition to a list of MIBs, other menu options include:

- **Controlled by Device Type** — ExtremeCloud IQ Site Engine reads the **Configuration Download MIB** on the first device of this device type that you add or import, and displays it here. ExtremeCloud IQ Site Engine uses that MIB to perform archive operations on all devices of this device type.
- **Disabled** — Archive functionality is not allowed for this device type.
- **Script** — Allows the archive function to be executed through the use of a script. Use this option for third-party devices that do not support the required SNMP MIBs.

Device Family Definition Filename

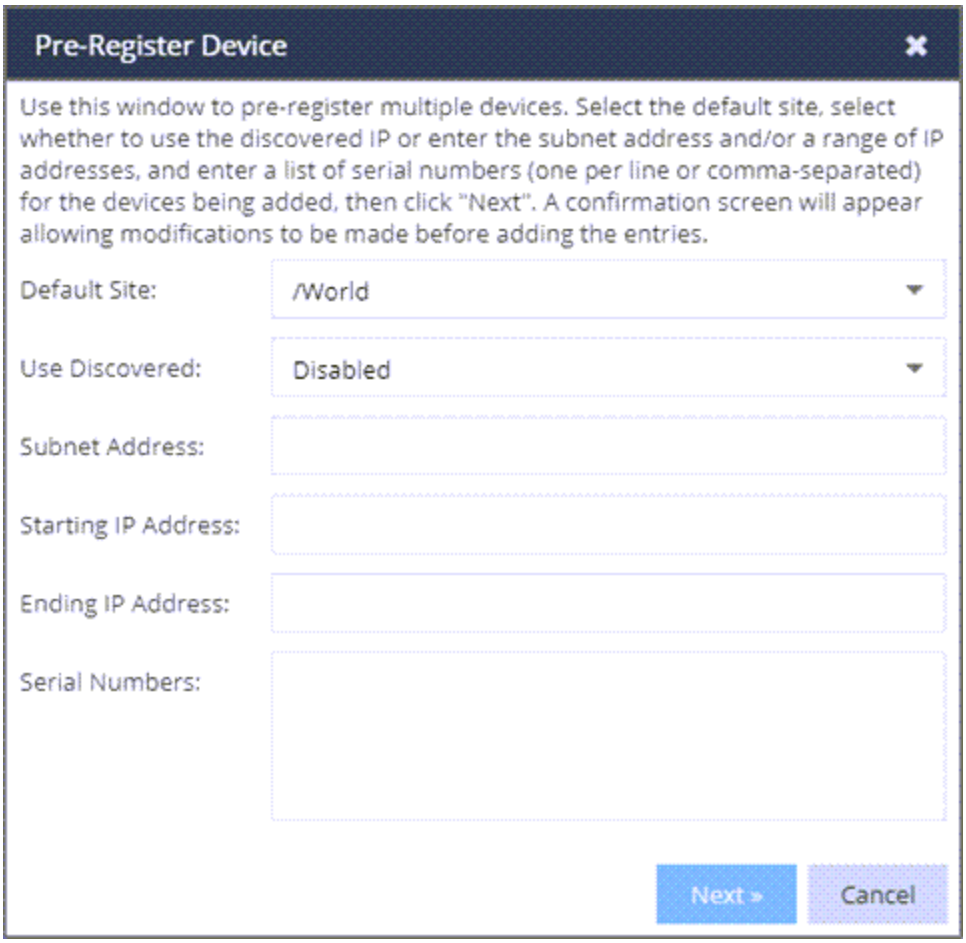
If **Script** is selected as **Firmware Download MIB** or **Configuration Download MIB**, select the file containing the scripts. Device Family Definition Files include all the scripts and data for each supported function for specific third-party devices. ExtremeCloud IQ Site Engine provides sample Definition Files for a variety of devices.

Pre-Register Device

Use this window to add multiple ZTP+ enabled devices to ExtremeCloud IQ Site Engine.

The **Pre-Register Device** window is accessible on the **Network** > **Discovered** tab by selecting the **Pre-Register Device** button.

Pre-Register Device Window



Default Site

The site to which the devices are to be added. If the site has ZTP+ Device Defaults configured, those values are populated in the **Pre-Register Device Window** when you select the site from the Default Site menu.

Use Discovered

Use the **Use Discovered** drop-down list to add the IP address or IP address and management interface the device uses when it contacts ExtremeCloud IQ Site Engine via ZTP+. Then, enter the Serial Number for the Discovered IP address.

Subnet Address

If you do not use the **Use Discovered** option, enter the device's IP subnet address (IPv4 or IPv6) in this field. The subnet must be separated from the IP address by a slash (/). Use either the mask bit notation (for example, /24), or the dotted-decimal notation (for example, /255.255.255.0.).

Starting IP Address

If you do not use the **Use Discovered IP**, you must add a range of at least two IP Addresses. Enter the first IP Address (IPv4 or IPv6) in your range of addresses in this field. The starting IP Address must be within the subnet address you specified. It must not match the ending IP Address.

Ending IP Address

If you do not use the **Use Discovered IP**, you must add a range of at least two IP Addresses. Enter the last IP Address (IPv4 or IPv6) in your range of addresses in this field. The ending IP Address must be within the subnet address you specified. It must not match the starting IP Address.

Serial Number

Enter the manufacturer-assigned serial numbers of the devices being added, separated by commas. You can also enter each serial number on its own line.

Next

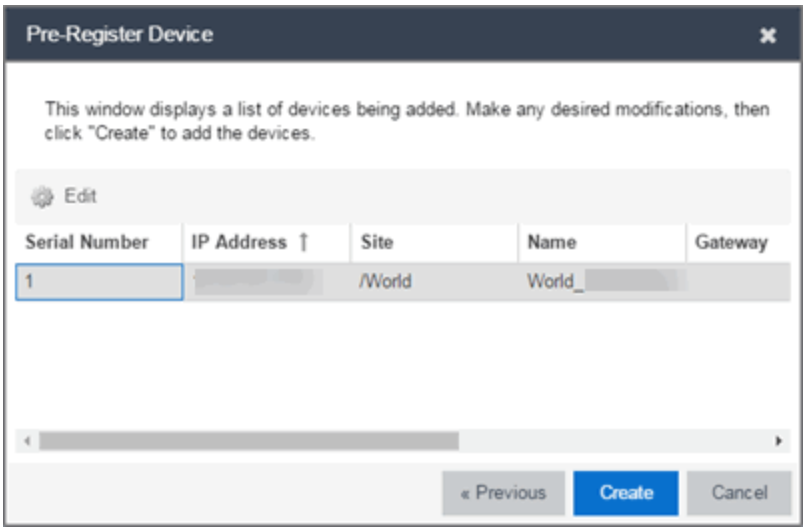
Select the **Next** button to open a confirmation window allowing you to verify the device information entered. Although it is recommended you enter device information in the site's **ZTP+ Device Defaults** window, you can also use this window to enter the Gateway, Domain Name, and DNS Server information for each device you are adding.

Cancel

Select the **Cancel** button to close the window with no devices added to the **Discovered** tab.

Pre-Register Device Confirmation Window

Use this window to confirm device information and supply any additional required information before adding devices to the **Discovered** tab in ExtremeCloud IQ Site Engine.



Serial Number
The serial number of the device. It is very important, especially for ZTP+-enabled devices, that the serial number entered here matches the device's serial number.

Use Discovered IP
Select to use discovered IP Address. You can also edit the discovered IP Address for a specific device.

IP Address
The device's IP address. The subnet mask is also displayed after the /.

Site
The site to which the device is to be added. To change the **Site**, use the Configure Device window.

Name
The name assigned to the device. The default **Name** includes the **Site** to which the device is assigned, followed by the device's Serial Number.

NOTE: If you are Pre-Registering Fabric Manager devices, the **Name** must be in hostname format (only ASCII a-z, digits 0-9 and hyphen -).

Gateway
Enter the IP address of the switch's default gateway. If a device is ZTP+-enabled, the site's ZTP+ Device default gateway displays.

Domain Name
Enter a value in the **Domain Name** field to configure the domain name on the devices being discovered. If a device is ZTP+-enabled, the site's ZTP+ Device default domain name displays.

DNS Server
Enter a DNS server address for the devices being discovered. If a device is ZTP+-enabled, the site's ZTP+ Device Default DNS Server displays.

NTP Server
Enter the NTP server address for the devices being discovered, if the devices are using an NTP server.

Create
Select the **Create** button to add the devices listed to the **Discovered** tab.

Sites

Use the **Sites tab** to define configuration templates. ExtremeCloud IQ Site Engine applies these configuration templates to devices you add to a site in your network. You can also use the tab to discover new devices in the site via device discovery or by using ZTP+ functionality.

NOTE: When adding an ExtremeXOS/Switch Engine device in ExtremeCloud IQ Site Engine, enter the following commands in the device CLI:

```
configure snmpv3 add community "private" name "private" user "v1v2c_rw"
configure snmpv3 add community "public" name "public" user "v1v2c_rw"
enable snmp access
enable snmp access snmp-v1v2c
disable snmp access snmpv3
```

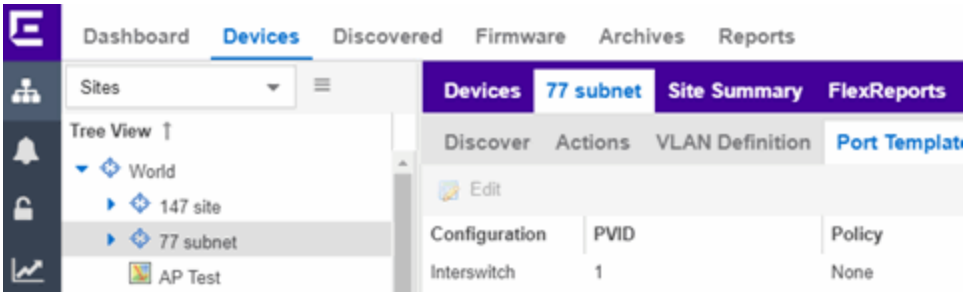
The **Sites tab** is divided into multiple sections, which you can expand to display more information.

NOTE: To save your changes and other additional functions for a device included in the site, right-click on the device and select **Configure Device** from the drop-down list. The **Configure Device** window opens. Use the buttons at the bottom of the **Configure Device** window to save, sync settings from the site to the device's configuration, enforce changes to the device, and more.

Access **Network** > Devices and select **Sites** from the left-panel drop-down list. The Sites Tree View opens, which includes the sites in your network, as well as **Topology Definitions** and **Service Definitions** tabs.

Right-click the Topology Definitions tab to create topology or LAG (link aggregation group) topology definitions. Right-click the Service Definitions tab to create service definitions. The topology, LAG and service definitions are used to create the templates that build Fabric technology.

Select a site from the left-panel Sites Tree View. A tab in the **Devices** window opens with the name of the site you selected. To create a new site, click the menu icon in the left-panel and select **Maps/Sites** > **Create Site**.



The **Site Name** tab contains the following tabs:

- Discover
- Actions
- VRF/VLAN
- Fabric Connect
- Services

- LAG Topologies
- Port Templates
- ZTP+ Device Defaults
- Endpoint Locations
- Analytics
- Custom Variables
- XIQ Location

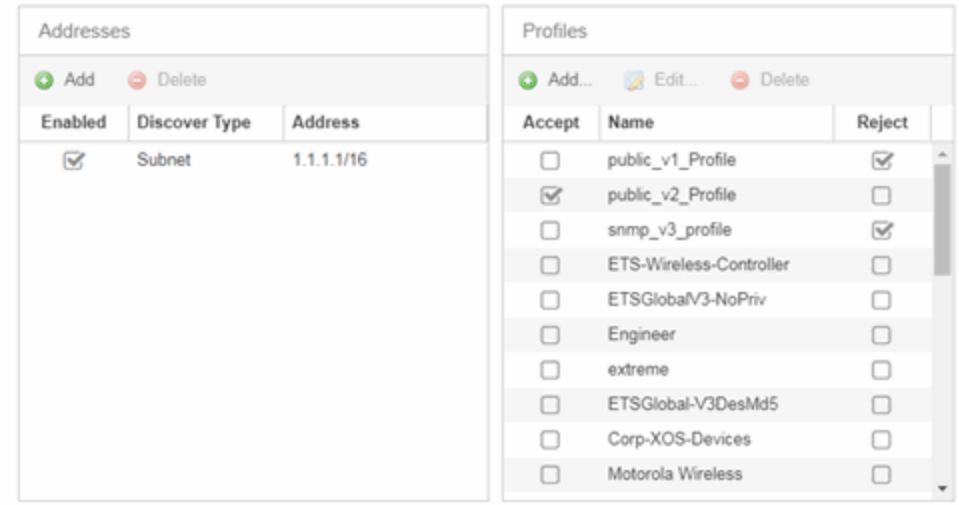
Additionally, the bottom of the tab contains buttons to save your configurations in ExtremeCloud IQ Site Engine and on the devices included in the site.

Discover

The **Discover** tab allows you to enter address information for new devices on your network, which adds them to the ExtremeCloud IQ Site Engine database in the current Site. You can perform a CDP (Cabletron Discovery Protocol) discover for CDP-compliant devices, an LLDP (Link Layer Discovery Protocol) discover for LLDP-compliant devices, and an EDP (Extreme Discovery Protocol) discover for EDP-compliant devices. Additionally, you can discover new devices based on subnets or IP address ranges. When discovering devices, you can choose to accept or reject devices based on the profile type using the respective checkboxes in the Profiles section.

NOTES: ExtremeCloud IQ Site Engine only allows a subnet search of a 16-bit mask or higher when discovering devices.

Discovering devices via the **Site** tab using a **Range**, **Subnet**, or **Seed** discover may not successfully add all expected devices. To correct the issue, increase the **Length of SNMP Timeout** value on the Administration > Options > Site tab in the Discover First SNMP Request section.



Addresses

Click the **Add** button in the Addresses list to allow you to add devices by seed address, subnet, or address range. Selecting **Seed Address** allows you to perform a discover for CDP, LLDP, SONMP, or EDP-compliant devices.

NOTE: The protocols for seed discovery are specified on the Administration tab.

Click the **Discover** button at the bottom of the tab to begin the device discover. The results of the Discover process are displayed in the left-panel tree when added to the ExtremeCloud IQ Site Engine database.

Profiles

Select the access Profile(s) that give you the access you need (for example, Read, or Read/Write) to the devices you wish to discover by selecting the **Accept** checkbox. Select the Profiles that are not valid on the device being discovered by selecting the **Reject** checkbox. To create a profile, click the **Add** button or edit a profile by selecting the **Edit** button. If you discover an existing device using a different profile than the device is already using in the database, click **Save** to overwrite the profile currently being used in the database.

Actions

The **Actions** tab contains basic information about the device being discovered.

Automatically Add Devices

Selecting the **Automatically Add Devices** checkbox causes ExtremeCloud IQ Site Engine to automatically add devices to the database that match the address information you entered in the Discover section of the tab. If a device is discovered with more than one profile, the device is listed on the **Network** > **Discovered** tab, where you can decide which profile you want to

add. When this box is NOT selected and a discover occurs, devices are added to the **Network** > **Discovered** tab, where they can be configured prior to being added to the database.

Add Trap Receiver

Select this checkbox to configure devices added to the site to send trap information to ExtremeCloud IQ Site Engine. You can define the trap configuration details on the **Options** > **Trap** tab. Depending on the device, ExtremeCloud IQ Site Engine creates the trap configuration via SNMP or a script.

Add Syslog Receiver

Select this checkbox to configure the devices added to the site to send syslog information to ExtremeCloud IQ Site Engine. You can define the syslog configuration details on the **Options** > **Syslog** tab. Depending on the device, ExtremeCloud IQ Site Engine creates the syslog configuration via SNMP or a script.

Collection Mode

Select **None**, **Threshold Alarms**, or **Historical** from the Collection Mode drop-down menu to indicate the mode used to collect device statistics on devices being discovered. ExtremeCloud IQ Site Engine uses the device and physical port statistics in reports.

Collection Interval (minutes)

Select the interval at which device and statistics (for devices being discovered) are collected. Extreme sets a minimum collection interval of five minutes and a maximum of 1440 minutes (24 hours).

Add to Archive

Select this checkbox to create an archive, which saves the configurations of the devices being discovered in the **Network** > **Archives** tab.

Add to Map

Select this checkbox to add the devices being discovered in the site to a map. To add a device to multiple maps, add it via this drop-down list and then manually add it via the **Maps** > **Add to Map** on the **Devices** tab.

Custom Configuration

Click the **Add** button to configure ExtremeCloud IQ Site Engine to automatically run a task (a script or workflow) when discovering a device in a particular device family that also matches the **Topology** you select.

CAUTION: If the script or workflow task selected for the Custom Configuration restarts the device, other actions selected to execute during discovery might not execute (for example, Add Trap Receiver).

NOTE: Selecting a **Topology** of **Any** runs the task on all devices in a device family, regardless of the **Topology** configuration.

Policy

Add Device to Policy Domain

Select this checkbox to add the device to a policy domain you create on the **Policy** tab. When the checkbox is selected, use the **Policy Domain** drop-down list to select the policy domain to which the device is added. ExtremeCloud IQ Site Engine enforces are done automatically when a newly added device is discovered and added.

Click the **Import VLANs** button to import the VLAN definitions from the policy selected in the Policy Domain drop-down list.

Access Control

Add Device to Access Control Engine Group

Select this checkbox to add the device to an Access Control Engine Group you create on the **Access Control** tab. When the checkbox is selected, use the Access Control **Engine Group** drop-down list to select the engine group to which the device is added.

- If the device is an Access Control engine, ExtremeCloud IQ Site Engine adds it as an engine to the engine group.
- If the device is not an engine, ExtremeCloud IQ Site Engine adds it as a switch to up to two engines in the engine group. ExtremeCloud IQ Site Engine runs an enforce against the engine group if a switch is added.
    - Enable RADIUS Accounting - defines if the RADIUS Accounting is enabled or disabled. If Enable RADIUS Accounting is checked and the "Authentication Access Type" is " Manual RADIUS Configuration" then the Access Control Engine accepts RADIUS Accounting packets from that device. If Enable RADIUS Accounting is checked and "Authentication Access Type" is not "Manual RADIUS Configuration" then Access Control Engine enables RADIUS Accounting on the device and accepts RADIUS Accounting packets from that device.
    - Message-Authenticator Attribute - defines if the Access-Request must contain the Message-Authenticator attribute in the RADIUS communication with this device. Not every RADIUS client supports this attribute, but the security best practice is to require the Message-Authenticator attribute. If set to "Required", then RADIUS packets without the Message-Authenticator attribute are dropped.
    - Authentication Access Type - defines if the device is configured to use "Network Access" or "Management Access" or "Any Access" or the "Manual RADIUS Configuration".
    - Override RADIUS Attributes to Send - if checked then you can define what "RADIUS Attributes to Send" will be used. If unchecked then default "RADIUS Attributes to Send" will be used. The default is:

- If the device is running the Fabric Engine operating system and the policy domain is specified, then Per-User ACLs RADIUS attributes are used.
- If the device is running Fabric Engine operating system and the policy domain is not specified, the Fabric Attach RADIUS attributes are used.
- If the device is running a policy capable operating system, for example, ExtremeXOS, then Extreme Policy RADIUS attributes are used.

- For more details, see Add Switches to Access Control Engine Group.

Enable Authentication Using Port Template
Select this checkbox to allow users to authenticate to the device using a port template. Configure Port Templates in the Port Templates section of the tab.

ExtremeAnalytics

Add as Flow/Telemetry Source to Home Engine using Management IP
Select this checkbox to add application telemetry to the ExtremeAnalytics engine configured as the site's home engine. Flow Source is preferred if the device can be added as Flow Source and Telemetry Source.

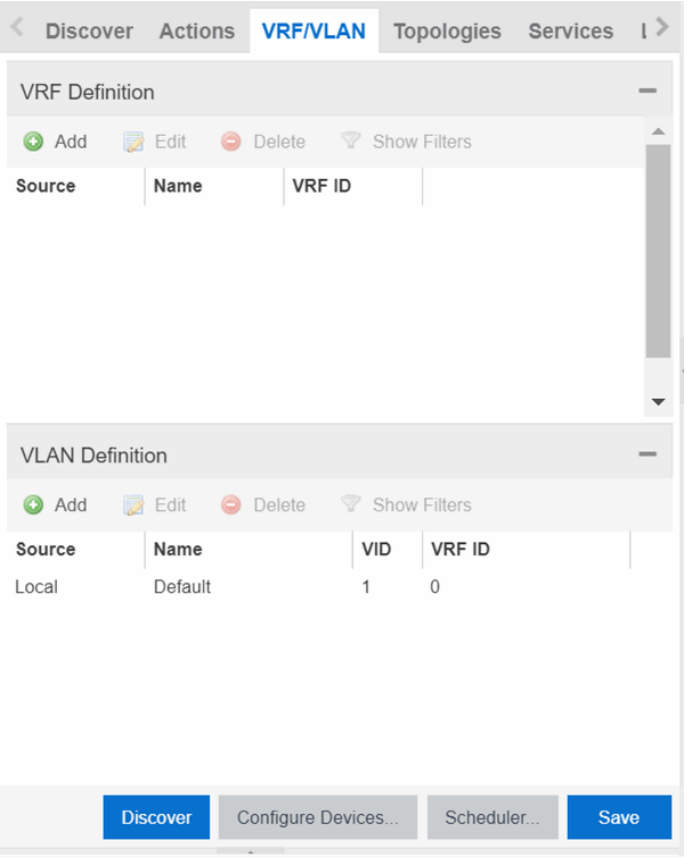
ERSPAN VLAN
Enter the Encapsulated Remote Switch Port Analyzer (ERSPAN) VLAN to add to devices added to the site.

Sample Rate
Enter the rate of traffic ExtremeAnalytics samples to determine application information.

VRF/VLAN

The **VRF/VLAN** tab allows you to configure and manage virtual routing and forwarding (VRF), VLANs on the devices included in the site. Add a VRF or VLAN definition by selecting **Add** in the VRF Definition or VLAN Definition table, respectively. Edit an existing VRF or VLAN definition by selecting a VRF/VLAN and selecting **Edit**, or remove a VRF or VLAN definition by selecting a VRF/VLAN and selecting **Delete**.

NOTE: You must have a Fabric Manager license to configure VRFs. If you do not have one, this tab is just called VLAN.



VRF Definition

Source

The **Source** represents the Site where the VRF settings were created. **Local** indicates the VRF was created in the selected site. When a VRF is created for a Site, any Sites created nested within that Site inherit the VRF settings from the Site. Changes or Deletions can only be made to the VRF in the site in which it was created (**Source** is **Local**).

Name

Displays the name of the VRF definition.

VRF ID

The ID number assigned to the VRF definition.

Multicast

Select to indicate the service sends IP packets to a group of recipients on the network.

Unicast

Select to indicate the service sends IP packets to a single recipient on the network.

Direct Route

Select to indicate the service sends IP packets directly to a another device without going through a third device.

VLAN Definition

Source

The **Source** represents the Site where the VLAN settings were created. **Local** indicates the VLAN was created in the selected site. When a VLAN is created for a Site, any Sites created nested within that Site inherit the VLAN settings from the Site. Changes or Deletions can only be made to the VLAN in the site in which it was created (**Source** is **Local**).

Name

Displays the name of the VLAN.

VID

Indicates the VLAN ID for the VLAN. A unique number between 1 and 4094 that identifies a particular VLAN. VID 1 is reserved for the Default VLAN.

VRF ID

The VRF ID associated with the VLAN definition.

Multicast

Select to configure the service to distribute data to multiple recipients. Using multicast, a source can send a single copy of data to a single multicast address, which is then distributed to an entire group of recipients.

IGMP Version

Indicates which version of IGMP is utilized (Version 1 or Version 2).

IGMP Querier

Enter the address of the IGMP Querier. Use this feature when there is no multicast router in the VLAN to originate the queries.

Querier Enable

Indicates whether an IGMP Query is enabled.

Virtual Routing

Displays the version of VRRP the default gateway is using:

- **NONE** — Virtual routing is not configured on the VLAN.
- **DvR** - DvR (Direct Virtual Routing) is configured.
- **VRRPv2** — VRRP version 2 is configured on the virtual router. VRRP version 2 only supports IP addresses in IPv4 format.
- **VRRPv3** — VRRP version 3 is configured on the virtual router. VRRP version 3 supports IP addresses in both IPv4 and IPv6 formats.
- **RSMLT** — Routing Redundancy Method is configured on the VLAN. RSMLT requires that a Virtual IST is configured. If the device is not configured as a vIST pair, **RSMLT** can be selected, but the feature is not active. Once the vIST is configured, RSMLT becomes active.

NOTE: Virtual Routing is only supported on Fabric Engine devices.

Virtual Routing Enable
Indicates whether virtual routing (DvR or VRRPs) is enabled for the VLAN.

Virtual Routing Address
The IP address for the virtual routing interface for either DvR or VRRP. The Virtual Routing address must be in the same subnet as the VLAN subnet address.

VRRP ID
An identifier devices use to determine peer devices that participate in a virtual routing interface.

VRRP Priority
A value used by VRRP peers to determine the role of each of the devices in the VLAN. The default value is **100**. The device with the largest value is assigned the role of Controller. For example, in a VLAN with two routers, one with a **VRRP Priority** of **200** and one with a **VRRP Priority** of **100**, the router with a **VRRP Priority** of **200** becomes the Controller. In the event of identical priority numbers, the devices use the MAC address to determine priority.

VRRP Backup Master
This option determines if the backup router is able to forward traffic independently outside of the VLAN (enabled), or must forward the traffic to the Controller router before it is forwarded outside of the VLAN (disabled).

VRRP Advertisement Interval
Indicates frequency (in seconds) that protocol packets are sent from the virtual router in the VLAN.

VRRP Hold Down Timer
Indicates the amount of time (in hundredths of a second) that the backup router waits for the primary router to respond before it becomes the primary router.

DHCP Relay
Indicates whether a Dynamic Host Configuration Protocol relay server is enabled for the VLAN. A DHCP relay receives and converts a DHCP broadcast message to dynamically assign an IP address to a device on the network.

DHCP Relay Servers
The IP addresses of the DHCP relay servers for the VLAN.

DHCP Snooping
Indicates whether DHCP snooping is enabled for the VLAN. DHCP Snooping is a Layer 2 security feature, that provides network security by filtering untrusted DHCP messages received from the external network causing traffic attacks within the network. DHCP Snooping is based on the concept of trusted versus untrusted switch ports. Switch ports configured as

trusted can forward DHCP Replies, and the untrusted switch ports cannot. DHCP Snooping acts like a firewall between untrusted hosts and DHCP servers.

ARP Inspection

Indicates whether ARP inspection is enabled. Dynamic ARP Inspection (DAI) is a security feature that validates ARP packets in the network. Without DAI, a malicious user can attack hosts, switches, and routers connected to the Layer 2 network by poisoning the ARP caches of systems connected to the subnet, and intercepting traffic intended for other hosts on the subnet. DAI prevents these attacks by intercepting, logging, and discarding the ARP packets with invalid IP to MAC address bindings. The switch dynamically builds the address binding table from the information gathered from the DHCP requests and replies when DHCP Snooping is enabled. The switch pairs the MAC address from the DHCP request with the IP address from the DHCP reply to create an entry in the DHCP binding table. When you enable DAI, the switch filters ARP packets on untrusted ports based on the source MAC and IP addresses seen on the switch port. The switch forwards an ARP packet when the source MAC and IP address matches an entry in the address binding table. Otherwise, the switch drops the ARP packet.

NOTE: **DHCP Snooping** must be enabled to use **ARP Inspection**.

DHCP Relay Servers

Source

Indicates the site from which the DHCP Relay Server is inherited. Currently, the VLAN definition Source can only be **Local**, indicating the DHCP Relay Server is configured in the current site.

Server IP

The IP address of the DHCP server.

Fabric Connect

The **Fabric Connect** tab allows you to select the topology definition. Use this tab to apply the fabric topology features you configure to a site.

Topology Definition

Select the Topology Definition that applies to the site. The Topology Definitions available in the drop-down list are configured in the **Topology Definition** tab.

DvR Domain ID

Select the DvR Domain ID that applies to the site. The DvR Domain IDs available in the drop-down list are configured in the **Topology Definition** tab.

Services

Select to configure the services configured in your virtual services network. Use this tab to select a service definition you create by configuring services on the Services tab to add to the site.

The **Services** tab displays all of the services included in a service application or all of the services included in a service definition, depending if you select a service application or a service definition in the left-panel, respectively. The Services tab is included in the **Sites** tab.

Services are created within service applications. You can include multiple services within an application. Service applications are then included within service definitions. You can also include multiple service applications within a service definition. A service definition that includes a complete set of services is then assigned to a site, which configures the fabric-enabled devices within that site.

Select the Service Definition assigned to the site from the Service Definition drop-down list. Select **NONE** if the services you configure are not assigned to a service definition.

NOTE: When services have been assigned to a site, they cannot be deleted; however, services not assigned to a service definition (where NONE has been selected) can be deleted from a site after they have been assigned to that site.

L2 VSN

Source
The service application to which the Layer 2 service has been assigned.

Name
The name of the Layer 2 service.

Service ID
The ID number of the fabric service.

UNI Type
The User-Network-Interface (UNI) of the fabric service. The following interface types are available:

- **Switched** — A VLAN-ID and a port (VID, port) mapped to a Layer 2 VSN I-SID. With UNI type, VLAN-IDs can be reused on other ports and mapped to different ISIDs.
- **Transparent** - A physical port maps to a Layer 2 VSN I-SID (all traffic through the port, 802.1Q tagged or untagged, ingress and egress maps to the I-SID).

  NOTE: All VLANs on a Transparent Port UNI interface now share the same single MAC learning table of the Transparent Port UNI I-SID.

- **CVLAN** — a platform customer VLAN-ID.

VLAN
The customer VLAN-ID of the associated CVLAN UNI type.

CVID
The customer VLAN-ID of the associated switched UNI port.

Management Service

Defines if the L2 VSN is used for switch management purposes.

AutoSense Service Type

Defines if the L2 VSN service is auto-assigned by the switch-level AutoSense detection. The following types are available:

- **AP Untagged** — If the AutoSense feature detects Access Point, then this service is automatically assigned to the port.
- **Camera Untagged** — If the AutoSense feature detects Camera then this service is automatically assigned to the port.
- **Voice Untagged** — If the AutoSense feature detects a VoIP device then this service is automatically assigned to the port.
- **Voice Tagged** — If the AutoSense feature detects a VoIP device then this service is automatically assigned to the port.
- **Proxy Switch Auth Tagged —** If the AutoSense feature detects a Fabric Attach switch capable of authenticating (ERS devices) then this service is automatically assigned to the port.
- **Proxy Switch No Auth Untagged —** If the AutoSense feature detects a Fabric Attach switch is not capable of authenticating (Switch Engine devices) then this service is automatically assigned to the port.
- **Proxy Switch Auth & Proxy Switch No Auth —** If the AutoSense feature detects any physical Fabric Attach switch (ERS/EXOS/Switch Engine device) then this service is automatically assigned to the port.
- **Data Untagged** — If the AutoSense feature does not detect a device type then this service is automatically assigned to the port.
- **None** — AutoSense is not related to this L2VSN service.

NOTE: Each AutoSense Service Type can only be used once on a switch. The switch cannot use two different service IDs with the same AutoSense Service Type.

AutoSense Service CVID

The AutoSense Service CVID value defines the 802.1q VLAN tag sent from the switch to the device. If the **AutoSense Service Type** is **Voice Tagged** or **Proxy Switch Auth Tagged** or **Proxy Switch Auth & Proxy Switch No Auth** then AutoSense Service CVID must be defined. The value range is 1-4094.

Port Template

If the **UNI Type** is **Switched** or **Transparent** you can select from the Global Port templates to define the purpose of the port.

L3 VSN

Name
The name of the Layer 3 service.

Service ID
The ID number assigned to the service.

VRF
Select the virtual routing and forwarding definition included as part of the service.

Multi Cast
Select to indicate the service sends IP packets to a group of hosts on the network.

Unicast
Select to indicate the service sends IP packets to a single recipient on the network.

Direct Route
Select to indicate the service sends IP packets directly to another device without going through a third device.

LAG Topologies

The LAG Topologies tab allows you to configure link aggregation group topologies you include on devices in the site.

Name
Displays the name of the LAG.

Topology Type
Select the type of LAG topology for the site.

Topology Definition
Select the Topology Definition for the LAG in the drop-down list.

Device 1/Cluster 1
Select the first device or cluster included in the LAG.

Device 2/Cluster 2
Select the second device or cluster included in the LAG.

Device 1 VLAN IP Address/Mask
Enter IP address and mask for the first device or cluster included in the LAG.

Device 2 VLAN IP Address/Mask
Enter IP address and mask for the second device or cluster included in the LAG.

LACP MAC
Enter the MAC address for the device located between two devices designed to detect when a link is down, if you use link aggregation control protocol (LACP).

MLAG ID
The ID number of the MLAG configured for the LAG topology.

L2 ISID
The service instance identifier.

vIST
Select the Virtual IST (vIST) type. vIST provides the ability to dual-home hosts, servers and other network devices to a pair of Multi-Chassis Link Aggregation (MLAG) enabled devices.

Port Templates

The **Port Templates** tab has two panels. The top panel displays information about user-defined port templates. For more information, see Port Templates Panel.

The bottom panel displays information about automated port templates. For more information, see ZTP+ Automated Templates Panel.

Port Templates Panel

The **Port Templates** panel displays port information for those devices discovered in a site. The port templates you configure in this table are available for the devices included in this site in the **Configure Device** window.

Click the **Add** (Add) button to add a port template to the table.

Select a port template and select the **Edit** (Edit) button to make changes to the selected port template.

Select a user-created port template and select the **Delete** (Delete) button to delete it from the table. You can not delete system-defined port templates.

Select the **Local Only** button as a toggle button to display local templates only and, alternately, to display all templates.

Click **Save** to save your additions or changes.

The following columns are included on the **Ports Templates** panel:

Source
Indicates the site which defines the values used for the Port Template.

- Port templates with a **Source** of **Global** can only be edited in the /World site.
- A **Source** of **Local** indicates that the values are coming from the currently selected site. In order to change the value of a Port Template, select the **Port Templates** tab for the site that shows the **Source** as **Local**. When creating a new site, the values of the new site's Port Templates are inherited from the parent site.

  When you create port template after creating a new site, the new port template is also

created in the /World site. All port templates in the /World site display a **Local** for **Source**. You can modify the values of the port template in both the /World site and in the site where the port template was created. Sites that are the children of the /World site display the **Source** for the port template values as /World. Sites that are the children of the site in which the port template was created display the **Source** for the port template values as the site where the port template was created.

When the **Source** is not **Local**, the port template values act like default values for the site. Editing the port template in the site and changing the **Source** to **Local** allows you to edit the port template for the current site and the sites that are children of that site.

Configuration

Indicates the purpose of a port. Defines the behavior of ports on devices in a site, based on the role of that port. After you configure your port templates in this table, select the **Configuration** for devices in the site in the **Configure Device** window. The configuration of the port is initially discovered by ExtremeCloud IQ Site Engine during discovery or during a ZTP+ process, but can be changed to meet the needs of the devices in your site. The following port types are included:

- **Access**
  Applies access port template settings to the device in the site.
- **Interswitch**
  Applies interswitch port template settings to the device in the site.
- **Management**
  Applies management port template settings to the device in the site.
- **AP**
  Applies AP port template settings to the device in the site.
- **Phone**
  Applies phone port template settings to the device in the site.
- **Router**
  Applies router port template settings to the device in the site.
- **Printer**
  Applies printer port template settings to the device in the site.
- **Security**
  Applies security port template settings to the device in the site.
- **IoT**
  Applies guest or external device port template settings to the device in the site.
- **vSwitch**

Applies virtual switch port template settings to the device in the site.

- **Other**

PVID

The port's VLAN ID.

The PVID value "None [0]" means incoming untagged traffic is not assigned to any VLAN. The value "None [0]" is compatible with Switch Engine persona devices.

Default Role

The policy role assigned to the selected port. To assign policy to the selected port, select **Add Device to Policy Domain** and select a **Policy Domain** from the drop-down list in the **Actions** tab. ExtremeCloud IQ Site Engine assigns policy to the port after a successful policy domain enforce.

Authentication

Use the drop-down list to determine whether authentication is configured to the port:

- **None** — No authentication is required to access the port.
- **802.1X** — Select this option to enable 802.1X authentication to the port.
- **MAC Auth** — Select this option to enable authentication based on the users MAC address.

WARNING: Configuring the authentication could affect communication to a device and result in loss of connectivity through the interswitch link ports if not detected or configured properly during the discovery process. If you are configuring the policy and authentication on the interswitch link, it's strongly recommended to ensure neighbor discovery protocols such as LLDP, EDP, and CDP are enabled before enabling the authentication using port templates.

VLAN Trunk

Automatically configures a port as a VLAN trunk when you check one box in the VLAN Trunk column. For more information, see Fabric Assist.

Tagged

Indicates the port's egress state is tagged. If you check the VLAN Trunk column, Fabric Assist automatically configures all the VLANs on the port as tagged. For more information, see Fabric Assist.

Fabric Enable

Indicates the fabric functionality is enabled on the port.

NOTE: **Fabric Enable** options are only configurable for Global port templates. You can create a global port template on the World site level.

ExtremeCloud IQ Site Engine can extend FA functionality to ExtremeXOS/Switch Engine devices and provision them as FA Proxy devices. Select **Fabric Attach** or **Fabric Attach and Switched UNI** or **Auto Sense** from the drop-down list to enable the port on a Fabric Engine device (acting as FA Server) to connect to an ExtremeXOS/Switch Engine device (acting as FA Proxy).

- **Fabric Attach** - Enable Fabric Attach server functionality on the port of a Fabric Engine device acting as a Fabric Attach server) to connect to an ExtremeXOS/Switch Engine device (acting as a Fabric Attach proxy).
- **Fabric Attach and Switched UNI** - Enable Fabric Attach server functionality on the port of a Fabric Engine device acting as a Fabric Attach server) to connect to an ExtremeXOS/Switch Engine device (acting as a Fabric Attach proxy). When selecting this option, the port is configured for both features, but only one feature is active at any one time.
- **Auto Sense** - Select **Auto Sense** on the port of a Fabric Engine device to enable the port to automatically sense and configure automatically sense and configure the appropriate Fabric settings for the port. These settings include the following:
  - PVID
  - VLAN Trunk
  - Tagged
  - Untagged
  - Fabric Mode
  - Fabric Auth Type
  - Fabric Auth Key
  - Fabric Connect Drop STP-BPDU
  - BPDU Guard
  - Authentication

NOTE: If **Fabric Enable** is **Auto Sense** the Fabric settings listed above are not configurable.

Fabric Auth Type
Indicates the fabric authentication type used on the port.

Fabric Auth Key
Indicates the fabric authentication key used for the port.

Fabric Connect Drop STP-BPDU
Indicates the fabric-enabled port drops Spanning Tree Protocol BPDUs.

Untagged
Indicates the port's egress state is untagged.

Node Alias
Select to enable the node alias function on the port. The node alias settings are automatically enabled if Access Control is enabled on the device.

Span Guard
Select to enable Span Guard, which allows the device to shut down a network port if it receives a BPDU (bridge protocol data unit). Enable this feature on network edge ports to prevent rogue STA-aware devices from disrupting the existing Spanning Tree.

Loop Protect
Select to prevent loop formation in a network with redundant paths by requiring ports to receive type 2 BPDUs (RSTP/MSTP) on point-to-point interswitch links.

- If the ports receive the BPDUs, the link's **State** becomes **Forwarding**.
- If a BPDU timeout occurs on the ports, its **State** becomes **Listening** until a BPDU is received.

MVRP
Indicates that the Multiple VLAN Registration Protocol (MVRP) is enabled for the port. If MVRP has been enabled globally, interswitch ports are automatically enabled and access ports default to disabled.

SLPP
Indicates Simple Loop Prevention Protocol (SLPP) is enabled on the port. SLPP provides active protection against Layer 2 network loops on a per-VLAN basis. If an SLPP packet is received, the port is disabled for the amount of time configured in the **SLPP Timer** field.

NOTE: If **SLPP** is enabled, **SLPP Guard** is not available.

SLPP Guard
Indicates whether SLPP Guard is enabled on the port. Use SLPP Guard to provide additional loop protection to protect wiring closets from erroneous connections. SLPP Guard requires **SLPP** to be enabled. SLPP detects loops in an SMLT network. Because SMLT networks disable Spanning Tree (STP), Rapid Spanning Tree (RSTP), or Multiple Spanning Tree Protocol (MSTP) for participating ports, SLPP Guard provides additional network loop protection, extending the loop detection to individual edge access ports. SLPP Guard can be configured on MLT or LAG ports. If the edge switch with SLPP Guard enabled receives an SLPP-PDU packet on a port, SLPP Guard operationally disables the port for the configured timeout interval in the **SLPP Guard Timer** field and appropriate log messages and SNMP traps are generated. If the disabled port does not receive any SLPP-PDU packets after the configured timeout interval expires, the port automatically reenables and generates a local log message, a syslog message, and SNMP traps, if configured.

NOTE: If **SLPP Guard** is enabled, **SLPP** is not available

SLPP Guard Timer
Indicates the amount of time after receiving an SLPP packet before the port is reenabled.

DHCP Snooping
Specifies the trust factor of the port for DHCP Snooping. The agent at the switch determines if DHCP reply packets are forwarded based on the DHCP Snooping mode of the VLAN and the trusted state of the port. If the value is "Trusted", the agent trusts the device on the port. If the value is "Untrusted", the agent does not trust the device on the port.

ARP Inspection
Dynamic ARP Inspection (DAI) is a security feature that validates ARP packets in the network. Without DAI, a malicious user can attack hosts, switches, and routers connected to the Layer 2 network by poisoning the ARP caches of systems connected to the subnet and intercepting traffic intended for other hosts on the subnet. DAI can prevent attacks by intercepting, logging, and discarding the ARP packets with invalid IP to MAC address bindings. The switch dynamically builds the address binding table from the information gathered from the DHCP requests and replies when DHCP Snooping is enabled. The switch pairs the MAC address from the DHCP request with the IP address from the DHCP reply to create an entry in the DHCP binding table. Values are "Trusted" and "Untrusted".

Source Guard
IP Source Guard (IPSG) is a Layer 2 port-to-port feature that works closely with DHCP Snooping. IPSG can prevent IP spoofing by allowing only IP addresses obtained using DHCP Snooping. When you enable IPSG on an untrusted port with DHCP Snooping enabled, an IP filter is automatically created or deleted for that port based on the information stored in the corresponding DHCP Snooping binding table entry. When a connecting client receives a valid IP address from the DHCP server, the filter installed on the port allows traffic only from that assigned IP address. If the value is "Disabled" the Source Guard is disabled. If the value is "IP" the IP Source Guard feature is enabled.

PoE Enable
Indicates that power over ethernet (PoE) is enabled for the port.

PoE Priority
Indicates the priority of PoE for the port; **LOW**, **HIGH**, or **CRITICAL**.

Collection Mode
Indicates the mode to collect port statistics.

Collection Interval (minutes)
Indicates the interval (in minutes) at which port statistics are collected.

ZTP+ Automated Templates

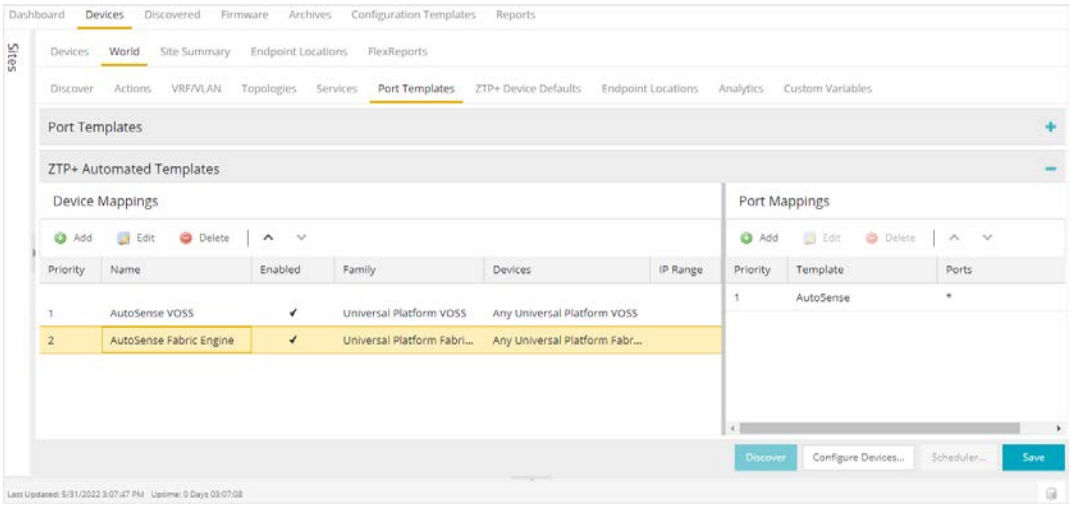
The **ZTP+ Automated Templates** displays information about templates configured by family. These templates are listed in priority order, which means they are evaluated in the order they are displayed. You can change the order by using the priority arrows in the toolbar or dragging and dropping a template.

NOTE: ExtremeCloud IQ Site Engine supports automated port templates for ZTP+ devices only.

The automated port templates panel has two sections: Device Mappings on the left and Port Mappings on the right.

On the left side, specify the name for the Device Mapping and then select the family and devices you want to apply the template to. Optionally, you can also match based on an IP range.

The right side displays the port mappings associated with the device mapping that you selected on the left side. The bindings are in priority order, and the template matches the ports in the order they are listed. You can change the order by using the priority arrows in the toolbar or dragging and dropping a template.



Click **Add** (Add) to add a device mapping to the table.

Select a device mapping and select **Edit** (Edit) to make changes.

Select a device mapping and select **Delete** (Delete) to delete it from the table.

Click **Save** to save your changes.

The following columns are included on the **Device Mappings** panel:

Priority
Displays the order in which device mappings are evaluated.

Name
The name of the device mapping.

Enabled
Indicates whether the device mapping is enabled or disabled.

Family
Specifies the family of devices to which the device mapping applies.

Devices
Specifies which device within the family to which the template applies.

IP Range
Specifies a single IP address or a range of addresses in the following formats:

- 1.2.3.4 (v4)
- 1111:2222::3333:4444 (v6)
- 1.2.3.4/24 (v4 with mask)
- ::1/64 (v6 with mask)
- 1.2.3.4-2.3.4.5 (range)
- 1::1-1::2 (range)

The following columns are included in the **Port Templates** panel:

Priority
Displays the order in which port templates are evaluated.

Template
Displays the list of available automated port templates.

Port Binding accepts any of the following formats (device dependent):

- 1 (single port)
- 1-5 (port range)
- 1,3,5 (comma separated ports)
- 1-3,5-7 (comma separated port ranges)
- * (wildcard)

Ports
Displays the list of configured ports next to their associated template. For devices that require slot and port numbers, use the appropriate format for the device:

- Single Port:
  - 210-Series: "1/1" or "1/1, 1/3, 1/5, 1/7"
  - 220-Series: "1/0/1" or "1/0/1, 1/0/3, 1/0/5, 1/0/7"
  - ERS: "1/1" or "1/1, 1/3, 1/5, 1/7"
  - ExtremeXOS/Switch Engine: "1:1" or "1:1,1:3,1:5,1:7"

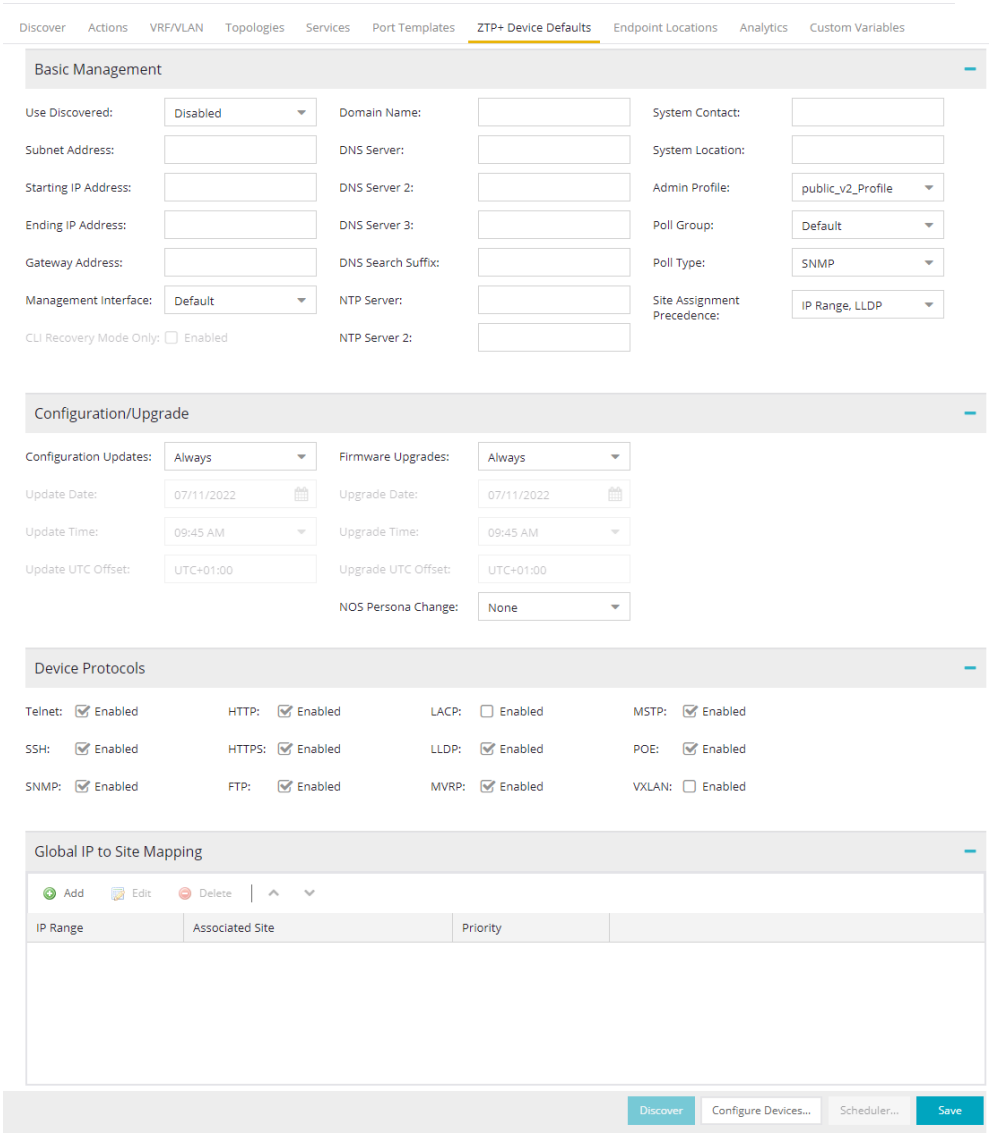
        - ExtremeXOS/Switch Engine Stack/VPEX: "1:1" or "1:1, 1:3, 1:5, 1:7"
        - SLX: "Ethernet 0/1" or "Ethernet 0/1, Ethernet 0/3"
    - Port Ranges:
        - 210-Series: "1/5-1/7" or "100/5-100/7, 111/9-111/12, 113/15-113/19"
        - 220-Series: "1/0/1-1/0/5" or "1/0/1, 1/0/3, 1/0/5, 1/0/7"
        - ERS: "1/5 - 1/7" or "100/5-100/7, 111/9-111/12, 113/15-113/19"
        - ExtremeXOS/Switch Engine: "1:5-1:7" or "1:5-1:7, 1:9-1:12, 1:15-1:19"
        - ExtremeXOS/Switch Engine Stack: "1:5-1:7" or "1:5-1:7, 2:9-2:12, 3:15-3:19"
        - ExtremeXOS/Switch Engine channelized ports are included in the master port: "1:24" is equal to "1:24:1,1:24:2,1:24:3,1:24:4"
        - SLX: "Ethernet 0/1-Ethernet 0/4" or "Ethernet 0/1-Ethernet 0/5, Ethernet 0/8-Ethernet 0/15"
    - Wildcarding:
        - "*" is always allowed, matches anything, useful as default rule at the end of a set of bindings
        - In a single port scenario, the wildcard may be applied as the slot or port value:
            - 210-Series: "*/1" or "1/*"
            - 220-Series: "*/0/1" or "1/0/*"
            - ERS: "*/1" or "1/*"
            - ExtremeXOS/Switch Engine: "*"
            - ExtremeXOS/Switch Engine Stack/VPEX: "*:1" or "1:*"
            - SLX: "Ethernet 0/*" or "Ethernet */3,Ethernet */5"
    - Port ranges support limited use of wildcards: for port ranges in the slot/port or slot/unit/port format, use the wildcard on the same item.

To refresh the port templates, go the **Devices** view and select one or more port templates. Then, right-click **More Actions > Refresh ZTP+ Automated Templates**. This updates the port template settings on all selected devices based on the configured automated port templates. This action also creates an operation in the Operations view and generates an event detailing the results.

After configuring the automated port templates, when ExtremeCloud IQ Site Engine discovers devices via ZTP+ and asks for configuration, the automated port templates are automatically assigned to the ports on the device.

ZTP+ Device Defaults

The **ZTP+ Device Defaults** tab contains information about a device with ZTP+ (Zero Touch Provisioning Plus) enabled. Use the following dialog to specify the parameters that should be used during the process of learning about a ZTP+ device. ExtremeCloud IQ Site Engine then applies these configuration templates to devices that you add to a site in your network.



Basic Management

Use Discovered

Use the drop-down list to select if ExtremeCloud IQ Site Engine assigns the IP address, IP address and Management Interface, or Management Interface to the ZTP+ device when it is discovered:

- **IP** — ExtremeCloud IQ Site Engine uses the **Discovered IP** assigned when the device was discovered. Select the **Management Interface** (the VLAN interface used to manage the device) manually.
- **IP and Management Interface** — ExtremeCloud IQ Site Engine uses the **Discovered IP** and the **Management Interface** that were assigned when the device was discovered.
- **Management Interface** — ExtremeCloud IQ Site Engine uses the **Management Interface** that was defined when the device was discovered. Enter the IP address and subnet, Gateway Address, Domain Name, and DNS Server in the tab (along with any of the optional fields) and then save.
- **Disabled** — Configure the IP address and subnet, Gateway Address, Domain Name and DNS Server in the tab (along with any of the optional fields) and then save.

Subnet Address

Enter the **Subnet Address** for the ZTP+ devices associated with the site.

Starting IP Address

The **Starting IP Address** field allows you to set the starting IP address of the IP address range for the ZTP+ devices associated with the site.

Ending IP Address

The **Ending IP Address** field allows you to set the ending IP address of the IP address range for the ZTP+ devices associated with the site.

Gateway Address

Enter the **Gateway Address** for the ZTP+ devices associated with the site.

Management Interface

Select the interface that the device uses for Management and assign the device IP to that interface.

CLI Recovery Mode Only

Select the checkbox to disable the CLI account while the device is able to communicate with ExtremeCloud IQ Site Engine. If connectivity between the device and ExtremeCloud IQ Site Engine is lost, the device enables the CLI account defined in the profile so the user can gain local access. When connectivity between the device and ExtremeCloud IQ Site Engine is re-established, the CLI account is disabled again.

NOTE: Only devices managed using ZTP+ support this functionality.

Domain Name

Enter a value in the **Domain Name** field to configure the domain name on the ZTP+ devices associated with the site.

DNS Server

The **DNS Server** field allows you to set the DNS server address on the ZTP+ devices associated with the site.

DNS Server 2

The **DNS Server 2** field allows you to set the secondary DNS server address on the ZTP+ devices associated with the site.

DNS Server 3

The **DNS Server 3** field allows you to set the tertiary DNS server address on the ZTP+ devices associated with the site.

DNS Search Suffix

The **DNS Search Suffix** field allows you add additional comma-separated entries to DNS search suffix list configured on the device. Support for the DNS search suffix is dependent on the device operating system and version. Refer to your device specifications to determine the maximum number of entries that you can add.

NTP Server

The **NTP Server** field allows you to set the NTP server address on the ZTP+ devices being discovered.

NTP Server 2

The **NTP Server 2** field allows you to set the secondary NTP server address on the ZTP+ devices associated with the site.

System Contact

Allows you to specify contact information for the person maintaining the device. Additionally, enter a backslash "\" between contacts to create a device group in a tiered tree structure. For example, to move the device into a device group called "John's Devices" within a device group called "Quality Assurance Testing", enter **Quality Assurance Testing\John's Devices** in this field.

System Location

A description of the location of the ZTP+ devices associated with the site.

Admin Profile

Use the drop-down list to select the access Profile that gives ExtremeCloud IQ Site Engine administrative access to the ZTP+ devices associated with the site. Use the Profiles list in the Discover section of the **Site** tab to create or edit a profile. If you discover an existing device using a different profile than the device is already using in the database, click **Save** to overwrite the device profile currently being used in the database.

Poll Group

Use the drop-down list to select a Poll Group for the discovered ZTP+ devices. ExtremeCloud IQ Site Engine provides three distinct poll groups (defined in the Status Polling options (**Administration** > **Options**) that each specify a unique poll frequency. When you save newly discovered devices to the database, they are polled with the poll group specified here. If you save discovered devices that already exist in the database, the poll group specified here overwrites the poll group currently being used in the database.

NOTE: If you select **Not Polled**, the **Poll Group** is only used if/when the **Poll Type** is changed to **SNMP** or **Ping**.

Poll Type

Use the drop-down list to select the Poll Type for devices included in the site:

- Select **Not Polled** if you do not want to poll the devices.
- Select **Ping** for the **Poll Type** if the **Profile** for the IP Range is also set to **Ping**.
- Select **SNMP** to poll the device using SNMP. The SNMP version (SNMPv1 or SNMPv3) is determined by the Profile specified for the IP Range.
- Select **Maintenance** if you do not want to poll the devices temporarily. Using this **Poll Type** allows you to search for devices set to **Maintenance** to change them back to their regular **Poll Type** when maintenance on the device is complete.
- Select **ZTP+** for devices managed by ZTP+ and created through the ZTP+ process. When the **Poll Type** is **ZTP+** the ExtremeCloud IQ Site Engine does not initiate a poll, instead the ExtremeCloud IQ Site Engine receives a message from the device to determine the status. The ZTP+ Poll Type is incompatible with Switch Engine devices running with FIPS mode enabled.

  For example, if ExtremeCloud IQ Site Engine does not receive a message from a device or Fabric Manager for three times the amount of time defined in the **Poll Interval** for the **Poll Group** of the device, then the **Status** is **Contact Lost**. When ExtremeCloud IQ Site Engine receives a message from the device, the **Device Status** is **Contact Established**.

Site Assignment Precedence

Set the precedence by which ZTP+ devices will be assigned to the site. This field is used in conjunction with the Global IP to Site Mapping settings in determining the site assignment. For example, during the device configuration, if the precedence is set to IP range only, the device will try to match any of the single IP addresses or fit within a range. If an IP does not match any value in the table then it will default to /World.

The following values can be configured:

- **IP Range, LLDP:** Uses IP range first. If no IP range is set, uses LLDP instead.
- **LLDP, IP Range:** Uses LLDP first. If LLDP is not available, uses IP range instead.
- **LLDP Only:** Uses LLDP only.
- **IP Range Only**: Uses IP range only.
- **None:** Uses neither LLDP or IP range.

All discovered ZTP+ devices are assigned to the site based on the this value. However, you can manually change the value for individual devices in the device configuration.

If there are multiple IP ranges that match the site, the device will use the mapping that has the highest priority.

Configuration/Upgrade

Configuration Updates

Select the frequency for which ExtremeCloud IQ Site Engine checks for configuration updates for devices with a **Poll Type** as **ZTP+** associated with the site.

The following values can be configured:

- **Always:** Operations are checked on every ZTP+ check-in.
- **Never:** Operations are skipped for every ZTP+ check-in.
- **Scheduled:** The operation only occurs after the selected date or time, then reverts to Never.
- **Suspend:** The operation is skipped until the selected date or time, then reverts to Always.

NOS Persona Change

Select To Fabric Engine to change the Network Operating System (NOS) of a universal switch currently running Switch Engine to Fabric Engine. The NOS Persona Change field has values of None and To Fabric Engine. The persona change to Fabric Engine requires a Fabric Engine firmware in Set as Reference image,

When the switch completes the persona change from Switch Engine to Fabric Engine, all previous Switch Engine references for the switch are removed from ExtremeCloud IQ Site Engine. Including but not limited to the Discovered panel, and the Device Tree. You must now stage configuration for the 'new' Fabric Engine switch in ExtremeCloud IQ Site Engine.

IMPORTANT:

The NOS persona change **To Fabric Engine** is ignored if:

- The universal switch is running EXOS (Upgrade to Switch Engine before changing persona)
- The non-universal switch is running EXOS (A firmware upgrade for EXOS occurs if the EXOS image is set as reference image)
- You did not specify a Fabric Engine reference image (The destination firmware must be a Fabric Engine firmware set as reference image)

A Switch Engine reference image is not required. If you only specify a Fabric Engine firmware in **Set as Reference Image**, then only one firmware upgrade occurs on the switch during the change from Switch Engine to Fabric Engine, which increases the persona change speed.

Upload the Fabric Engine firmware to both of the TFTP and SFTP directories (Network > Firmware > Upload...). You must specify the Fabric Engine firmware located in the SFTP directory as a reference image.

NOTE:

You can specify one reference image for upgrading EXOS to Switch Engine, and another reference image for a persona change from Switch Engine to Fabric Engine.

If you specify reference images for Switch Engine and for Fabric Engine and the universal switch is not currently running the Switch Engine reference image, a firmware upgrade for Switch Engine occurs before the persona change to Fabric Engine.

Update Date

Select the date on which ExtremeCloud IQ Site Engine updates the configuration for your devices with a **Poll Type** as **ZTP+** associated with the site when you select **Scheduled** for **Configuration Updates**.

Update Time

Select the time at which ExtremeCloud IQ Site Engine updates the configuration for your devices with a **Poll Type** as **ZTP+** associated with the site when you select **Scheduled** for **Configuration Updates**.

Update UTC Offset

Select your time zone based on the number of hours you are offset from the Universal Time Coordinated.

Firmware Upgrades

Select the frequency for which ExtremeCloud IQ Site Engine checks for firmware upgrades for your devices with a **Poll Type** as **ZTP+** associated with the site.

Upgrade Date
Select the date on which ExtremeCloud IQ Site Engine upgrades the firmware for your devices with a **Poll Type** as **ZTP+** associated with the site when you select **Scheduled** for **Firmware Upgrades**.

Upgrade Time
Select the time at which ExtremeCloud IQ Site Engine upgrades the firmware for your devices with a **Poll Type** as **ZTP+** associated with the site when you select **Scheduled** for **Firmware Upgrades**.

Upgrade UTC Offset
Select your time zone based on the number of hours you are offset from the Universal Time Coordinated.

Device Protocols/Features

Telnet
Select the checkbox to enable Telnet access on the ZTP+ device.

SSH
Select the checkbox to enable SSH (Secure Shell) access on the ZTP+ device.

HTTP
Select the checkbox to enable HTTP (Hypertext Transfer Protocol) access on the ZTP+ device.

HTTPS
Select the checkbox to enable HTTPS (Hypertext Transfer Protocol Secure) access on the ZTP+ device.

NOTE: To enable HTTPS access, an SSL certificate must be configured on the device.

SNMP
Select the checkbox to enable SNMP (Simple Network Management Protocol) access on the ZTP+ device.

LACP
Select the checkbox to enable LACP (Link Aggregation Control Protocol) access on the ZTP+ device.

LLDP
Select the checkbox to enable LLDP (Link Layer Discovery Protocol) access on the ZTP+ device.

MSTP
Select the checkbox to enable MSTP (Multiple Spanning Tree Protocol) access on the ZTP+ device.

MVRP
Select the checkbox to enable MVRP (Multiple VLAN Registration Protocol) access on the ZTP+ device.

POE
Select the checkbox to indicate the ZTP+ devices being discovered for the site are electrically powered by Ethernet cable.

VXLAN
Select the checkbox to indicate the ZTP+ devices being discovered for this site use VXLAN to tunnel Layer 2 traffic over a Layer 3 network.

NOTE: ZTP+ does not currently provision a Layer 3 network with which VXLAN operates. If your ZTP+ devices use VXLAN, the Layer 3 underlay network must be manually provisioned.

DvR Leaf
Select the checkbox to indicate the ZTP+ devices being discovered for the site operate in DvR Leaf mode. The DvR Leaf flag is enabled. Only devices running Fabric Engine support the DvR Leaf feature.

Global IP To Site Mapping

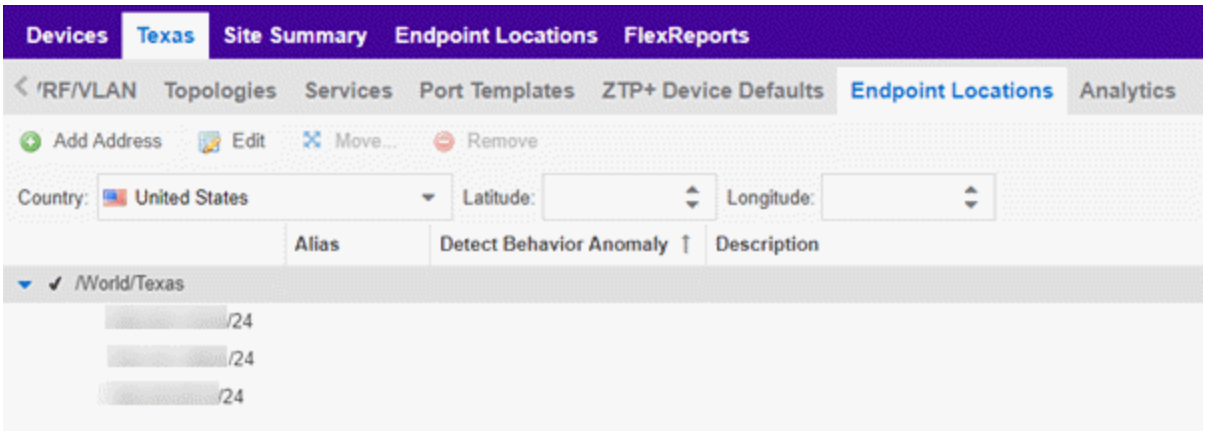
IP Range
Select **Add** or **Edit** to enter a single IP address or an IP range.

Associated Site
Select a site from the drop-down list that the discovered ZTP+ devices will be associated with when the devices are discovered.

Endpoint Locations

Use the **Endpoint Locations** tab to define the geographical location of the site and addresses in it. After the geographical locations are defined for your devices, flows on the Application Flows tab display geographical information depending on the device on which the flow is observed.

Select the **Add Address** button at the top of the table to add an additional address to the table. Select the **Edit** button to modify the site or selected address of the site. The **Move** button allows you to move an address to a different site in the drop-down list. Select the **Remove** button to delete a selected address from the table. These options are also accessible when you right-click an address in the table.



Use the Country, Latitude, and Longitude drop-down lists to configure or change the following information for the site:

Country
: Select the country in which the site is located.

Latitude
: Enter the site's latitude location in decimal degrees.

Longitude
: Enter the site's longitude location in decimal degrees.

The following columns are displayed in the Endpoint Locations table:

Tracked
: This column displays the name of the site or the IP Address/Mask of the devices on the site. A check mark to the left of the site name indicates it is a Tracked Site. Right-click any site to either add or remove the site from your Tracked Sites list.

Alias
: An alternate name for the site, or a specific subnet of the site.

Description
: A description of the site location.

Analytics

The **Analytics** tab allows you to configure the default ExtremeAnalytics functionality for the devices in the site.

Analytics Role
: Allows you to indicate the purpose of the devices added to the site: **Access**, **Core**, **Data Center**, **DMZ**. This field is informational only.

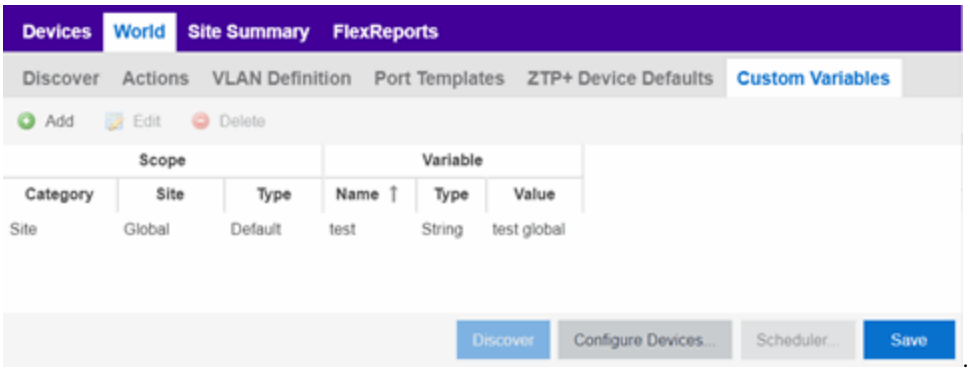
Analytics Home Engine
: Displays the ExtremeAnalytics engine located with the devices associated with the site.

Custom Variables

The **Custom Variables** tab allows you to add, edit, or delete variables used in ExtremeCloud IQ Site Engine.

Variables you create serve as a placeholder for a specific value. The fields included in the **Scope** section determine where the variable is used in ExtremeCloud IQ Site Engine, while the fields in the **Variable** section allow you to define a value for the variable. After you create a variable, ExtremeCloud IQ Site Engine automatically substitutes the **Value** you define in the appropriate feature of ExtremeCloud IQ Site Engine when the criteria specified in the **Scope** section is met. Variables you create on the **Site** tab can then be used in a configuration template, script or workflow, in a CLI command, or in a third-party application via the Northbound Interface.

NOTE: Custom variables you create are not displayed in ExtremeCloud IQ Site Engine. To view and reference the variables, use the Northbound Interface functionality in the **Diagnostics** tab.



Scope

Category

Displays where the variable is used in ExtremeCloud IQ Site Engine. Select **Port Template**, **Site**, or **Topology** from the drop-down list, depending on the purpose of the variable.

Site

Defines the site in which the variable is used.

- **Global** indicates ExtremeCloud IQ Site Engine uses the variable for all sites.
- Selecting **/World** indicates ExtremeCloud IQ Site Engine uses the variable for all devices added to the /World site. Devices added to a site other than /World do not use the variable.
- Selecting the current site also creates an additional variable with a **Site** of **Global**. This allows you to use the variable in workflows run on devices not included in the current site.

Type
Defines the type of Port Template or Topology for which the variable applies. The values in this drop-down list change depending on what **Category** you select.

- Port Template — Indicates the Port Configuration for which the variable is used by ExtremeCloud IQ Site Engine.
- Topology — Displays the type of network topology for which the variable is used by ExtremeCloud IQ Site Engine.

Variable

Name
Displays the name of the variable.

Type
Defines the type of information the variable is substituting. Select **Boolean**, **IP**, **MAC Address**, **Number**, **String**, or **Subnet** from the drop-down list.

Value
Displays the value ExtremeCloud IQ Site Engine uses when substituting the variable. Enter a value associated with the variable type you define. For example, if the variable type is **Boolean**, choose **True** or **False**; if the attribute type is **IP**, enter the IP Address of the variable).

Add
Click the button to add a row to the table where you can create a new custom variable.

Edit
Select a variable in the table and select **Edit** to make changes to a custom variable.

Delete
Select a variable in the table and select **Delete** to remove a custom variable from the table.

Update
Click the **Update** button when you finish adding a new or editing an existing custom variable.

Cancel
Click the **Cancel** button to cancel the new variable or the changes you made to an existing variable.

XIQ Location

Devices assigned to the site are automatically mapped to the specified locations in ExtremeCloud IQ, and the XIQ location is assigned on the site level. Values in the drop down are obtained from ExtremeCloud IQ. The assignment of the device to the XIQ location is configurable in the ExtremeCloud IQ Site Engine, but not in ExtremeCloud IQ.

NOTE: The XIQ Location tab is only displayed in connected deployment mode.

Buttons

Edit Devices

Clicking **Configure Devices** opens the **Configure Device** window for all of the devices added to the site. This allows you to change the configuration of a single device or a subset of devices within the site.

Save

Clicking **Save** saves any changes you make to a site. This button displays after making a change to the tab.

Cancel

Clicking **Cancel** discards any changes you make to a site. This button displays after making a change to the tab.

Discover

Clicking **Discover** adds to the site any new devices that match the criteria entered in the Discover section of the window. This button displays after selecting **Create** or **Save**.

Scheduler

Clicking **Scheduler** opens the **Add Scheduled Task** window, where you can create a new task that automatically adds devices matching the criteria entered in the Discover section of the **Site** tab to the site. This button displays after selecting **Create** or **Save**.

NOTE: After you create a scheduled task to discover devices, edit or delete the task on the **Scheduled Tasks** tab.

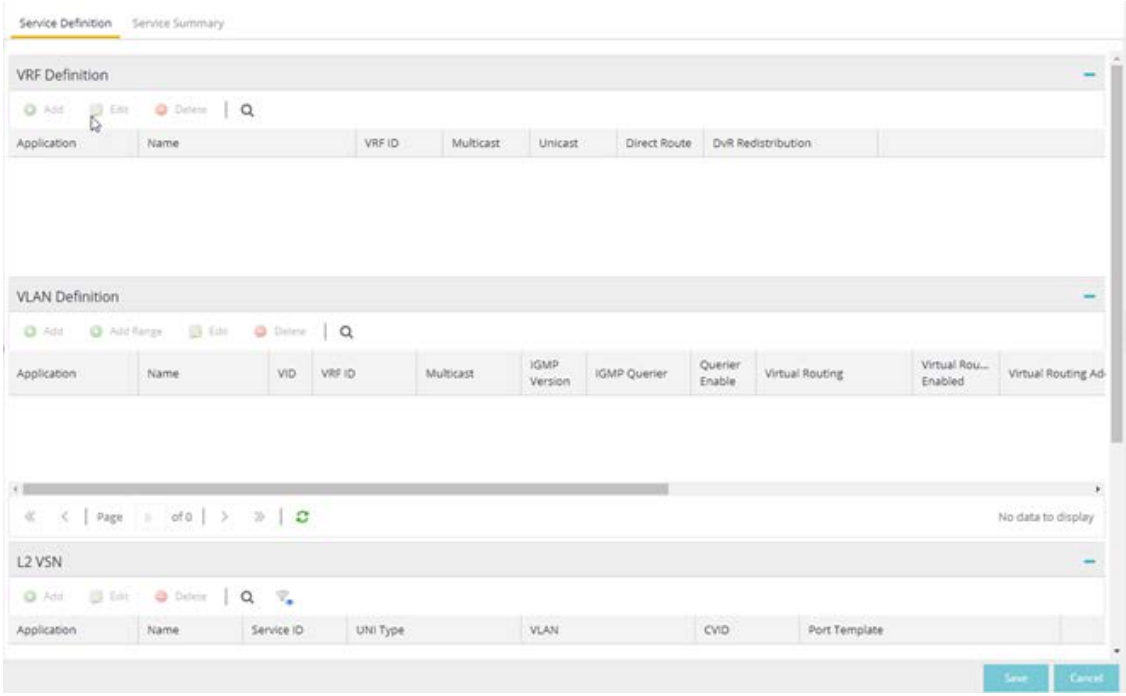
For information on related topics:

- How to Discover Devices in ExtremeCloud IQ Site Engine
- Devices
- Maps
- How to Create and Edit Maps
- Advanced Map Features

Services

The **Services** tab displays virtual routing and forwarding functionality configured as part of a service application, the virtual local area networks defined for the service application, as well as all of the services included in a service application or all of the services included in a service definition, depending if you select a service application or a service definition in the left-panel, respectively.

The **Services** tab is included in the **Sites** tab.



The Services tab includes three tables:

- **VRF Definition** — Create and configure VRF (Virtual Routing and Forwarding) definitions for the service application. VRFs allow for networking paths to be segmented without using multiple devices.
- **VLAN Definition** — Create and configure VLAN (Virtual Local Area Network) definitions for the service application.
- **L2 VSN** — Configure the L2 Virtual Services Networks (VSNs).
- **L3 VSN** — Configure the L3 Virtual Services Networks (VSNs).

VRF Definition

The VRF Definition table allows you to configure virtual routing and forwarding definitions included as part of the service.

Name
The name of the VRF definition.

VRF ID
The ID number assigned to the VRF definition.

Multicast
Select to indicate the service sends IP packets to a group of recipients on the network.

Unicast
Select to indicate the service sends IP packets to a single recipient on the network.

Direct Route
Select to indicate the service sends IP packets directly to another device without going through a third device.

VLAN Definition

The VLAN Definition table allows you to configure virtual local area network definitions included as part of the service.

Name
The name of the VLAN definition.

VID
The ID number assigned to the VLAN.

VRF ID
The ID number assigned to the VRF definition.

Multicast
Indicates the service sends IP packets to a group of hosts on the network.

IGMP Version
Indicates which version of IGMP is utilized on the port (Version 1 or Version 2).

IGMP Querier
The address of the IGMP Querier. This feature is used when there is no multicast router in the VLAN to originate the queries.

Querier Enable
Indicates whether an IGMP Query is enabled.

Virtual Routing
Displays the version of VRRP the default gateway is using:

- **NONE** — Virtual routing is not configured on the VLAN.
- **VRRPv2** — VRRP version 2 is configured on the VLAN. VRRP version 2 only supports IP addresses in IPv4 format.
- **VRRPv3** — VRRP version 3 is configured on the VLAN. VRRP version 3 supports IP addresses in both IPv4 and IPv6 formats.
- **DvR –** DvR functionality is configured on the VLAN.

NOTE: Virtual Routing is only supported on Fabric Engine devices.

Virtual Routing Enable
Indicates whether virtual routing is enabled for the VLAN.

Virtual Routing Address

The IP address for the virtual routing interface. The Virtual Routing address must be in the same subnet as the VLAN subnet address.

VRRP ID

An identifier devices use to determine peer devices that participate in a virtual routing interface.

VRRP Priority

A value used by VRRP peers to determine the role of each of the devices in the VLAN. The default value is **100**. The device with the largest value is assigned the role of Master. For example, in a VLAN with two routers, one with a **VRRP Priority** of **200** and one with a **VRRP Priority** of **100**, the router with a **VRRP Priority** of **200** becomes the Master. In the event of identical priority numbers, the devices use the MAC address to determine priority.

VRRP Backup Master

This option determines if the backup router is able to forward traffic independently outside of the VLAN (enabled), or must forward the traffic to the Master router before it is forwarded outside of the VLAN (disabled).

VRRP Advertisement Interval

Indicates frequency (in seconds) that protocol packets are sent from the virtual router in the VLAN.

VRRP Hold Down Timer

Indicates the amount of time (in hundredths of a second) that the backup router waits for the primary router to respond before it becomes the primary router.

DHCP Snooping

Indicates whether DHCP snooping is enabled for the VLAN. DHCP Snooping is a Layer 2 security feature, that provides network security by filtering untrusted DHCP messages received from the external network causing traffic attacks within the network. DHCP Snooping is based on the concept of trusted versus untrusted switch ports. Switch ports configured as trusted can forward DHCP Replies, and the untrusted switch ports cannot. DHCP Snooping acts like a firewall between untrusted hosts and DHCP servers.

ARP Inspection

Indicates whether ARP inspection is enabled. Dynamic ARP Inspection (DAI) is a security feature that validates ARP packets in the network. Without DAI, a malicious user can attack hosts, switches, and routers connected to the Layer 2 network by poisoning the ARP caches of systems connected to the subnet, and intercepting traffic intended for other hosts on the subnet. DAI prevents these attacks by intercepting, logging, and discarding the ARP packets with invalid IP to MAC address bindings. The switch dynamically builds the address binding table from the information gathered from the DHCP requests and replies when DHCP Snooping is enabled. The switch pairs the MAC address from the DHCP request with the IP address from the DHCP reply to create an entry in the DHCP binding table. When you enable DAI, the switch filters ARP packets on untrusted ports based on the source MAC and IP addresses seen on the

switch port. The switch forwards an ARP packet when the source MAC and IP address matches an entry in the address binding table. Otherwise, the switch drops the ARP packet.

NOTE: **DHCP Snooping** must be enabled to use **ARP Inspection**.

Service Application Name

The **Service Application Name** table displays all of the services included in a service application or all of the services included in a service definition, depending if you select a service application or a service definition in the left-panel, respectively. The Services tab is included in the **Sites** tab.

Services are created within service applications. You can include multiple services within an application. Service applications are then included within service definitions. You can also include multiple service applications within a service definition. A service definition that includes a complete set of services is then assigned to a site, which configures the fabric-enabled devices within that site.

The **Services** tab is only configurable when you select a service application. The services displayed when selecting a service definition are read-only.

L2 VSN

Name
The name of the Layer 2 service.

Service ID
The I-SID, which is the system-defined ID number assigned to the fabric service.

UNI Type
The User-Network-Interface (UNI) of the fabric service. The following interface types are available:

- **Switched** — A VLAN-ID and a port (VID, port) mapped to a Layer 2 VSN I-SID. With UNI type, VLAN-IDs can be reused on other ports and mapped to different ISIDs.
- **Transparent** - A physical port maps to a Layer 2 VSN I-SID (all traffic through the port, 802.1Q tagged or untagged, ingress and egress maps to the I-SID).

  NOTE: All VLANs on a Transparent Port UNI interface now share the same single MAC learning table of the Transparent Port UNI I-SID.

- **CVLAN** — a platform customer VLAN-ID.

VLAN
The customer VLAN-ID of the associated CVLAN UNI type.

CVID
Specifies the customer VLAN ID of the associated switched UNI port.

Management Service

Defines is the L2 VSN is used for switch management purposes.

AutoSense Service Type

Defines if the L2 VSN service is auto-assigned by the switch-level AutoSense detection. The following types are available:

- **AP Untagged** — If the AutoSense feature detects Access Point, then this service is automatically assigned to the port.
- **Camera Untagged** — If the AutoSense feature detects Camera then this service is automatically assigned to the port.
- **Voice Untagged** — If the AutoSense feature detects a VoIP device then this service is automatically assigned to the port.
- **Voice Tagged** — If the AutoSense feature detects a VoIP device then this service is automatically assigned to the port.
- **Proxy Switch Auth Tagged —** If the AutoSense feature detects a Fabric Attach switch capable of authenticating (ERS devices) then this service is automatically assigned to the port.
- **Proxy Switch No Auth Untagged —** If the AutoSense feature detects a Fabric Attach switch is not capable of authenticating (Switch Engine devices) then this service is automatically assigned to the port.
- **Proxy Switch Auth & Proxy Switch No Auth —** If the AutoSense feature detects any physical Fabric Attach switch (ERS/EXOS/Switch Engine device) then this service is automatically assigned to the port.
- **Data Untagged** — If the AutoSense feature does not detect a device type then this service is automatically assigned to the port.
- **None** — AutoSense is not related to this L2VSN service.

NOTE: Each AutoSense Service Type can only be used once on a switch. The switch cannot use two different service IDs with the same AutoSense Service Type.

AutoSense Service CVID

The AutoSense Service CVID value defines the 802.1q VLAN tag sent from the switch to the device. If the **AutoSense Service Type** is **Voice Tagged** or **Proxy Switch Auth Tagged** or **Proxy Switch Auth & Proxy Switch No Auth** then AutoSense Service CVID must be defined. The value range is 1-4094.

Port Template

If the **UNI Type** is **Switched** or **Transparent** you can select from the Global Port templates to define the purpose of the port.

L3 VSN

Name
The name of the Layer 3 service.

Service ID
The I-SID, which is the system-defined ID number assigned to the service.

VRF
Select the virtual routing and forwarding definition included as part of the service.

Multi Cast
Select to indicate that the service sends IP packets to a group of hosts on the network.

Unicast
Select to indicate that the service sends IP packets to a single recipient on the network.

Direct Route
Select to indicate that the service sends IP packets directly to another device without going through a third device.

Fabric Topology Definition on the Sites Tab

Use the **Fabric Topology Definition** tab to create a fabric topology definition, configure fabric topology settings, and review fabric topology paths and sites. You can also rename or delete a fabric topology definition.

Create a Topology Definition

You can create a Topology Definition on the **Sites** tab in ExtremeCloud IQ Site Engine. After you create topology definitions, you can add them to sites in your network to build a fabric topology map.

To create a topology definition:

1. Access the **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Navigate to **Topology Definitions** in the left-panel tree.
4. Right-click **Topology Definitions**.
5. Select **Create Topology Definition**.

   The **Create Topology Definition** window opens.
6. Enter a name in the **Name** field.

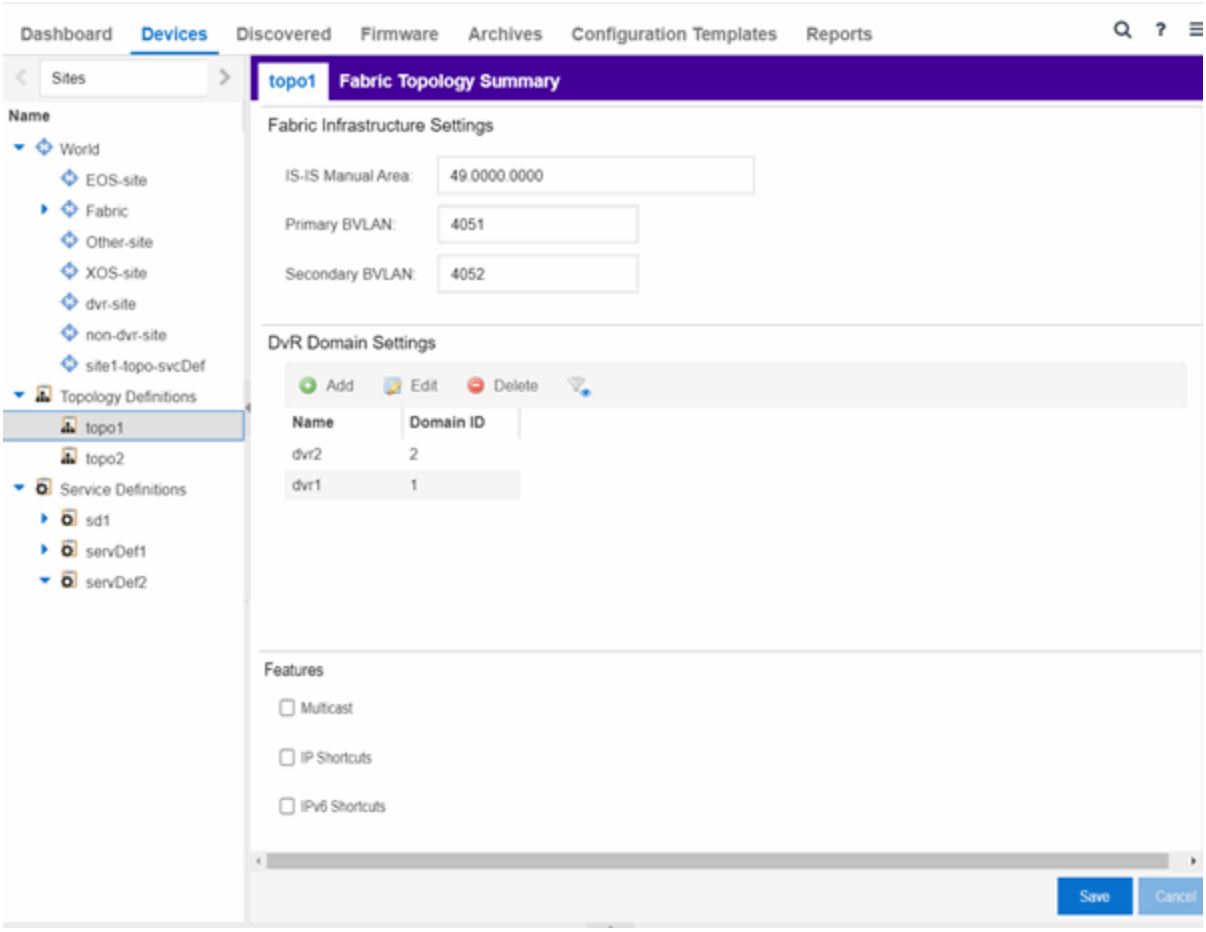
7. Select **Fabric Connect** from the **Fabric Type** drop-down.
8. Select **OK** to create the topology definition.

Configure a Topology Definition

After the topology definition is created, it is available in the **Sites tab** left-panel tree. Select it to open a new right panel that includes the Fabric Name tab and a Fabric Summary tab.

Fabric Name Tab

Use the **Fabric Name** tab to configure the topology definition.



The Topology Definition tab includes the following sections:

Fabric Infrastructure Settings

The following fields are included in the Fabric Infrastructure Settings section:

- ISIS Manual Area - Use a xx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx format (1-13 bytes).
- Primary BVLAN - Enter the Primary Backbone VLAN (BVLAN).

- Secondary BVLAN - Enter the Secondary BVLAN.

DvR Domain Settings

The following fields are included in the DvR Domain Settings section:

- Name - The Domain name assigned to the DvR Domain. Select the down arrow to open the drop-down list to access sort, hide columns and search filter functionality for the domain name column.
- Domain ID - The identifying number assigned to the DvR Domain. Select the down arrow to open the drop-down list to access sort, hide columns and numeric filter functionality for the Domain ID column.

You can also Add, Edit, or Delete DvR Domain settings.

Features

The following fields are included in the Features section:

- Multicast - Select the check box to configure to distribute data to multiple recipients.
- IP Shortcuts - Select the check box to enable IPv4 Shortcuts for the topology definition.
- IPv6 Shortcuts - Select the check box to enable IPv6 Shortcuts for the topology definition.

Select **Save** to save the topology definition settings you selected.

After the topology definition is created and configured, you can apply it to a site within your network. After fabric topologies have been assigned to a site, they cannot be deleted.

Fabric Summary tab

The Fabric Summary tab lists any fabric topologies you have created and the sites to which they are assigned.

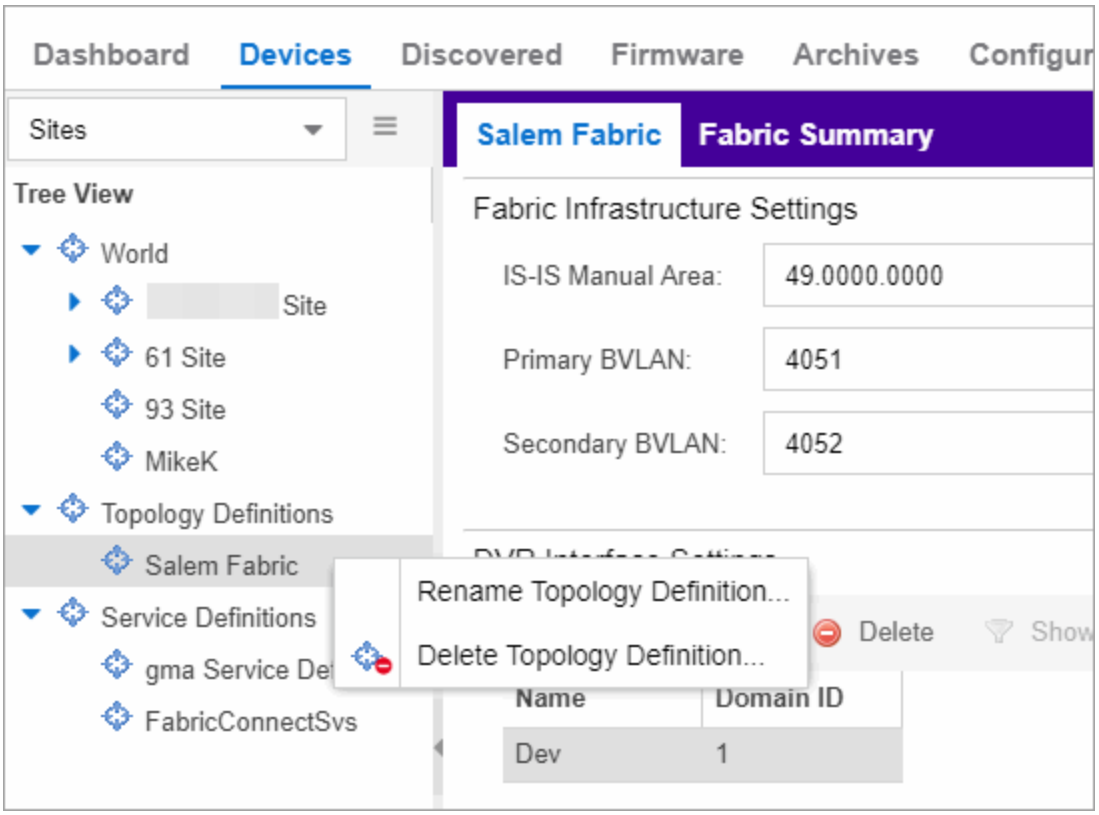
Rename a Topology Definition

After a topology definition has been created and configured, you can change or modify its name.

To rename a topology definition:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Expand **Topology Definitions** in the left-panel.

4. Right-click the topology definition you are renaming.



5. Select **Rename Topology Definition**.
6. Enter a new name in the **Name** field.
7. Select **OK** to change the topology name.

Delete a Topology Definition

After a topology definition has been created and configured, you can delete it; however, a topology definition cannot be deleted if it has been assigned to a site.

To delete a topology definition:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Expand the **Topology Definitions** in the left-panel.
4. Right-click the topology definition you are deleting.
5. Select **Delete Topology Definition**.
6. Select **Yes** to delete the topology definition you selected.

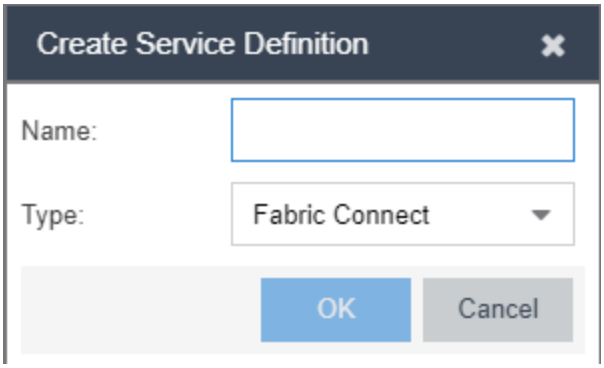
How to Create a Fabric Service Definition

You can create a service definition in the **Sites tab** in ExtremeCloud IQ Site Engine. Service definitions display information configured in service applications definitions. When created, service definitions are added to sites in your network and are used to build a fabric topology map.

Create a Service Definition

To create a service definition:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Select **Service Definitions** in the left-panel.
4. Right-click **Service Definitions**.
5. Select **Create Service Definition**.



   The **Create Service Definition** window opens.
6. Enter a name in the **Name** field.
7. Select **Fabric Connect** from the **Type** drop-down list.
8. Select **OK** to create the service definition.

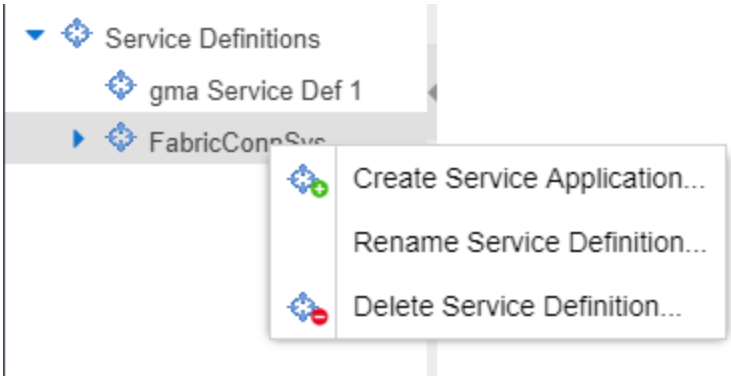
After the service definition is created and configured, you can apply it to a site within your network. When fabric services have been assigned to a site, they cannot be deleted.

Service Definition Panel

After the service definition is created, it is available in the left-panel tree. Select it to open a new right panel that includes a **Services** tab and a **Service Summary** tab.

Rename a Service Definition

After a service definition has been created and configured, you can change or modify its name.

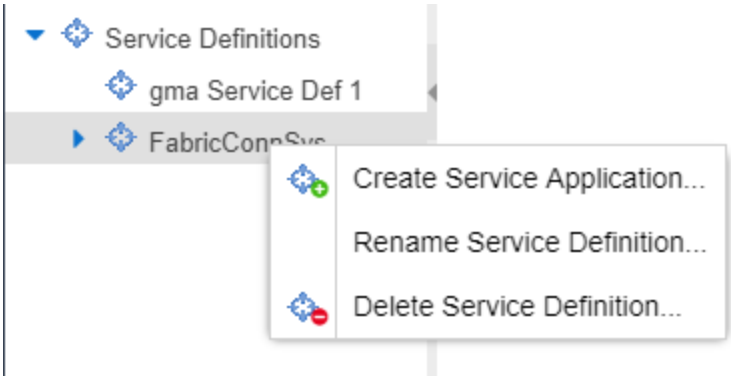


To rename a service definition:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Expand **Service Definitions** in the left-panel.
4. Right-click the service definition you are renaming.
5. Select **Rename Service Definition**.
6. Enter a new name in the **Name** field.
7. Select **OK** to rename the service definition.

Delete a Service Definition

When a service definition has been created and configured, you can delete it; however, a service definition or any of its associated service applications cannot be deleted if it has been assigned to a site.



To delete a service definition:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Expand **Service Definitions** in the left-panel.
4. Right-click the service definition you are deleting.
5. Select **Delete Service Definition**.
6. Select **Yes** to delete a service definition.

For information on related topics:

- Services
- Fabric
- Sites
- Devices

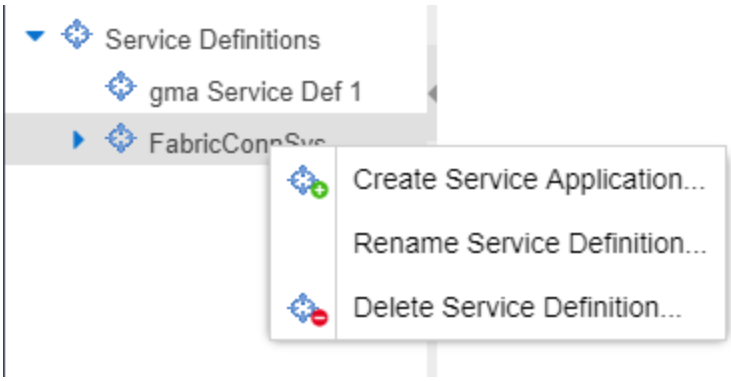
How to Create a Service Application

You can create a service application via the **Sites** tab in ExtremeCloud IQ Site Engine. Service definitions display information from service applications. When created, service applications are added to sites in your network and are used to build a topology map.

Create a Service Application

To create a service application:

1. Access the **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Expand **Service Definitions** in the left-panel.
4. Right-click the service definition in which you want to create the service application.



5. Select **Create Service Application**.

   The **Create Service Application** window opens.
6. Enter a name in the **Name** field.
7. Select **OK**.
8. Select the newly created service application.
9. Use the Services tab and a Service Summary tab to configure the service application.

The service application is created. After the service application is created and configured, you can apply it to a site within your network. After services have been assigned to a site, they cannot be deleted.

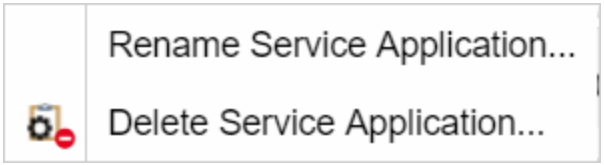
NOTE: A Service Application must have the same fabric type as its associated Service Definition. For example, if a Service Definition is created with Fabric Connect type, it can only have Service Applications of Fabric Connect type. Currently, Fabric Connect is the only fabric type available.

After the service application is created, it is available in the left-panel tree and a new right panel opens that includes a Services tab and a Service Summary tab.

Rename a Service Application

To change the name of a service application:

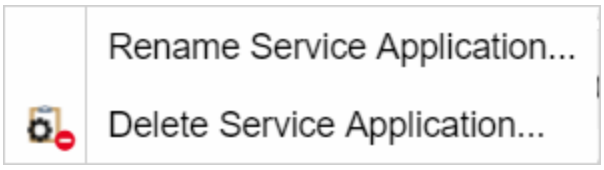
1. Open the **Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Expand **Service Definitions** in the left-panel.
4. Right-click the service application you are renaming.



5. Select **Rename Service Application**.
6. Enter a new name in the **Name** field.
7. Select **OK** to change the name of the service application.

Delete a Service Application

You can delete all user-defined service applications, unless the service application or any of its associated service definitions are assigned to a site.



To delete a service application:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Expand **Service Definitions** in the left-panel.
4. Right-click the service application you are deleting.
5. Select **Delete Service Application**.
6. Select **Yes** to delete the service application.

For information on related topics:

- Services
- Fabric
- Sites
- Devices

Maps Overview

The ExtremeCloud IQ Site Engine Maps feature on the **Network** > **Devices** tab enables you to view and search maps of the devices on your network. Use maps to view network connections and alarm status. You can also search for devices, APs, and wired or wireless clients. .

ExtremeCloud IQ Site Engine supports the following types of maps:

- Geographical and Floorplan Maps – Use these maps to create geographical maps of devices or floor plans of wireless access points (APs).

All maps work the same way in terms of creating new maps, and deleting or renaming existing maps. The way that you add or delete devices to a map is also the same for all maps.

To view or search Maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read Access or Maps Read/Write Access capability.

Accessing Maps

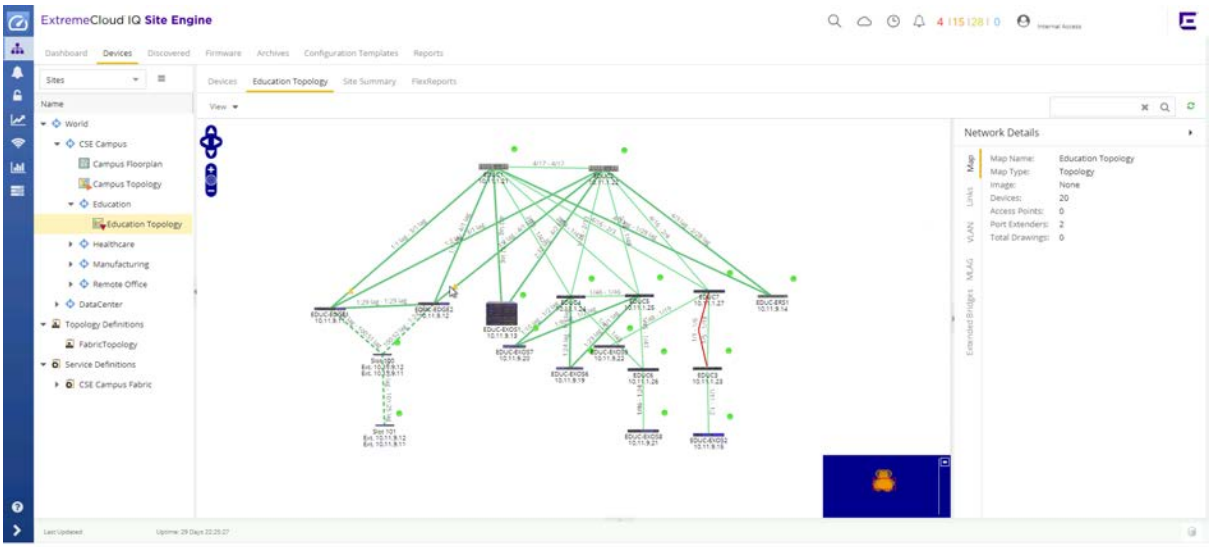
Access the **Network** > **Devices** tab and select **Sites** from the left-panel drop-down list.

Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.

When opening the World map for the first time, the map is blank. As you create maps, add links to them from the World map as shown in the diagram below, allowing you to find individual maps quickly from one map.

Navigating Maps

Selecting a map in the left-panel provides you with tabs at the top of the right-panel that allow you to view information about the devices included in the map:



Devices

This tab displays a table of the devices contained within the map. This table is identical to the Devices list available by selecting All Devices in the left-panel drop-down list, but is filtered to only show the devices added to the map. For additional information about operations available on this tab, see the **Devices** tab.

Map

This tab, which will show the name of the map you selected from the left-panel, contains the map of the devices. Using Maps, five types of maps are available, Physical, Fabric VCS, Fabric Connect, Floorplan, and Geographic. For additional information about operations available on this tab, see the **Map** tab.

For information on creating maps, see How to Create and Edit Maps.

Site Summary

The **Site Summary** tab contains a table showing the site paths and configuration information for each site.

FlexReports

This tab contains reports available for the devices included in the site, filtered to display the information selected in the tree (e.g. a site, map, device, controller). Use the drop-down menus to change the report displayed. Each report allows you to configure how the information displays. You can configure ExtremeCloud IQ Site Engine to automatically create FlexReports on a scheduled basis by selecting the **Schedule** icon, which opens Scheduler. Additionally, FlexReports can be exported in PDF format.

For information on related topics:

- Devices
- Maps
- Sites
- How to Create and Edit Maps
- Advanced Map Features

Geographic and Floorplan Maps

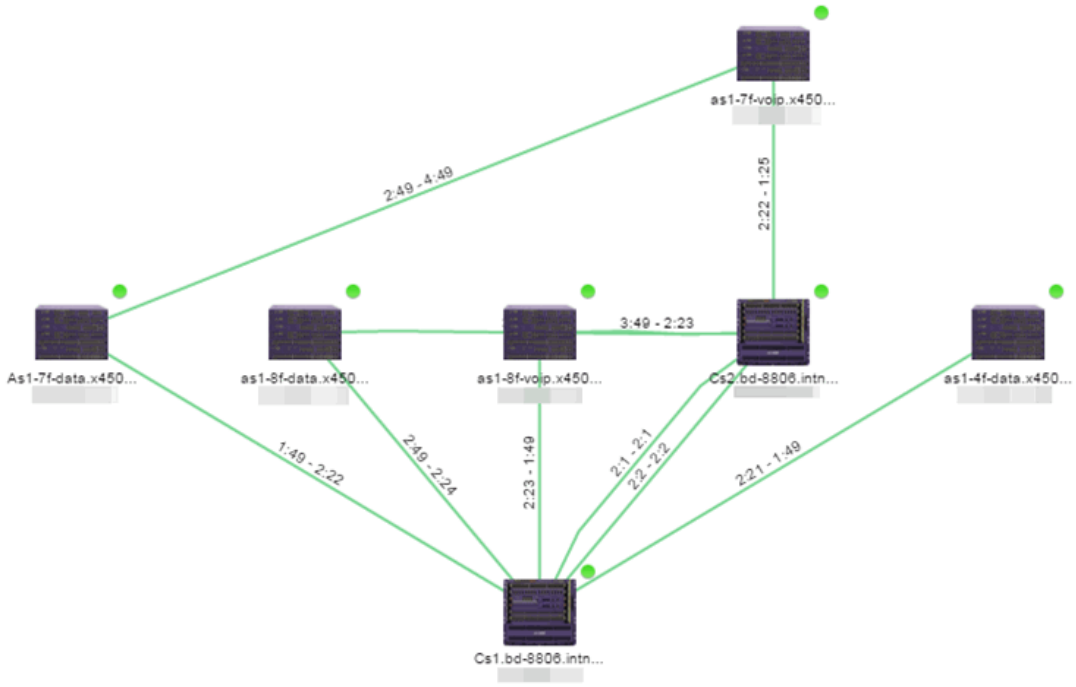
ExtremeCloud IQ Site Engine includes tools that you can use to create geographic and topology maps of devices and floor plans of wireless access points (APs) on your network. Use maps to view devices and network connections, device and alarm status; access device and connection information via a right-click menu off the device; and search for devices, APs, and wired or wireless clients.

You can include port extenders in a map. If you choose not to add port extenders to a map, the ports on the port extender are shown as part of the controlling bridge.

Maps are configured in various places on the **Network** > **Devices** tab.

You can create three types of maps, each presenting a different visual representation of your network:

- Topology *(default)* — A topology map shows how devices are connected in a network, specifically, the state and speed of the network connections between devices as well as the state of the devices in the network. You can also create a topology map with a background image, giving you additional information about the devices and connections that make up the network.



For additional information about devices and links in a Topology map, see the Viewing Alarm and Device Status and Link Information sections.

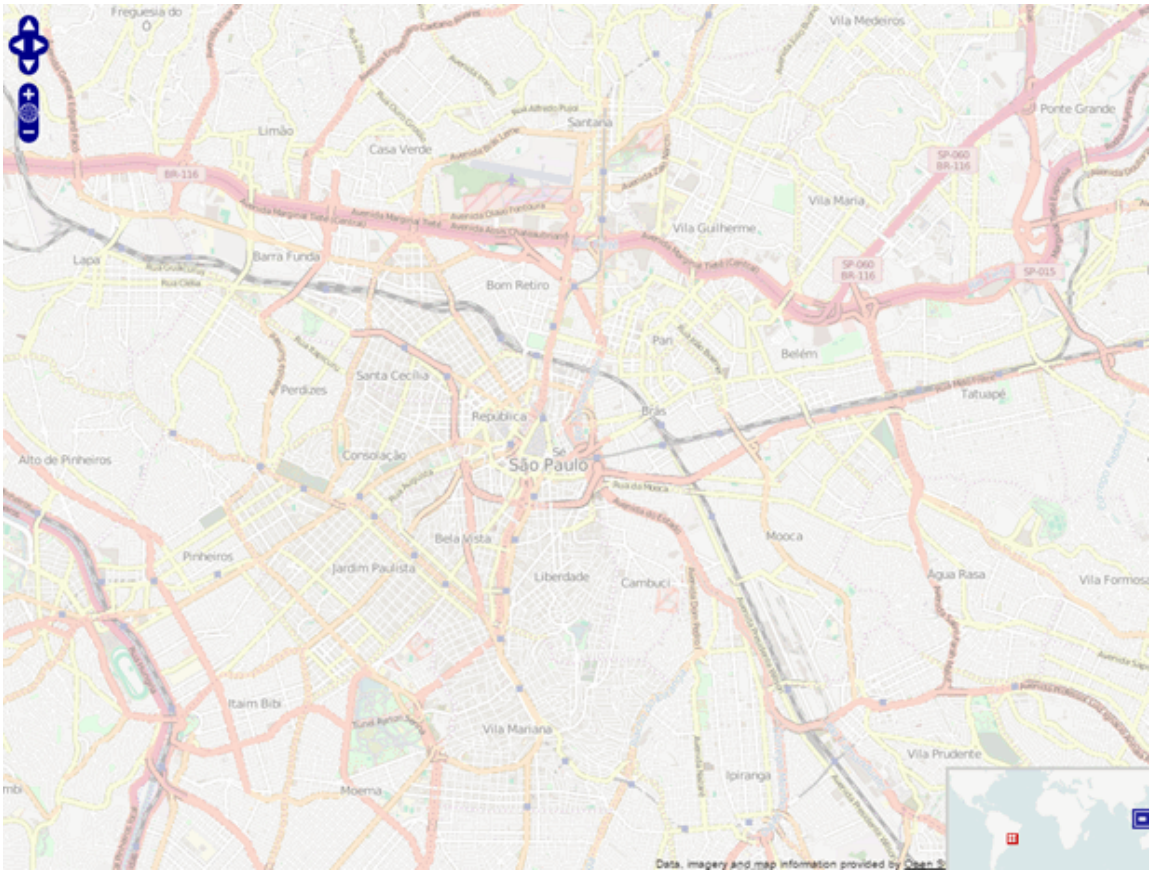
- Floorplan — The floorplan map displays the location of APs in a floorplan you configure. Using information about the size and composition of the building, this map provides an overview of the coverage of wireless APs.



NOTE: For additional information, see Advanced Map Features.

- Geographic — The Geographic map shows a global or regional view where network locations are shown geographically. This map is useful for networks spread across large geographical areas or as a top-level map used to organize multiple networks in different locations.

NOTE: The geographic map type is hosted by OpenStreetMap on an external server. For users with security concerns or if access to third-party servers is prohibited, use the topology map type.



This Help topic provides the following information for **Maps**.

- Navigating Maps
    - World Map Navigation Tree
    - Main Map View
    - Viewing Alarm/Device Status
    - Accessing Device Information
    - Link Information
    - Network Details Section
- Performing a Search
    - Finding a Wireless Client
    - Finding an Access Point
    - Finding a Device
    - Finding a Wired Client
- Using Map Links

For information on creating maps, see How to Create and Edit Maps.

For information on advanced location (triangulation) and wireless coverage maps, see Advanced Map Features.

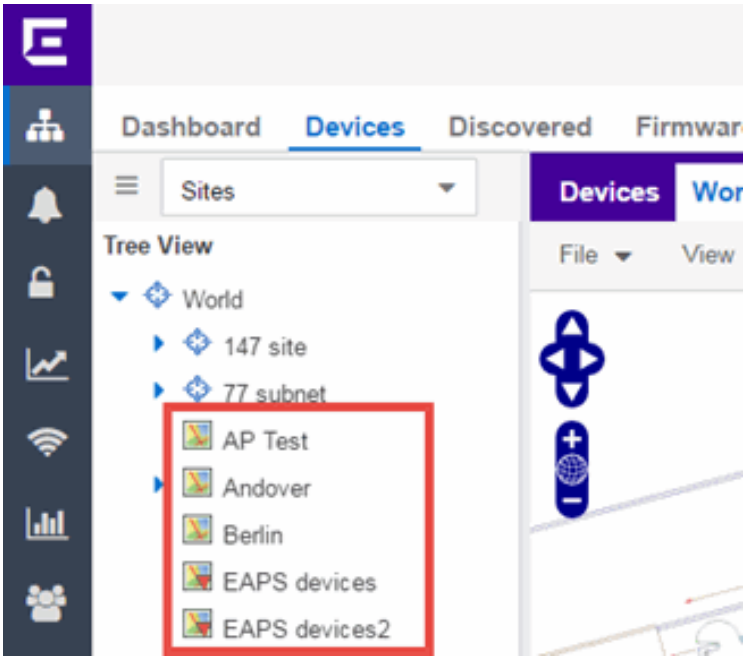
To view or search Maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read Access or Maps Read/Write Access capability.

After you create a map, you can then make it a site. Sites allow you to set a default configuration for devices added to your network.

Navigating the Map Tab

World Map Navigation Tree

As you create your maps, they appear in the **Network** > **Devices** tab navigation tree by selecting **Sites**, nested under the map you configure as the **Parent Map**.



As shown in the image above, you also have the ability to nest maps within other maps. This allows you to organize certain maps as a subset of other maps (for example, creating a building map and then creating a map for each of the floors of the building).

Create Map

Right-click a map in the right-panel navigation tree and select **Maps** > **Create New Map** to create a new map. The first map you create is nested under the World Map. All subsequent maps are nested under the map you right-click when creating the new map.

Edit Map

Right-click a map in the navigation tree and select **Maps** > **Edit Map** to open an existing map in . Edit mode allows you to add new or move existing devices, APs, and map links on a map.

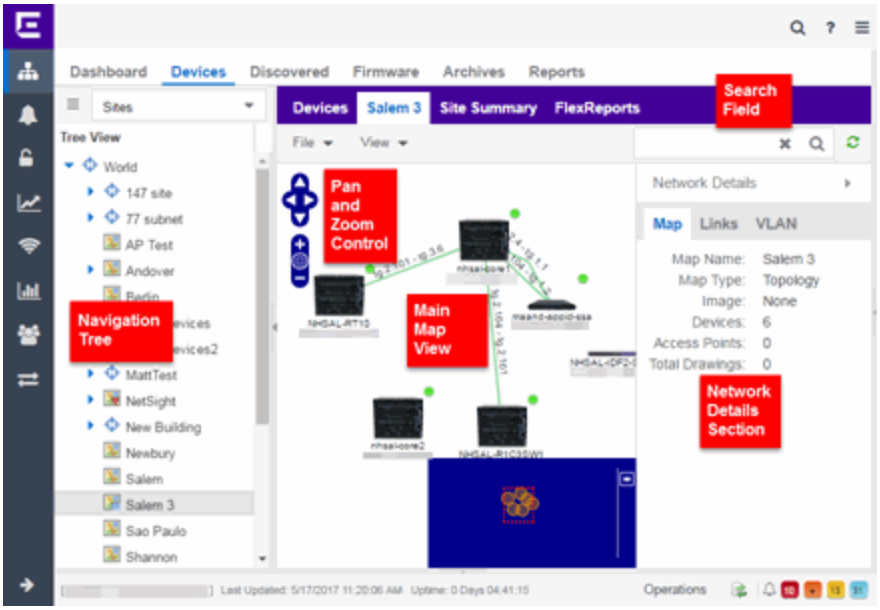
Import Map

You can also import a saved map by right-clicking a map in the navigation tree and selecting **Maps** > **Import Map**. This opens the Import Map window.

Main Map View

The Main Map view displays your map with all of the devices, network connections, links, or APs, depending on the type of map. In the Main Map view, you can reorganize the orientation of elements in your map and view the status and details of the elements within the map. The Main Map view also contains the following controls for working with maps:

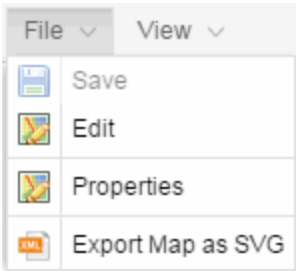
- File, View, and Tool Menus
- Pan and Zoom Control
- Search Field



File, View, and Tool Menus

File Menu

The **File** menu allows you to change the map information, the devices, APs, and links displayed on the map, and export the map from ExtremeCloud IQ Site Engine.



NOTE: To change the image used for a device type in a map, right-click the device and select **Customize Device Type Image**. The **Upload Custom Device Type Image** window appears where you can drag and drop the new image file. The height and width of image files must be less than 1,000 pixels.

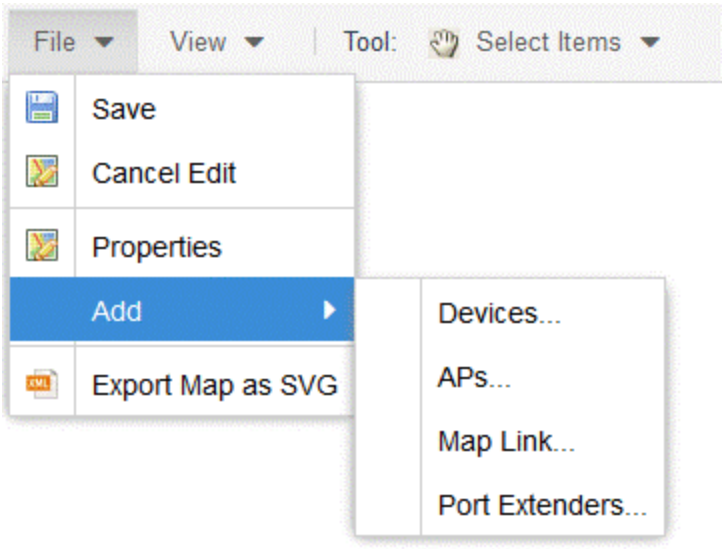
Selecting **Properties** opens the Map Properties window, which allows you to view and edit information about the map, including the map type, name, and background image. The **Export Map as SVG** and **Export Map as ZIP** options are available in the **File** menu, which allow you to export the map in SVG or ZIP format, respectively.

When exporting a map in SVG format, the exported SVG file may open in a new tab or window, depending on how your browser is configured. The SVG file displays your exact view when you select **Export Map as SVG**. For example, if your map is zoomed in to only show two devices and the VLANs associated with those devices, your SVG file is identical to the view on your screen; displaying the two devices surrounded by boxes containing the VLAN names. To save the SVG file locally, right-click the map and select **Save as**.

NOTE: For additional information regarding displaying VLANs in a map, see the VLAN tab section.

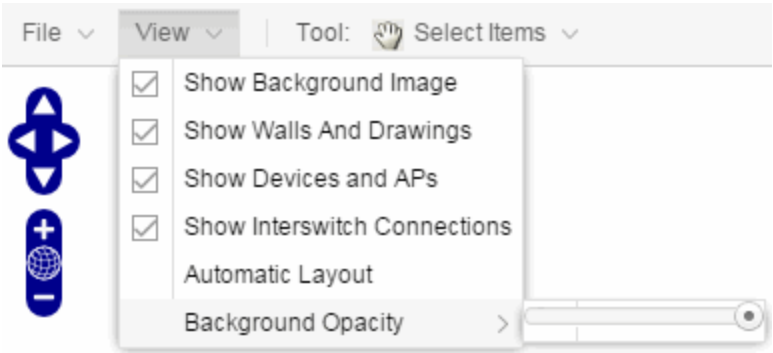
Only floorplan maps can be exported as a ZIP file. Floorplan maps you export as a ZIP file are typically used to import a floorplan into another instance of ExtremeCloud IQ Site Engine.

The **Add** submenu is available, from which you can add Devices, APs, Map Links, and Port Extenders to the map. Edit mode also allows you to manipulate the existing Devices, APs, Map Links, and Port Extenders currently displayed on the map. Select **Cancel Edit** to exit Edit mode. If you made any changes to the map, a dialog box appears from which you can choose to save the changes or exit Edit mode without saving your changes.



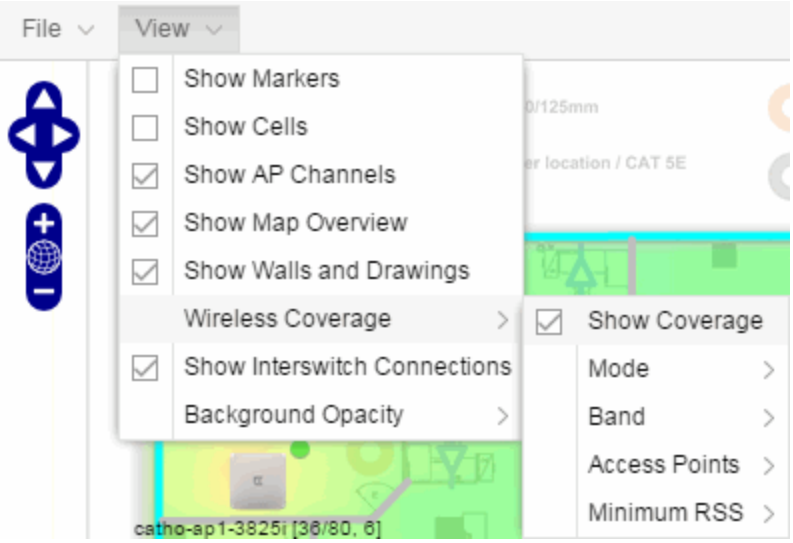
View Menu

The **View** menu allows you to show or hide parts of your map. The options in the **View** menu do not change the information in the map, only allow you to show or hide additional information.



These options vary depending on the map Type and devices on the map. For example, floorplan maps display additional options, including the image you selected as the background of your map, the grid cells that establish the scale of the floorplan, the AP channels for floorplans, the map overview, the walls and drawings of the building, the wireless coverage within a floorplan, the interswitch connections, and the opacity of the background image.

NOTE: Show Fabric Connect is available when at least one Fabric Connect link can be displayed on the map.



NOTE: For additional information, see Advanced Map Features.

Tool Menu

The **Tool** menu allows you to add lines and shapes to your maps. The following table includes descriptions of the various drawing tools accessed from the Tool menu.

Drawing Tool	Definition
	**Select Items** Select a line or shape to select it for dragging or modification. Use the yellow drag handle to reposition the item; use the blue vertex to modify the shape. Select anywhere on the map and drag to reposition the map image.
	**Draw Polygon** Position your cursor where you want to start drawing the polygon shape. Select and draw the first line of the polygon. Select each corner of the polygon. Double-click to release the polygon line. When you are finished drawing, right-click to release the draw polygon tool.
	**Draw Rectangle** Position the cursor where you want the rectangle. Select and drag to draw the rectangle. When you are finished drawing, right-click to release the draw rectangle tool.
	**Add Text** Select the map to open the Enter Text window. When you are finished entering your text, select **OK**. Position the cursor where you want to place the text and select to add the text to your map. Use the **Style** menu to change the text appearance.

Drawing Tool	Definition
	**Draw Triangle** Position the cursor where you want the triangle. Select and drag to draw the triangle. When you are finished drawing, right-click to release the draw triangle tool.
	**Draw Line** Position your cursor where you want to start drawing the line. Select and draw the line. Select to change line direction. While drawing, press the Delete key to delete the last vertex in the line. Double-click to release the line. When you are finished drawing, right-click to release the draw line tool.
	**Rotate Shape** Select the shape you want to rotate. Use the blue handle to rotate the shape to the desired position. (You can also right-click on an image and select Rotate Shape from the menu.)

Pan and Zoom Control

Pan Control



The **Pan** control allows you to move left/right and up/down in the map. You can also change the position of the map by selecting and dragging the map in any direction.

Zoom Control



The **Zoom** control lets you zoom in and out of the map. You can also zoom in and out of the map by rotating the mouse scroll wheel forward and backward, respectively. Selecting the globe icon in the center of the **Zoom** control resets the zoom and positioning for the map to the last view configured in edit mode.

NOTE: Changing the location and zoom using these controls and then saving the map saves those orientation changes to the map.

Search Field

The **Search** field allows you to search for a wireless client, an AP, or for a device or wired client. Enter a MAC address, IP address, hostname, user name, or AP serial number in the **Search** field and press **Enter** to start a search for a device or wired client.

Selecting the **Refresh** button to the right of the **Search** field refreshes the map, including the position of mobile devices connected to an AP. When you select the **Refresh** button, the position of mobile devices updates according to their most recent location.

Selecting the **Rediscover all devices on the Map** button to the right of the **Search** field rediscovers all devices on the map. Rediscover also refreshes the Network Monitor Cache, Host Name Cache, and Historical Collection targets for all devices on the map. Rediscover can be used to update the fabric-related information from switches.

For additional information, see Performing a Search.

Viewing Alarm/Device Status

Maps display an integrated alarm/device status either to the right of a device or AP image, or incorporated as part of a map marker (if you have **Show Markers** selected from the map View menu). For example, the device below is down and a critical alarm is triggered (shown as a device image and as a marker).



Alarm status automatically updates every 30 seconds. Change this status refresh interval in the ExtremeCloud IQ Site Engine options (Administration > Options > OneView > Map).

- (Red) Critical — There is a critical alarm and the device is down.
- (Orange) Error — There is a problem with limited implications on the device.
- (Yellow) Warning — There is a condition that might lead to a problem on the device.
- (Blue) Info — There is an information-only alarm on the device.
- (Green) Clear — There are no alarms and the device is up.

Hover over a device or AP to view a pop-up that displays the IP address for a device or channels for an AP. Additionally, select the **more** link in the pop-up to access the Device View or additional information about the AP for a device or AP, respectively.

Accessing Device Information

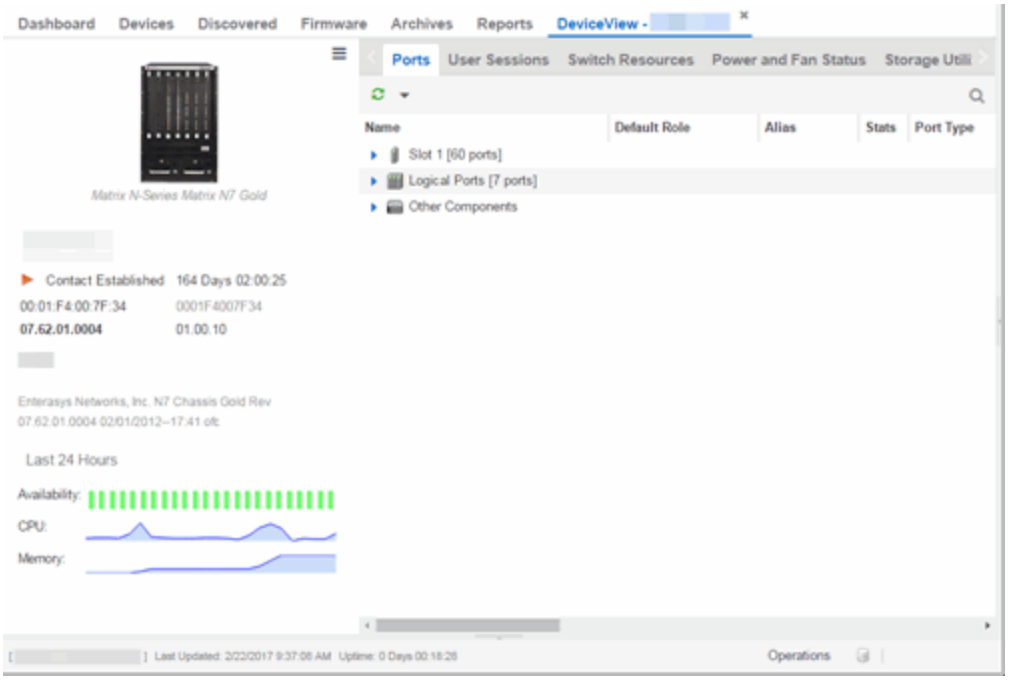
There are two ways to access additional device information from a map.

Device Reports

Launch device information reports from a right-click menu on a device or AP in a map. The menu displays different options based on the device type. You must be in Edit mode to see the **Remove From Map** option.

Device/AP Details

Right-click on a device in a map and select **Device View** or right-click on an AP in a map and select **AP Summary** to open a Device View (like the example shown below) or AP PortView window where you can see a device image and other important device information.



Additionally, the Device View and AP PortView windows contain tabs with additional information about the device or AP.

Link Information

Links are displayed on Topology maps as lines between devices in your network. The line colors indicate the state and status of the link:

Color	Link State	Status
Green	Up	Operational
Red	Down	Not Operational
Yellow	Impaired	Partially Operational
Grey	Unknown	Operation Status Unknown
Purple	Up	Fabric Connect link with ISIS adjacency
Pacific Blue	Up	LLDP link with Fabric Attach
Navy Blue	Up	Fabric Extend link or virtual link with ISIS adjacency

Each connection type is represented by a different line style:

- Basic links appear as thin green lines with no outlining.

- Shared links appear as basic links when the EAPS domain is not highlighted and appear as thick green lines outlined by a black solid line when you highlight the associated EAPS domain.
- Lag links also appear as thick green, but a bit darker than basic links.



- Blocked links appear as a thin green line (similar to a Basic link) outlined by a dashed black line with a red ball icon on the end of the link where the port is blocked when you highlight the associated EAPS domain. Blocked links with both ports blocked display a red ball icon on both ends of the link. Blocked links appear as basic links when the EAPS domain is not highlighted.



- Links connecting a port extender to its controlling bridge appear as dashed lines. If these links are LAG links, they appear as thick dashed lines.



- Links with active ISIS adjacency connecting Fabric Connect devices appear as a thin purple line with no outlining.



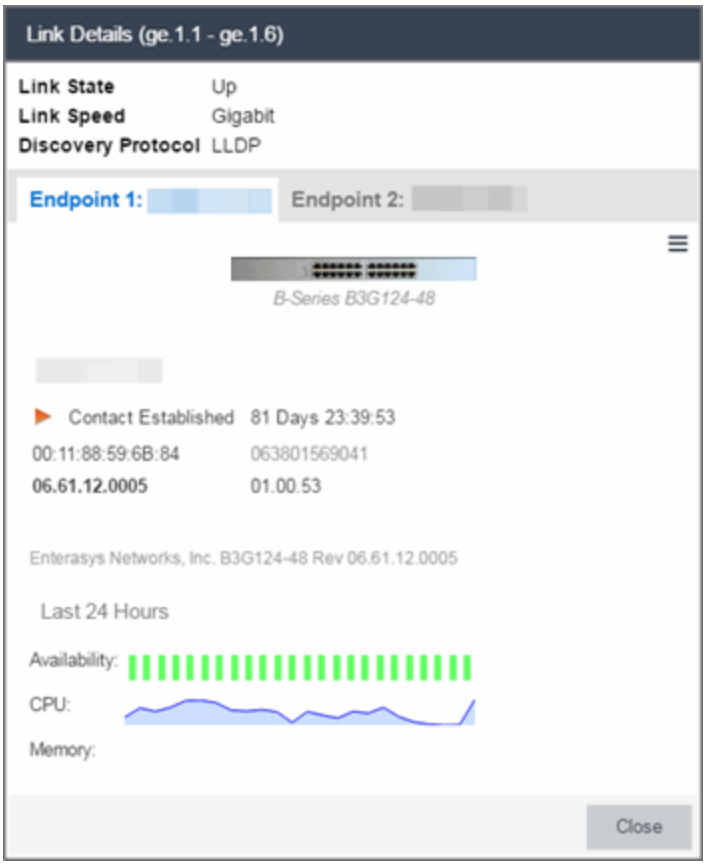
- Links with LLDP signaling active Fabric Attach appear as a thin pacific blue line with no outlining.



- Links with active ISIS adjacency connecting through Fabric Extend appear as a thin navy blue line with no outlining.



Double-clicking a connection opens the Link Details window from which you can view additional details about the network connection and the devices it links.



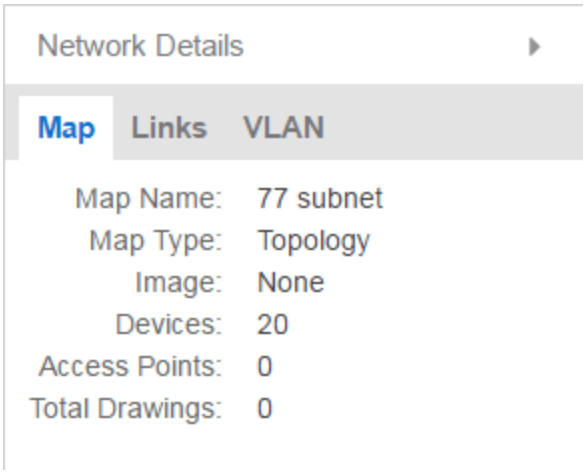
Network Details Section

The Network Details section is available in topology and geographic maps. The Network Details section contains multiple tabs, depending on the devices included in the map:

- Map tab — Displays information about the map
- Links tab — Displays information about the network connections between devices
- VLAN tab — Lists any virtual local area networks within the map
- MLAG tab — Lists devices configured in a multi-switch link aggregation group
- EAPS tab — Lists information about any devices configured with Extreme's Ethernet Automatic Protection Switching feature
- Extended Bridges tab — Lists any devices that support VPEX or any Extended Bridges included in the map.
- Services tab — Displays information about Fabric Connect L2 VSN and L3 VSN services
- ISIS Areas tab — Displays information about Fabric Connect ISIS areas
- ISIS Links tab — Displays information about Fabric Connect ISIS links
- Fabric Attach tab — Displays information about Fabric Attach links

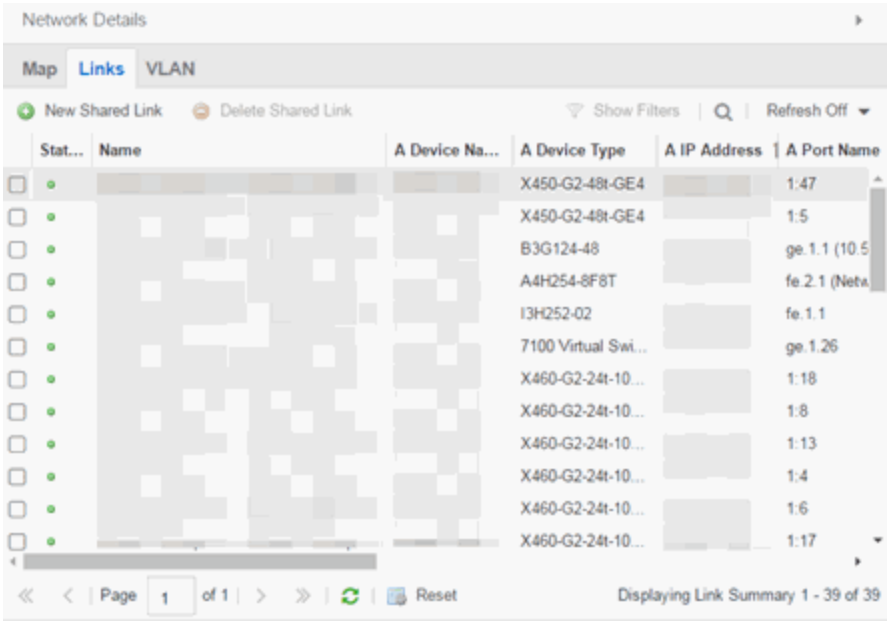
Map tab

The **Map** tab displays basic information about the map, including the name of the map, the map type, and the background image, as well as the number of devices, APs, and drawings on the map.



Links tab

The **Links** tab displays the Link Summary table for maps with one or more network connections, which contains detailed information about the network connections between devices. Selecting one of the links in the table highlights the link in the map.



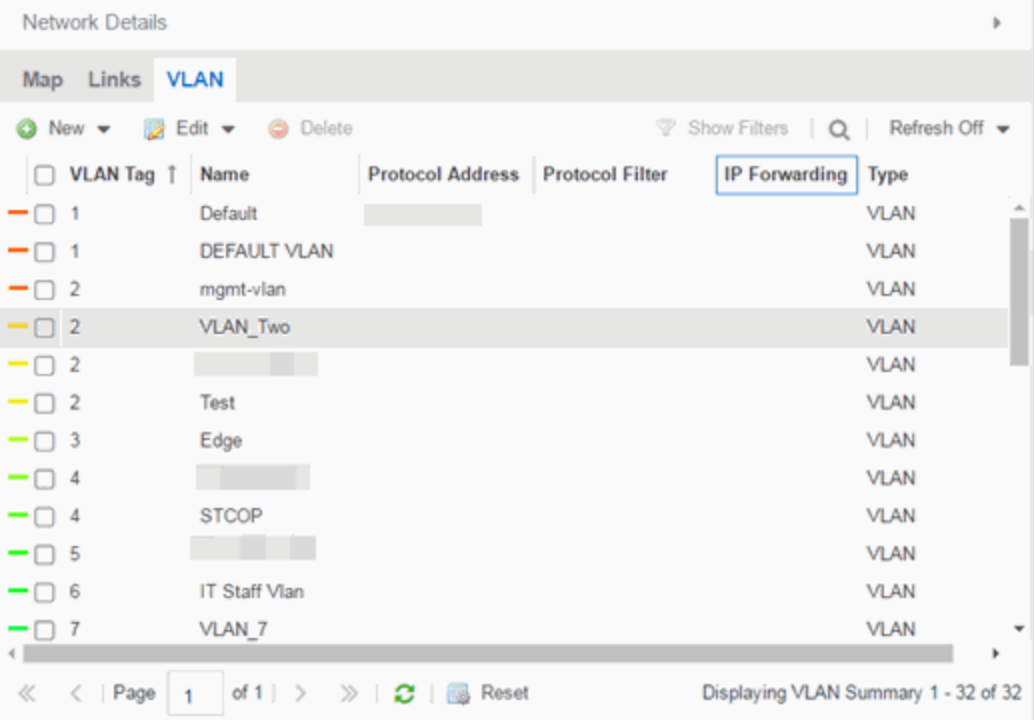
The top of the **Links** tab contains a search field, which allows you to find a particular Link by entering specific criteria. Additionally, you can manually browse links using the scroll bar and page navigation at the bottom of the section.

Double-clicking a link opens the Link Details window.

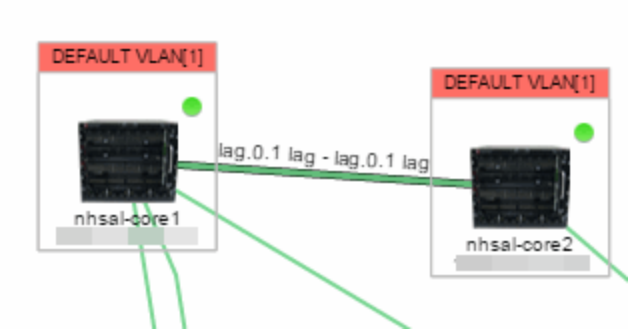
The top of the window displays information about the link, while information about the devices it connects are contained on two tabs, Endpoint 1 and Endpoint 2.

VLAN tab

The **VLAN** tab displays VLANs configured as part of devices included in the map. Columns in the **VLAN** tab provide additional information, including the VLAN tag, the name of the VLAN, any protocol filters applied for devices on which the VLAN is configured, and whether or not IP forwarding is enabled for the VLAN.



Selecting the checkbox associated with a VLAN highlights any devices to which that VLAN is assigned by surrounding the device in a box with a color-coded title bar containing the VLAN name.



Selecting multiple VLANs assigned to the same device adds a new title bar to the box that displays the VLAN name and associated color.

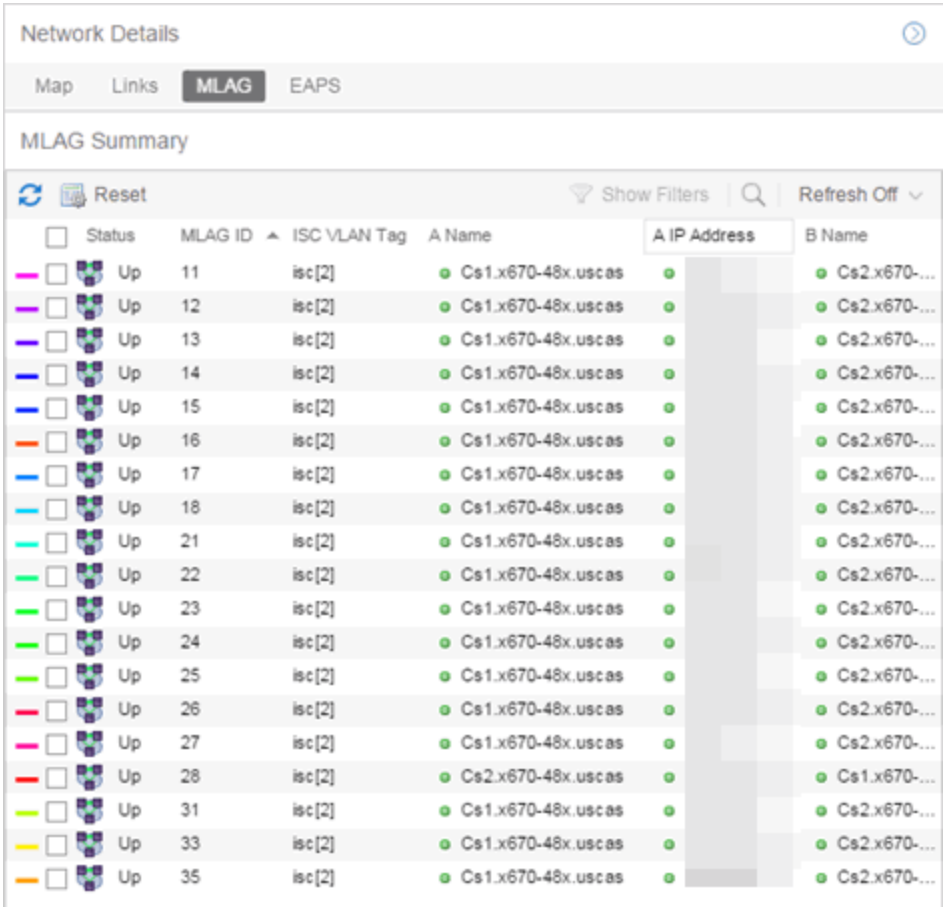


Additionally, from the **VLAN** tab, you can create a new VLAN and create a VLAN protected by an EAPS domain via the New drop-down list or edit the ports, name, and devices associated with an existing VLAN via the **Edit** drop-down list. For more information, see How to Create and Edit VLANs.

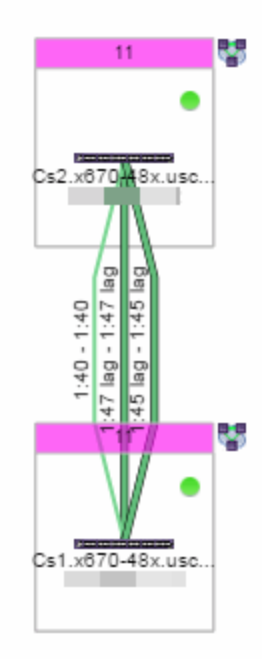
MLAG tab

The **MLAG** Summary tab provides a list of the MLAGs (ports combined as a common logical connection on devices) included in the map. The list provides the MLAG's status, ID, ISC VLAN tag, the names and addresses of the devices configured as part of the MLAG, and the ports on those devices assigned as part of the MLAG. Additionally, the Connected IP column displays the IP of the switch to which the MLAG is connected.

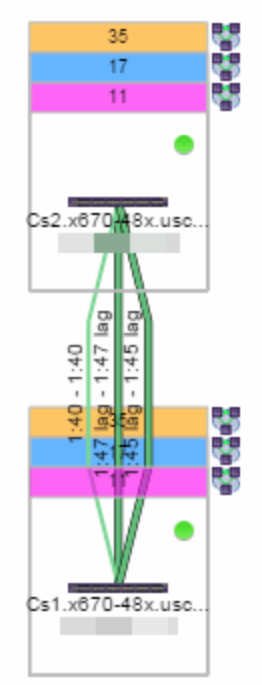
NOTE: One-armed MLAGs, which may be utilized in a VPEX Ring topology, will normally display an MLAG port on only one of the devices.



Selecting the checkbox associated with an MLAG highlights any devices containing ports associated with the MLAG by surrounding the device in a box with a color-coded title bar containing the MLAG ID.

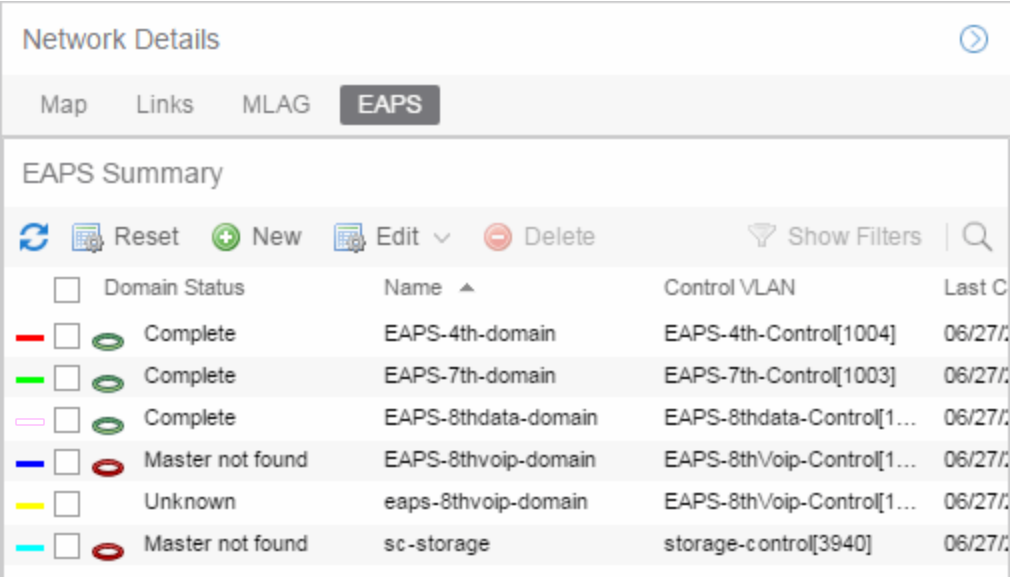


Selecting multiple MLAGs assigned to the same device adds a new title bar to the box containing the VLAN name and associated color.

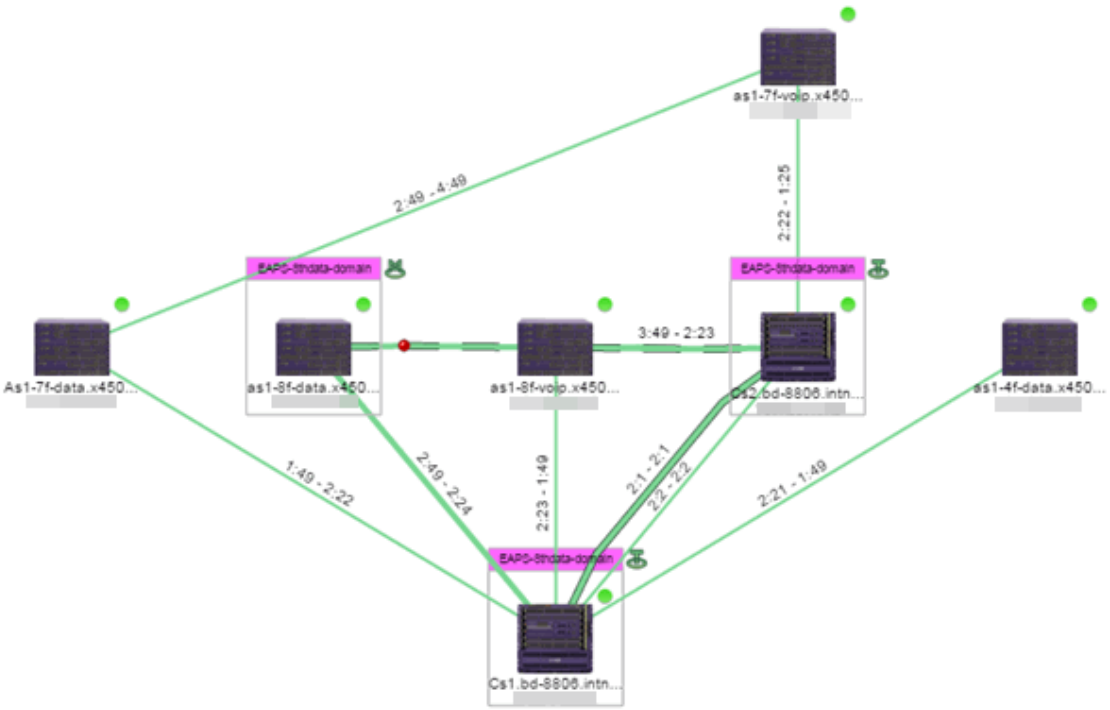


EAPS tab

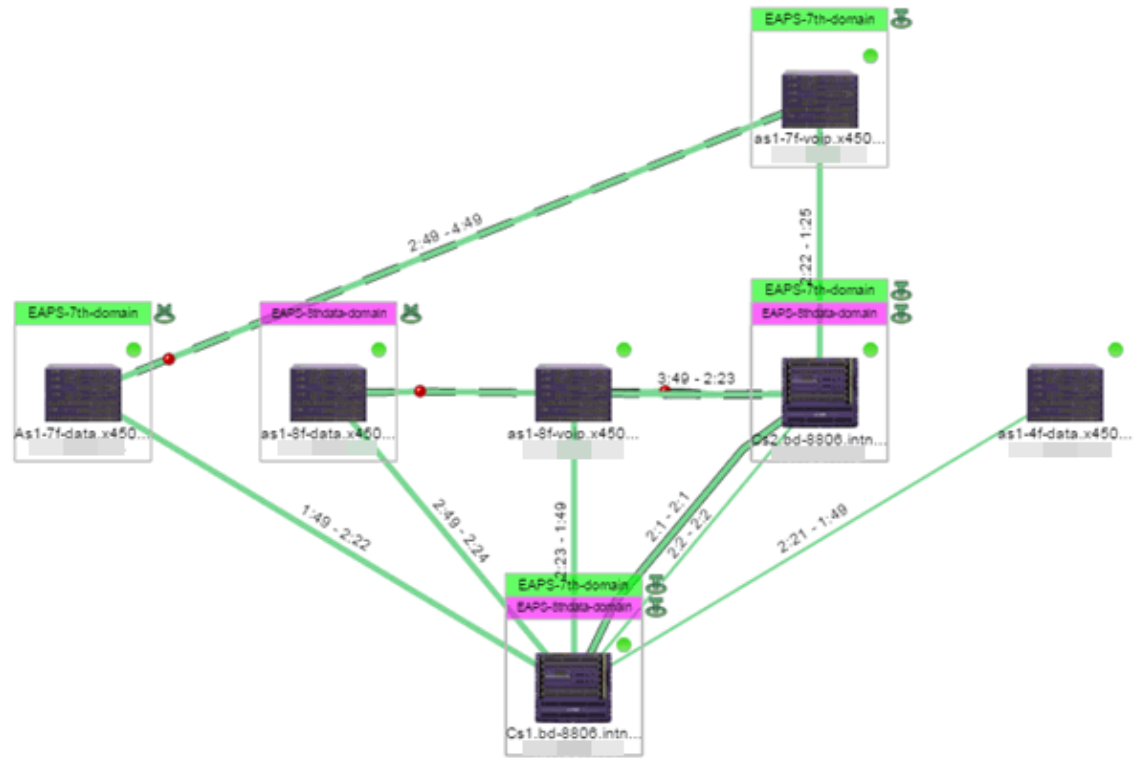
The **EAPS** tab displays a list of the EAPS domains, including their status, name, the control VLAN name, and the IP addresses of the devices utilizing the EAPS domain.



Selecting the checkbox associated with an EAPS domain highlights any devices containing ports associated with the EAPS domain by surrounding the device in a box with a color-coded title bar containing the EAPS name.



Selecting multiple EAPS domains assigned to the same device adds a new title bar to the box containing the EAPS name and associated color.



An icon next to the title bar indicates if the node is a master node, indicated by an "M" icon , or if the node is a transit node, indicated by a "T" icon .

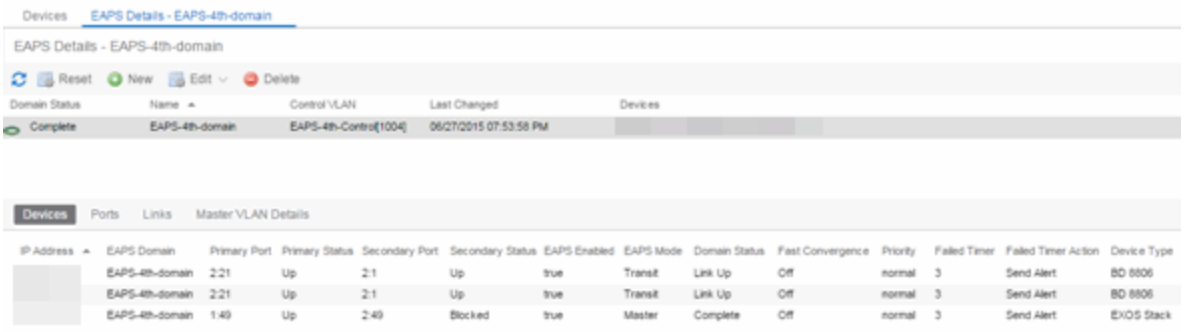
The color of the ring icon indicates the status of the domain:

- Green — Indicates all domains in which this device participates are fully operational
- Yellow — Indicates one or more of the domains is not fully operational, but is in a transitional state or an unknown state (as when the device is SNMP unreachable)
- Red — Indicates one or more of the domains is not operational (the device's master domain is in a failed state or a transit node is in a "links down" state)
- Grey — Indicates the EAPS domain is disabled

When selecting an EAPS domain, link information is also displayed. A single green line means a link that is not shared, while a dashed line between devices means the link is shared. A red dot icon on a shared link indicates the secondary link is blocked.

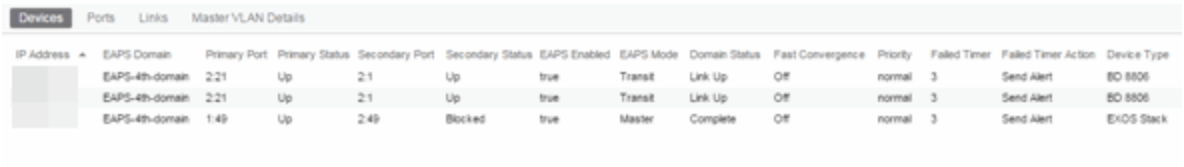


You can view additional details about the EAPS domain by right-clicking an EAPS domain on the **EAPS** tab and selecting **EAPS Details** to open the EAPS Detail view.

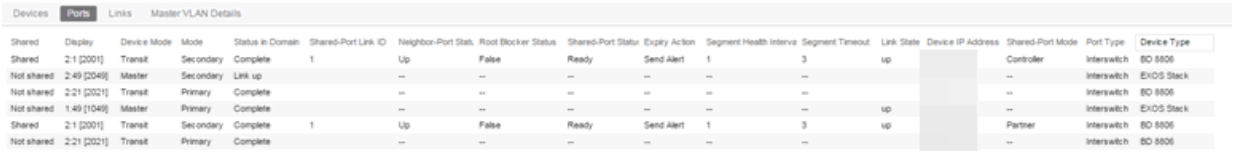


The top of the EAPS Details view displays a summary of the EAPS domain, identical to the information displayed in the **EAPS** tab. At the bottom of the window are three sub-tabs, which display additional information:

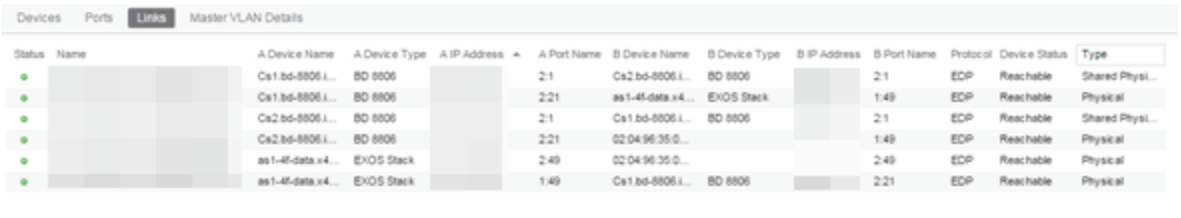
- **Devices** — Displays information about the devices using the EAPS domain.



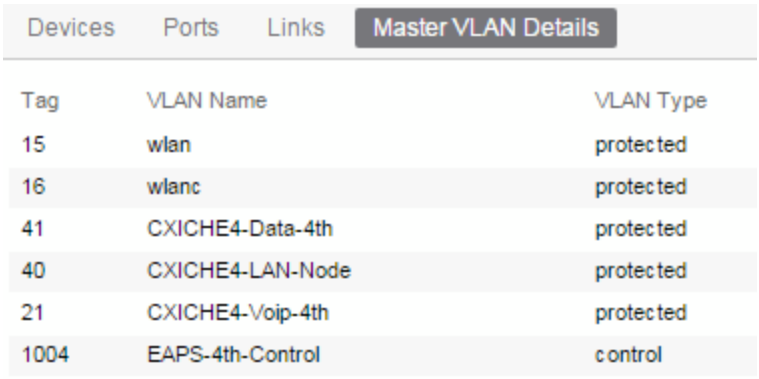
- **Ports** — Displays information about the shared ports associated with the EAPS domain.



- **Links** — Displays links between devices using the EAPS domain.



- **Master VLAN Details** — Displays details about the master VLAN associated with the EAPS domain.



selecting the **New EAPS Domain** button opens the New EAPS Domain wizard, which allows you to create a new EAPS domain. For additional information, see How to Create a New EAPS Domain.

Services tab

The **Services** tab displays Fabric Connect L2 VSN and L3 VSN services configured as part of devices included in the map. Columns in the **Services** tab provide additional information, including the Service ID, Service Name, and Service Type. The top of the **Services** tab contains a search field you can use to find a Service by specific criteria. You can also manually browse services using the page navigation at the bottom of the section.

Selecting the checkbox associated with a Service highlights all devices with that specific Service assigned in a box with a color-coded title bar containing the Service.

ISIS Areas tab

The **ISIS Areas** tab displays Fabric Connect ISIS Areas configured as part of devices included in the map. Each ISIS Area is identified by area number. The top of the **ISIS Areas** tab contains a search field you can use to find an ISIS Area by area number. You can also manually browse Areas using the page navigation at the bottom of the section.

Selecting the checkbox associated with an ISIS Area highlights all devices with that specific Area assigned in a box with a color-coded title bar containing the ISIS Area.

ISIS Links tab

The **ISIS Links** tab displays the Fabric Connect Link Summary table for maps with one or more network connections, which contains detailed information about the network connections between devices. Selecting one of the links in the table highlights the link in the map. The top of the **ISIS Links** tab contains a search field you can use to find a Link by specific criteria. You can also manually browse Links using the page navigation at the bottom of the section.

The **Unicast Path...** option in the **ISIS Links** tab can display the Primary or Secondary Fabric Connect path between two devices running Fabric Connect. You can use the **Unicast Path...** menu to select the

From Device, To Device, Path Type, and then click Show to display the Fabric Connect path. The path must exist and all devices on the path must be on the map used to be shown, If there is no path then the path display returns an error message.

The following details are available about the ISIS link:

- Name
- A Device Name
- A Device Type
- A IP Address
- A Port Name
- B Device Name
- B Device Type
- B IP Address
- B Port Name
- ISIS Area
- A Area = the A node can be Home or Remote
- B Area = the B node can be Home or Remote
- A AutoSense = true if the A port is AutoSense, false if the A port is manually configured
- B AutoSense = true if the B port is AutoSense, false if the B port is manually configured

Fabric Attach tab

The Fabric Attach tab displays the Fabric Attach Link Summary table for maps with one or more network connections, which contains detailed information about the network connections between devices. Selecting one of the links in the table highlights the link in the map. The top of the Fabric Attach tab contains a search field you can use to find a Link by specific criteria. You can also manually browse Links using the page navigation at the bottom of the section.

The following details are available about the Fabric Attach link:

- Name
- A Device Name
- A Device Type
- A IP Address
- A Port Name

- A Port Number
- B Device Name
- B Device Type
- B IP Address
- B Port Name
- B Port Number
- A Device Status
- Type
- LAG ID / Master

Topology and Geographic map refresh

Links and the status information in the Network Details map periodically update. An on-demand update is triggered by a Rediscover action or NBI call, or from receiving SNMP Trap or SNMP Inform information.

You can configure the device to send SNMP Traps or SNMP Informs to ExtremeCloud IQ Site Engine by enabling the **Register Trap Receiver**:

- SNMPv3 Informs is the best practice and most reliable configuration.
- SNMPv1, SNMPv2, and SNMPv3 Traps are supported.
- For Interswitch Connections information to update near real-time, you must enable the linkDown/linkUP SNMP Traps or SNMP Inform.
- For Fabric Connect information to update near real-time, you must enable the ISIS LSDB Traps or ISIS LSDB Informs. You can use the script **Factory script to enable the ISIS LSDB Traps on VOSS devices.**

NOTE: Some ERS devices do not reliably send Informs. Workaround is to use Traps for these devices.

Performing a Search

You can search for a wireless client, an AP, a device, or a wired client on the **Search** tab. From the tab, select **Search Maps** from the Search drop-down list, enter the MAC Address, IP Address, hostname, user name, AP serial number or ExtremeControl custom field information, and press **Enter**.

You can also search for specific wireless clients, access points, devices, and wired clients from different locations in ExtremeCloud IQ Site Engine, outlined below.

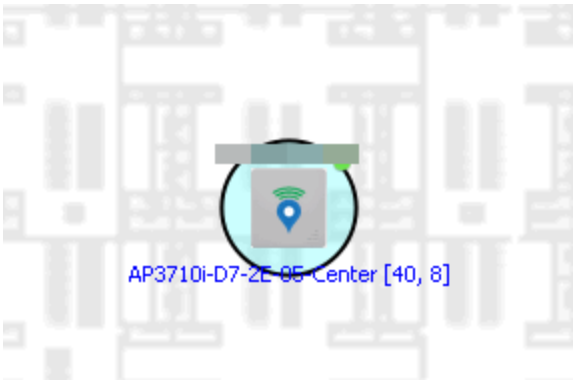
Finding a Wireless Client

From the Search Field on the Network Tab

You can locate a wireless client connected to an AP added to a map by selecting a map or the map navigation tree and use the **Search** field on the **Network** tab. To start a search for a wireless client, enter a MAC address, IP address, hostname, or user name in the map **Search** field and press **Enter** .

The search uses RSS-based (Received Signal Strength) location services to locate the wireless client and display the approximate location of the client on the map. For more information, see Advanced Map Features.

The map opens with the AP centered on the map, with a circle showing the possible area where the client is located. If that information is not available, a square is drawn around the AP last associated with the client.



From the Wireless Tab

In addition to using the **Network** tab Search, you can locate a wireless client from the **Wireless** tab. Select a client in the Clients view, right-click and select **Search Maps**. The map opens centered on the AP, with a circle showing the possible area where the client is located. Mouse over the client icon to see a tooltip with client information.

NOTE: Tooltip information is based on current data from the wireless domain unless the client icon displays a clock in the center. In that case, the tooltip information is based on historic data from the Wireless > Clients page.

Radius Distance Calculation

The following distance calculation defines the radius of the circle displayed around the wireless client located on the map.

Path loss per meter in free space =
L1 = 20 * log (10) (f) – 28

where:

- [f] is the frequency in MHz
  (Uses Source SNMP MIB dot11ExtSmtCurrentChannel
  or if that value is 0, uses MIB dot11ExtSmtCurChanSelectedByAP)
- [L1] is the path loss on distance of 1 meter

Radial distance for location =
d(RSS,n) = 10 ^(pTx – RSS – L1)/(10*n)

where:

- [n] is the coefficient for the environment
- [pTx] is the transmit power (dB)
- [RSS] is the Received Signal Strength
- [d] is the distance in meters

Finding an Access Point

From the Wireless Tab

You can locate an AP from the Access Points table in the **Wireless** tab. Select an AP in the table, right-click and select **Search Maps**. If a map contains the AP, the map opens with the AP centered on the map.

From the Reports Page

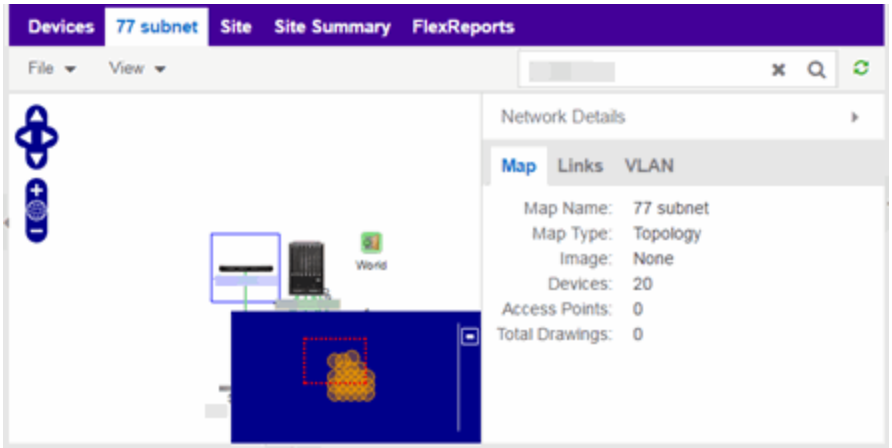
You can locate an AP from the Wireless > APs Summary report on the **Reports** tab. Select an AP in the table, right-click and select **Search Maps**. If a map contains the AP, the map opens with the AP centered on the map.

Finding a Device

From the Network Page Search Field

Select a map or the map navigation tree, enter an IP address or hostname for the device in the **Network** tab **Search** box and press **Enter** to start a search.

The search locates a device added to a map. The map centers on the device. The screen shot below shows the results for a search on a specific IP address.



Finding a Wired Client

From the Network Tab Search Field

Select a map or the map navigation tree, enter a MAC address, IP address, hostname, or user name in the **Network** tab **Search** box and press **Enter** to start a search for a wired client.

The search locates a wired client if the client is Access Control authenticated and is connected to a switch added to a map. The map centers on the wired client.

From the Control Tab

You can also locate an Access Control authenticated wired client from the **Control > Access Control** tab. Select an end-system in the End-Systems view, right-click and select **Search Maps**. If the end-system is connected to a switch added to a map, the map opens with the end-system centered on the map.

Using Map Links

You can use map links to jump from one map to another. Map links display the name of the map and an aggregated alarm/device status for the linked map. Double-click on the link to go to the linked map. You must be in Edit mode to add a link to a map.

For example, the following map link lets you jump to the Second Floor map. The link is green, indicating that there are no devices with alarms on the Second Floor map.



The following map link lets you jump to the First Floor map. The link is red, indicating that there is an alarm for a device on the First Floor map.



Additionally, you can use map links to display Application data based on ExtremeAnalytics network locations. For additional information, see Advanced Map Features.

Navigating the Map Tab

The ExtremeCloud IQ Site Engine Map Tab gives you access to a number of powerful tools that will allow you to create, view, import, edit and search maps of devices and floor plans of wireless access points (APs) on your network. Maps are configured in various places on the **Network** > **Devices** tab. This topic shows you how to navigate the Map Tab and its many tools and features.

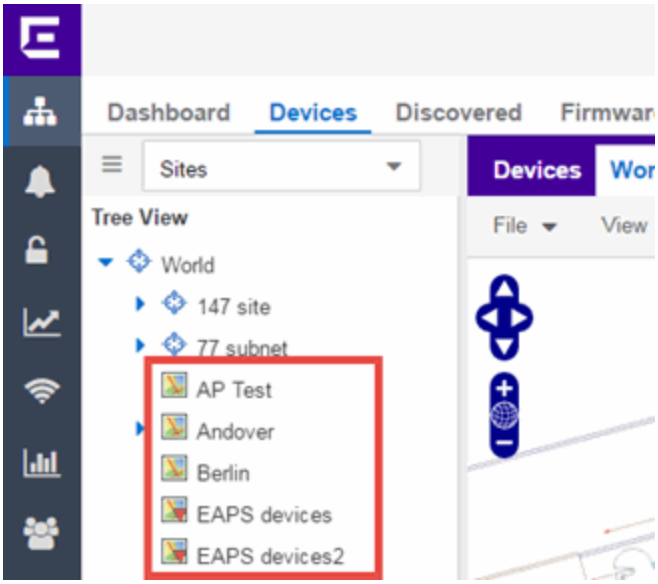
To view or search maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read Access or Maps Read/Write Access capability.

To access maps of your devices:

1. Launch ExtremeCloud IQ Site Engine.
2. Select the **Network** > **Devices** tab.
3. Select **Sites** from the left-panel drop-down list. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.
4. Expand a site from the left-panel tree to display the maps on that site.
5. Select a map to open the Map Name tab in the right panel.

World Map Navigation Tree

Select the World Map tree in the left-panel. As you create your maps, they appear in the navigation tree, nested under the map you configure as the **Parent Map**.



As shown in the image above, you also have the ability to nest maps within other maps. This allows you to organize certain maps as a subset of other maps (for example, creating a building map and then creating a map for each of the floors of the building).

Create Map

Right-click a map in the left-panel navigation tree and select **Maps** > **Create New Map** to create a new map. The first map you create is nested under the World Map. All subsequent maps are nested under the map you right-click when creating the new map.

Edit Map

Right-click a map in the navigation tree and select **Maps** > **Edit Map** to open an existing map in edit mode. Edit mode allows you to add new or move existing devices, APs, and map links on a map.

Import Map

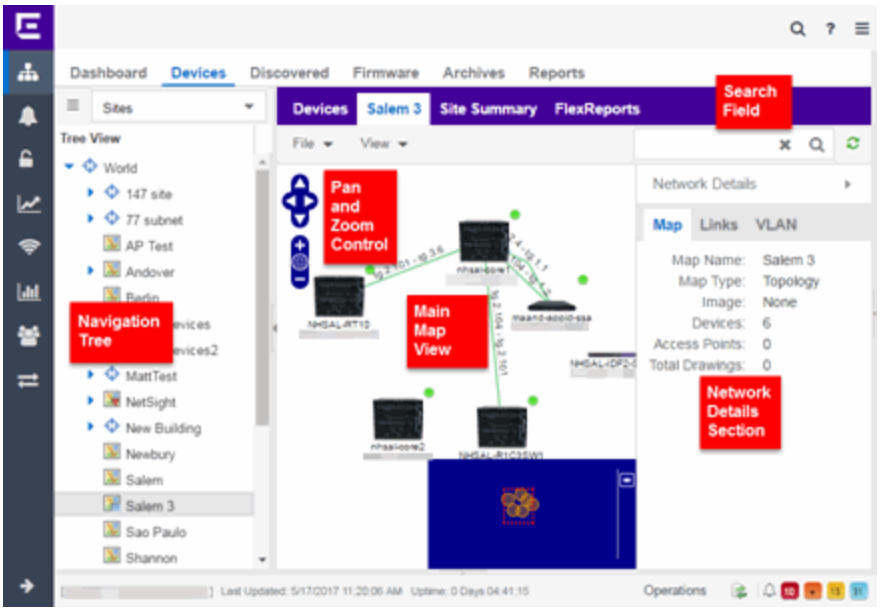
You can also import a saved map by right-clicking a map in the navigation tree and selecting **Maps** > **Import Map**. This opens the Import Map window.

Main Map View

The Main Map view displays your map with all of the devices, network connections, links, or APs, depending on the type of map.

In the Main Map view, you can reorganize the orientation of elements in your map and view the status and details of the elements within the map. The Main Map view also contains the following controls for working with maps:

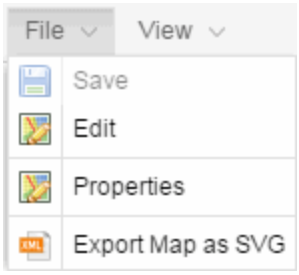
- File, View, and Tool Menus
- Pan and Zoom Control
- Search Field



File, View, and Tool Menus

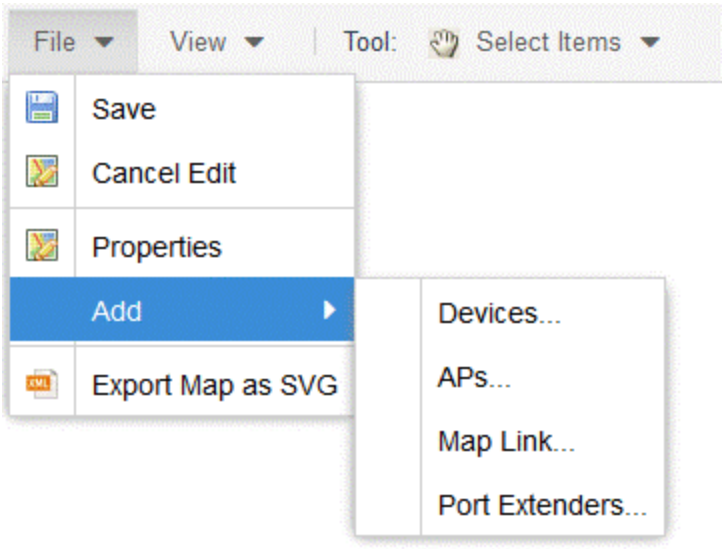
File Menu

The **File** menu allows you to change the map information, the devices, APs, and links displayed on the map, and export the map from ExtremeCloud IQ Site Engine.



NOTE: To change the image used for a device type in a map, right-click the device and select Customize Device Type Image. The Upload Custom Device Type Image window appears where you can drag and drop the new image file. The height and width of image files must be less than 1,000 pixels.

Selecting **Edit** opens the map in Edit mode and the **Add** menu is available, as shown below.



Selecting **Properties** opens the Map Properties window, which allows you to view and edit information about the map, including the map type, name, and background image. With an NMS-ADV license, the **Export Map as SVG** and **Export Map as ZIP** options are available in the **File** menu, which allow you to export the map in SVG or ZIP format, respectively.

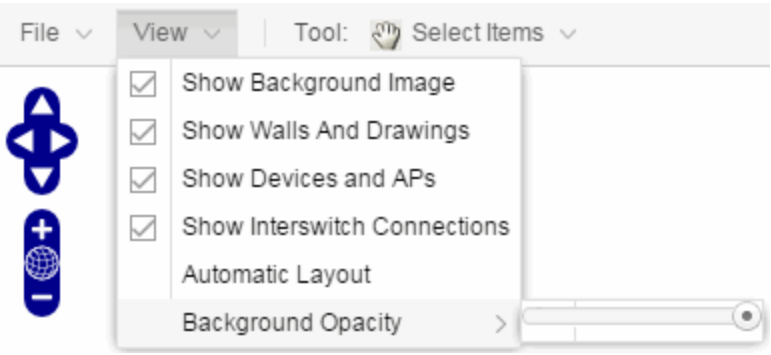
When exporting a map in SVG format, the exported SVG file may open in a new tab or window, depending on how your browser is configured. The SVG file displays your exact view when you select **Export Map as SVG**. For example, if your map is zoomed in to only show two devices and the VLANs associated with those devices, your SVG file is identical to the view on your screen; displaying the two devices surrounded by boxes containing the VLAN names. To save the SVG file locally, right-click the map and select **Save as**.

Only floorplan maps can be exported as a ZIP file. Floorplan maps you export as a ZIP file are typically used to import a floorplan into another instance of ExtremeCloud IQ Site Engine.

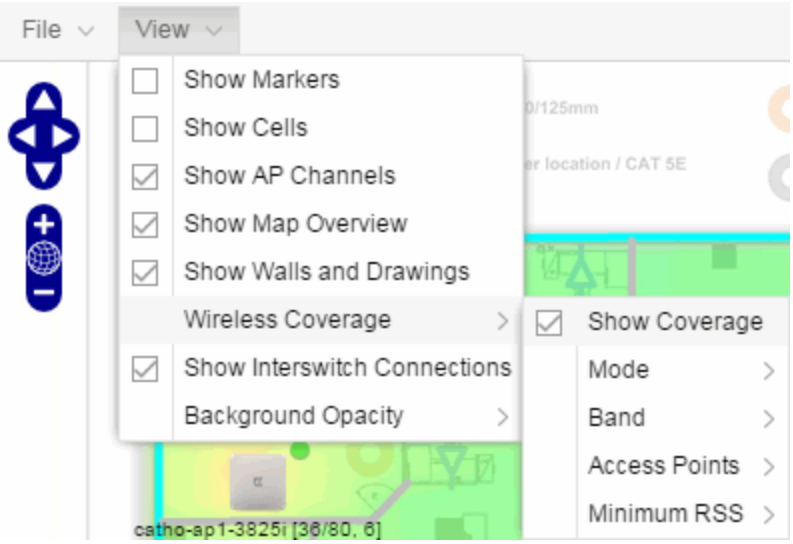
Additionally, by selecting **Edit** in the **File** menu, the map changes to Edit mode and the **Add** submenu is available, from which you can add devices, APs, and map links to the map. Edit mode also allows you to manipulate the existing devices, APs, and map links currently displayed on the map. Select **Cancel Edit** to exit Edit mode. If you made any changes to the map, a dialog box appears from which you can choose to save the changes or exit Edit mode without saving your changes.

View Menu

The **View** menu allows you to show or hide parts of your map. The options in the **View** menu do not change the information in the map, only allow you to show or hide additional information.



These options vary depending on the map Type. For example, floorplan maps display additional options, including the image you selected as the background of your map, the grid cells that establish the scale of the floorplan, the AP channels for floorplans, the map overview, the walls and drawings of the building, the wireless coverage within a floorplan, the interswitch connections, and the opacity of the background image.



Tool Menu

The **Tool** menu allows you to add lines and shapes to your maps. The following table includes descriptions of the various drawing tools accessed from the Tool menu.

Drawing Tool	Definition
	**Select Items** Select a line or shape for dragging or modification. Use the yellow drag handle to reposition the item; use the blue vertex to modify the shape. Select anywhere on the map and drag to reposition the map image.

Drawing Tool	Definition
	**Draw Polygon** Position your cursor where you want to start drawing the polygon shape. Select and draw the first line of the polygon. Select each corner of the polygon. Double-click to release the polygon line. When you are finished drawing, right-click to release the draw polygon tool.
	**Draw Rectangle** Position the cursor where you want the rectangle. Select and drag to draw the rectangle. When you are finished drawing, right-click to release the draw rectangle tool.
	**Add Text** Select the map to open the Enter Text window. When you are finished entering your text, select **OK**. Position the cursor where you want to place the text and select to add the text to your map. Use the **Style** menu to change the text appearance.
	**Draw Triangle** Position the cursor where you want the triangle. Select and drag to draw the triangle. When you are finished drawing, right-click to release the draw triangle tool.
	**Draw Line** Position your cursor where you want to start drawing the line. Select and draw the line. Select to change line direction. While drawing, press the Delete key to delete the last vertex in the line. Double-click to release the line. When you are finished drawing, right-click to release the draw line tool.
	**Rotate Shape** Select the shape you want to rotate. Use the blue handle to rotate the shape to the desired position. (You can also right-click on an image and select Rotate Shape from the menu.)

Pan and Zoom Control

Pan Control



The Pan control allows you to move left/right and up/down in the map. You can also change the position of the map by selecting and dragging the map in any direction.

Zoom Control



The **Zoom** control lets you zoom in and out of the map. You can also zoom in and out of the map by rotating the mouse scroll wheel forward and backward, respectively. Selecting the globe icon in the center of the **Zoom** control resets the zoom and positioning for the map to the last view configured in edit mode.

NOTE: Changing the location and zoom using these controls and then saving the map saves those orientation changes to the map.

Search Field

Use the **Search** field to search for a wireless client, an AP, or for a device or wired client. Enter a MAC address, IP address, hostname, user name, or AP serial number in the **Search** field and press **Enter** to start a search for a device or wired client.

Selecting the **Refresh** button to the right of the **Search** field refreshes the map, including the position of mobile devices connected to an AP. When you select the **Refresh** button, the position of mobile devices updates according to their most recent location.

Viewing Alarm/Device Status

Maps display an integrated alarm/device status either to the right of a device or AP image, or incorporated as part of a map marker (if you have **Show Markers** selected from the map View menu). For example, the device below is down and a critical alarm is triggered (shown as a device image and as a marker).



Alarm status automatically updates every 30 seconds. Change this status refresh interval in the ExtremeCloud IQ Site Engine options (Administration > Options > OneView > Map).

- (Red) Critical — There is a critical alarm and the device is down.
- (Orange) Error — There is a problem with limited implications on the device.
- (Yellow) Warning — There is a condition that might lead to a problem on the device.
- (Blue) Info — There is an information-only alarm on the device.
- (Green) Clear — There are no alarms and the device is up.

Hover over a device or AP to view a pop-up that displays the IP address for a device or channels for an AP. Additionally, select the **more** link in the pop-up to access the Device View or additional information about the AP for a device or AP, respectively.

Accessing Device Information

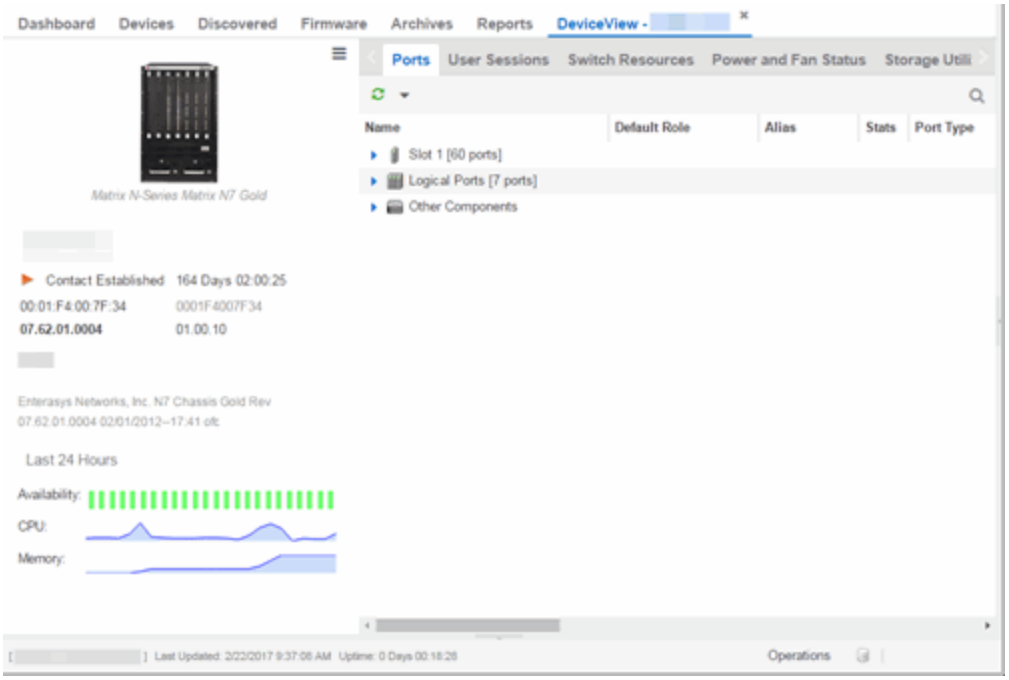
There are two ways to access additional device information from a map.

Device Reports

Launch device information reports from a right-click menu on a device or AP in a map. The menu displays different options based on the device type. You must be in Edit mode to see the **Remove From Map** option.

Device/AP Details

Right-click on a device in a map and select **Device View** or right-click on an AP in a map and select **AP Summary** to open a Device View (like the example shown below) or AP PortView window where you can see a device image and other important device information.



Additionally, the Device View and AP PortView windows contain tabs with additional information about the device or AP.

Link Information

Links are displayed on Topology maps as lines between devices in your network. The line colors indicate the state and status of the link:

Color	Link State	Status
Green	Up	Operational
Red	Down	Not Operational
Yellow	Impaired	Partially Operational
Grey	Unknown	Operation Status Unknown

Each connection type is represented by a different line style:

- Basic links appear as thin green lines with no outlining.

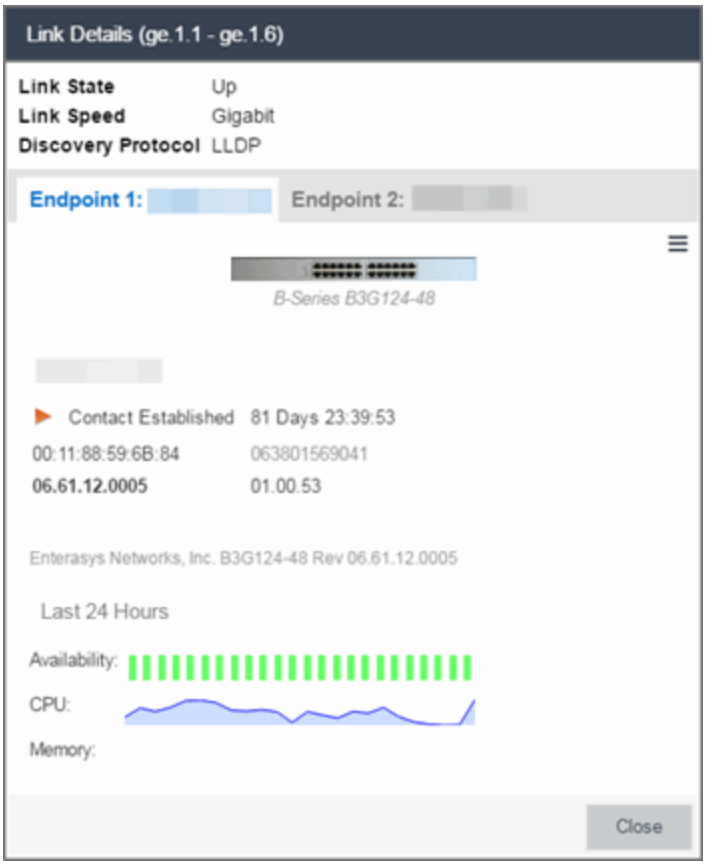
- Shared links appear as basic links when the EAPS domain is not highlighted and appear as thick green lines outlined by a black solid line when you highlight the associated EAPS domain.
- Lag links also appear as thick green lines outlined by a black solid line, but are thicker than shared links and display regardless of what you highlight.



- Blocked links appear as a thin green line (similar to a Basic link) outlined by a dashed black line with a red ball icon on the end of the link where the port is blocked when you highlight the associated EAPS domain. Blocked links with both ports blocked display a red ball icon on both ends of the link. Blocked links appear as basic links when the EAPS domain is not highlighted.



Double-clicking a connection opens the Link Details window from which you can view additional details about the network connection and the devices it links.



Network Details Section

The Network Details section is available in topology and geographic maps. It contains several tabs, depending on the devices included in the map:

- Map tab — Displays information about the map
- EAPS Summary tab — Lists information about any devices configured with Extreme's Ethernet Automatic Protection Switching feature
- Link Summary tab — Displays information about the network connections between devices
- VLAN Summary tab — Lists any virtual local area networks within the map
- MLAG Summary tab — Lists devices configured in a multi-switch link aggregation group
- VPLS Summary tab — Displays information about site connectivity within a private VLAN
- Extended Bridges tab — Displays the extended bridges within the map
- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

Create and Edit Maps

The ExtremeCloud IQ Site Engine Maps feature lets you create maps of the devices and wireless access points (APs) on your network. Begin by selecting a background image to serve as a map, such as a building or floor plan, and then position your managed devices and wireless APs on the map. For example, a typical map might present an office floor plan that shows the location of wireless access points.

For introductory information on maps in ExtremeCloud IQ Site Engine, see ExtremeCloud IQ Site Engine Maps.

This Help topic provides the following information on creating and editing maps.

- Creating a New Map
- Importing a Map
- Adding Devices/APs from ExtremeCloud IQ Site Engine Devices and Wireless
    - Add to a Specific Map
    - Add to New Maps Based on Location
- Creating a Manual Link Between Devices
- Adding Map Links
- Setting the Map Scale

For information on creating custom floor plans, advanced location (triangulation), and wireless coverage maps, see Advanced Map Features.

In order to create or edit Maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

Creating a Map

The instructions in this section describe how to create a new Device map.

1. Launch ExtremeCloud IQ Site Engine and select the **Network** tab.
2. Open the **Devices** tab.
3. In the left-panel select **Sites**.
4. Right-click a site or map and select **Maps/Sites** > **Create Map**.

   NOTE: You cannot create a new map if you are currently editing another map.

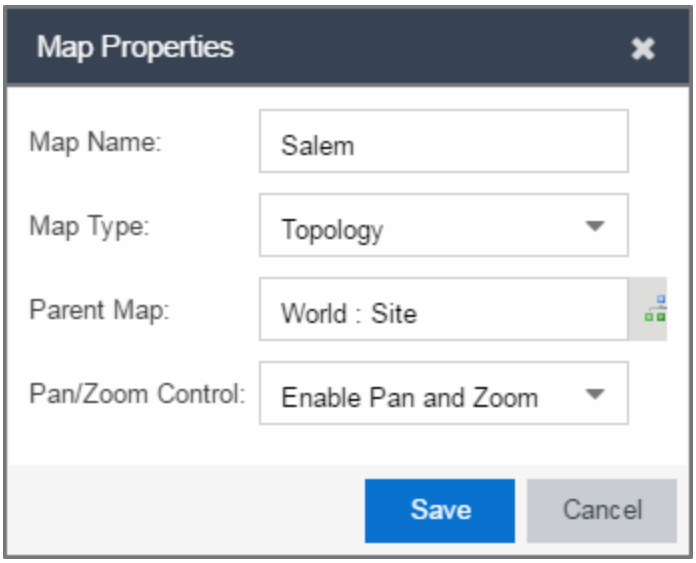
5. Enter a name for the map and select **OK**.

   A new map is added to the tree underneath the map you selected and the Maps section of the

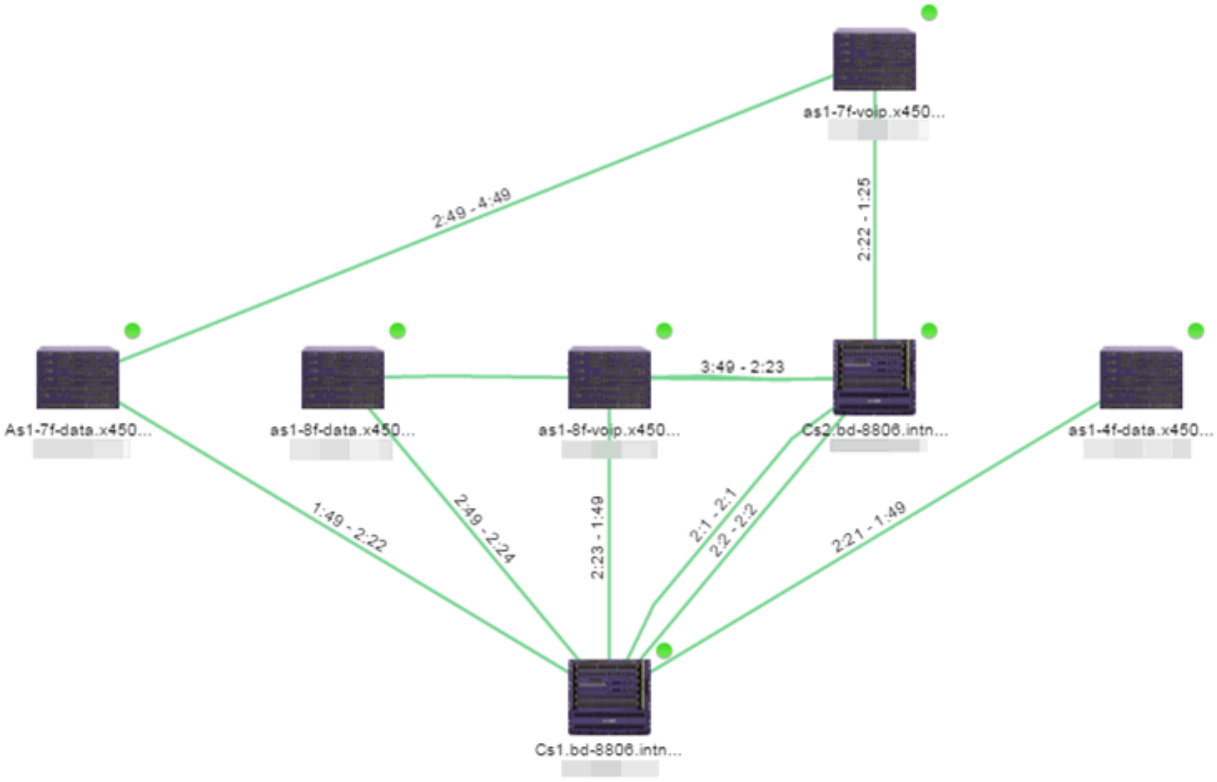
window opens.

The new map is initially blank unless you create it from a device or AP by selecting the device or AP, selecting the **Menu** icon (☰) or right-clicking the device or AP and selecting **Maps** > **Create Map**. To begin adding devices, APs and links to the map, proceed to Step 7. Proceed to the following step to edit the map properties.

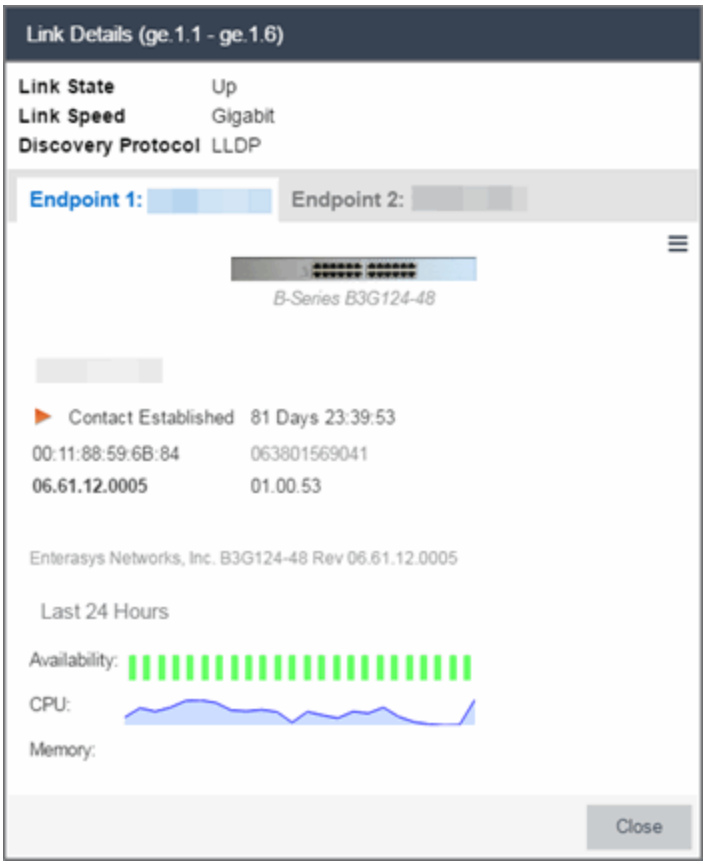
6. Select **File** > **Properties** to open the Map Properties window from which you can edit the map criteria.



   a. In the **Map Name** field, change the name for the map, if necessary.
   b. In the **Map Type** drop-down list, select the type of map you are creating.
      - Topology *(default)* - A topology map shows the state and speed of the network connections between devices as well as the state of the devices in the network.



Double-clicking a connection opens the Link Details window from which you can view additional details about the network connection and the devices it links.



- Topology - Background — Use a custom image to serve as the background of your map. The Map feature supports images in PNG, GIF, and JPG (without transparency) formats. The maximum image size is 3,000 x 2,000 pixels. Images larger than this are automatically scaled down to the maximum size allowed. To use an image larger than 3,000 x 2,000 pixels, open the `NSJBoss.properties` file and edit the pixel value of the `oneView.maxImageSize=3000x2000` line.

CAUTION: Increasing the oneView.maxImageSize value may cause stability issues.

If you select this option, a **Map Image** field displays under the **Map Type** field. In the **Map Image** field, use the drop-down list to select an image or select the button to open a window where you can select a local image and upload it to the ExtremeCloud IQ Site Engine server.

CAUTION: If you upload a map image and an image with the same name already exists, the existing image is replaced.

- Floorplan — Use the Floorplan map to display coverage of wireless APs within a building floorplan.



If you select Floorplan, select the map Environment, which is the type of environment where your network devices are physically located. If your map includes wireless APs, the environment is used for RSS-based (Received Signal Strength) location services to help determine the radius of the circle displayed around an AP following a wireless client search. The radius shows the possible area where the client is located. For example, if you select open space environment, then the radius of the circle is larger than if you select brick walls environment because the AP's radio frequencies are not be obstructed by any walls, and the area where a client might be located is larger. See Finding a Wireless Client for more information.

- Open space — The wireless APs are located in an environment with no walls or cubicles.

- Office cubicles — The wireless APs are located in an environment with cubicle offices present.
- Drywall — The wireless APs are located in an environment where the office wall composition is drywall.
- Brick walls — The wireless APs are located in an environment where there are brick walls present.
- Custom — Use this option to create custom floor plans. For more information, see Advanced Map Features.

For information on creating a custom floor plan design, see Designing a Floor Plan.

A **Map Image** field is displayed under the **Environment** field. In the **Map Image** field, use the drop-down list to select an image or select **Add** () to open a window where you can select a local image and upload it to the ExtremeCloud IQ Site Engine server.

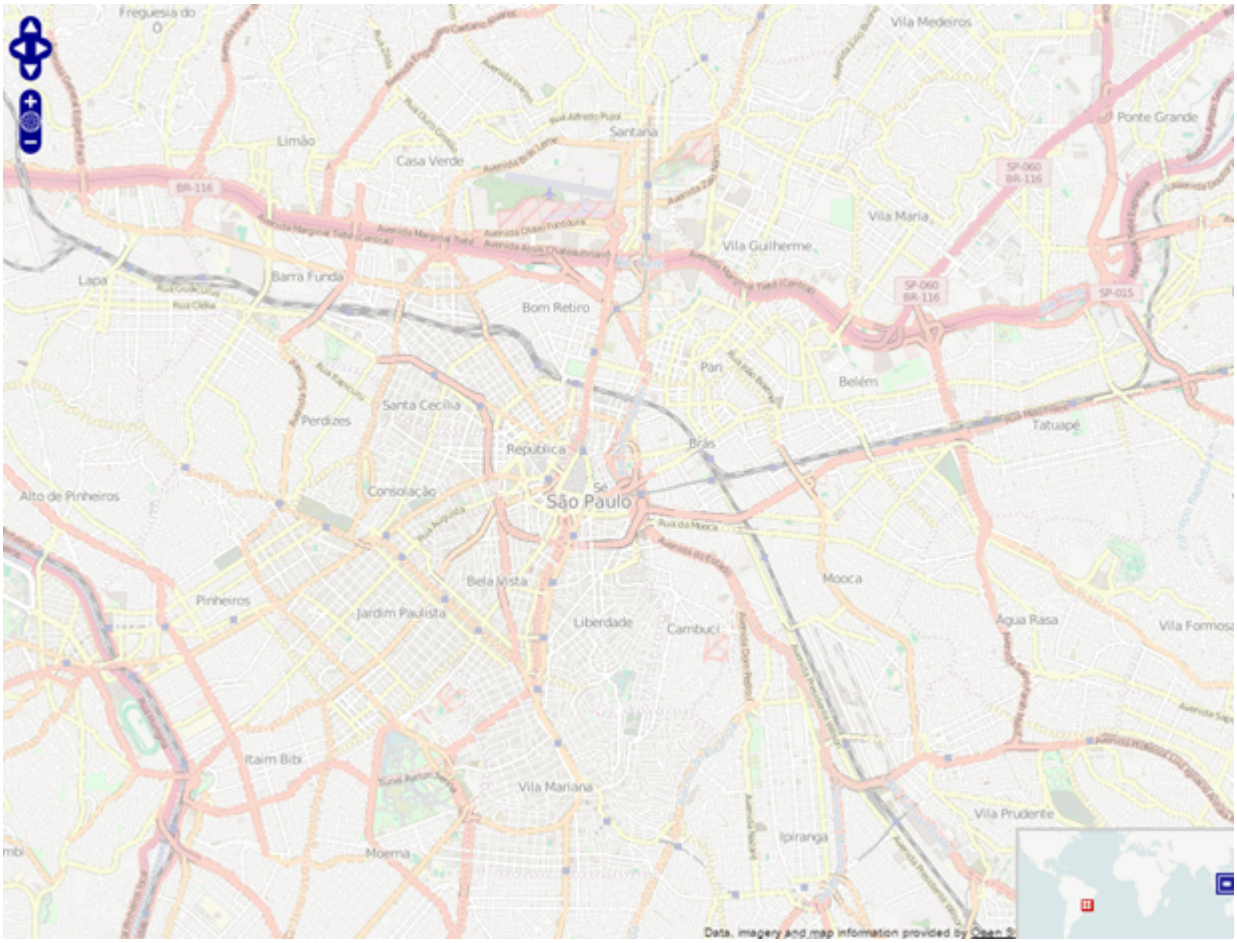
NOTE: If you upload a map image and an image with the same name already exists, the existing image is replaced.

The Map feature supports images in PNG, GIF, and JPG (without transparency) formats.. The maximum image size is 3,000 x 2,000 pixels. Images larger than this are automatically scaled down to the maximum size allowed. To use an image larger than 3,000 x 2,000 pixels, open the `NSJBoss.properties` file and edit the pixel value of the `oneView.maxImageSize=3000x2000` line.

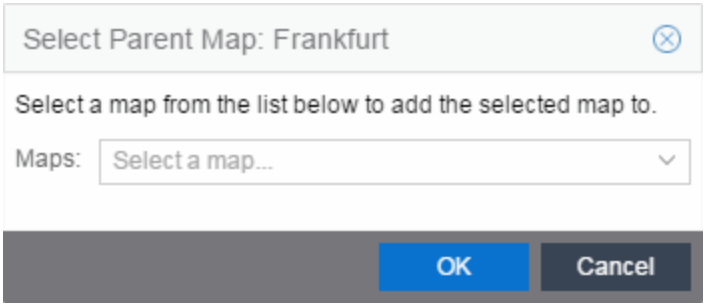
CAUTION: Increasing the oneView.maxImageSize value may cause stability issues and performance issues when generating a heatmap.

- Geographic — Displays a global or regional map where network locations are shown geographically.

NOTE: The geographic map type is hosted by OpenStreetMap on an external server. For users with security concerns or if access to third-party servers is prohibited, use the topology map type.



c. Use the button to select the Parent Map, the map the new map is nested under in the Maps navigation tree. Changing the map's parent saves the current map properties and updates the map tree.



d. Select **Save**.

e. Select the Pan/Zoom Control option. This option determines whether or not the Pan and/or Zoom controls are available when viewing the map. (Pan and Zoom are always available while editing a map.) This allows you to disable the controls for fixed maps, like

world or city maps. For example, if a person viewing a map changes the location and zoom using these controls, those changes are saved and presented to the next person who views the map. This might create confusion over what the map is designed to display.



The Pan control allows you to move left/right and up/down in the map.



The Zoom control lets you zoom in and out of the map.

7. Add your devices, APs, Links, or port extenders to the map you are currently editing by selecting **File** > **Add** > **Devices/APs/Map Link/Port Extenders**. This opens the Add window.



Use the **Search** icon to locate a specific device, AP, or port extender in the Add Device, Add AP, or Add Port Extenders windows, respectively, or select another Map to which to link from the drop-down list in the Add Link To Map window. Select the **Add** button to add the device, AP, link, or port extender to your network map.

8. After your devices and/or APs and port extenders are located on your map, manually manipulate the devices, APs, links, and port extenders on the map, or organize them automatically by selecting **View** > **Automatic Layout**. The Device Layout window opens. Select one of the following layouts to automatically organize the devices, APs and links on your map:
    - Natural — Organizes devices, APs, and links such that the fewest number of network connections overlap.
    - Hierarchical — Organizes devices, APs, and links in a tree pattern.
    - Circular — Organizes devices, APs, and links in a circular pattern.
9. Select **File** > **Save** button to save the map.

NOTE: Map devices and APs do not show their current status until you save the map.

10. The map is now available for viewing by selecting it in the navigation tree. To edit a map, right-click on the map and select **Maps** > **Edit Map** or select the **Edit** button in the Map Properties panel.

Importing a Map

You can also import a saved map by performing the following steps.

1. Launch ExtremeCloud IQ Site Engine and select the **Network** tab.
2. Open the **Devices** tab.
3. Right-click a map in the left-panel Groups/Maps Navigation Tree and select **Maps** > **Import Map**.
   The Import Map window opens.
4. Navigate to the Map file on your local drive or network drive.
5. Configure your import options.
6. Select **Import**.

Adding Devices/APs from ExtremeCloud IQ Site Engine Devices and Wireless

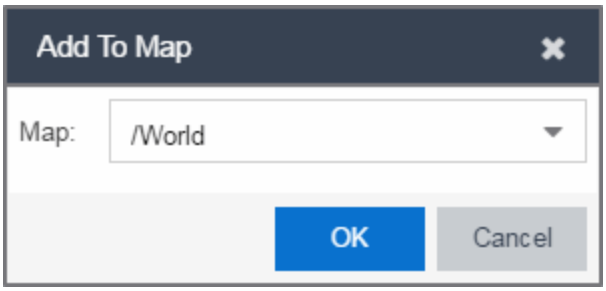
You can quickly add devices and APs to your maps directly from the Devices list or from the navigation tree on the ExtremeCloud IQ Site Engine Network and Wireless tabs. You can add them to a specific map, or create new maps based on device or AP system location.

Add to a Specific Map

Use these steps to add devices or APs to a map you created. For example, use these steps to search for all your S-Series devices on the Network tab and add them to a map.

1. On the **Network** > **Devices** tab, select **All Devices** in the drop-down list in the left-panel.
2. Right-click on one or more devices and select **Maps** > **Add to Map** (as shown below). On the **Wireless** tab, select the Access Points report, right-click on one or more APs, and select **Add to Map**.

3. In the Add to Map window, use the drop-down list to select the desired map. Select **OK** to add the devices or APs to the map.



4. Open the Maps page and select the map to which you added the devices. Right-click on the map and select **Edit Map**. You can now position the devices as desired.
5. Select the **Save** button to save the device to the map.

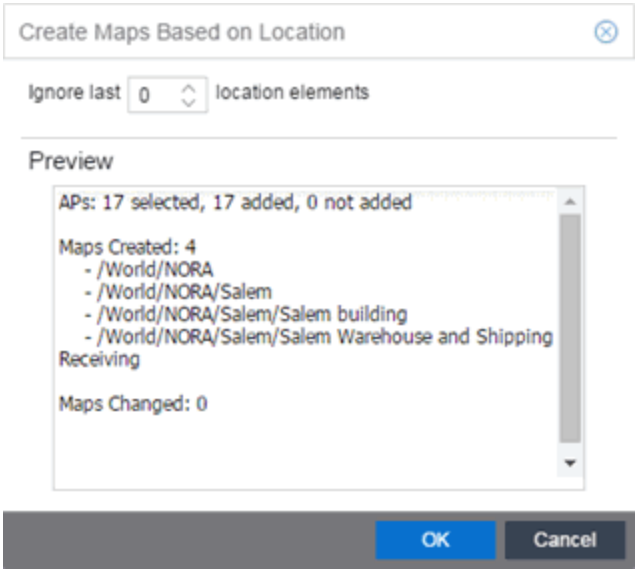
Add to New Maps Based on Location

Use these steps to add devices or APs to new maps based on well-named system locations that reflect the desired map structure. For example, if your devices are assigned system locations according to the following structure: US/Boston/Third Floor/Closet One/Rack One/Shelf One, typically, a map would be created to the Third Floor level, and then you manually position the devices in the correct location on the map.

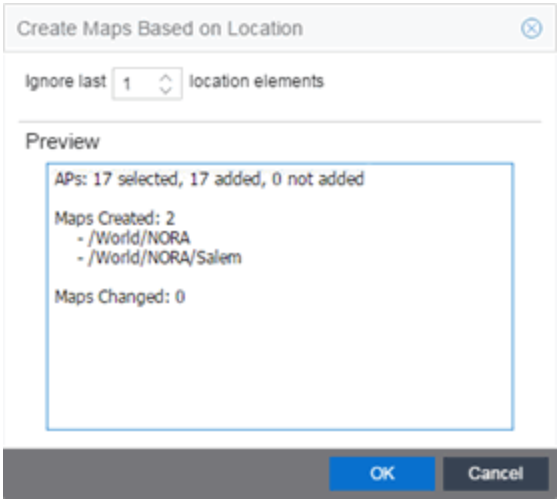
NOTE: The map is not created if the endpoint location matches a site that currently exists in ExtremeCloud IQ Site Engine.

1. On the **Network** > **Devices** tab, right-click on one or more devices and select **Maps** > **Create Maps for Locations**.
   On the **Wireless** tab, select the Access Points report, right-click on one or more APs, and select **Maps** > **Create Maps for Locations**.
2. The Create Maps Based on Location window opens. The window contains a preview panel displaying the number of maps and the map titles that result, based on the system locations of your selected devices or APs.

   For example, as shown in the following screen shot, you are adding 17 APs to a map. This creates four new maps based on the access points' system location structure: NORA, Salem, Salem building, and Salem Warehouse and Shipping.



If you want all the devices on one map, set the Location Option to ignore the last 1 location elements, which is the Salem building location. If you do that, then only two maps are created: NORA and Salem.



3. Select **OK** to create the maps and add the APs.
4. Open the World Site navigation tree in the left-panel and locate the new maps. Right-click on the map and select **Maps** > **Edit Map**. You can now position the APs as desired.
5. Select the **Save** button to save the devices/APs to the map.

Creating a Manual Link Between Devices

You can manually create links between devices on a map.

1. Right-click one of the devices to which you are adding the link.
2. Select **Create Link**.

   The Create a Manual Link window displays.
3. Expand the device in the **Name** column of the From Port section of the window and select the port to which the link connects.
4. Select the other device to which the link connects in the **Select Device** drop-down list.
5. Expand the device in the **Name** column of the To Port section of the window and select the port to which the link connects.
6. Select **OK** to add the link to the map.

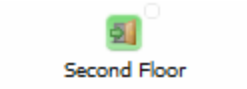
NOTES: The **Link State** for a manual link is derived from the **Status** of the ports to which it connects.

Delete a manual link via the Link Details window by double-clicking the link in the map.

Adding Map Links

You can use map links to jump from one map to another. Map links display the name of the map and an aggregated alarm/device status for the linked map. Double-click on the link to go to the linked map.

For example, the following map link lets you jump to the Second Floor map. The link is green, indicating there are no devices with alarms on the Second Floor map.



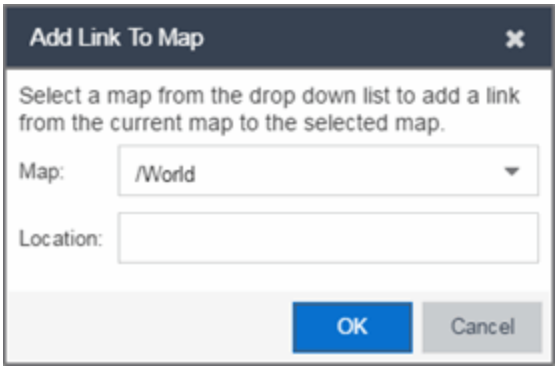
The following map link lets you jump to the First Floor map. The link is red, indicating there is an alarm for a device on the First Floor map.



Use the following steps to add a link to a map.

1. In the Maps navigation tree, right-click on the map from which you want to link and select **Maps** > **Edit Map** or select **File** > **Edit** button in the map properties panel.
2. The map's property panel opens in Edit mode. Select **File** > **Add** > **Map Link**.

3. The **Add Link to Map** window opens.



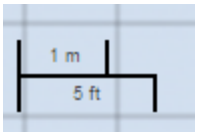
4. From the **Map** drop-down list, select the map to which you want to link.
5. Enter information in **Location** about the location to which the link connects and select **OK**.
6. The map link is added to the map and can be repositioned, if desired.
7. Select the **Save** button to save the map and close the properties panel.

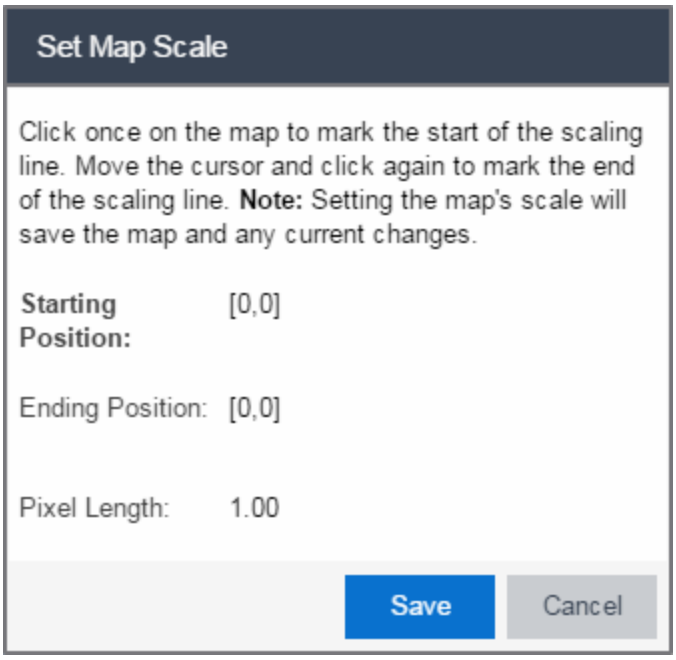
Setting the Map Scale

The map scale appears in the lower left corner of a map and can be changed to accurately reflect your map image.

Use the following steps to set the scale for a map.

1. In the Maps page's navigation tree, right-click on the map and select **Maps** > **Edit Map** or select the **File** > **Edit** button in the map properties panel.
2. Select the map scale in the map's footer panel to open the Set Map Scale window.





3. To set the scale, you must measure something in the map using a scaling line, and then set the measurement for the line. For example, in an office floor plan measure a scaling line on the opening of an office. If you know the office doors are 33 inches wide, enter that as the scaling line measurement.
    a. Select on the map to mark the start of the scaling line. Move the cursor and select again to mark the end of the scaling line.
    b. Enter the line length and units.
4. Select **Save**. The map scale is automatically adjusted and the map is saved.

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

How to Add Devices and APs to Maps

Adding Devices/APs from ExtremeCloud IQ Site Engine Devices and Wireless

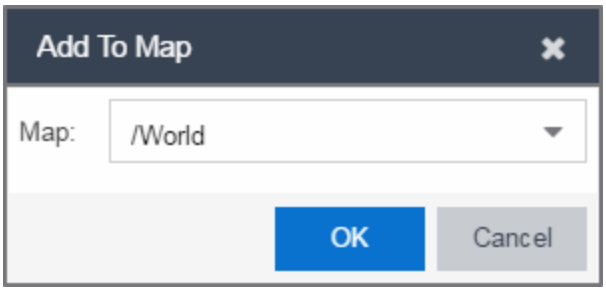
Using the ExtremeCloud IQ Site Engine Maps feature, you can quickly add devices and wireless access points (APs) to your maps directly from the Devices list or from the navigation tree on the ExtremeCloud IQ Site Engine **Network** and **Wireless** tabs. You can add them to a specific map, or create new maps based on device or AP system location.

In order to edit maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

Add to a Specific Map

Use these steps to add devices or APs to a map you created. For example, use these steps to search for all your S-Series devices on the Network tab and add them to a map.

1. On the **Network** > **Devices** tab, select **All Devices** in the drop-down list in the left-panel.
2. Right-click on one or more devices and select **Maps** > **Add to Map** (as shown below). On the **Wireless** tab, select on the Access Points report, right-click on one or more APs, and select **Add to Map**.
3. In the Add to Map window, use the drop-down list to select the desired map. Select **OK** to add the devices or APs to the map.



4. Open the Maps page and select the map to which you added the devices. Right-click on the map and select **Edit Map**. You can now position the devices as desired.
5. Select the **Save** button to save the device to the map.

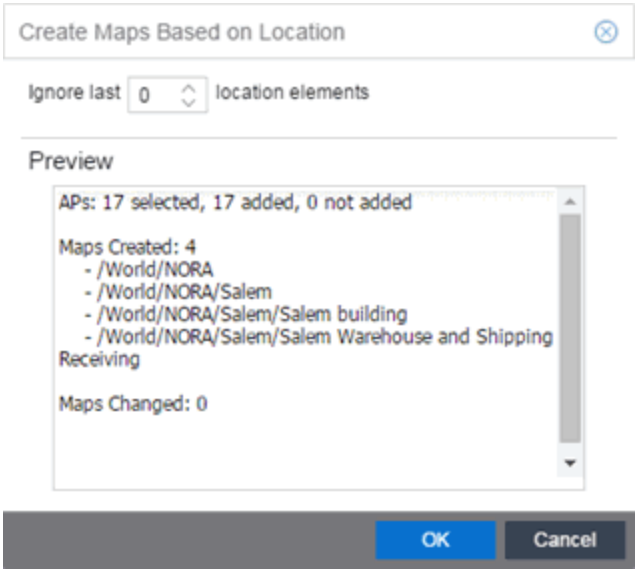
Add to New Maps Based on Location

Use these steps to add devices or APs to new maps based on well-named system locations that reflect the desired map structure. For example, if your devices are assigned system locations according to the following structure: US/Boston/Third Floor/Closet One/Rack One/Shelf One, typically, a map would be created to the Third Floor level, and then you manually position the devices in the correct location on the map.

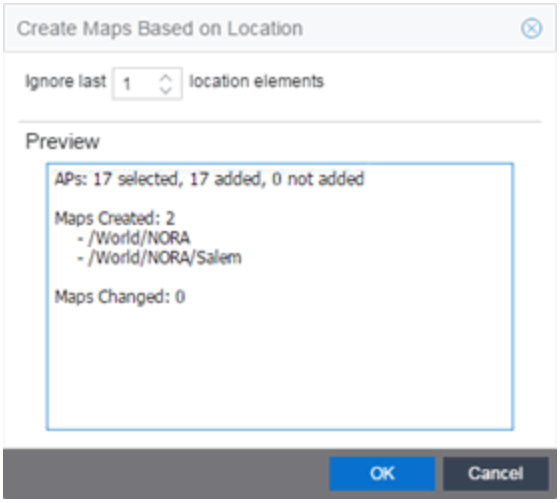
1. On the **Network** > **Devices** tab, right-click on one or more devices and select **Maps** > **Create Maps for Locations**.
   On the **Wireless** tab, select the Access Points report, right-click on one or more APs, and select **Maps** > **Create Maps for Locations**.
2. The Create Maps Based on Location window opens. The window contains a preview panel displaying the number of maps and the map titles that result, based on the system locations of your selected devices or APs.

   For example, as shown in the following screen shot, you are adding 9 APs to a map. This creates

eight new maps based on the access points' system location structure: NORA, Salem, Salem building, and Salem Warehouse and Shipping.



If you want all the devices on one map, set the Location Option to ignore the last 1 location elements, which is the Salem building location. If you do that, then only two maps are created: NORA and Salem.



3. Select **OK** to create the maps and add the APs.
4. Open the World Site navigation tree in the left-panel and locate the new maps.
5. Right-click on the map and select **Maps** > **Edit Map**. You can now position the APs as desired.
6. Select the **Save** button to save the devices/APs to the map.

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

How to Create Maps Using the Map Tab

Use the ExtremeCloud IQ Site Engine Maps feature to create maps of the devices and wireless access points (APs) on your network. Begin by selecting a background image to serve as a map, such as a building or floor plan, and then position your managed devices and wireless APs on the map. For example, a typical map might present an office floor plan that shows the location of wireless access points.

In order to create maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

To access maps of your devices:

1. Launch ExtremeCloud IQ Site Engine.
2. Select the **Network** > **Devices** tab.
3. Select **Sites** from the left-panel drop-down list. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.
4. Expand a site from the left-panel tree to display the maps on that site.
5. Select a map to open the Map Name tab in the right panel.

Creating a Map

To create a new device map:

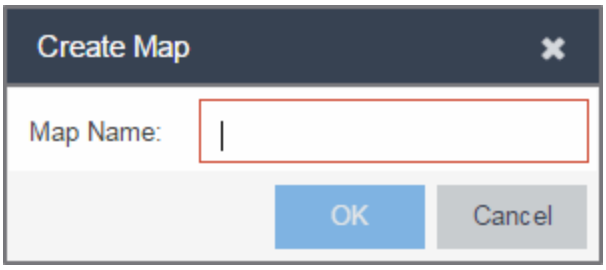
1. In the left-panel Groups/Maps navigation tree, right-click on the World Site (or any other map in the tree) and select **Maps** > **Create Map**.

   NOTES: You cannot create a new map if you are currently editing another map.

   The map is not created if the endpoint location matches a site that currently exists in ExtremeCloud IQ Site Engine.

   The Create Map window opens.

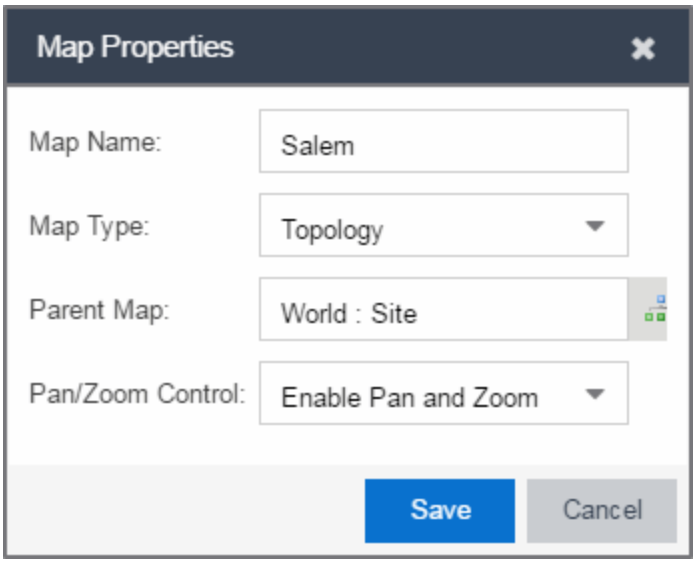
2. Enter a name for the map and select **OK**.



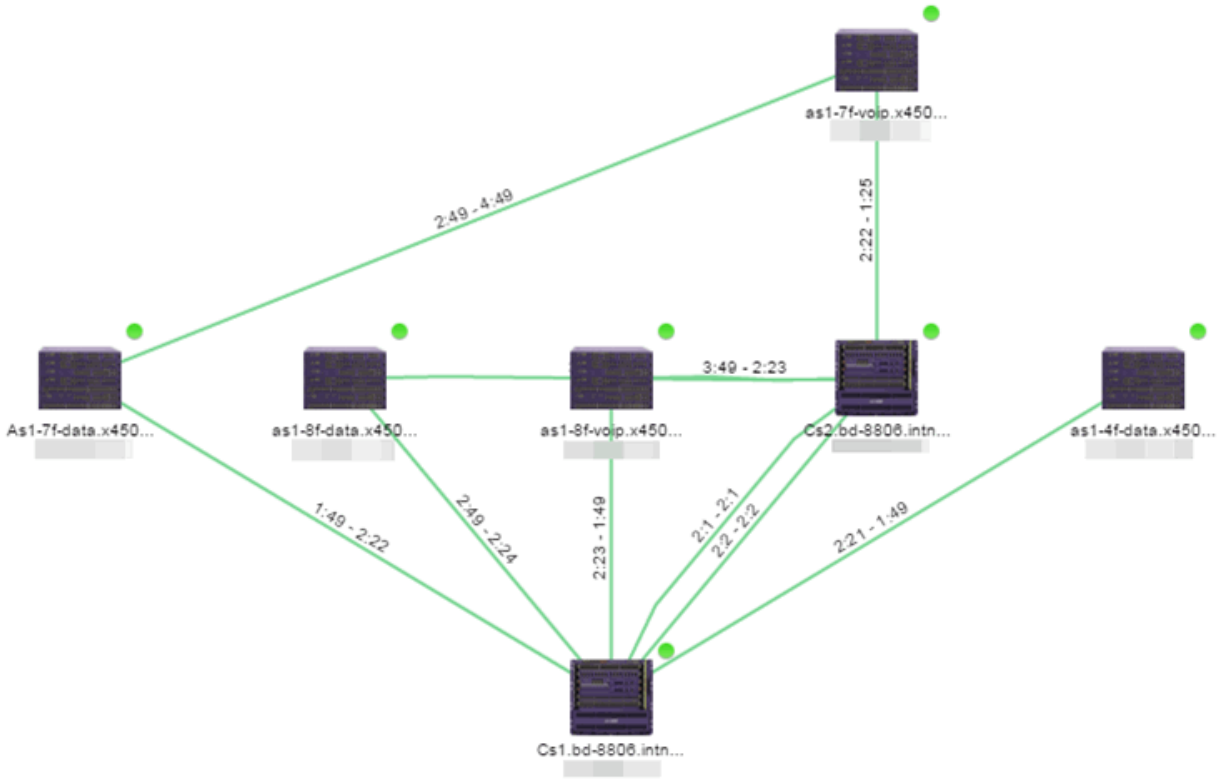
A new map is added to the tree underneath the map you selected and the Maps section of the window opens.

The new map is initially blank unless you create it from a device or AP by selecting the device or AP, selecting the **Menu** icon (☰) or right-clicking the device or AP and selecting **Maps** > **Create Map**. To begin adding devices, APs and links to the map, proceed to Step 4.

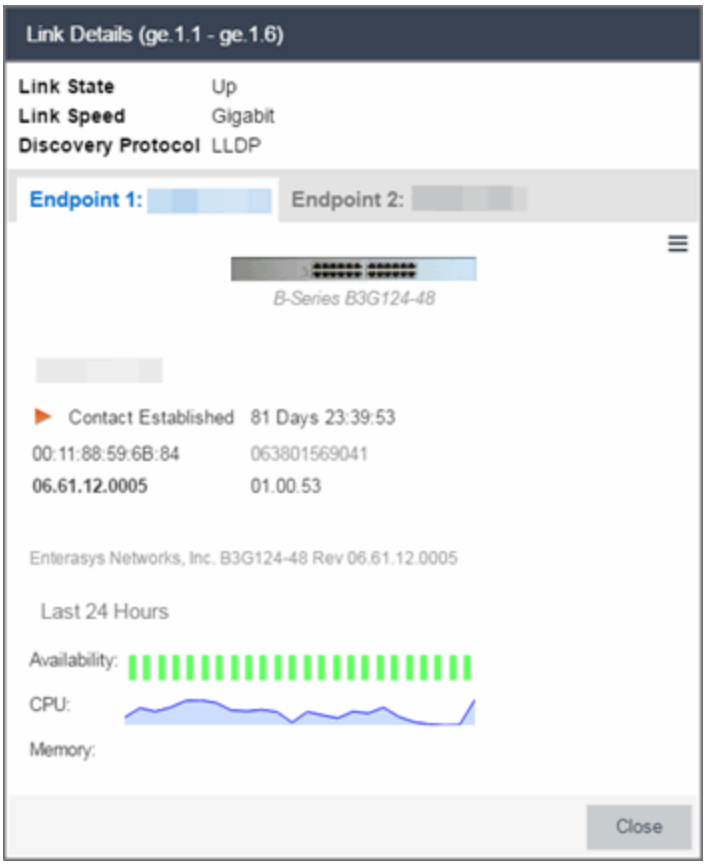
3. Select **File** > **Properties** to open the Map Properties window from which you can edit the map criteria.



   a. In the **Map Name** field, change the name for the map, if necessary.
   b. In the **Map Type** drop-down list, select the type of map you are creating:
      - Topology *(default)* - A topology map shows the state and speed of the network connections between devices as well as the state of the devices in the network.



Double-clicking a connection opens the Link Details window from which you can view additional details about the network connection and the devices it links.



- Topology - Background — Use a custom image to serve as the background of your map. The Map feature supports images in PNG, GIF, and JPG (without transparency) formats. The maximum image size is 3,000 x 2,000 pixels. Images larger than this are automatically scaled down to the maximum size allowed.

  If you select this option, a **Map Image** field displays under the **Map Type** field. In the **Map Image** field, use the drop-down list to select an image or select the button to open a window where you can select a local image and upload it to the ExtremeCloud IQ Site Engine server.

  CAUTION: If you upload a map image and an image with the same name already exists, the existing image is replaced.

- Floorplan — Use the Floorplan map to display coverage of wireless APs within a building floorplan.



If you select Floorplan, select the map Environment, which is the type of environment where your network devices are physically located.

If your map includes wireless APs, the environment is used for RSS-based (Received Signal Strength) location services to help determine the radius of the circle displayed around an AP following a wireless client search. The radius shows the possible area where the client is located. For example, if you select open space environment, then the radius of the circle is larger than if you select brick walls environment because the AP's radio frequencies are not being obstructed by any walls, and the area where a client might be located is larger.

- Open space — The wireless APs are located in an environment with no walls or cubicles.

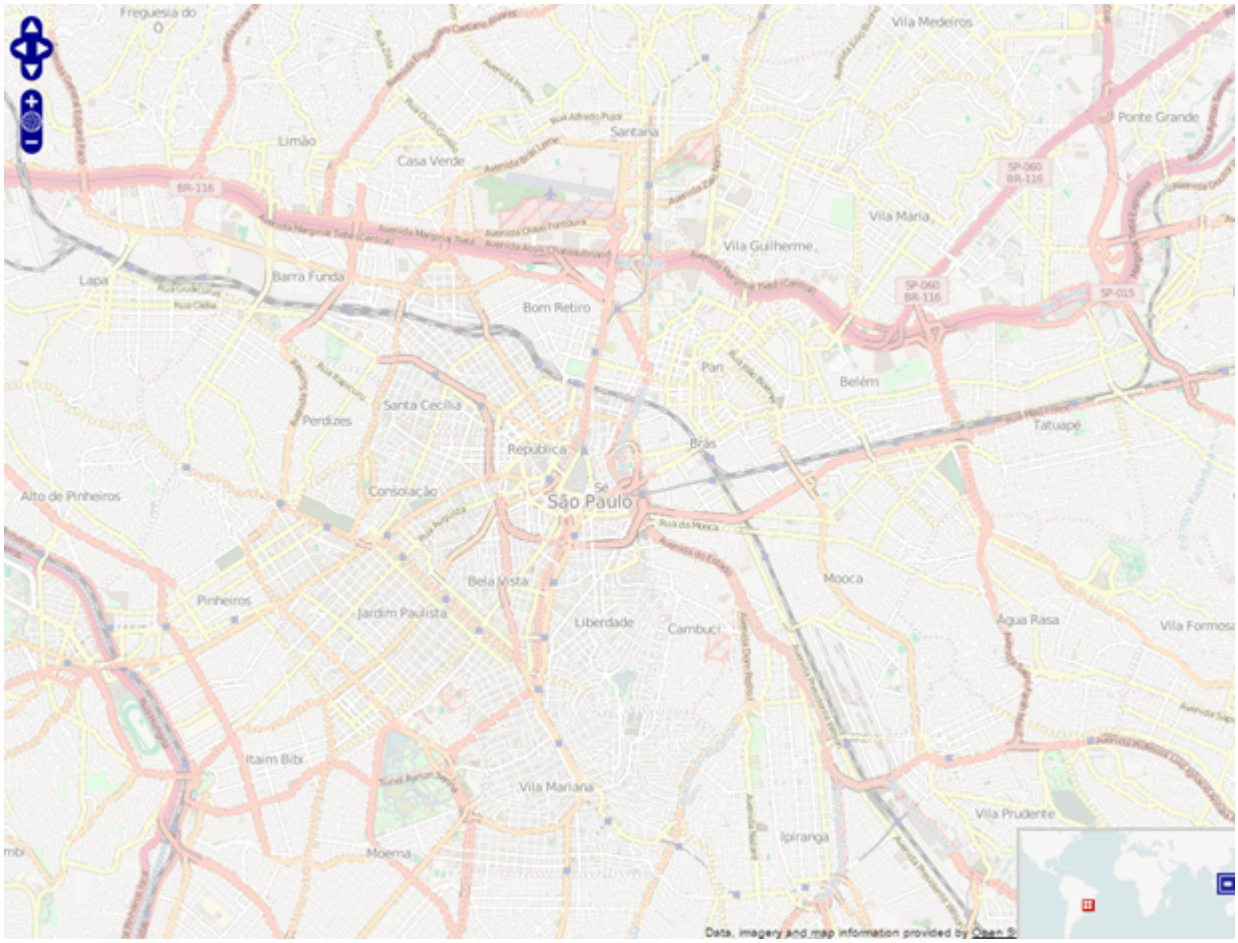
- Office cubicles — The wireless APs are located in an environment with cubicle offices present.
- Drywall — The wireless APs are located in an environment where the office wall composition is drywall.
- Brick walls — The wireless APs are located in an environment where there are brick walls present.
- Custom — Use this option to create custom floorplans.

A **Map Image** field is displayed under the **Environment** field. In the **Map Image** field, use the drop-down list to select an image or select **Add** () to open a window where you can select a local image and upload it to the ExtremeCloud IQ Site Engine server.

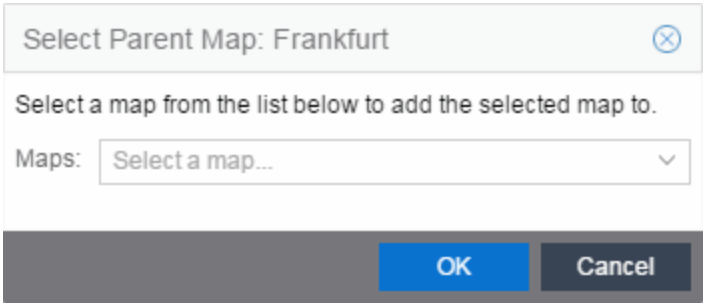
NOTE: If you upload a map image and an image with the same name already exists, the existing image is replaced.

- Geographic — Displays a global or regional map where network locations are shown geographically.

NOTE: The geographic map type is hosted by OpenStreetMap on an external server. For users with security concerns or if access to third-party servers is prohibited, use the topology map type.



c. Use the button to select the Parent Map, the map the new map is nested under in the Maps navigation tree. Changing the map's parent saves the current map properties and updates the map tree.



d. Select **Save**.

e. Select the Pan/Zoom Control option. This option determines whether or not the Pan and/or Zoom controls are available when viewing the map. (Pan and Zoom are always available while editing a map.) This allows you to disable the controls for fixed maps, like

world or city maps. For example, if a person viewing a map changes the location and zoom using these controls, those changes are saved and presented to the next person who views the map. This might create confusion over what the map is designed to display.


The Pan control allows you to move left/right and up/down in the map.


The Zoom control lets you zoom in and out of the map.

4. Add your devices, APs, or Links to the map you are currently editing by selecting **File** > **Add** > **Devices/APs/Map Link**. This opens the Add window.



Use the **Search** icon to locate a specific device or AP in the Add Device or Add AP windows, respectively, or select another Map to which to link from the drop-down list in the Add Link To Map window. Select the **Add** button to add the device, AP, or link to your network map.

5. Once your devices and/or APs are located on your map, manually manipulate the devices, APs, and links on the map, or organize them automatically by selecting **View** > **Automatic Layout**. The Device Layout window opens. Select one of the following layouts to automatically organize the devices, APs and links on your map:
    - Natural — Organizes devices, APs, and links such that the fewest number of network connections overlap.
    - Hierarchical — Organizes devices, APs, and links in a tree pattern.
    - Circular — Organizes devices, APs, and links in a circular pattern.
6. Select **File** > **Save** button to save the map.

NOTE: Map devices and APs do not show their current status until you save the map.

7. The map is now available for viewing by selecting it in the navigation tree. To edit a map, right-click on the map and select **Maps** > **Edit Map** or select the **Edit** button in the Map Properties panel.

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

How to Edit Maps

The ExtremeCloud IQ Site Engine Maps feature lets you edit newly created maps of the devices and wireless access points (APs) on your network.

In order to edit maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

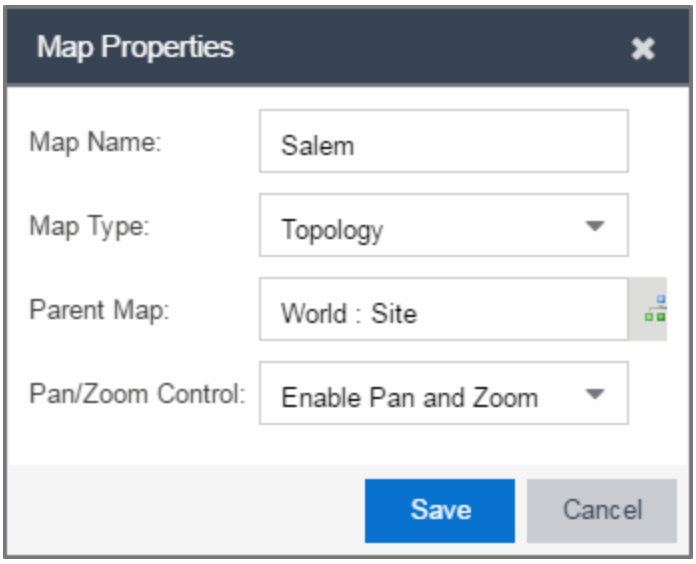
To access maps of your devices:

1. Launch ExtremeCloud IQ Site Engine.
2. Select the **Network** > **Devices** tab.
3. Select **Sites** from the left-panel drop-down list. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.
4. Expand a site from the left-panel tree to display the maps on that site.
5. Select a map to open the Map Name tab in the right panel.

Editing a Map

To edit a new Device map properties:

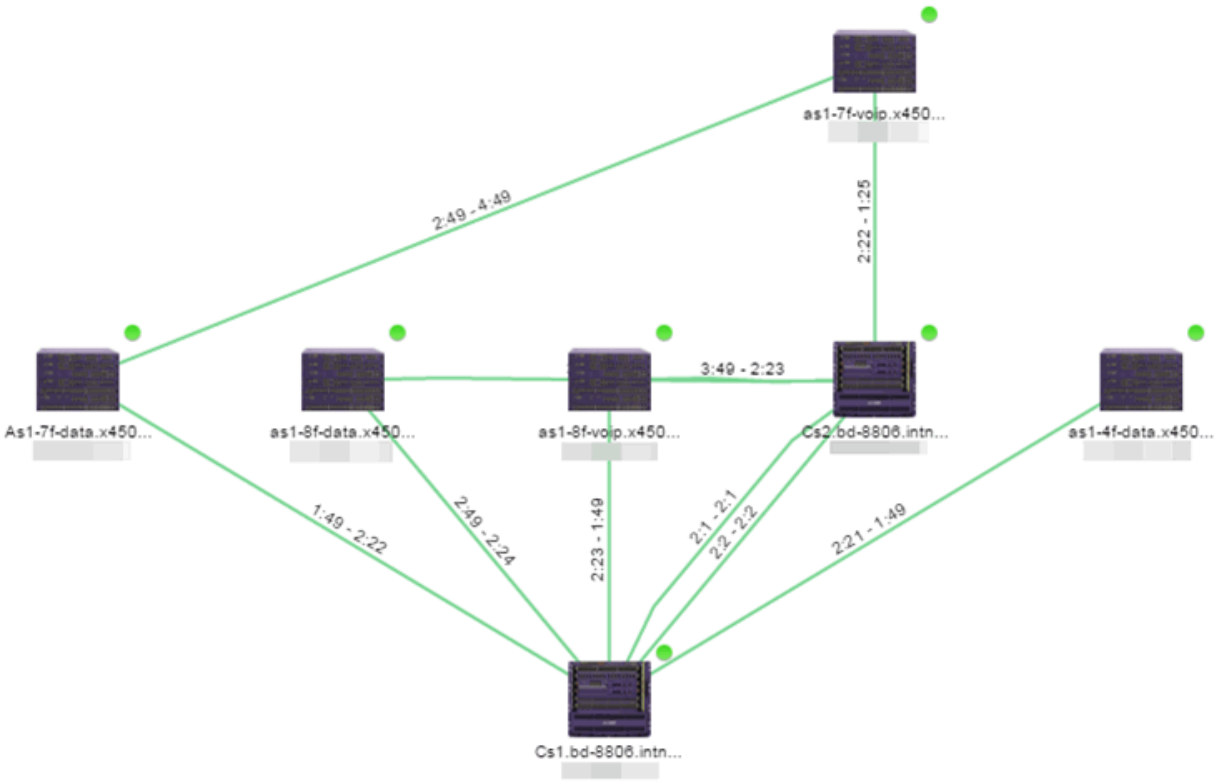
1. Select a new map from the left-panel. The new map is initially blank unless you create it from a device or AP by selecting the device or AP, selecting the **Menu** icon (☰) or right-clicking the device or AP and selecting **Maps** > **Create Map**.
2. Select **File** > **Properties** to open the Map Properties window from which you can edit the map criteria.



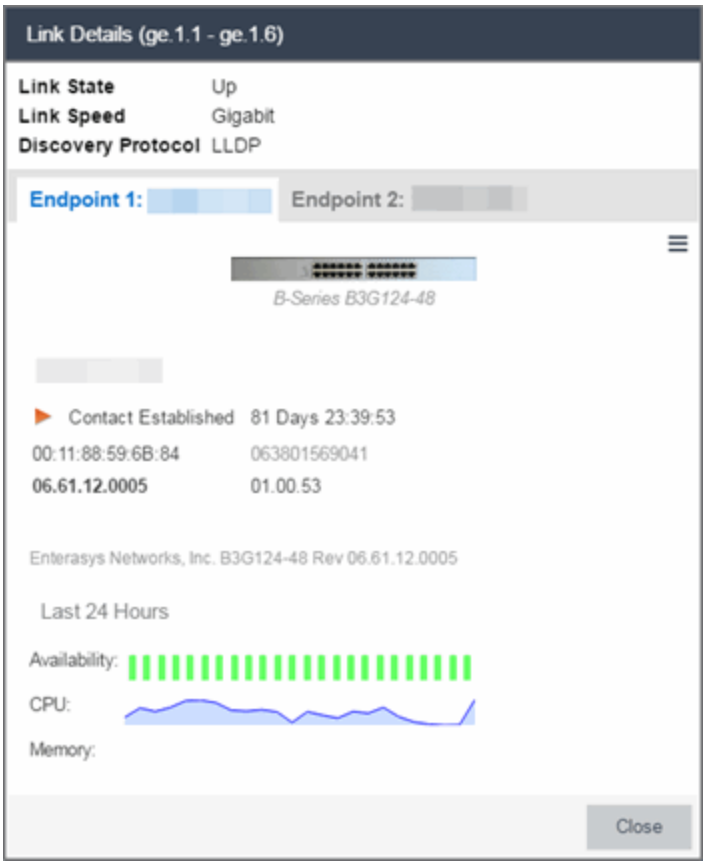
a. In the **Map Name** field, change the name for the map, if necessary.

b. In the **Map Type** drop-down list, select the type of map you are creating.

- Topology *(default)* - A topology map shows the state and speed of the network connections between devices as well as the state of the devices in the network.



Double-clicking a connection opens the Link Details window from which you can view additional details about the network connection and the devices it links.



- Topology - Background — Use a custom image to serve as the background of your map. The Map feature supports images in PNG, GIF, and JPG (without transparency) formats. The maximum image size is 3,000 x 2,000 pixels. Images larger than this are automatically scaled down to the maximum size allowed.

  If you select this option, a **Map Image** field displays under the **Map Type** field. In the **Map Image** field, use the drop-down list to select an image or select the button to open a window where you can select a local image and upload it to the ExtremeCloud IQ Site Engine server.

CAUTION: If you upload a map image and an image with the same name already exists, the existing image is replaced.

- Floorplan — Use the Floorplan map to display coverage of wireless APs within a building floorplan.



If you select Floorplan, select the map Environment, which is the type of environment where your network devices are physically located.

If your map includes wireless APs, the environment is used for RSS-based (Received Signal Strength) location services to help determine the radius of the circle displayed around an AP following a wireless client search. The radius shows the possible area where the client is located. For example, if you select open space environment, then the radius of the circle is larger than if you select brick walls environment because the AP's radio frequencies are not be obstructed by any walls, and the area where a client might be located is larger.

- Open space — The wireless APs are located in an environment with no walls or cubicles.

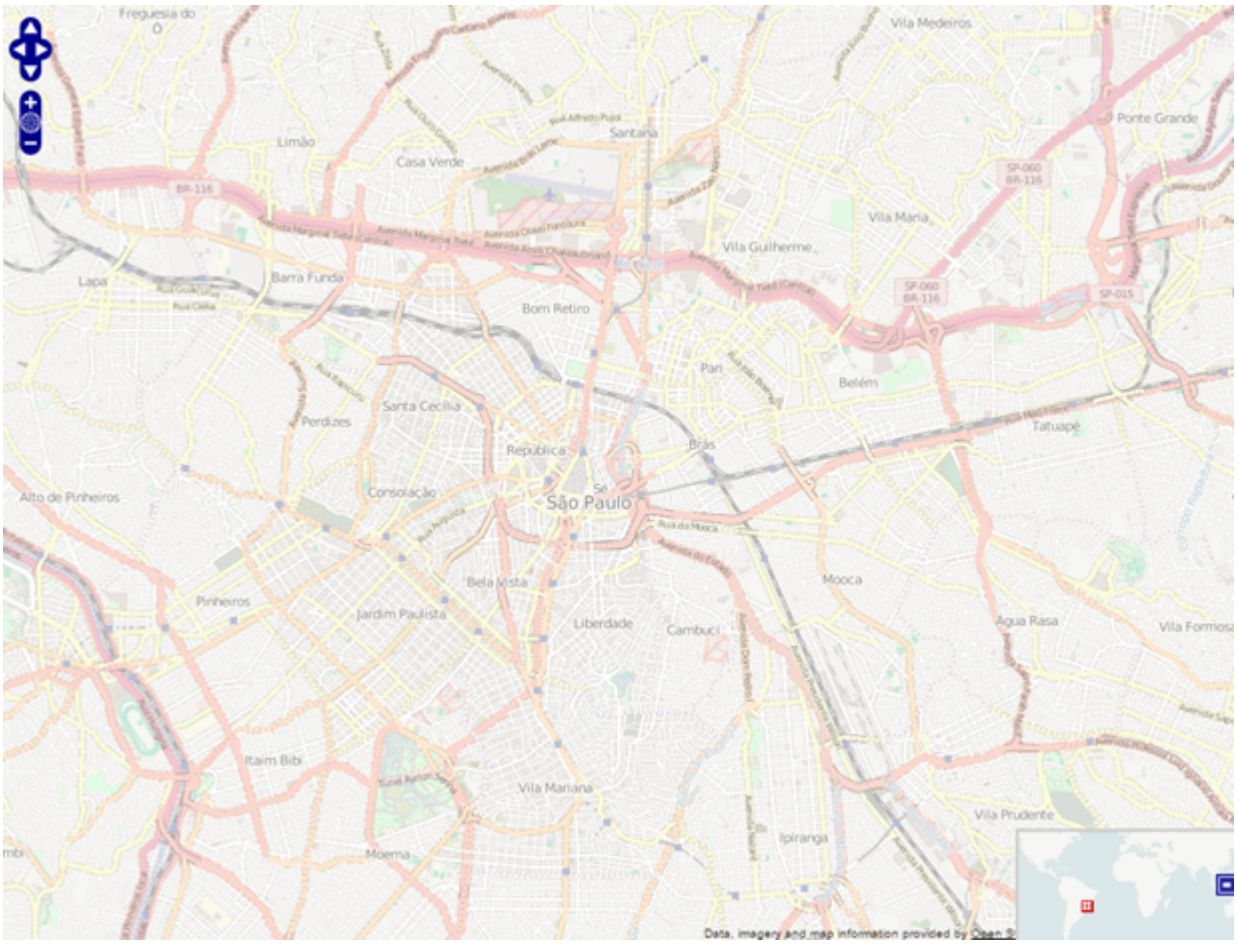
- Office cubicles — The wireless APs are located in an environment with cubicle offices present.
- Drywall — The wireless APs are located in an environment where the office wall composition is drywall.
- Brick walls — The wireless APs are located in an environment where there are brick walls present.
- Custom — Use this option to create custom floorplans.

A **Map Image** field is displayed under the **Environment** field. In the **Map Image** field, use the drop-down list to select an image or select **Add** ( ) to open a window where you can select a local image and upload it to the ExtremeCloud IQ Site Engine server.

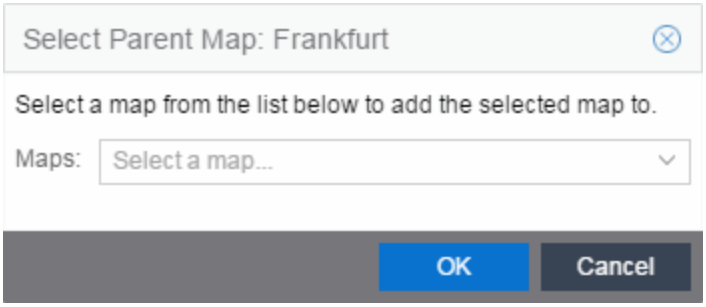
NOTE: If you upload a map image and an image with the same name already exists, the existing image is replaced.

- Geographic — Displays a global or regional map where network locations are shown geographically.

NOTE: The geographic map type is hosted by OpenStreetMap on an external server. For users with security concerns or if access to third-party servers is prohibited, use the topology map type.



c. Use the button to select the Parent Map, the map the new map is nested under in the Maps navigation tree. Changing the map's parent saves the current map properties and updates the map tree.



d. Select **Save**.

e. Select the Pan/Zoom Control option. This option determines whether or not the Pan and/or Zoom controls are available when viewing the map. (Pan and Zoom are always available while editing a map.) This allows you to disable the controls for fixed maps, like world or city maps. For example, if a person viewing a map changes the location and

zoom using these controls, those changes are saved and presented to the next person who views the map. This might create confusion over what the map is designed to display.


The Pan control allows you to move left/right and up/down in the map.


The Zoom control lets you zoom in and out of the map.

Adding Devices, APs and Links to a Map

1. Select **File** > **Add** > **Devices/APs/Map Link** to add your devices, APs, or Links to the map you are currently editing. This opens the Add window.



2. Use the **Search** icon to locate a specific device or AP in the Add Device or Add AP windows, respectively, or select another Map to which to link from the drop-down list in the Add Link To Map window. Select the **Add** button to add the device, AP, or link to your network map.
3. Once your devices and/or APs are located on your map, manually manipulate the devices, APs, and links on the map, or organize them automatically by selecting **View** > **Automatic Layout**. The Device Layout window opens. Select one of the following layouts to automatically organize the devices, APs and links on your map:
    - Natural — Organizes devices, APs, and links such that the fewest number of network connections overlap.
    - Hierarchical — Organizes devices, APs, and links in a tree pattern.
    - Circular — Organizes devices, APs, and links in a circular pattern.
4. Select **File** > **Save** button to save the map.

NOTE:	Map devices and APs do not show their current status until you save the map.

5. The map is now available for viewing by selecting it in the navigation tree. To edit a map, right-click on the map and select **Maps** > **Edit Map** or select the **Edit** button in the Map Properties panel.

- ExtremeCloud IQ Site Engine Maps
    - Types of Maps
    - Navigate Map Tab
        - Network Details Overview
        - EAPS Summary Tab
        - Link Summary Tab
        - VLAN Summary Tab
        - MLAG Summary Tab
        - VPLS Summary Tab
    - Search Maps
    - Create Maps
    - Add Devices or APs to Maps
    - Add Links Between Devices and Maps
    - Import Maps
    - Export Maps
    - Set Map Scale
- Advanced Map Overview
    - Design Map Floorplans
    - Display Map Application Data
    - Locate Wireless Clients
    - View Wireless Coverage

Advanced Map Features Overview

The **Network** > **Devices** tab contains Map features that let you create geographic and topological maps of the devices and floor plans of wireless access points (APs) on your network. The advanced Map features include custom floor plan design, triangulated wireless client location, and wireless coverage maps to identify coverage trouble spots for your wireless network.

Overview

ExtremeCloud IQ Site Engine advanced Map features provide the following enhanced functionality:

- **Detailed Floor Plans** — Advanced map functionality lets you create detailed floor plans for both your wired and wireless networks. Using floor plans provides greater accuracy in calculations of wireless client location and displays wireless device coverage. You can upload and modify existing floor plans or create new floor plans from scratch. Use the Map drawing tools and menus to specify wall types, material, and thickness and then configure AP locations, type, and orientation.
- **Wireless Location** — Advanced location (triangulation) enhances client location results, improving visibility when investigating wireless trouble spots. Colored distribution displays high, medium, and low confidence locations, with the client icon displayed in the highest confidence location. Using floor plan data, a single client's location is triangulated based on the client's contact with multiple access points in the covered area. The floor plan wall type information helps determine the degradation of signal strength that occurs as a wireless radio signal passes through the walls. This helps define the probable distance of a client from a given access point. You need at least three access points to report triangulated location. You can also view time-lapse location coverage for a client, using historic triangulated location results.
- **Wireless Coverage** — This feature provide a graphical view of wireless coverage, allowing quick identification of possible coverage trouble spots. Wireless coverage is displayed using different colors to indicate radio signal strength based on the distance from access points included on the map. Coverage is determined by computing the approximate radio signal strength at fixed distances from access points, with floor plan and wall information used to provide accuracy in the signal strength computation.
- **Import and Export Maps** — This feature lets you export floorplan maps to a ZIP file, and import an exported map if needed.
- **Show Application Data in Maps** — Use map links tied to ExtremeAnalytics network locations to display network application flow data in a map.

Prerequisites

In order to create or edit Maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

The following requirements pertain to wireless location and coverage features:

- The ExtremeWireless Controller must be a model C25 or better, running firmware version 8.31 or higher.
- The Location Engine on the wireless controller must be enabled. (For information on how to enable the Location Engine, refer to the *Extreme Networks Wireless Convergence Software*

User Guide.)

- The Access Points must be model 37xx, 38xx, or 39xx.

For information on related topics:

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

Advanced Map Features

The **Network** > **Devices** tab contains Map features that let you create geographic and topological maps of the devices and floorplans of wireless access points (APs) on your network. The advanced Map features include custom floorplan design, triangulated wireless client location, and wireless coverage maps to identify coverage trouble spots for your wireless network.

This Help topic provides the following information:

- Overview of Advanced Map Features
- Prerequisites
- Designing a Floorplan
    - Drawing Tools
    - Configure Area Window
    - Style Menu
- Wireless Client Location
    - Time-Lapse Location
- Wireless Coverage
- Import and Export Maps
    - Importing Maps
    - Exporting Maps
- Show Application Data
    - Adding a Map Link with Location
- Wireless Map Limits

For information on viewing and searching maps, see View and Search Maps.

Overview

ExtremeCloud IQ Site Engine advanced Map features provide the following enhanced functionality:

- **Detailed Floorplans** — Advanced map functionality lets you create detailed floorplans for both your wired and wireless networks. Using floorplans provides greater accuracy in calculations of wireless client location and displays wireless device coverage. You can upload and modify existing floorplans or create new floorplans from scratch. Use the Map drawing tools and menus to specify wall types, material, and thickness and then configure AP locations, type, and orientation.

- **Wireless Location** — Advanced location (triangulation) enhances client location results, improving visibility when investigating wireless trouble spots. Colored distribution displays high, medium, and low confidence locations, with the client icon displayed in the highest confidence location. Using floorplan data, a single client's location is triangulated based on the client's contact with multiple access points in the covered area. The floorplan wall type information helps determine the degradation of signal strength that occurs as a wireless radio signal passes through the walls. This helps define the probable distance of a client from a given access point. You need at least three access points to report triangulated location. You can also view time-lapse location coverage for a client, using historic triangulated location results.
- **Wireless Coverage** — This feature provides a graphical view of wireless coverage, allowing quick identification of possible coverage trouble spots. Wireless coverage is displayed using different colors to indicate radio signal strength based on the distance from access points included on the map. Coverage is determined by computing the approximate radio signal strength at fixed distances from access points, with floorplan and wall information used to provide accuracy in the signal strength computation.
- **Import and Export Maps** — This feature lets you export floorplan maps to a ZIP file, and import an exported map if needed.
- **Show Application Data in Maps** — Use map links tied to ExtremeAnalytics network locations to display network application flow data in a map.

Prerequisites

In order to create or edit Maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

The following requirements pertain to wireless location and coverage features:

- The ExtremeWireless Controller must be a model C25 or better, running firmware version 8.31 or higher.
- The Location Engine on the wireless controller must be enabled. (For information on how to enable the Location Engine, refer to the *Extreme Networks Wireless Convergence Software User Guide*.)
- The Access Points must be model 37xx, 38xx, or 39xx.

Designing a Floorplan

You can design and enhance floorplans of your wired and wireless network environment by editing your maps using the drawing and style tools. These editing tools allow you to create detailed visual representations of your network. You can also use floorplans to provide greater accuracy in the calculation of AP client location and in determining signal strength coverage for the wireless devices on your network.

NOTE: You can only use an AP in one floorplan.

Managed wireless controllers are automatically synchronized to match map floorplan data. If the floorplan data defined in ExtremeCloud IQ Site Engine maps is not consistent with data on the controller, the controller is updated accordingly.

NOTE: To prevent the automatic synchronization between ExtremeCloud IQ Site Engine maps and controllers, go to the **Administration** > **Diagnostics** tab, access System > Map Server Details from the left-panel and select the **Do Not Upload Maps** checkbox. Selecting this checkbox also prevents manually triggered map changes from being uploaded to a controller.

In floorplan design, use the map drawing tools to draw walls (or other objects) over an existing map image or on a blank canvas. The Style menu allows you to specify wall thickness, color, and wall materials.

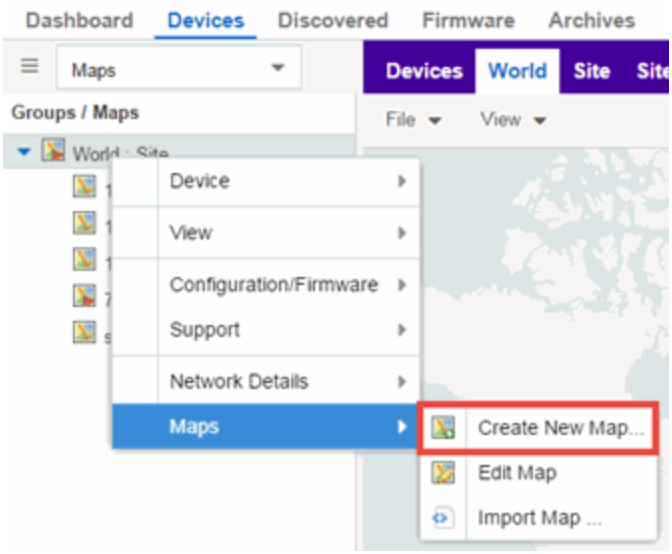
The wall information from the floorplan is used to help determine the degradation of signal strength that occurs as a wireless radio signal passes through the walls, and helps define the probable distance of a client from a given access point. ExtremeCloud IQ Site Engine uses the wall information to provide accuracy in determining wireless device signal strength.

A floorplan can be created with or without a reference background image, however it is much easier to use the drawing features with an existing image. (The Map feature supports images in PNG, GIF, and JPG (without transparency) formats.) For example, you can trace the outline of a floorplan image using the drawing tools to provide the wall information used for wireless calculations. You can use the Style and Wall menus to specify different wall material types, wall thickness, and wall color to customize the appearance of the floorplan.

When editing a floorplan, use the View menu to select whether to view or hide the background image, map cells, floorplan walls and drawings, devices and APs, and interswitch connections. You can also set the background image opacity.

The following steps provide a workflow for creating a floorplan showing the exterior and interior walls of a building. By drawing the walls over an existing floorplan image, you can add information that provide greater accuracy in wireless calculations.

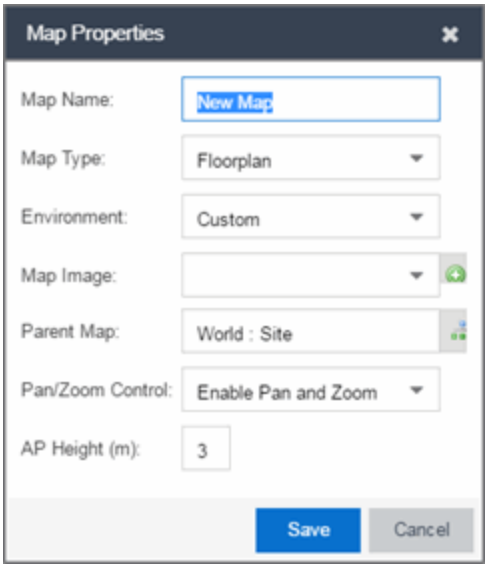
1. **Create and configure a new map.**
    a. Launch ExtremeCloud IQ Site Engine and select the **Network** > **Devices** tab.
    b. In the left-panel Groups/Maps navigation tree, right-click on the World map (or any other map that you want as the parent of the new map) and select **Maps** > **Create New Map**.



The Create New Map window opens.

c. Enter a name for the Map.

d. Open the Map Properties window by selecting **File** > **Properties**.



e. Change the **Map Type** drop-down list to **Floorplan**.

f. Set the **Environment** option to **Custom**. This allows you to draw walls over the existing image.

g. Upload the floorplan image you want to use in the **Map Image** field. The Map feature supports images in PNG, GIF, and JPG (without transparency) formats. The maximum

image size is 3000 x 2000 pixels. Images that are larger than this are automatically scaled down to the maximum size allowed.

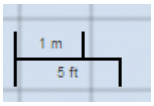
h. Set the **AP Height** property. This value is the distance from the floor to the AP position on the wall or ceiling in meters. This is a single value used for all access points. Setting a reasonable value helps with the accuracy of the location feature. The default for this value is three meters, which is at the top of a wall with a nine foot ceiling.

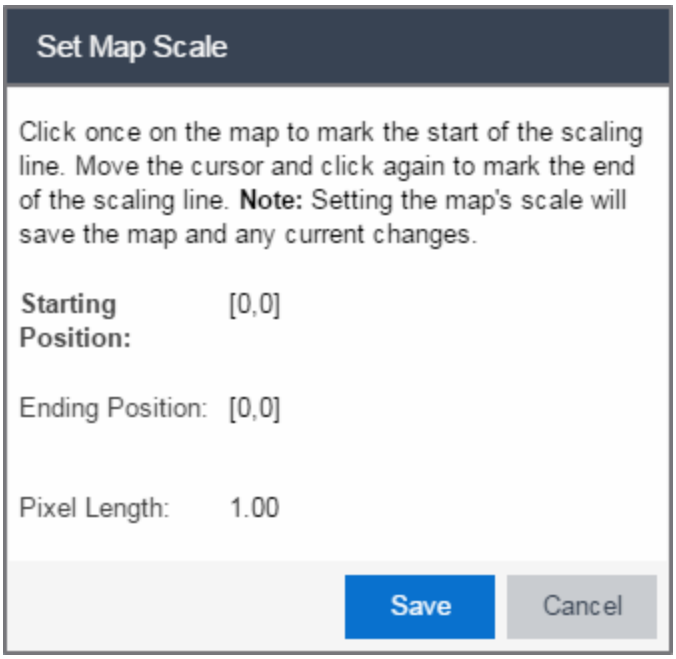
i. Select **Save** to save the map and display the image.

2. **Set the map scale.** It is important to set the scale before adding devices or walls, since changing the scale later may cause the object positions to be realigned. Try to make the scale as accurate as possible, as this affects triangulation accuracy.

   a. Select **File** > **Edit** to open the map in edit mode.

   b. Select the map scale in the map's footer panel to open the Set Map Scale window. (You can also access the Set Map Scale window from the Tools menu.)





   c. To set the scale, you must measure something in the map using a scaling line, and then set the measurement for the line. For example, in an office floorplan you could measure a scaling line on the opening of an office. If you know that the office doors are 33 inches wide, enter that as the scaling line measurement.

i. Select on the map to mark the start of the scaling line. Move the cursor and select again to mark the end of the scaling line.

ii. Enter the line length and units.

d. Select **OK**. The map scale is automatically adjusted and the map is saved.

3. **Draw floorplan walls.** Select the **Edit** button to open the map in edit mode. By default you see a grid of cells displayed over the background image. (It can be turned off in the **View** menu.) This grid can help with positioning walls and access points. Add walls to the floorplan using the drawing tools accessed from the **Tools** menu (at the upper left corner of the Map main view).

   a. Define an exterior wall. The exterior wall is used to define the floorplan area included in wireless client location and wireless coverage maps, and should be drawn around the entire perimeter of the floorplan area, without any gaps.

   b. Select the appropriate drawing tool from the **Tools** menu. Use the Style menu to configure the wall color, thickness, and transparency. Select the wall material using the Wall drop-down list and select the checkbox to specify that the wall is an exterior wall.



   c. Draw the exterior wall using the selected drawing tool. You can double-click or hit **Escape** to terminate the drawing.

   d. Use these same steps to draw the remaining walls on your floorplan. Be sure to deselect the **Exterior** checkbox for the other walls.

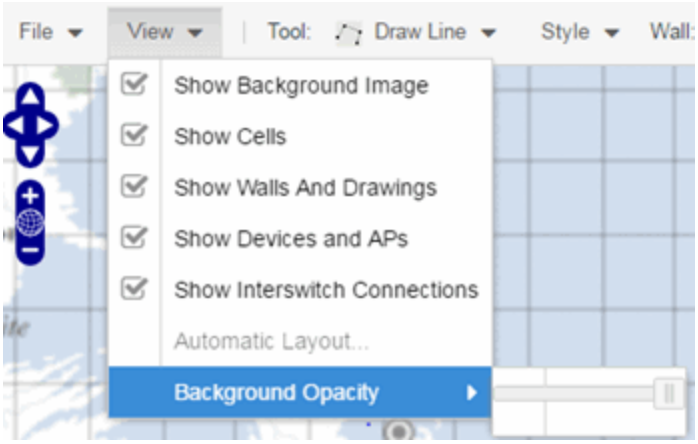
      You can trace over existing walls on the floorplan or add new walls, if necessary. Focus on high attenuation walls like concrete or large sections of glass. It is not necessary to incorporate walls and structures that do not fully divide the space, such as half-walls or cubicles.

      Ensure that the wall positioning is as accurate as possible, and define the proper material for each wall. Select a material that most closely represents the actual wall construction if it is different than the available options. Keep your colors consistent for the various wall types. The more accurately the map reflects the true environment, the more precise the wireless location and coverage results are in the map.

To remove a line or shape, select **Select Items** in the **Tool** menu, select the shape, and press **Delete**, or right-click on the shape and select **Remove from Map** from the menu. Use the Ctrl+Z key combination to restore deleted items back to the map. Selecting Ctrl+Z multiple times undoes multiple deleted items in the reverse order in which you deleted them.



e. While editing, use the **View** menu to select whether to view or hide the background image, map cells, floorplan walls and drawings, devices and APs, and interswitch connections. You can also select an automatic layout and set the background image opacity.

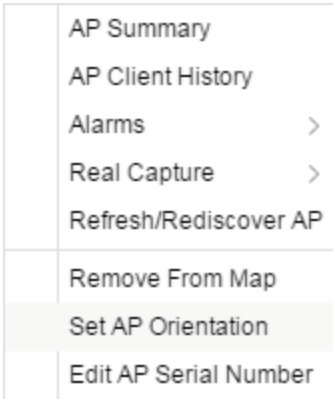


4. **Add your APs to the map.** In Edit mode, a panel that lists equipment available to add to the map is visible beneath the properties panel. The display is filtered on either the currently discovered devices or the APs known to wireless controllers on your network, depending on your selection (APs or Devices) in the panel title bar. You can use the search field to locate a specific device or AP.

   Drag the desired devices and APs onto the map area and position them to produce your network map. Be sure the APs are in the correct location, so your location and coverage maps are accurate. The center of the image is roughly the position of the AP. Be sure to place an AP on the correct side of a wall.



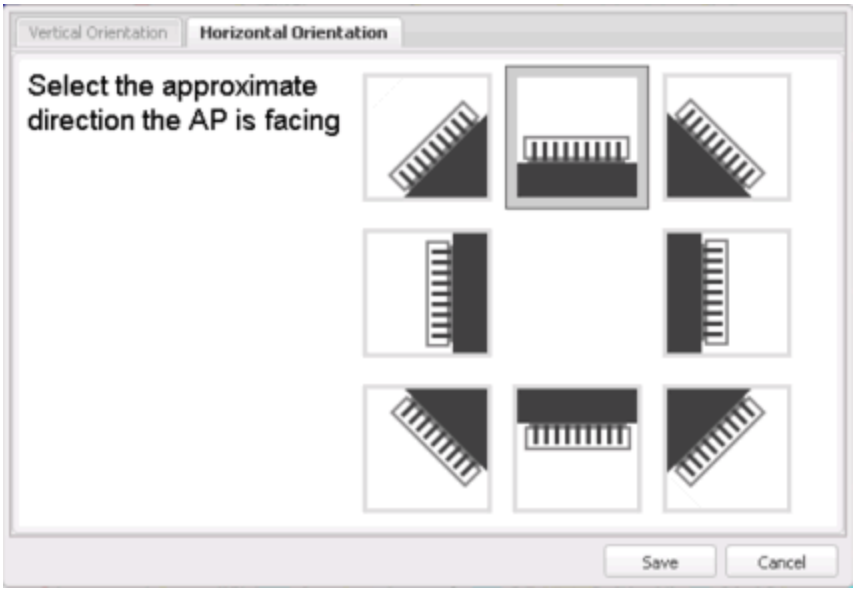
5. Set AP orientation.
   a. Right-click on an AP in the map and select **Set AP Orientation**.



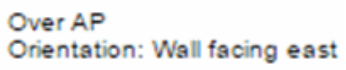
b. Select the **Vertical Orientation** tab to set whether the AP is on the ceiling or wall.



c. If the AP is on a wall, the **Horizontal Orientation** tab appears and allows you to select the approximate direction the AP is facing.



d. Select **Save** to close the window. **TIP:** You can view AP orientation information by mousing over an AP. The AP orientation (if set) is displayed in the bottom right corner of the main map view.



6. Select **Save** to save the map. The floorplan is uploaded to the controllers that manage the access points placed on the map. The map is now ready to display wireless location and coverage information. See the sections on wireless location and wireless coverage.
7. **Select the desired map view mode.** When viewing a map, use the **View** drop-down list to specify whether to:
    - Display markers instead of device images on your map
    - Display cells on the map image to show the map's actual image area
    - Display AP channel information (if available)
    - Display walls and drawings
    - Show application data for map links (if available)
    - Set the map's background opacity
    - Set the minimum location confidence to filter location confidence colors in triangulated location search results

Drawing Tools

The drawing tools allow you to add lines and shapes to your custom floorplans. The following table includes descriptions of the various drawing tools accessed from the Tool menu.

Drawing Tool	Definition
	**Select Items** Select a line or shape to select it for dragging or modification. Use the yellow drag handle to reposition the item; use the blue vertex to modify the shape. Select anywhere on the map and drag to reposition the map image.
	**Draw Area** Location areas allow you to set policies for clients based on their location on a map. Position your cursor where you want to start drawing an area location. Select and draw the first line of the polygon. Select at each corner of the area location. To open the Configure Area window with the Draw Area tool active, double-click the area line. To open the Configure Area window and close the Draw Area tool, right-click the area line.
	**Draw Polygon** Position your cursor where you want to start drawing the polygon shape. Select and draw the first line of the polygon. Select each corner of the polygon. Double-click to release the polygon line. When you are finished drawing, right-click to release the draw polygon tool.

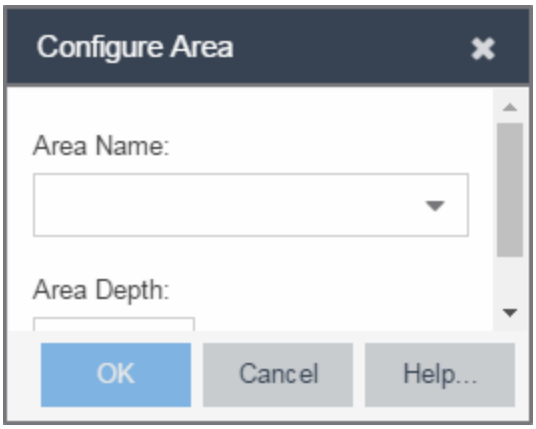
Drawing Tool	Definition
	**Draw Rectangle** Position the cursor where you want the rectangle. Select and drag to draw the rectangle. When you are finished drawing, right-click to release the draw rectangle tool.
	**Add Text** Select the map to open the Enter Text window. When you are finished entering your text, select **OK**. Position the cursor where you want to place the text and select to add the text to your map. Use the **Style** menu to change the text appearance.
	**Draw Triangle** Position the cursor where you want the triangle. Select and drag to draw the triangle. When you are finished drawing, right-click to release the draw triangle tool.
	**Draw Line** Position your cursor where you want to start drawing the line. Select and draw the line. Select to change line direction. While drawing, press the Delete key to delete the last vertex in the line. Double-click to release the line. When you are finished drawing, right-click to release the draw line tool.
	**Rotate Shape** Select the shape you want to rotate. Use the blue handle to rotate the shape to the desired position. (You can also right-click on an image and select Rotate Shape from the menu.)
	**Set Scale** Opens the Set Map Scale window from which you can determine the scale of your map.

Configure Area Window

The Configure Area window, accessible from the Draw Area tool, allows you to name and determine the depth of an area.

- **Area Name** — The name of the area you are creating.
- **Depth** — A unique identifier for the area used when two areas overlap. In the event a client is located in a location shared by two areas, the client displays in the area with the higher **Depth** value.

> **NOTE:** The **Depth** must be a value of 10 or higher. Values of 1 - 9 are reserved by the system.



Area locations allow you to define up to 16 specific areas per floor on your map to determine whether a client position is inside or outside of each area. Additionally, you can create areas located inside of other areas. A client can only be located in one area at a time and based on the area in which the client is located, you can apply different policies to the client. For example, a client accessing the network from an area located in a classroom may be granted different access than a client accessing the network in an area located in a professor's office.

Style Menu

Use the Style menu to define the characteristics of the walls and other shapes you add to your custom floorplans. Following are definitions of the Style menu options.

Style Option	Description
Font Color	Specify the color of the text added to the map.
Font Size	Specify the size of the text added to the map.
Line Thickness	Specify the thickness of the shape border in pixels.
Line Color	Specify the color used in shape borders.
Line Opacity	Specify the opacity of the shape borders. This allows you to shade the floorplan.
Shape Filled	Select the checkbox to fill shapes with the specified shape color.
Shape Color	Select the color used to fill the shapes you create.
Shape Opacity	Specify the opacity of the shape color.

Wireless Client Location

The wireless location feature requires you enable the location engine on the wireless controller. After you add APs to your custom floorplan and save the map, a copy of the floorplan is sent to each controller. The location engine incorporates information defined in the floorplan data and signal

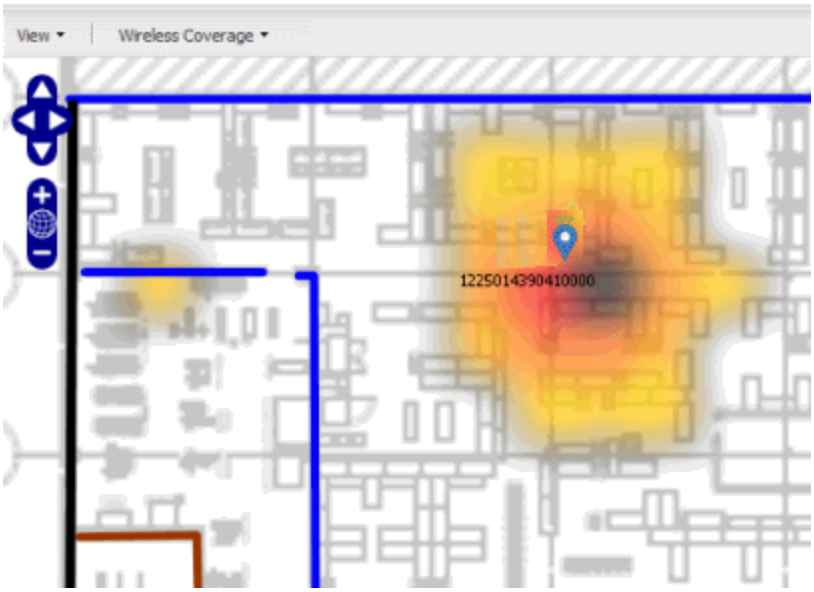
information from a client's contact with APs in order to calculate a client's precise location in the covered area. Client information from within a short time frame must be reported by at least three APs in order to determine a client's triangulated location.

To search for a wireless client, enter a MAC address, IP address, hostname, or user name in the map **Search** box and press **Enter**. (The client must be connected to an AP added to a map.)

The map containing the AP is displayed with an icon for the client. A colored distribution of location confidence is shown on the map with black being highest confidence, red medium confidence, and yellow lowest confidence. You can use the **Min. Location Confidence** slider on the **View** menu to filter out lower confidence colors. As you drag the slider, colors below the selected confidence level are no longer displayed. If you set the slider to the right-most point, only black is displayed.

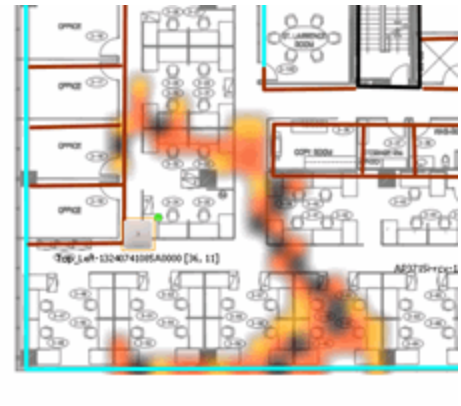
Mouse over the client icon to see a tooltip with client information.

NOTE: The tooltip information is based on current data from the wireless domain unless the client icon displays a clock in the center. In that case, the tooltip information is based on historic data from the **Wireless** > **Clients** tab and the confidence colors are not displayed.

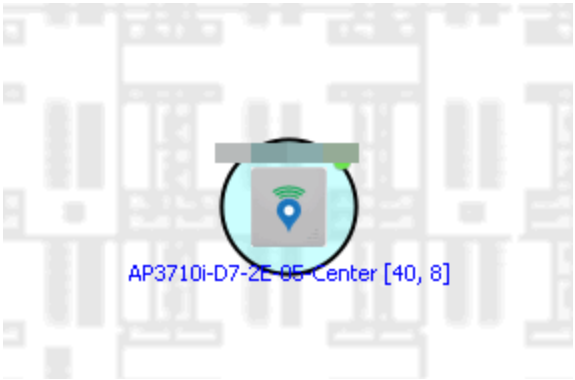


If the location result is based on only one AP, the map displays probabilities for the location but with a few differences:

- No client icon is displayed.
- The location confidence distribution area is larger and generally displayed in a circular pattern.
- The associated AP is highlighted.
- The distance is shown beside the confidence legend at the foot of the map.



If there is insufficient data to provide triangulated results, the map displays the AP in the center, with a circle showing the possible area where the client may be located, based on the client's RSS (Received Signal Strength).



Time-Lapse Location

The wireless location feature provides the ability to view time-lapse location coverage for a client, using historic triangulated location results. This allows you to understand a wireless client's movement through the network and provides for better network troubleshooting.

When a current triangulated location search result displays, a checkbox is available in the upper right corner to enable time-lapse location.

When the checkbox is selected, a set of controls appears to the left of the checkbox, indicating the date of the displayed result. If there are historic events available, the Rewind arrow is enabled and you can scroll through the history. Note that for a historic location, the client icon displays a small clock inside it.

The Rewind and Fast-Forward arrows are disabled if there is no more history in that direction. After viewing historic locations, if you fast forward to the current location and it changed, the location updates.



Wireless Coverage

After you finish your custom floorplan and saved the map, the map is ready to display wireless coverage information. Select **View** > **Wireless Coverage** > **Show Coverage** to show wireless coverage of the APs on the map and to enable the wireless coverage options. Use the **View** > **Wireless Coverage** menu available at the top of the map to select from the following coverage display options.

- **Mode** — Select from the different options for coverage display:
  - **Signal Strength**— Use this mode to view AP signal strength. Set the Band, Access Points, and Minimum RSS options.
  - **Channel Coverage** — Use this mode to view channel coverage and AP health. Set the Select Channel, Band, and Access Points options. This mode provides a graphical overview of channel allocation, helping to visualize radio management issues or locate potential interference.
  - **Data Rate** — This mode shows a coverage map indicating the expected physical rate for all of the cells on the floor. Set the Minimum Physical Rate, Band, and Access Points options. Use this mode to ensure proper wireless performance throughout the network.

NOTE: Wireless coverage maps are divided into cells. Each cell displays a signal strength with which it is associated, used to determine wireless coverage and the location probability of a user.

  - **Location Readiness** — Use this mode to view the expected quality of location search results for each map cell, given the current placement of APs. Colors denote readiness for each cell:
    - Green — Good readiness. There are four or more APs with visibility of the cell, with at least three of them within 20 meters.
    - Yellow — Moderate readiness. There are three APs with visibility of the cell, with at least two within 20 meters.
    - Orange — Poor readiness. There are less than three APs with visibility of the cell.
    - Red — No triangulation. Only Cell of Origin location results are available in this area.
- **Select Channel** — Used to select the channels to view for Channel Coverage mode. If "All" is selected, each distinct channel is assigned a color as shown in the legend at the foot of the map, and the color brightness varies to indicate coverage intensity. Selecting a single channel shows a coverage map for that one channel's signal strength and displays a Channel Health window that shows the average and maximum utilization and noise levels for each applicable AP.
    - Utilization — The percentage of busy time for the channel during the last 100 seconds. A channel is busy either because of an interference with energy above a threshold (-62dBm) or because of an active transmission of other stations or APs. This is an indicator of the congestion and interference on the channel.
    - Noise — The noise floor measured by the AP on the 802.11 channel over the last 30 seconds. Noise floor is measured during the quiet time, between the valid transmission or reception of 802.11 frames.
- **Min. Physical Rate** — Used for Data Rate mode to set the minimum physical rate to display. A legend for the Physical Rate by color is visible at the bottom of the map.
- **Band** — Select the desired band (radio frequency).
- **Access Points** — Select which access points to include. These buttons allow you to select or deselect all APs. This option also contains a checkbox that allows you to use default values if a radio is off. When this checkbox is selected, you can view an estimate of coverage using default values; otherwise, no coverage is shown.
- **Minimum RSS** — Used to set the minimum RSS to display (default is -80) for Signal Strength mode. A legend for the RSS by color is visible at the bottom of the map.

When these options are set, the map displays the selected coverage information. The following map shows signal strength coverage.



Import and Export Maps

This section describes the map import and export functions. The map import function allows you to import exported maps into ExtremeCloud IQ Site Engine floorplan maps. The map export function exports floorplan maps to a ZIP file.

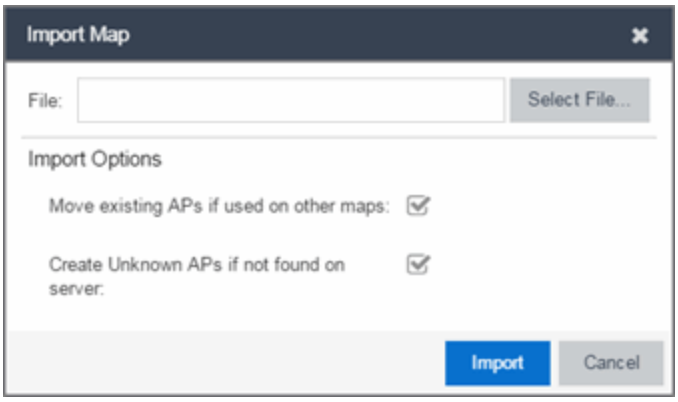
Importing Maps

The map import function gives you the ability to import maps into ExtremeCloud IQ Site Engine floorplan maps and gives you the ability to import floorplan maps are previously exported from ExtremeCloud IQ Site Engine maps.

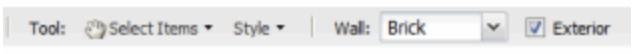
When a map is imported, it is added as a child map of the World map. If the map's name is not unique, a number is appended to the end of the name. After the map is imported it can be moved and renamed, if desired.

To import a map:

1. Launch ExtremeCloud IQ Site Engine and select the **Network** > **Devices** tab.
2. In the left-panel, select Maps from the drop-down list.
3. In the Groups/Maps navigation tree, right-click on the World map and select **Maps** > **Import Map**.
4. The Import Map window opens. Use the **Select File** button to navigate to the map file to import.



5. Select the appropriate import options:
   - **Move existing APs if used on other maps** — An AP can only be added to a single map. If you select this option and import an AP that already exists on another map, the AP is moved from the existing map to the imported map.
   - **Create Unknown APs if not found on server** — If an AP is being imported that does not exist in ExtremeCloud IQ Site Engine, a placeholder AP is created. After the map is imported, you can edit the placeholder and map it to an existing AP not currently in use on another map. To do this, right-click on the placeholder and select **Edit AP Serial Number**.
6. Select **Import**.
7. The map is imported and positioned under the World map. It can be moved and renamed, if desired.
8. Manually edit the exterior walls after the floorplan is imported.
   a. Select the map and select **Edit** to edit the map.
   b. Select the exterior wall and then select the **Exterior** checkbox. This designates the wall as an exterior wall.



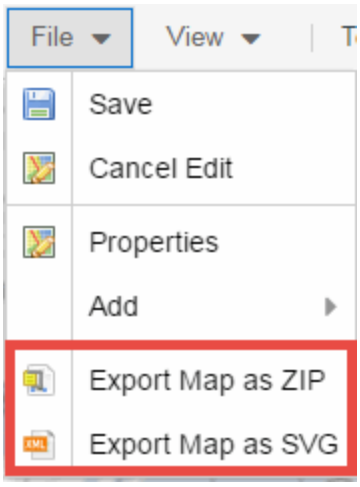
   c. Select **Save** to save the map.

Exporting Maps

The map export function gives you the ability to export floorplan maps as a ZIP or SVG file.

To export a map:

1. Launch ExtremeCloud IQ Site Engine and select the **Network** tab.
2. In the left-panel Maps navigation tree, select the map you want to export.
3. The map opens in Edit mode. Select **File** > **Export Map as ZIP** or **Export Map as SVG**.



- If you select **Export Map as ZIP**, the map is saved in a ZIP file in your browsers default download location.
- If you select **Export Map as SVG**, the map opens in a new tab, allowing you to save the map in the desired location.

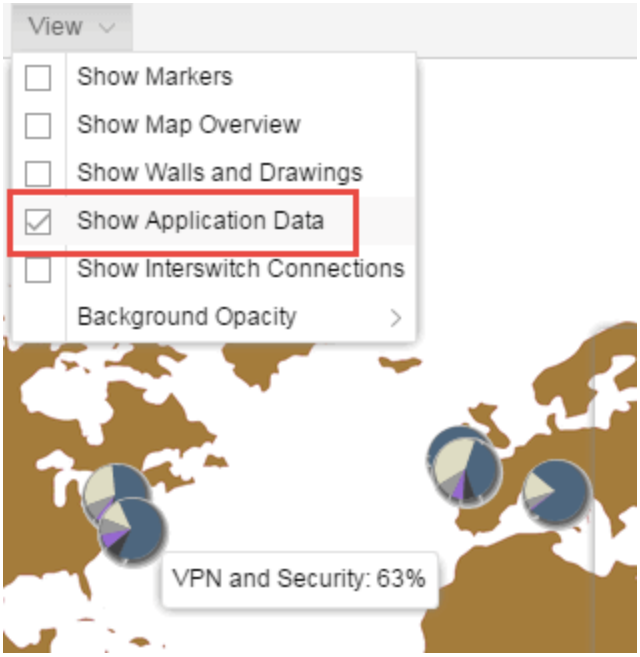
NOTE: The Export Map as ZIP option is only available for Floorplan map types.

Show Application Data

You can display application data in maps by creating map links tied to ExtremeAnalytics network locations. Application data for the location tied to the link displays in the map.

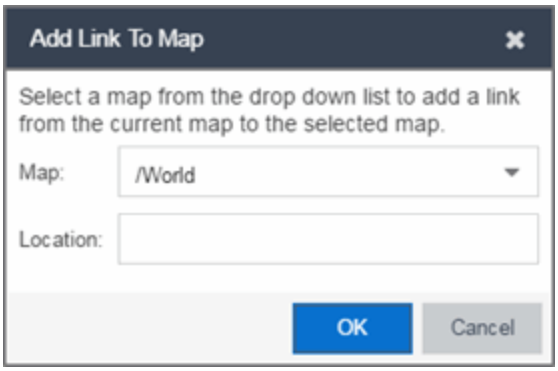
When the **Show Application Data** checkbox in the **View** menu is selected, a pie chart is generated for every map link on the current map. The application data in the pie chart is based on the **Site** field specified for the link and corresponds to a site defined in the Site tab.

The pie chart displays the top five application groups (by bytes transferred) for the location specified for the map link. Rest the cursor over the pie chart to view a tooltip. If there is no application data, nothing displays.



Adding a Map Link with Location

1. In the Maps navigation tree, right-click on the map you want to link from and select **Maps** > **Edit Map** or select **File** > **Edit** in the map properties panel.
2. The map's property panel opens in Edit mode. Select **File** > **Add** > **Map Link**.
3. The Add Link to Map window opens.



4. From the drop-down list, select the map to which you want to link.
5. Enter a site and select **OK**
6. The map link is added to the map. You can reposition the map, if desired, or edit a link by right-clicking on the link (in Edit mode) and selecting **Edit Link** from the menu.
7. Select the **Save** button to save the map.

NOTE: You can edit a map link created before link locations were supported by right-clicking on the link (in Edit mode) and selecting **Edit Link** from the menu. This allows you to specify a location for a link without having to delete and re-add the link.

Wireless Map Limits

The following sections provide information about limits for wireless client location and wireless coverage maps.

Active Client Tracking

The number of active clients the location engine on the wireless controller can track simultaneously depends on the wireless controller model. Refer to your wireless controller documentation for information.

Maximum Number of Maps

A wireless controller on which version 10.01.01 or higher is installed can store a maximum of 200 maps. Wireless controllers running a version lower than 10 can store a maximum of 100 maps.

Maximum Number of APs per floorplan

A single floorplan allows a maximum of 2,000 APs when version 10.01.01 is installed on the wireless controller. A floorplan with a wireless controller on which a version lower than 10 is installed allows 100 APs.

- ExtremeCloud IQ Site Engine Maps Overview
- How to Create and Edit Maps

How to Design Floorplans

The **Network** > **Devices** tab contains Map features that let you create geographic and topological maps of the devices and floorplans of wireless access points (APs) on your network. The advanced Map features allow you to design and enhance custom floorplans of your wired and wireless network environment using drawing tools and the style menu.

Designing a Floorplan

Using the drawing and style tools, you can create detailed visual representations of your network. You can also use floorplans to provide greater accuracy in the calculation of AP client location and in determining signal strength coverage for the wireless devices on your network.

NOTE: You can only use an AP in one floorplan.

Managed wireless controllers are automatically synchronized to match map floorplan data. If the floorplan data defined in ExtremeCloud IQ Site Engine maps is not consistent with data on the controller, the controller is updated accordingly.

NOTE: To prevent the automatic synchronization between ExtremeCloud IQ Site Engine maps and controllers, go to the **Administration** > **Diagnostics** tab, access System > Map Server Details from the left-panel and select the **Do Not Upload Maps** checkbox. Selecting this checkbox also prevents manually triggered map changes from being uploaded to a controller.

In floorplan design, use the map drawing tools to draw walls (or other objects) over an existing map image or on a blank canvas. The Style menu allows you to specify wall thickness, color, and wall materials.

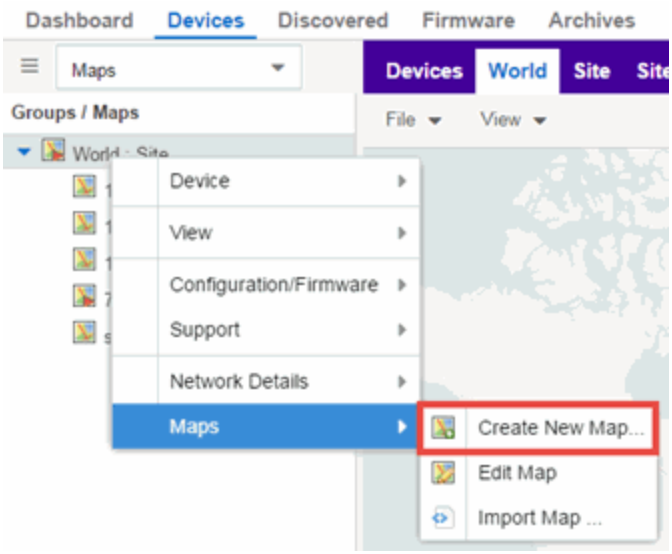
The wall information from the floorplan is used to help determine the degradation of signal strength that occurs as a wireless radio signal passes through the walls, and helps define the probable distance of a client from a given access point. ExtremeCloud IQ Site Engine uses the wall information to provide accuracy in determining wireless device signal strength.

A floorplan can be created with or without a reference background image; however it is much easier to use the drawing features with an existing image. (The Map feature supports images in PNG, GIF, and JPG (without transparency) formats.) For example, you can trace the outline of a floorplan image using the drawing tools to provide the wall information used for wireless calculations. You can use the Style and Wall menus to specify different wall material types, wall thicknesses, and wall colors to customize the appearance of the floorplan.

When editing a floorplan, use the View menu to select whether to view or hide the background image, map cells, floorplan walls and drawings, devices and APs, and interswitch connections. You can also set the background image opacity.

The following steps provide a workflow for creating a floorplan showing the exterior and interior walls of a building. By drawing the walls over an existing floorplan image, you can add information that provides greater accuracy in wireless calculations.

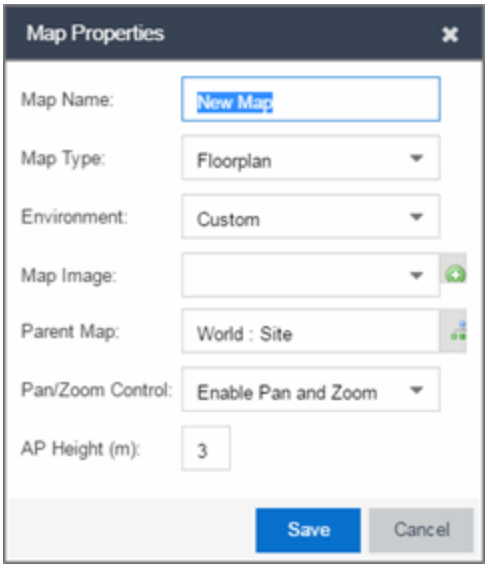
1. **Create and configure a new map.**
    a. Launch ExtremeCloud IQ Site Engine and select the **Network** > **Devices** tab.
    b. In the left-panel Groups/Maps navigation tree, right-click on the World map (or any other map that you want as the parent of the new map) and select **Maps** > **Create New Map**.



The Create New Map window opens.

c. Enter a name for the Map.

d. Open the Map Properties window by selecting **File** > **Properties**.



e. Change the **Map Type** drop-down list to **Floorplan**.

f. Set the **Environment** option to **Custom**. This allows you to draw walls over the existing image.

g. Upload the floorplan image you want to use in the **Map Image** field. The Map feature supports images in PNG, GIF, and JPG (without transparency) formats. The maximum

image size is 3000 x 2000 pixels. Images that are larger than this are automatically scaled down to the maximum size allowed.

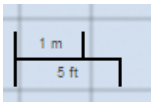
h. Set the **AP Height** property. This value is the distance from the floor to the AP position on the wall or ceiling in meters. This is a single value used for all access points. Setting a reasonable value helps with the accuracy of the location feature. The default for this value is three meters, which is at the top of a wall with a nine foot ceiling.

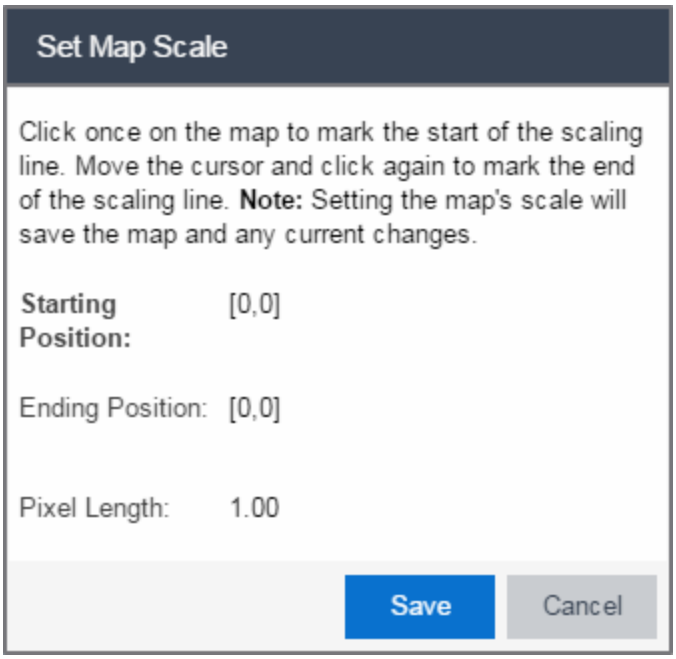
i. Select **Save** to save the map and display the image.

2. **Set the map scale.** It is important to set the scale before adding devices or walls, since changing the scale later may cause the object positions to be realigned. Try to make the scale as accurate as possible, as this affects triangulation accuracy.

   a. Select **File** > **Edit** to open the map in edit mode.

   b. Select the map scale in the map's footer panel to open the Set Map Scale window. (You can also access the Set Map Scale window from the Tools menu.)





   c. To set the scale, you must measure something in the map using a scaling line, and then set the measurement for the line. For example, in an office floorplan you could measure a scaling line on the opening of an office. If you know that the office doors are 33 inches wide, enter that as the scaling line measurement.

i. Select on the map to mark the start of the scaling line. Move the cursor and select again to mark the end of the scaling line.

ii. Enter the line length and units.

d. Select **OK**. The map scale is automatically adjusted and the map is saved.

3. **Draw floorplan walls.** Select the **Edit** button to open the map in edit mode. By default you see a grid of cells displayed over the background image. (It can be turned off in the **View** menu.) This grid can help with positioning walls and access points. Add walls to the floorplan using the drawing tools accessed from the **Tools** menu (at the upper left corner of the Map main view).

   a. Define an exterior wall. The exterior wall is used to define the floorplan area included in wireless client location and wireless coverage maps, and should be drawn around the entire perimeter of the floorplan area, without any gaps.

   b. Select the appropriate drawing tool from the **Tools** menu. Use the Style menu to configure the wall color, thickness, and transparency. Select the wall material using the Wall drop-down list and select the checkbox to specify that the wall is an exterior wall.



   c. Draw the exterior wall using the selected drawing tool. You can double-click or hit **Escape** to terminate the drawing.

   d. Use these same steps to draw the remaining walls on your floorplan. Be sure to deselect the **Exterior** checkbox for the other walls.

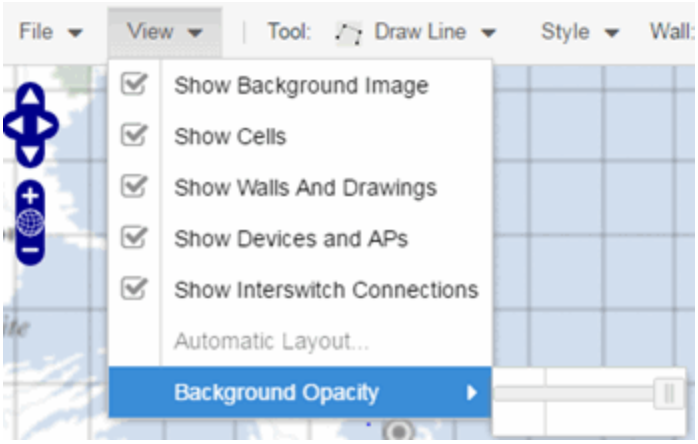
      You can trace over existing walls on the floorplan or add new walls, if necessary. Focus on high attenuation walls like concrete or large sections of glass. It is not necessary to incorporate walls and structures that do not fully divide the space, such as half-walls or cubicles.

      Ensure that the wall positioning is as accurate as possible, and define the proper material for each wall. Select a material that most closely represents the actual wall construction if it is different than the available options. Keep your colors consistent for the various wall types. The more accurately the map reflects the true environment, the more precise the wireless location and coverage results are in the map.

To remove a line or shape, select **Select Items** in the **Tool** menu, select the shape, and press **Delete**, or right-click on the shape and select **Remove from Map** from the menu. Use the Ctrl+Z key combination to restore deleted items back to the map. Selecting Ctrl+Z multiple times undoes multiple deleted items in the reverse order in which you deleted them.



e. While editing, use the **View** menu to select whether to view or hide the background image, map cells, floorplan walls and drawings, devices and APs, and interswitch connections. You can also select an automatic layout and set the background image opacity.

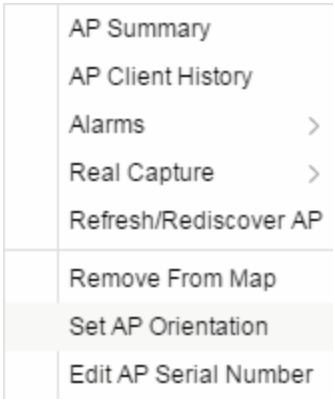


4. **Add your APs to the map.** In Edit mode, a panel that lists equipment available to add to the map is visible beneath the properties panel. The display is filtered on either the currently discovered devices or the APs known to wireless controllers on your network, depending on your selection (APs or Devices) in the panel title bar. You can use the search field to locate a specific device or AP.

   Drag the desired devices and APs onto the map area and position them to produce your network map. Be sure the APs are in the correct location, so your location and coverage maps are accurate. The center of the image is roughly the position of the AP. Be sure to place an AP on the correct side of a wall.



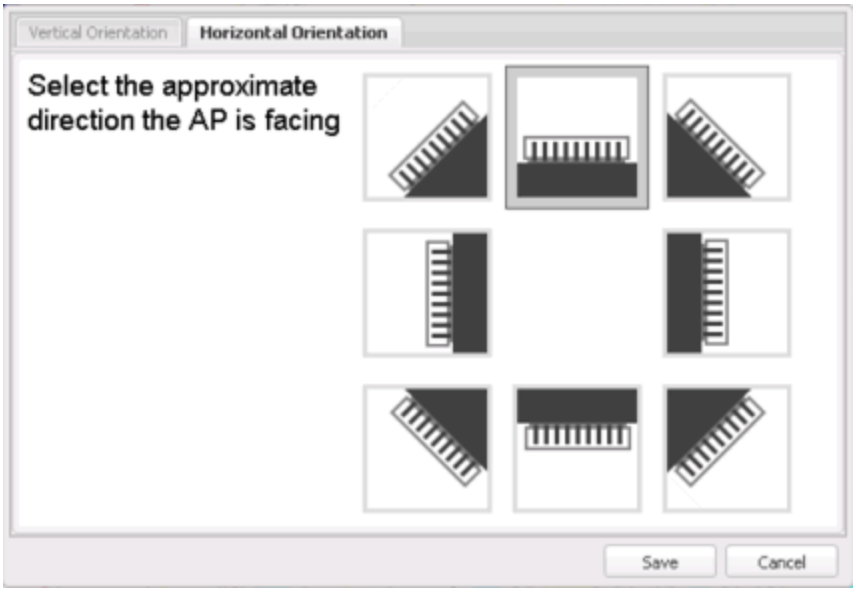
5. Set AP orientation.
   a. Right-click on an AP in the map and select **Set AP Orientation**.



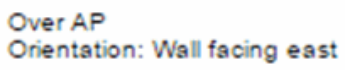
b. Select the **Vertical Orientation** tab to set whether the AP is on the ceiling or wall.



c. If the AP is on a wall, the **Horizontal Orientation** tab appears and allows you to select the approximate direction the AP is facing.



d. Select **Save** to close the window. **TIP:** You can view AP orientation information by mousing over an AP. The AP orientation (if set) is displayed in the bottom right corner of the main map view.



6. Select **Save** to save the map. The floorplan is uploaded to the controllers that manage the access points placed on the map. The map is now ready to display wireless location and wireless coverage information.
7. **Select the desired map view mode.** When viewing a map, use the **View** drop-down list to specify whether to:
    - Display markers instead of device images on your map
    - Display cells on the map image to show the map's actual image area
    - Display AP channel information (if available)
    - Display walls and drawings
    - Show application data for map links (if available)
    - Set the map's background opacity
    - Set the minimum location confidence to filter location confidence colors in triangulated location search results

Drawing Tools

The drawing tools allow you to add lines and shapes to your custom floorplans. The following table includes descriptions of the various drawing tools accessed from the Tool menu.

Drawing Tool	Definition
	**Select Items** Select a line or shape to select it for dragging or modification. Use the yellow drag handle to reposition the item; use the blue vertex to modify the shape. Select anywhere on the map and drag to reposition the map image.
	**Draw Area** Location areas allow you to set policies for clients based on their location on a map. Position your cursor where you want to start drawing an area location. Select and draw the first line of the polygon. Select each corner of the area location. To open the Configure Area window with the Draw Area tool active, double-click the area line. To open the Configure Area window and close the Draw Area tool, right-click the area line.
	**Draw Polygon** Position your cursor where you want to start drawing the polygon shape. Select and draw the first line of the polygon. Select each corner of the polygon. Double-click to release the polygon line. When you are finished drawing, right-click to release the draw polygon tool.

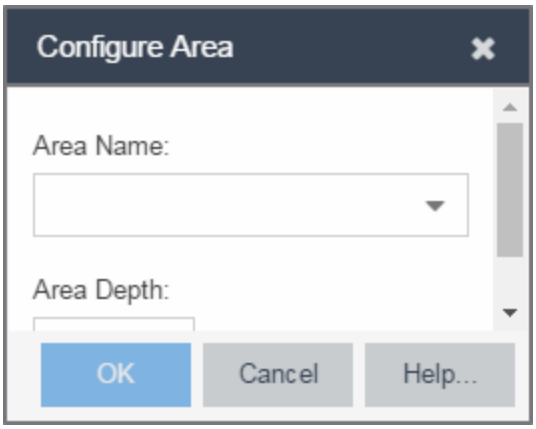
Drawing Tool	Definition
	**Draw Rectangle** Position the cursor where you want the rectangle. Select and drag to draw the rectangle. When you are finished drawing, right-click to release the draw rectangle tool.
	**Add Text** Select the map to open the Enter Text window. When you are finished entering your text, select **OK**. Position the cursor where you want to place the text and select to add the text to your map. Use the **Style** menu to change the text appearance.
	**Draw Triangle** Position the cursor where you want the triangle. Select and drag to draw the triangle. When you are finished drawing, right-click to release the draw triangle tool.
	**Draw Line** Position your cursor where you want to start drawing the line. Select and draw the line. Select to change line direction. While drawing, press the Delete key to delete the last vertex in the line. Double-click to release the line. When you are finished drawing, right-click to release the draw line tool.
	**Rotate Shape** Select the shape you want to rotate. Use the blue handle to rotate the shape to the desired position. (You can also right-click on an image and select Rotate Shape from the menu.)
	**Set Scale** Opens the Set Map Scale window from which you can determine the scale of your map.

Configure Area Window

The Configure Area window, accessible from the Draw Area tool, allows you to name and determine the depth of an area.

- **Area Name** — The name of the area you are creating.
- **Depth** — A unique identifier for the area used when two areas overlap. In the event a client is located in a location shared by two areas, the client displays in the area with the higher **Depth** value.

> **NOTE:** The **Depth** must be a value of 10 or higher. Values of 1 - 9 are reserved by the system.



Area locations allow you to define up to 16 specific areas per floor on your map to determine whether a client position is inside or outside of each area. Additionally, you can create areas located inside of other areas. A client can only be located in one area at a time and based on the area in which the client is located, you can apply different policies to the client. For example, a client accessing the network from an area located in a classroom may be granted different access than a client accessing the network in an area located in a professor's office.

Style Menu

Use the Style menu to define the characteristics of the walls and other shapes you add to your custom floorplans. Following are definitions of the Style menu options.

Style Option	Description
Font Color	Specify the color of the text added to the map.
Font Size	Specify the size of the text added to the map.
Line Thickness	Specify the thickness of the shape border in pixels.
Line Color	Specify the color used in shape borders.
Line Opacity	Specify the opacity of the shape borders. This allows you to shade the floorplan.
Shape Filled	Select the checkbox to fill shapes with the specified shape color.
Shape Color	Select the color used to fill the shapes you create.
Shape Opacity	Specify the opacity of the shape color.

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

How to Add Devices and APs to Maps

Adding Devices/APs from ExtremeCloud IQ Site Engine Devices and Wireless

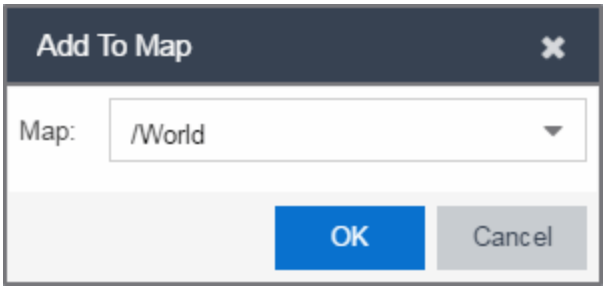
Using the ExtremeCloud IQ Site Engine Maps feature, you can quickly add devices and wireless access points (APs) to your maps directly from the Devices list or from the navigation tree on the ExtremeCloud IQ Site Engine **Network** and **Wireless** tabs. You can add them to a specific map, or create new maps based on device or AP system location.

In order to edit maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

Add to a Specific Map

Use these steps to add devices or APs to a map you created. For example, use these steps to search for all your S-Series devices on the **Network** tab and add them to a map.

1. On the **Network** > **Devices** tab, select **All Devices** in the drop-down list in the left-panel.
2. Right-click on one or more devices and select **Maps** > **Add to Map** (as shown below). On the **Wireless** tab, select on the Access Points report, right-click on one or more APs, and select **Add to Map**.
3. In the Add to Map window, use the drop-down list to select the desired map. Select **OK** to add the devices or APs to the map.



4. Open the Maps page and select the map to which you added the devices. Right-click on the map and select **Edit Map**. You can now position the devices as desired.
5. Select the **Save** button to save the device to the map.

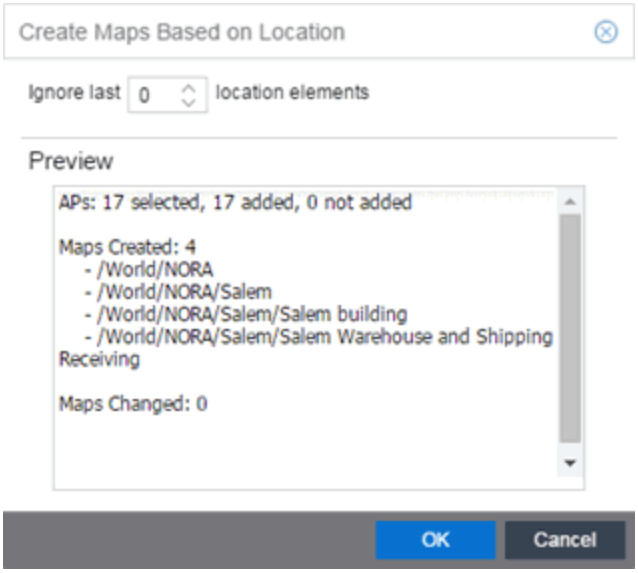
Add to New Maps Based on Location

Use these steps to add devices or APs to new maps based on well-named system locations that reflect the desired map structure. For example, if your devices are assigned system locations according to the following structure: US/Boston/Third Floor/Closet One/Rack One/Shelf One, typically, a map would be

created to the Third Floor level, and then you manually position the devices in the correct location on the map.

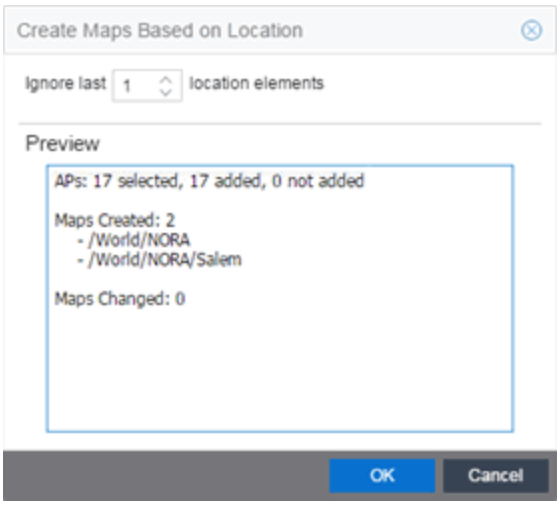
1. On the **Network** > **Devices** tab, right-click on one or more devices and select **Maps** > **Create Maps for Locations**.
   On the **Wireless** tab, select the Access Points report, right-click on one or more APs, and select **Maps** > **Create Maps for Locations**.
2. The Create Maps Based on Location window opens. The window contains a preview panel displaying the number of maps and the map titles that result, based on the system locations of your selected devices or APs.

   For example, as shown in the following screen shot, you are adding 9 APs to a map. This creates eight new maps based on the access points' system location structure: NORA, Salem, Salem building, and Salem Warehouse and Shipping.



   If you want all the devices on one map, set the Location Option to ignore the last 1 location elements, which is the Salem building location. If you do that, then only two maps are created:

NORA and Salem.



3. Select **OK** to create the maps and add the APs.
4. Open the World Site navigation tree in the left-panel and locate the new maps.
5. Right-click on the map and select **Maps** > **Edit Map**. You can now position the APs as desired.
6. Select the **Save** button to save the devices/APs to the map.

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

How to Display Map Application Data

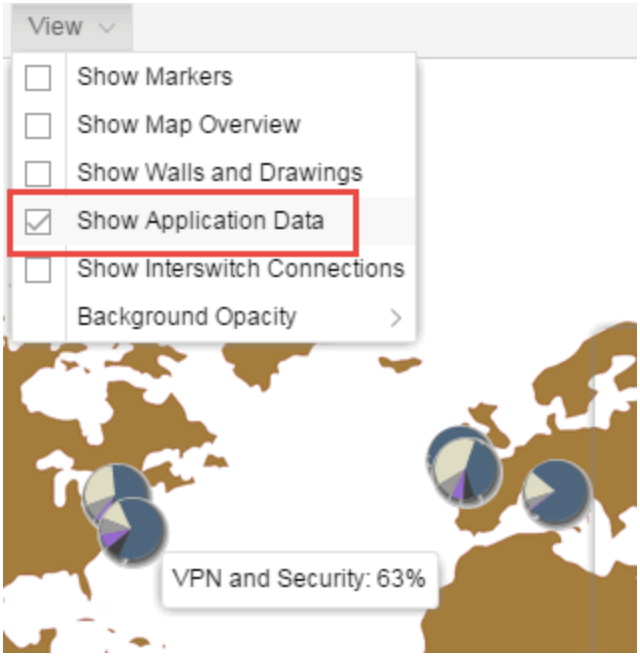
The **Network** > **Devices** tab contains Map features that let you create geographic and topological maps of the devices and floor plans of wireless access points (APs) on your network. The advanced Map features allows you to display application data in maps by creating map links tied to sites. Application data for the site tied to the link displays in the map.

Show Application Data

When the **Show Application Data** checkbox in the **View** menu is selected, a pie chart is generated for every map link on the current map. The application data in the pie chart is based on the **Sites** field specified for the link and corresponds to a network site.

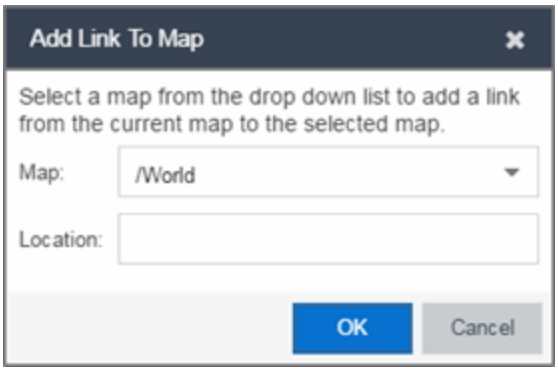
The pie chart displays the top five application groups (by bytes transferred) for the site specified for the map link.

Rest the cursor over the pie chart to view a tooltip. If there is no application data, nothing displays.



Adding a Map Link with Location

1. In the Maps navigation tree, right-click on the map you want to link from and select **Maps** > **Edit Map** or select **File** > **Edit** in the map properties panel.
2. The map's property panel opens in Edit mode. Select **File** > **Add** > **Map Link**.
3. The Add Link to Map window opens.



4. From the drop-down list, select the map to which you want to link.
5. Enter a site and select **OK.**
6. The map link is added to the map. You can reposition the map, if desired, or edit a link by right-clicking on the link (in Edit mode) and selecting **Edit Link** from the menu.
7. Select the **Save** button to save the map.

NOTE: You can edit a map link created before link locations were supported by right-clicking on the link (in Edit mode) and selecting **Edit Link** from the menu. This allows you to specify a location for a link without having to delete and re-add the link.

For information on related topics:

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

How to Use Maps to Locate Wireless Clients

The **Network** > **Devices** tab in the ExtremeCloud IQ Site Enginecontains Map features that let you create geographic and topological maps of the devices and floorplans of wireless access points (APs) on your network.

The advanced map features allow you to design and enhance custom floorplans of your wired and wireless network environment. The wireless location feature provides the ability, using historic triangulated location results, to view time-lapse location coverage for a client. This allows you to understand a wireless client's movement through the network and provides for better network troubleshooting.

This topic also provides information about limits for wireless client location and wireless coverage maps.

Wireless Client Location

The wireless location feature requires you enable the location engine on the wireless controller. After you add APs to your custom floor plan and save the map, a copy of the floorplan is sent to each controller.

The location engine incorporates information defined in the floorplan data and signal information from a client's contact with APs in order to calculate a client's precise location in the covered area. Client information from within a short time frame must be reported by at least three APs in order to determine a client's triangulated location.

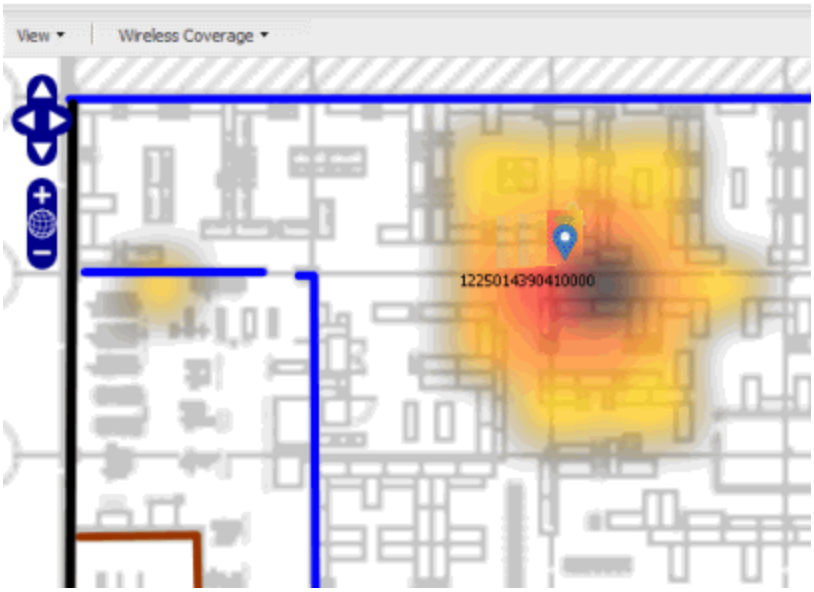
To search for a wireless client:

1. Launch ExtremeCloud IQ Site Engine.
2. In the **SearchNetwork** box, select **Advanced** .
3. Enter the MAC Address, IP Address, hostname, user name, AP serial number or ExtremeControl custom field information in the open **Search** box.
4. Press **Enter**. (The client must be connected to an AP added to a map.)

The map containing the AP is displayed with an icon for the client. A colored distribution of location confidence is shown on the map with black being highest confidence, red medium confidence, and yellow lowest confidence.

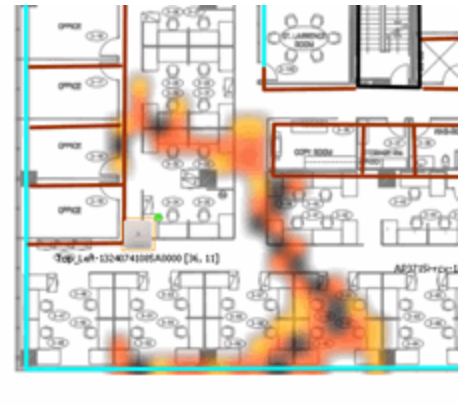
5. On the View tab, use the **Min. Location Confidence** slider to filter out lower confidence colors:
    a. Drag the slider to eliminate colors below the selected confidence level
    b. Drag the slider all the way to the right to display only black.
6. Mouse over the client icon to see a tooltip with client information.

NOTE: The tooltip information is based on current data from the wireless domain unless the client icon displays a clock in the center. In that case, the tooltip information is based on historic data from the **Wireless** > **Clients** tab and the confidence colors are not displayed.

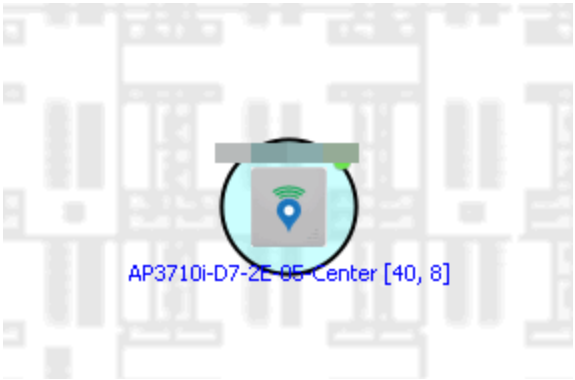


If the location result is based on only one AP, the map displays probabilities for the location but with a few differences:

- No client icon is displayed.
- The location confidence distribution area is larger and generally displayed in a circular pattern.
- The associated AP is highlighted.
- The distance is shown beside the confidence legend at the foot of the map.



If there is insufficient data to provide triangulated results, the map displays the AP in the center, with a circle showing the possible area where the client may be located, based on the client's RSS (Received Signal Strength).



Time-Lapse Location

To enable time-lapse location:

1. Select the Time-Lapse Location checkbox in the upper right corner of the a triangulated location search result window.
2. Locate the set of controls that appears to the left of the checkbox that indicate the date of the displayed result.
3. If there are historic events available, the Rewind and Fast-Forward arrows are enabled:
    a. Select the left arrow to rewind.

b. Select the right arrow to fast-forward.



NOTES: Note that for a historic location, the client icon displays a small clock inside it.

The Rewind and Fast-Forward arrows are disabled if there is no more history in that direction.
After viewing historic locations, if you fast forward to the current location and it changed, the location updates.

Wireless Map Limits

The following sections provide information about limits for wireless client location and wireless coverage maps.

Active Client Tracking

The number of active clients that the location engine on the wireless controller can track simultaneously depends on the wireless controller model. Refer to your wireless controller documentation for information.

Maximum Number of Maps

A wireless controller on which version 10.01.01 or higher is installed can store a maximum of 200 maps. Wireless controllers running a version lower than 10 can store a maximum of 100 maps.

Maximum Number of APs per Floor Plan

A single floor plan allows a maximum of 2,000 APs when version 10.01.01 is installed on the wireless controller. A floor plan with a wireless controller on which a version lower than 10 is installed allows 100 APs.

For information on related topics:

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

How to View Wireless Coverage

The **Network** > **Devices** tab contains Map features that let you create geographic and topological maps of the devices and floor plans of wireless access points (APs) on your network. The advanced Map features include wireless coverage maps to identify coverage trouble spots for your wireless network.

Wireless Coverage

After you finish your custom floor plan and save the map, the map is ready to display wireless coverage information.

1. Select **View** > **Wireless Coverage** > **Show Coverage** to show wireless coverage of the APs on the map and to enable the wireless coverage options.
2. Use the **View** > **Wireless Coverage** menu available at the top of the map to select from the following coverage display options.
    - **Mode** — Select from the different options for coverage display:
        - **Signal Strength**— Use this mode to view AP signal strength. Set the Band, Access Points, and Minimum RSS options.
        - **Channel Coverage** — Use this mode to view channel coverage and AP health. Set the Select Channel, Band, and Access Points options. This mode provides a graphical overview of channel allocation, helping to visualize radio management issues or locate potential interference.
        - **Data Rate** — This mode shows a coverage map indicating the expected physical rate for all of the cells on the floor. Set the Minimum Physical Rate, Band, and

Access Points options. Use this mode to ensure proper wireless performance throughout the network.

NOTE: Wireless coverage maps are divided into cells. Each cell displays a signal strength with which it is associated, used to determine wireless coverage and the location probability of a user.

- **Location Readiness** — Use this mode to view the expected quality of location search results for each map cell, given the current placement of APs. Colors denote readiness for each cell:
  - Green — Good readiness. There are four or more APs with visibility of the cell, with at least three of them within 20 meters.
  - Yellow — Moderate readiness. There are three APs with visibility of the cell, with at least two within 20 meters.
  - Orange — Poor readiness. There are less than three APs with visibility of the cell.
  - Red — No triangulation. Only Cell of Origin location results are available in this area.

- **Select Channel** — Used to select the channels to view for Channel Coverage mode. If "All" is selected, each distinct channel is assigned a color as shown in the legend at the foot of the map, and the color brightness varies to indicate coverage intensity. Selecting a single channel shows a coverage map for that one channel's signal strength and displays a Channel Health window that shows the average and maximum utilization and noise levels for each applicable AP.
  - Utilization — The percentage of busy time for the channel during the last 100 seconds. A channel is busy either because of an interference with energy above a threshold (-62dBm) or because of an active transmission of other stations or APs. This is an indicator of the congestion and interference on the channel.
  - Noise — The noise floor measured by the AP on the 802.11 channel over the last 30 seconds. Noise floor is measured during the quiet time, between the valid transmission or reception of 802.11 frames.
- **Min. Physical Rate** — Used for Data Rate mode to set the minimum physical rate to display. A legend for the Physical Rate by color is visible at the bottom of the map.
- **Band** — Select the desired band (radio frequency).
- **Access Points** — Select which access points to include. These buttons allow you to select or deselect all APs. This option also contains a checkbox that allows you to use default values if a radio is off. When this checkbox is selected, you can view an estimate of coverage using default values; otherwise, no coverage is shown.
- **Minimum RSS** — Used to set the minimum RSS to display (default is -80) for Signal Strength mode. A legend for the RSS by color is visible at the bottom of the map.

Once these options are set, the map displays the selected coverage information. The following map shows signal strength coverage.



Wireless Map Limits

The following sections provide information about limits for wireless client location and wireless coverage maps.

Active Client Tracking

The number of active clients the location engine on the wireless controller can track simultaneously depends on the wireless controller model. Refer to your wireless controller documentation for information.

Maximum Number of Maps

A wireless controller on which version 10.01.01 or higher is installed can store a maximum of 200 maps. Wireless controllers running a version lower than 10 can store a maximum of 100 maps.

Maximum Number of APs per Floor Plan

A single floor plan allows a maximum of 2,000 APs when version 10.01.01 is installed on the wireless controller. A floor plan with a wireless controller on which a version lower than 10 is installed allows 100 APs.

For information on related topics:

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

How to Export Maps

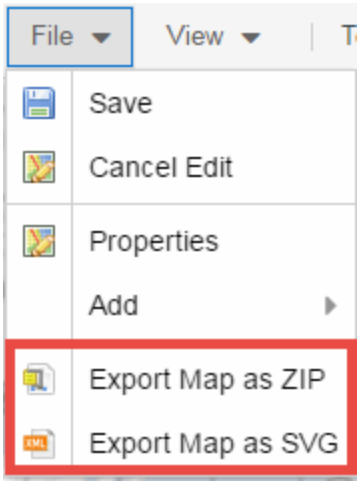
The ExtremeCloud IQ Site Engine Maps lets you import saved maps of devices and wireless access points (APs) from your local drive or network, and configure the behavior of the imported maps.

In order to edit maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

The **Network** > **Devices** tab contains Map features that let you create geographic and topological maps of the devices and floor plans of wireless access points (APs) on your network. The advanced Map features include the map export function, which gives you the ability to export floor plan maps as a ZIP or SVG file.

Exporting Maps

1. Launch ExtremeCloud IQ Site Engine and select the **Network** tab.
2. In the left-panel Maps navigation tree, select the map you want to export.
3. The map opens in Edit mode. Select **File** > **Export Map as ZIP** or **Export Map as SVG**.



- If you select **Export Map as ZIP**, the map is saved in a ZIP file in your browser's default download location.

  NOTE: The Export Map as ZIP option is only available for floorplan map types.

- If you select **Export Map as SVG**, the map opens in a new tab, allowing you to save the map in the desired location.

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

How to Design Floorplans

The **Network** > **Devices** tab contains Map features that let you create geographic and topological maps of the devices and floorplans of wireless access points (APs) on your network. The advanced Map features allow you to design and enhance custom floorplans of your wired and wireless network environment using drawing tools and the style menu.

Designing a Floorplan

Using the drawing and style tools, you can create detailed visual representations of your network. You can also use floorplans to provide greater accuracy in the calculation of AP client location and in determining signal strength coverage for the wireless devices on your network.

NOTE: You can only use an AP in one floorplan.

Managed wireless controllers are automatically synchronized to match map floorplan data. If the floorplan data defined in ExtremeCloud IQ Site Engine maps is not consistent with data on the controller, the controller is updated accordingly.

NOTE: To prevent the automatic synchronization between ExtremeCloud IQ Site Engine maps and controllers, go to the **Administration** > **Diagnostics** tab, access System > Map Server Details from the left-panel and select the **Do Not Upload Maps** checkbox. Selecting this checkbox also prevents manually triggered map changes from being uploaded to a controller.

In floorplan design, use the map drawing tools to draw walls (or other objects) over an existing map image or on a blank canvas. The Style menu allows you to specify wall thickness, color, and wall materials.

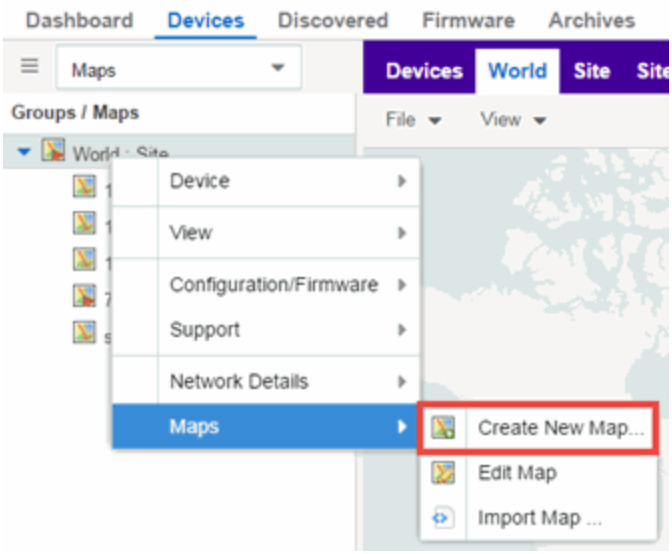
The wall information from the floorplan is used to help determine the degradation of signal strength that occurs as a wireless radio signal passes through the walls, and helps define the probable distance of a client from a given access point. ExtremeCloud IQ Site Engine uses the wall information to provide accuracy in determining wireless device signal strength.

A floorplan can be created with or without a reference background image; however it is much easier to use the drawing features with an existing image. (The Map feature supports images in PNG, GIF, and JPG (without transparency) formats.) For example, you can trace the outline of a floorplan image using the drawing tools to provide the wall information used for wireless calculations. You can use the Style and Wall menus to specify different wall material types, wall thicknesses, and wall colors to customize the appearance of the floorplan.

When editing a floorplan, use the View menu to select whether to view or hide the background image, map cells, floorplan walls and drawings, devices and APs, and interswitch connections. You can also set the background image opacity.

The following steps provide a workflow for creating a floorplan showing the exterior and interior walls of a building. By drawing the walls over an existing floorplan image, you can add information that provides greater accuracy in wireless calculations.

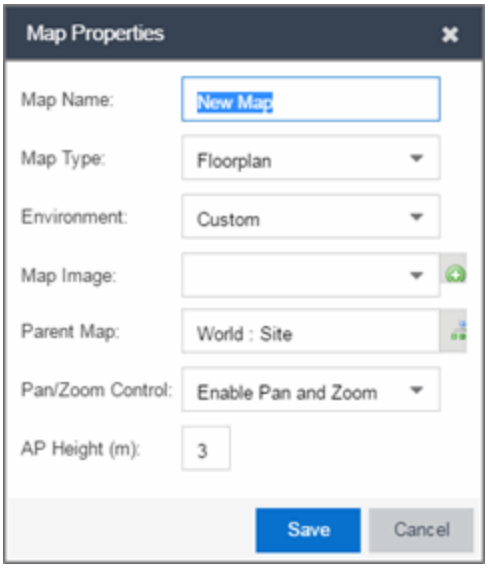
1. **Create and configure a new map.**
    a. Launch ExtremeCloud IQ Site Engine and select the **Network** > **Devices** tab.
    b. In the left-panel Groups/Maps navigation tree, right-click on the World map (or any other map that you want as the parent of the new map) and select **Maps** > **Create New Map**.



The Create New Map window opens.

c. Enter a name for the Map.

d. Open the Map Properties window by selecting **File** > **Properties**.



e. Change the **Map Type** drop-down list to **Floorplan**.

f. Set the **Environment** option to **Custom**. This allows you to draw walls over the existing image.

g. Upload the floorplan image you want to use in the **Map Image** field. The Map feature supports images in PNG, GIF, and JPG (without transparency) formats. The maximum

image size is 3000 x 2000 pixels. Images that are larger than this are automatically scaled down to the maximum size allowed.

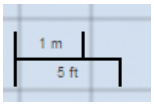
h. Set the **AP Height** property. This value is the distance from the floor to the AP position on the wall or ceiling in meters. This is a single value used for all access points. Setting a reasonable value helps with the accuracy of the location feature. The default for this value is three meters, which is at the top of a wall with a nine foot ceiling.

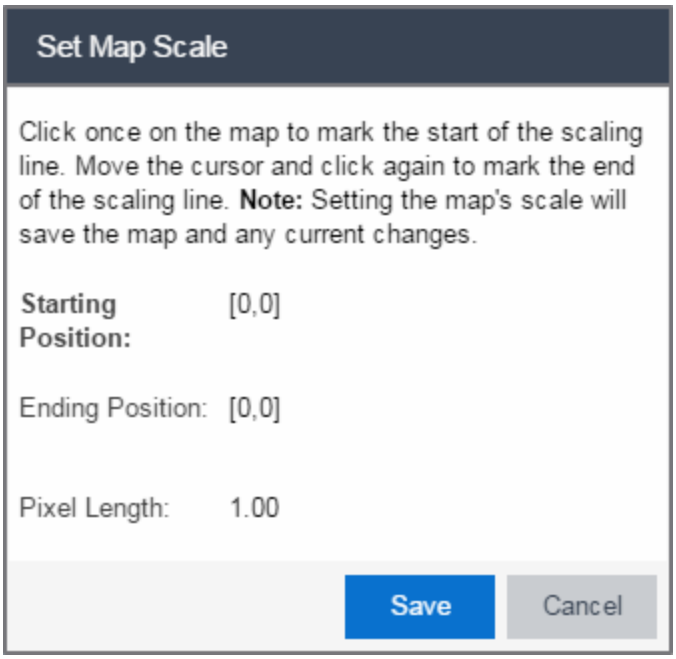
i. Select **Save** to save the map and display the image.

2. **Set the map scale.** It is important to set the scale before adding devices or walls, since changing the scale later may cause the object positions to be realigned. Try to make the scale as accurate as possible, as this affects triangulation accuracy.

   a. Select **File** > **Edit** to open the map in edit mode.

   b. Select the map scale in the map's footer panel to open the Set Map Scale window. (You can also access the Set Map Scale window from the Tools menu.)





   c. To set the scale, you must measure something in the map using a scaling line, and then set the measurement for the line. For example, in an office floorplan you could measure a scaling line on the opening of an office. If you know that the office doors are 33 inches wide, enter that as the scaling line measurement.

i. Select on the map to mark the start of the scaling line. Move the cursor and select again to mark the end of the scaling line.

ii. Enter the line length and units.

d. Select **OK**. The map scale is automatically adjusted and the map is saved.

3. **Draw floorplan walls.** Select the **Edit** button to open the map in edit mode. By default you see a grid of cells displayed over the background image. (It can be turned off in the **View** menu.) This grid can help with positioning walls and access points. Add walls to the floorplan using the drawing tools accessed from the **Tools** menu (at the upper left corner of the Map main view).

   a. Define an exterior wall. The exterior wall is used to define the floorplan area included in wireless client location and wireless coverage maps, and should be drawn around the entire perimeter of the floorplan area, without any gaps.

   b. Select the appropriate drawing tool from the **Tools** menu. Use the Style menu to configure the wall color, thickness, and transparency. Select the wall material using the Wall drop-down list and select the checkbox to specify that the wall is an exterior wall.



   c. Draw the exterior wall using the selected drawing tool. You can double-click or hit **Escape** to terminate the drawing.

   d. Use these same steps to draw the remaining walls on your floorplan. Be sure to deselect the **Exterior** checkbox for the other walls.

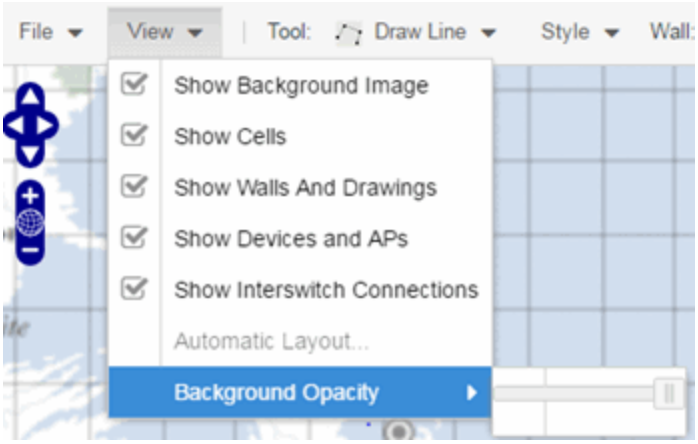
      You can trace over existing walls on the floorplan or add new walls, if necessary. Focus on high attenuation walls like concrete or large sections of glass. It is not necessary to incorporate walls and structures that do not fully divide the space, such as half-walls or cubicles.

      Ensure that the wall positioning is as accurate as possible, and define the proper material for each wall. Select a material that most closely represents the actual wall construction if it is different than the available options. Keep your colors consistent for the various wall types. The more accurately the map reflects the true environment, the more precise the wireless location and coverage results are in the map.

To remove a line or shape, select **Select Items** in the **Tool** menu, select the shape, and press **Delete**, or right-click on the shape and select **Remove from Map** from the menu. Use the Ctrl+Z key combination to restore deleted items back to the map. Selecting Ctrl+Z multiple times undoes multiple deleted items in the reverse order in which you deleted them.



e. While editing, use the **View** menu to select whether to view or hide the background image, map cells, floorplan walls and drawings, devices and APs, and interswitch connections. You can also select an automatic layout and set the background image opacity.

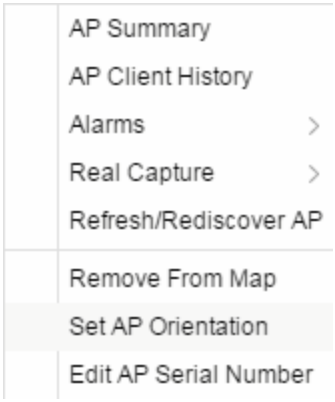


4. **Add your APs to the map.** In Edit mode, a panel that lists equipment available to add to the map is visible beneath the properties panel. The display is filtered on either the currently discovered devices or the APs known to wireless controllers on your network, depending on your selection (APs or Devices) in the panel title bar. You can use the search field to locate a specific device or AP.

   Drag the desired devices and APs onto the map area and position them to produce your network map. Be sure the APs are in the correct location, so your location and coverage maps are accurate. The center of the image is roughly the position of the AP. Be sure to place an AP on the correct side of a wall.



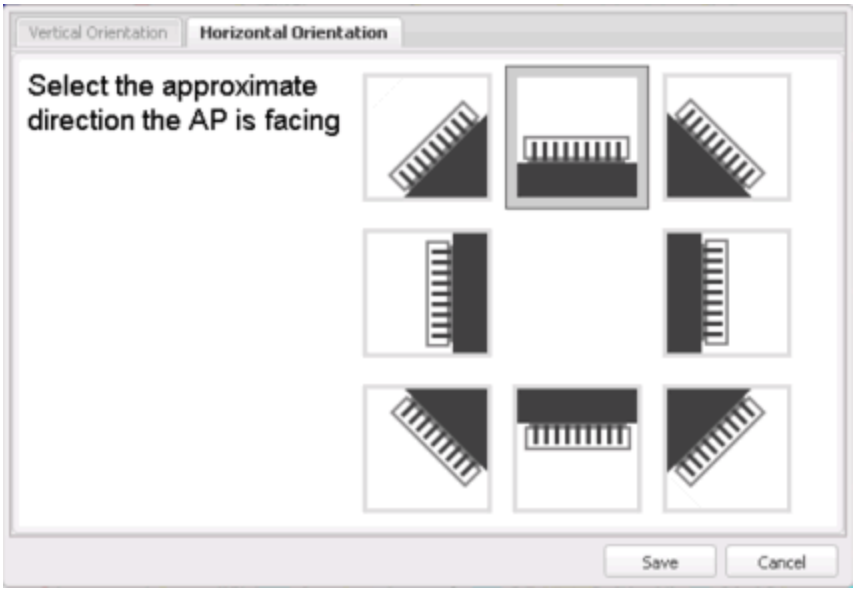
5. Set AP orientation.
   a. Right-click on an AP in the map and select **Set AP Orientation**.



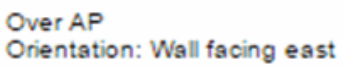
b. Select the **Vertical Orientation** tab to set whether the AP is on the ceiling or wall.



c. If the AP is on a wall, the **Horizontal Orientation** tab appears and allows you to select the approximate direction the AP is facing.



d. Select **Save** to close the window. **TIP:** You can view AP orientation information by mousing over an AP. The AP orientation (if set) is displayed in the bottom right corner of the main map view.



6. Select **Save** to save the map. The floorplan is uploaded to the controllers that manage the access points placed on the map. The map is now ready to display wireless location and wireless coverage information.
7. **Select the desired map view mode.** When viewing a map, use the **View** drop-down list to specify whether to:
    - Display markers instead of device images on your map
    - Display cells on the map image to show the map's actual image area
    - Display AP channel information (if available)
    - Display walls and drawings
    - Show application data for map links (if available)
    - Set the map's background opacity
    - Set the minimum location confidence to filter location confidence colors in triangulated location search results

Drawing Tools

The drawing tools allow you to add lines and shapes to your custom floorplans. The following table includes descriptions of the various drawing tools accessed from the Tool menu.

Drawing Tool	Definition
	**Select Items** Select a line or shape to select it for dragging or modification. Use the yellow drag handle to reposition the item; use the blue vertex to modify the shape. Select anywhere on the map and drag to reposition the map image.
	**Draw Area** Location areas allow you to set policies for clients based on their location on a map. Position your cursor where you want to start drawing an area location. Select and draw the first line of the polygon. Select each corner of the area location. To open the Configure Area window with the Draw Area tool active, double-click the area line. To open the Configure Area window and close the Draw Area tool, right-click the area line.
	**Draw Polygon** Position your cursor where you want to start drawing the polygon shape. Select and draw the first line of the polygon. Select each corner of the polygon. Double-click to release the polygon line. When you are finished drawing, right-click to release the draw polygon tool.

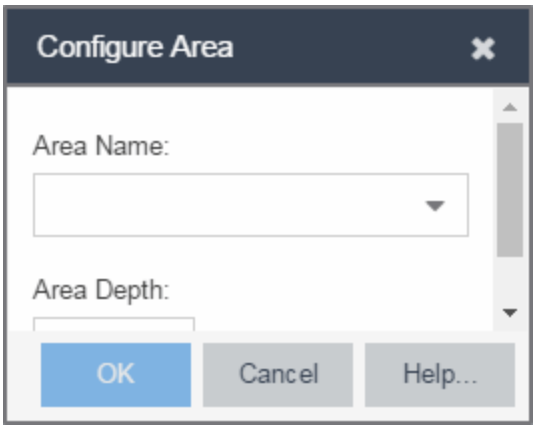
Drawing Tool	Definition
	**Draw Rectangle** Position the cursor where you want the rectangle. Select and drag to draw the rectangle. When you are finished drawing, right-click to release the draw rectangle tool.
	**Add Text** Select the map to open the Enter Text window. When you are finished entering your text, select **OK**. Position the cursor where you want to place the text and select to add the text to your map. Use the **Style** menu to change the text appearance.
	**Draw Triangle** Position the cursor where you want the triangle. Select and drag to draw the triangle. When you are finished drawing, right-click to release the draw triangle tool.
	**Draw Line** Position your cursor where you want to start drawing the line. Select and draw the line. Select to change line direction. While drawing, press the Delete key to delete the last vertex in the line. Double-click to release the line. When you are finished drawing, right-click to release the draw line tool.
	**Rotate Shape** Select the shape you want to rotate. Use the blue handle to rotate the shape to the desired position. (You can also right-click on an image and select Rotate Shape from the menu.)
	**Set Scale** Opens the Set Map Scale window from which you can determine the scale of your map.

Configure Area Window

The Configure Area window, accessible from the Draw Area tool, allows you to name and determine the depth of an area.

- **Area Name** — The name of the area you are creating.
- **Depth** — A unique identifier for the area used when two areas overlap. In the event a client is located in a location shared by two areas, the client displays in the area with the higher **Depth** value.

> **NOTE:** The **Depth** must be a value of 10 or higher. Values of 1 - 9 are reserved by the system.



Area locations allow you to define up to 16 specific areas per floor on your map to determine whether a client position is inside or outside of each area. Additionally, you can create areas located inside of other areas. A client can only be located in one area at a time and based on the area in which the client is located, you can apply different policies to the client. For example, a client accessing the network from an area located in a classroom may be granted different access than a client accessing the network in an area located in a professor's office.

Style Menu

Use the Style menu to define the characteristics of the walls and other shapes you add to your custom floorplans. Following are definitions of the Style menu options.

Style Option	Description
Font Color	Specify the color of the text added to the map.
Font Size	Specify the size of the text added to the map.
Line Thickness	Specify the thickness of the shape border in pixels.
Line Color	Specify the color used in shape borders.
Line Opacity	Specify the opacity of the shape borders. This allows you to shade the floorplan.
Shape Filled	Select the checkbox to fill shapes with the specified shape color.
Shape Color	Select the color used to fill the shapes you create.
Shape Opacity	Specify the opacity of the shape color.

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

How to Export Maps

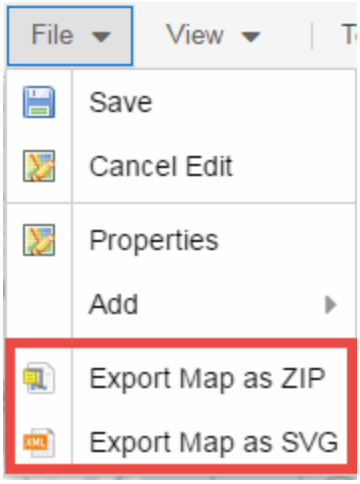
The ExtremeCloud IQ Site Engine Maps lets you import saved maps of devices and wireless access points (APs) from your local drive or network, and configure the behavior of the imported maps.

In order to edit maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

The **Network** > **Devices** tab contains Map features that let you create geographic and topological maps of the devices and floor plans of wireless access points (APs) on your network. The advanced Map features include the map export function, which gives you the ability to export floor plan maps as a ZIP or SVG file.

Exporting Maps

1. Launch ExtremeCloud IQ Site Engine and select the **Network** tab.
2. In the left-panel Maps navigation tree, select the map you want to export.
3. The map opens in Edit mode. Select **File** > **Export Map as ZIP** or **Export Map as SVG**.



   - If you select **Export Map as ZIP**, the map is saved in a ZIP file in your browser's default download location.

     NOTE: The Export Map as ZIP option is only available for floorplan map types.

   - If you select **Export Map as SVG**, the map opens in a new tab, allowing you to save the map in the desired location.

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

Network Details

The ExtremeCloud IQ Site Engine Map Tab gives you access to a number of powerful tools that will allow you to create, view, import, edit and search maps of devices and floor plans of wireless access points (APs) on your network. Maps are configured in various places on the **Network** > **Devices** tab.

The Network Details section, available in topology and geographic maps, gives you access to information about links, LANS, ports, and switches in your map network. The **EAPS tab** allows you to access information about any devices configured with Extreme's Ethernet Automatic Protection Switching feature.

To view or search maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read Access or Maps Read/Write Access capability.

To access maps of your devices:

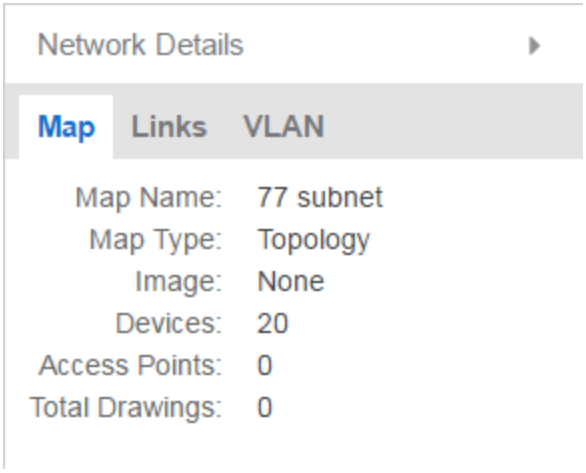
1. Launch ExtremeCloud IQ Site Engine.
2. Select the **Network** > **Devices** tab.
3. Select **Sites** from the left-panel drop-down list. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.
4. Expand a site from the left-panel tree to display the maps on that site.
5. Select a map to open the Map Name tab in the right panel.

Accessing Network Details

1. Right-click the map or map tree in the left-panel.
2. Select **Network Details** from the drop-down list. Several additional tabs are available, depending on the devices included in the map:
    a. EAPS Summary tab — Lists information about any devices configured with Extreme's Ethernet Automatic Protection Switching feature.
    b. Link Summary tab — Displays information about the network connections between devices
    c. VLAN Summary tab — Lists any virtual local area networks within the map
    d. MLAG Summary tab — Lists devices configured in a multi-switch link aggregation group
    e. VPLS Summary tab — Displays information about site connectivity within a private VLAN
    f. Extended Bridges tab — Displays the extended bridges within the map

NOTE: For an alternate way to access the additional tabs:

1. Select **Network > Devices**
2. Select the second tab of the open **Devices** window, which is the **Map Tab** for the map you selected.
3. The **Network Details** panel at the far right. The panel also includes a Map tab that displays basic information about the map, including the name of the map, the map type, and the background image, as well as the number of devices, APs, and drawings on the map.



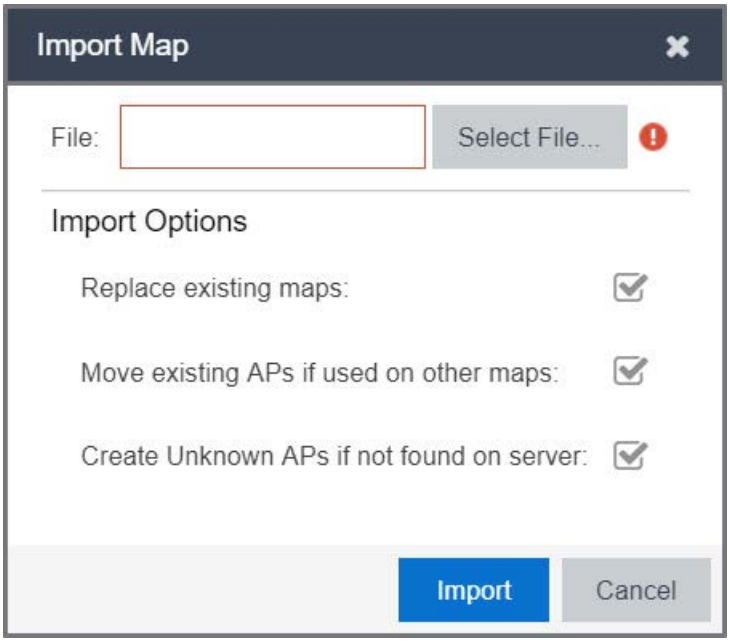
For information on related topics:

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

Import Map

Use this window to import a saved map. From this window you can navigate to a saved map file and configure the behavior of the imported map.

Access this window by right-clicking a map in the Groups/Maps Navigation Tree left-panel on the **Network** > **Devices** tab, and selecting **Maps** > **Import Map**.



File

The file path to the saved map file. Select the **Select File** button to navigate to the file on your local drive or network.

Import Options

The Import Options section determines the behavior of APs on the map being imported.

Replace existing maps

When this checkbox is selected, maps you import replace existing maps with the same name currently in ExtremeCloud IQ Site Engine.

Move existing APs if used on other maps

Select this checkbox to move APs currently located on another map in ExtremeCloud IQ Site Engine to the map being imported.

Create Unknown APs if not found on server

When this checkbox is selected, APs located on the map being imported not found on the ExtremeCloud IQ Site Engine server are created as unknown APs.

EAPS

The EAPS tab allows you to access information about any devices configured with Extreme's Ethernet Automatic Protection Switching feature.

Accessing Network Details

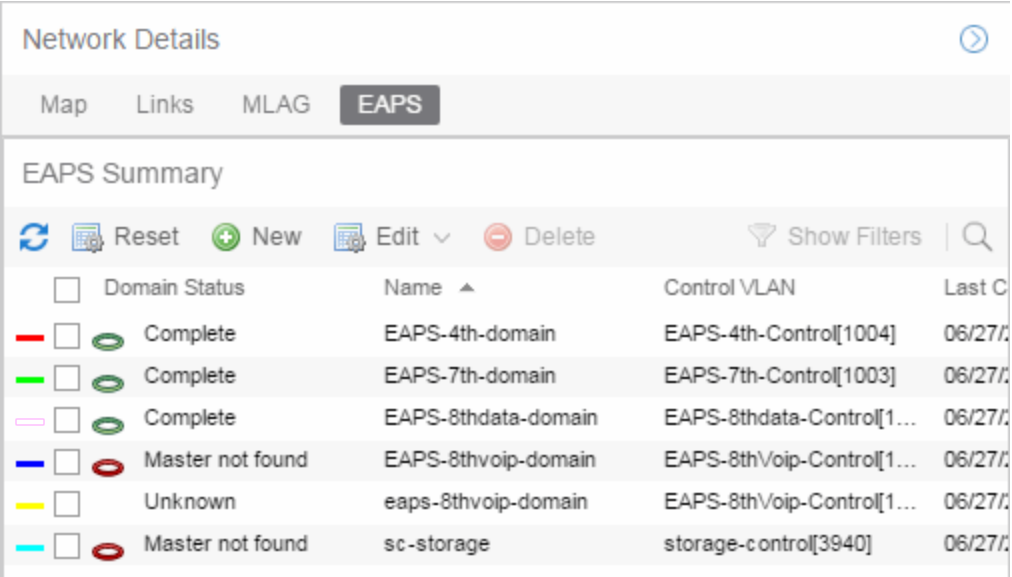
1. Right-click a map or map tree in the left-panel.
2. Select **Network Details** from the drop-down list.
3. Select **EAPS Summary.**

NOTE: For an alternate way to access the EAPS Summary tab:

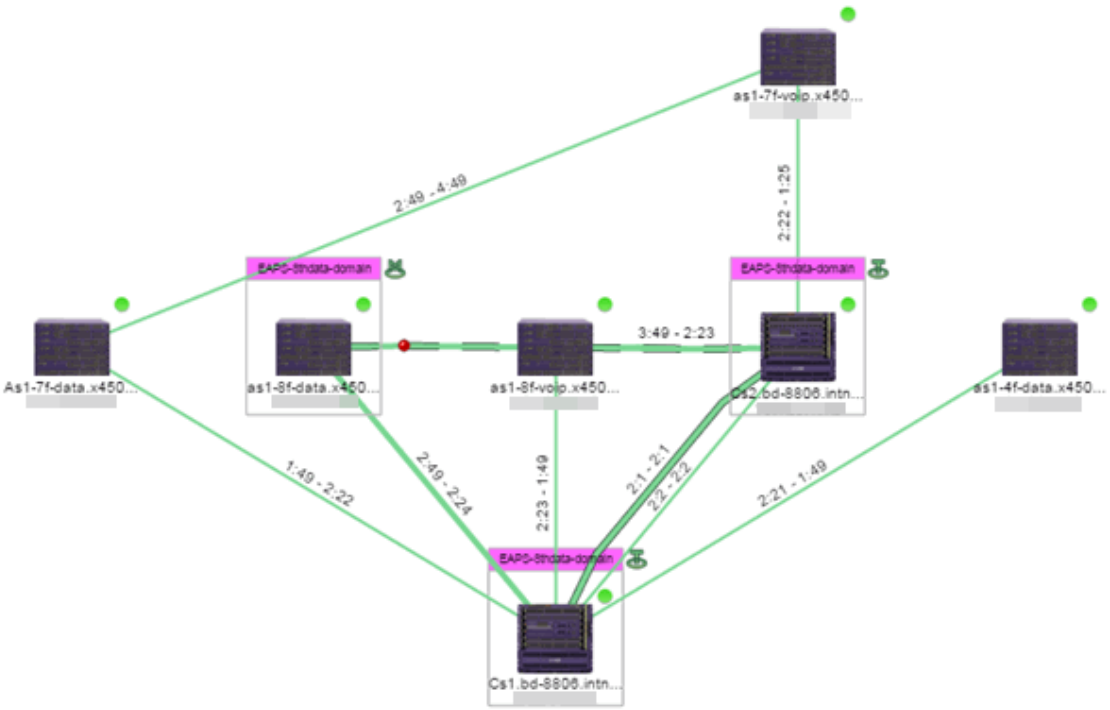
1. Select **Network > Devices**.
2. Select the second tab of the open **Devices** window, which is the **Map Tab** for the map you selected.
3. The **EAPS** tab will be included in the **Network Details** panel at the far right of the open **Devices** window.

EAPS Summary Tab

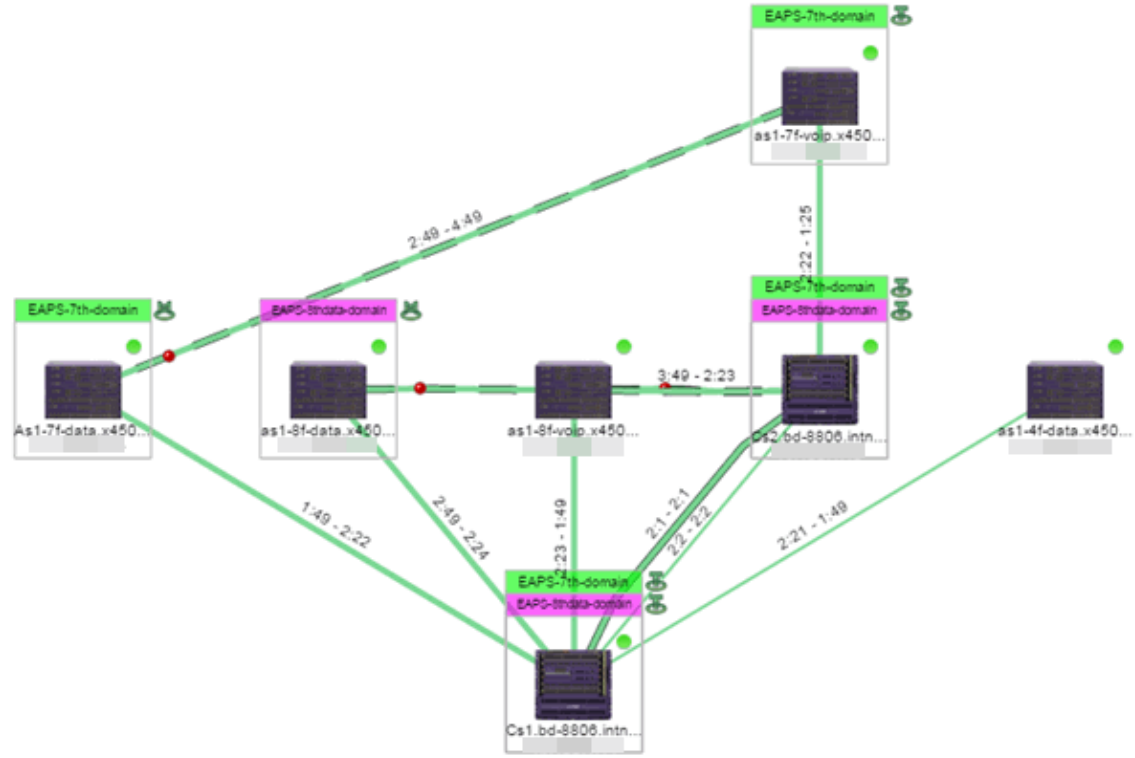
The EAPS Summary tab displays a list of the EAPS domains, including their status, name, the control VLAN name, and the IP addresses of the devices utilizing the EAPS domain.



Selecting the checkbox associated with an EAPS domain highlights any devices containing ports associated with the EAPS domain by surrounding the device in a box with a color-coded title bar containing the EAPS name.



Selecting multiple EAPS domains assigned to the same device adds a new title bar to the box containing the EAPS name and associated color.



An icon next to the title bar indicates if the node is a master node, indicated by an "M" icon , or if the node is a transit node, indicated by a "T" icon .

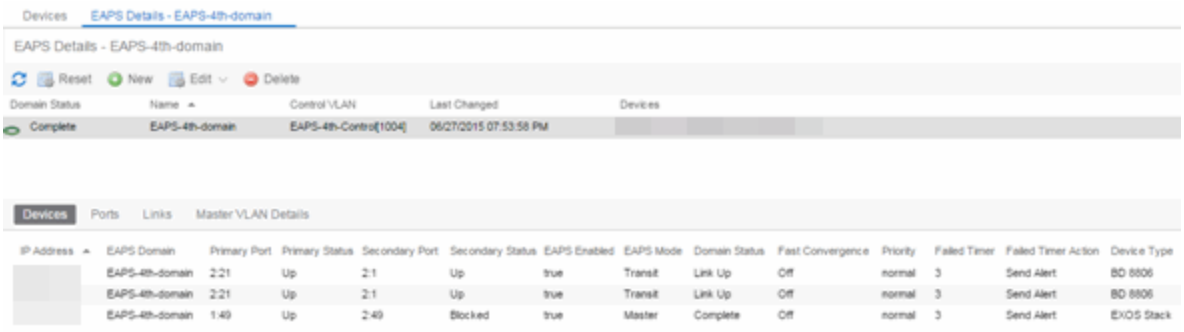
The color of the ring icon indicates the status of the domain:

- Green — Indicates all domains in which this device participates are fully operational
- Yellow — Indicates one or more of the domains is not fully operational, but is in a transitional state or an unknown state (as when the device is SNMP unreachable)
- Red — Indicates one or more of the domains is not operational (the device's master domain is in a failed state or a transit node is in a "links down" state)
- Grey — Indicates the EAPS domain is disabled

When selecting an EAPS domain, link information is also displayed. A single green line means a link that is not shared, while a dashed line between devices means the link is shared. A red dot icon on a shared link indicates the secondary link is blocked.

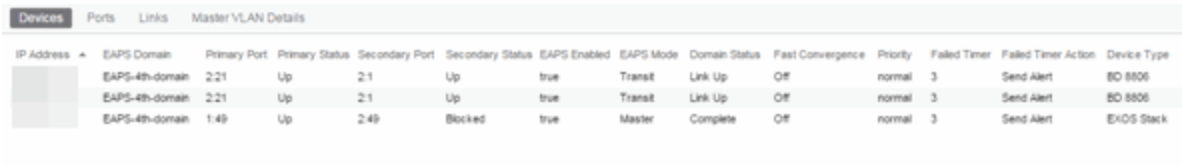


You can view additional details about the EAPS domain by right-clicking an EAPS domain on the **EAPS** tab and selecting **EAPS Details** to open the EAPS Detail view.

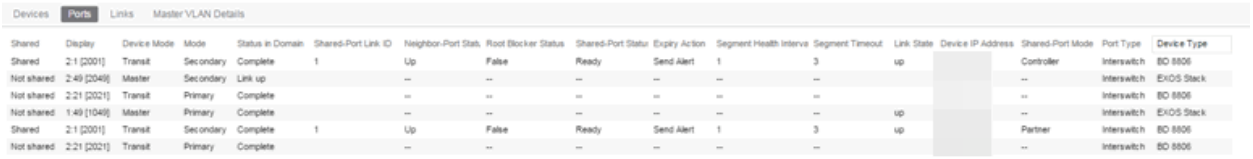


The top of the EAPS Details view displays a summary of the EAPS domain, identical to the information displayed in the **EAPS** tab. At the bottom of the window are three sub-tabs, which display additional information:

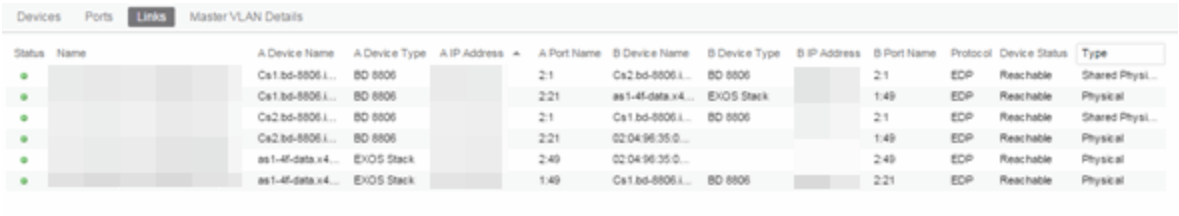
- **Devices** — Displays information about the devices using the EAPS domain.



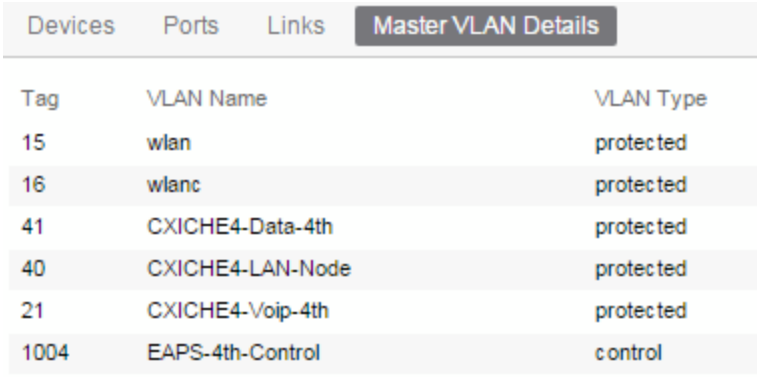
- **Ports** — Displays information about the shared ports associated with the EAPS domain.



- **Links** — Displays links between devices using the EAPS domain.



- **Master VLAN Details** — Displays details about the master VLAN associated with the EAPS domain.



Selecting the **New EAPS Domain** button opens the New EAPS Domain wizard, which allows you to create a create a new EAPS Domain.

For information on related topics:

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

Links

The **Links** tab displays information about the network connections between devices.

Accessing Network Details

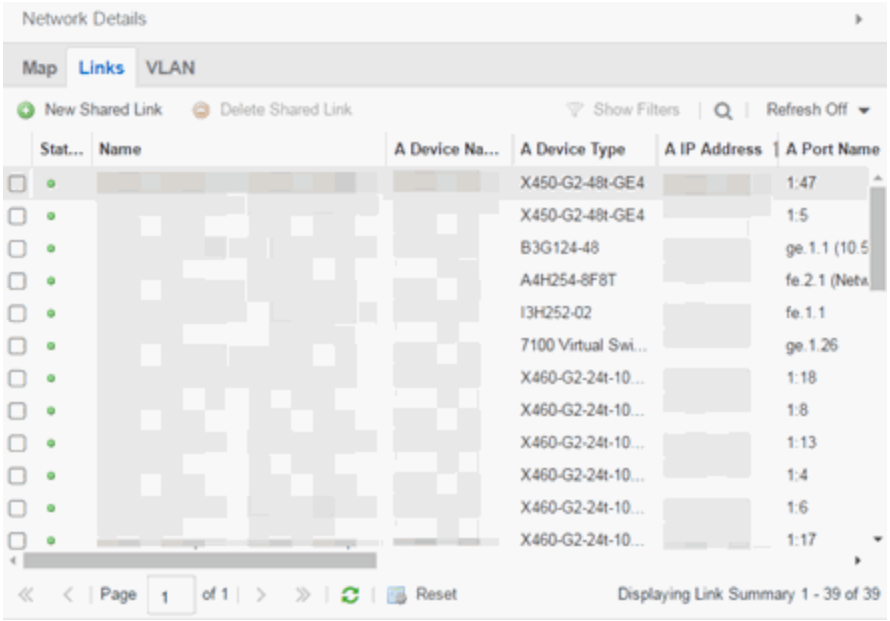
1. Right-click a map or map tree in the left-panel.
2. Select **Network Details** from the drop-down list.
3. Select **Links**.

NOTE: For an alternate way to access the Link Summary tab:

1. Select **Network > Devices**.
2. Select the second tab of the open **Devices** window, which is the **Map Tab** for the map you selected.
3. The **Links** tab will be included in the **Network Details** panel at the far right of the open **Devices** window.

Links tab

The **Links** tab displays the Links table for maps with one or more network connections, which contains detailed information about the network connections between devices. Selecting one of the links in the table highlights the link in the map.



The top of the **Links** tab contains a search field, which allows you to find a particular Link by entering specific criteria. Additionally, you can manually browse links using the scroll bar and page navigation at the bottom of the section.

The top of the window displays information about the link, while information about the devices it connects are contained on two tabs, Endpoint 1 and Endpoint 2.

For information on related topics:

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

VLAN

The **VLAN tab** Lists any virtual local area networks within the map.

Accessing Network Details

1. Right-click a map or map tree in the left-panel.
2. Select **Network Details** from the drop-down list.

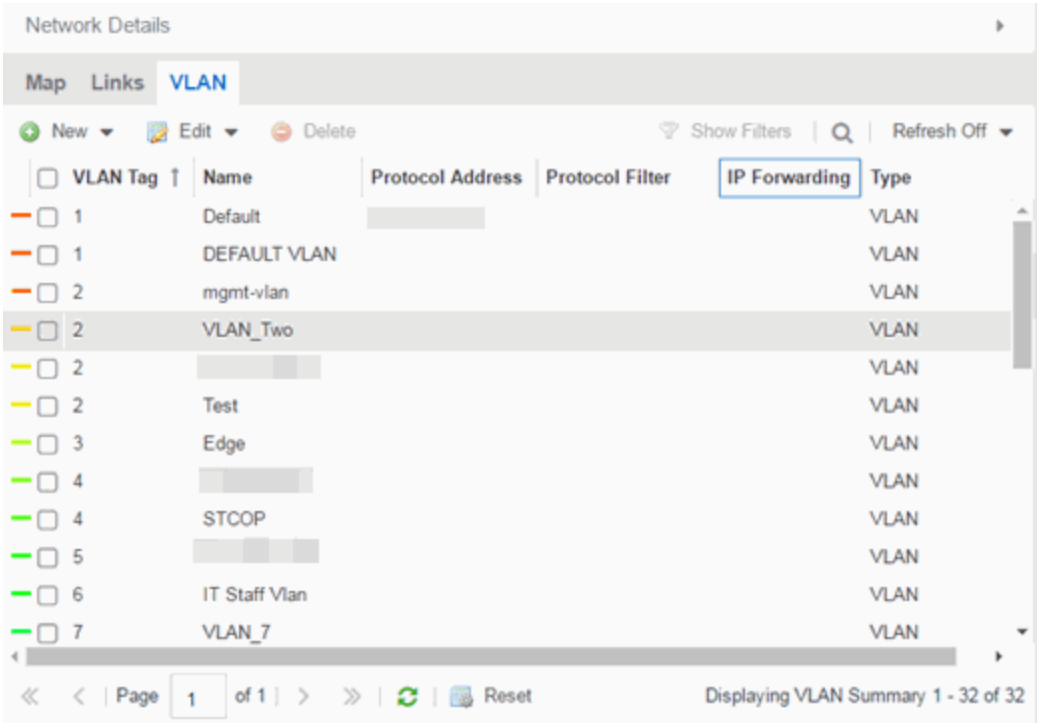
3. Select **VLAN Summary**.

NOTE: For an alternate way to access the VLAN Summary tab:

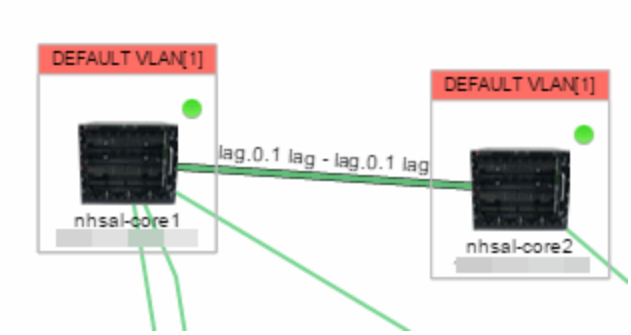
1. Select **Network > Devices**.
2. Select the second tab of the open **Devices** window, which is the **Map Tab** for the map you selected.
3. The **VLAN** tab will be included in the **Network Details** panel at the far right of the open **Devices** window.

VLAN Summary tab

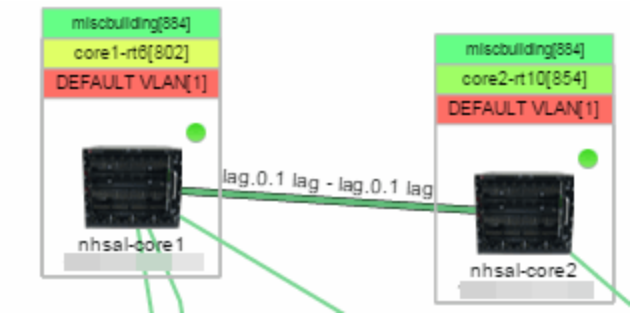
The VLAN Summary tab displays VLANs configured as part of devices included in the map. Columns in the VLAN tab provide additional information, including the VLAN tag, the name of the VLAN, any protocol filters applied for devices on which the VLAN is configured, and whether or not IP forwarding is enabled for the VLAN.



Selecting the checkbox associated with a VLAN highlights any devices to which that VLAN is assigned by surrounding the device in a box with a color-coded title bar containing the VLAN name.



Selecting multiple VLANs assigned to the same device adds a new title bar to the box that displays the VLAN name and associated color.



Additionally, from the **VLAN** tab, you can create a new VLAN or create a VLAN protected by an EAPS domain via the **New** drop-down list. You can edit the ports, name, and devices associated with an existing VLAN via the **Edit** drop-down list.

For information on related topics:

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

MLAG

The **MLAG** tab lists devices configured in a multi-switch link aggregation group.

Accessing Network Details

1. Right-click a map or map tree in the left-panel.
2. Select **Network Details** from the drop-down list.
3. Select **MLAG Summary**.

NOTE: For an alternate way to access the MLAG Summary tab:

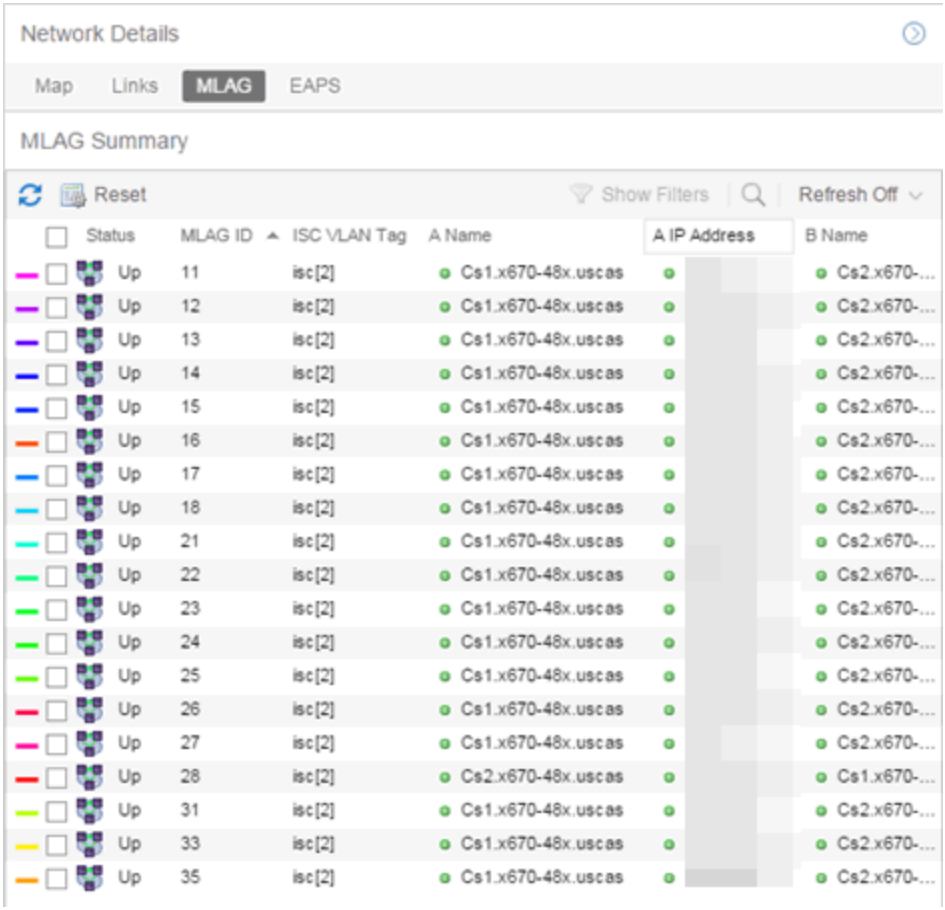
1. Select **Network > Devices**.
2. Select the second tab of the open **Devices** window, which is the **Map Tab** for the map you selected.
3. The **MLAG** tab will be included in the **Network Details** panel at the far right of the open **Devices** window.

MLAG Summary tab

The **MLAG** Summary tab provides a list of the MLAGs (ports combined as a common logical connection on devices) included in the map.

The **MLAG** Summary tab provides a list of the MLAGs (ports combined as a common logical connection on devices) included in the map. The list provides the MLAG's status, ID, ISC VLAN tag, the names and addresses of the devices configured as part of the MLAG, and the ports on those devices assigned as part of the MLAG. Additionally, the Connected IP column displays the IP of the switch to which the MLAG is connected.

NOTE: One-armed MLAGs, which may be utilized in a VPEX Ring topology, will normally display an MLAG port on only one of the devices.



The following columns are included in the MLAG Summary table:

Status

Displays the status of ISC links and MLAG ports:

- **Up** — All ISC links are up and all MLAG ports are up.
- **Degraded** — One or more ISC links are down and all MLAG ports are up, or one or more ISC links are down and one or more MLAGs are down.
- **Protecting** — All ISC links are up and one or more MLAG ports are down.
- **Unprotected** — All ISC links are down and all MLAG ports are up, or all ISC links are down and one or more MLAG ports are down.
- **Down** — All ISC links are down and all MLAG ports are down, or all ISC links are up and all MLAG ports are down, or one or more ISC links are down and all MLAG ports are down.
- **Unknown** — MLAG is only configured on one side of the MLAG paired devices (regardless of whether any or all ISC links are up or down).

ID

The ID number assigned to the port

ISC VLAN Tag

Displays the ISC VLAN tag assigned to the port.

Name

Name of the devices configured as part of the MLAG.

IP Address

IP address of the devices configured as part of the MLAG.

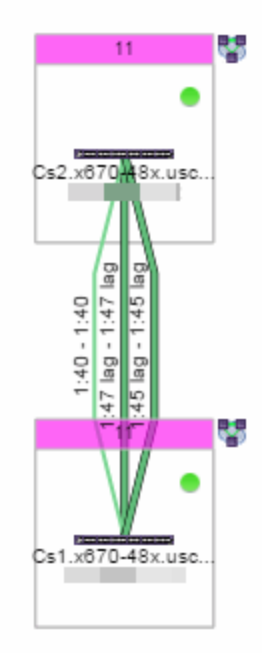
Ports

Lists the ports on those devices assigned as part of the MLAG.

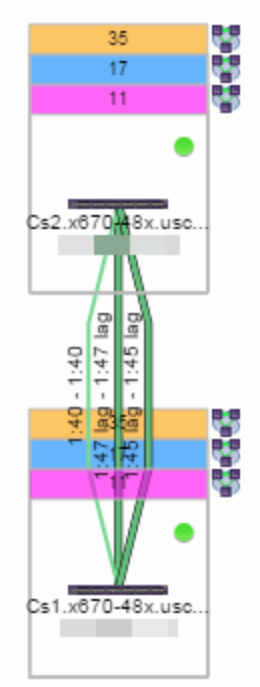
Connected IP

Displays the IP of the switch to which the MLAG is connected.

Selecting the checkbox associated with an MLAG highlights any devices containing ports associated with the MLAG by surrounding the device in a box with a color-coded title bar containing the MLAG ID.



Selecting multiple MLAGs assigned to the same device adds a new title bar to the box containing the VLAN name and associated color.



For information on related topics:

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

VPLS

The VPLS tab displays information about site connectivity within a private VLAN.

Accessing Network Details

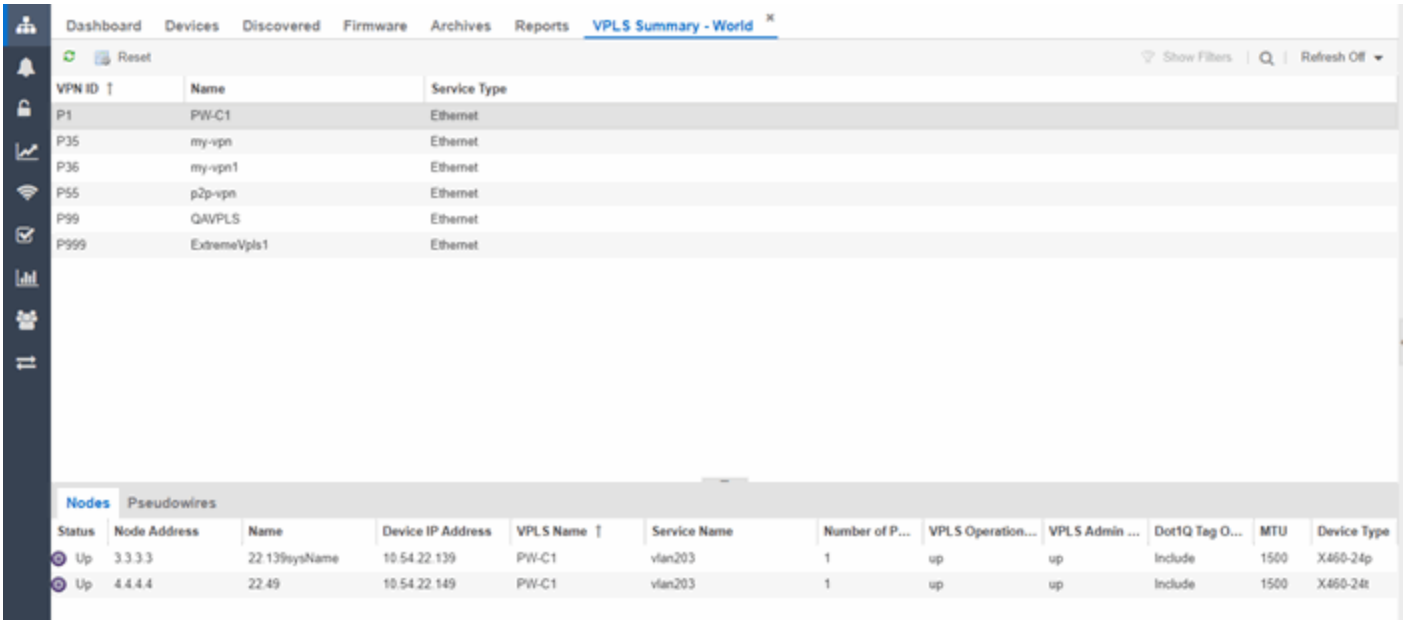
1. Right-click a map or map tree in the left-panel.
2. Select Network Details from the drop-down list.
3. Select **VPLS Summary**.

NOTE: For an alternate way to access the VPLS Summary tab:

1. Select **Network > Devices**.
2. Select the second tab of the open **Devices** window, which is the **Map Tab** for the map you selected.
3. The **VPLS** tab will be included in the **Network Details** panel at the far right of the open **Devices** window.

VPLS Summary Tab

VPLS Summary Tab provides information about the virtual private networks (VPNs) within a map. The tab displays the VPN ID, name and service type for each VPN in the map. In addition, the Nodes and Pseudowires (PW) tabs provide more detailed operational information specific to each VPN.



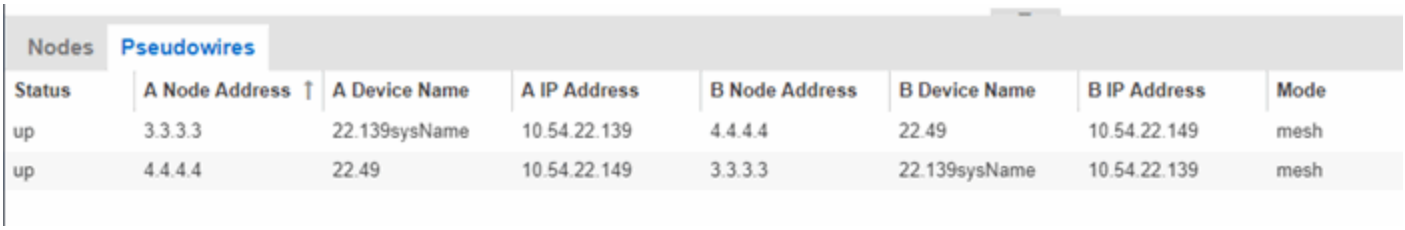
Nodes

The **Nodes tab** includes the following:

- Status – operational status of the node
- Node Address – node location within the VPN
- Name – name of the node
- Device IP Address –
- VPLS Name – name of the VPLS in which the node resides
- Service Name – name of the virtual private LAN in which the node resides
- Number of Peers – number other nodes in the VPN
- VPLS Operational Status – operational status of the virtual private LAN services
- VPLS Admin Status – administrative status of the virtual private LAN services
- Dot1Q Tag Option –
- MTU – the maximum number of transmission units allowed between nodes
- Device Type –

Pseudowires

Select the **Pseudowires Tab** for access to the status and mode for each PW in the VPN, as well as the addresses, device names, and IP addresses for each node within the VPN.



Nodes | Pseudowires

Status	A Node Address	A Device Name	A IP Address	B Node Address	B Device Name	B IP Address	Mode
up	3.3.3.3	22.139sysName	10.54.22.139	4.4.4.4	22.49	10.54.22.149	mesh
up	4.4.4.4	22.49	10.54.22.149	3.3.3.3	22.139sysName	10.54.22.139	mesh

For information on related topics:

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

Map Types

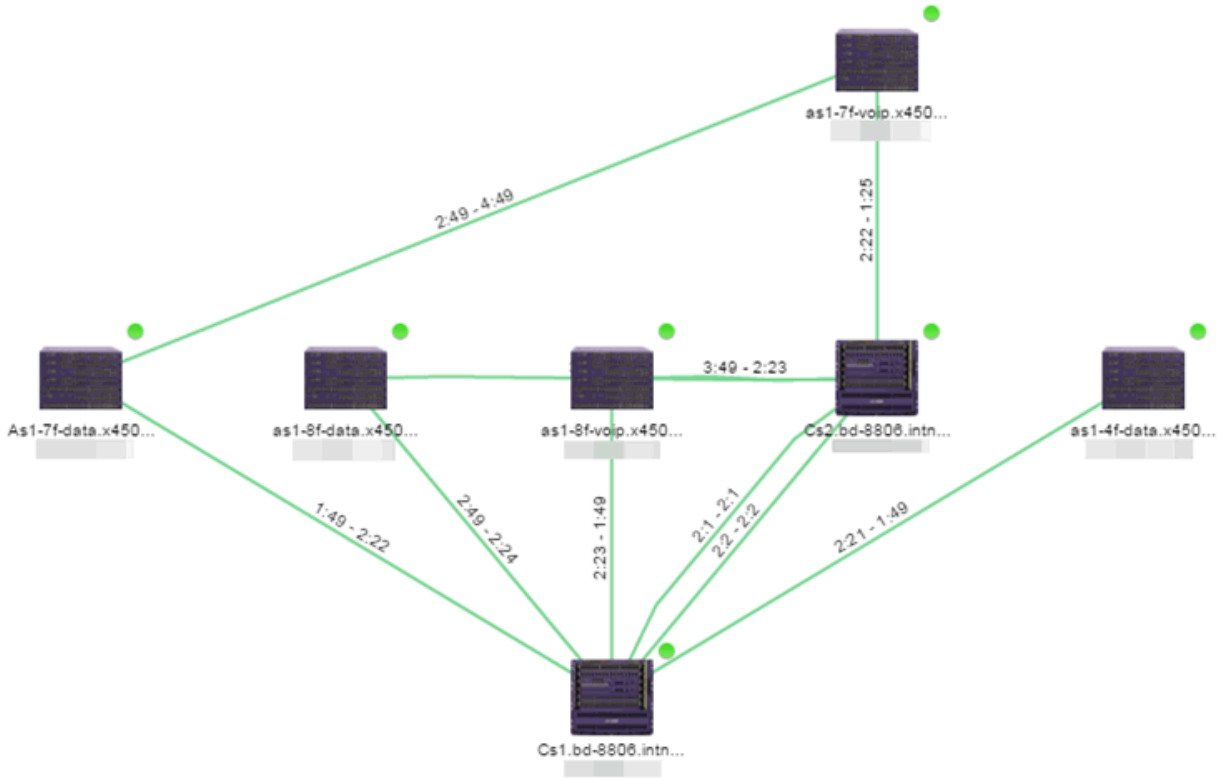
ExtremeCloud IQ Site Engine allows you to create geographic and topology maps of devices and floorplans of wireless access points (APs) on your network.

To view maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read Access or Maps Read/Write Access capability.

Types of Maps

Using ExtremeCloud IQ Site Engine Maps, you can create three types of maps, each presenting a different visual representation of your network:

- Topology *(default)* — A topology map shows how devices are connected in a network, specifically, the state and speed of the network connections between devices as well as the state of the devices in the network. You can also create a topology map with a background image, giving you additional information about the devices and connections that make up the network.

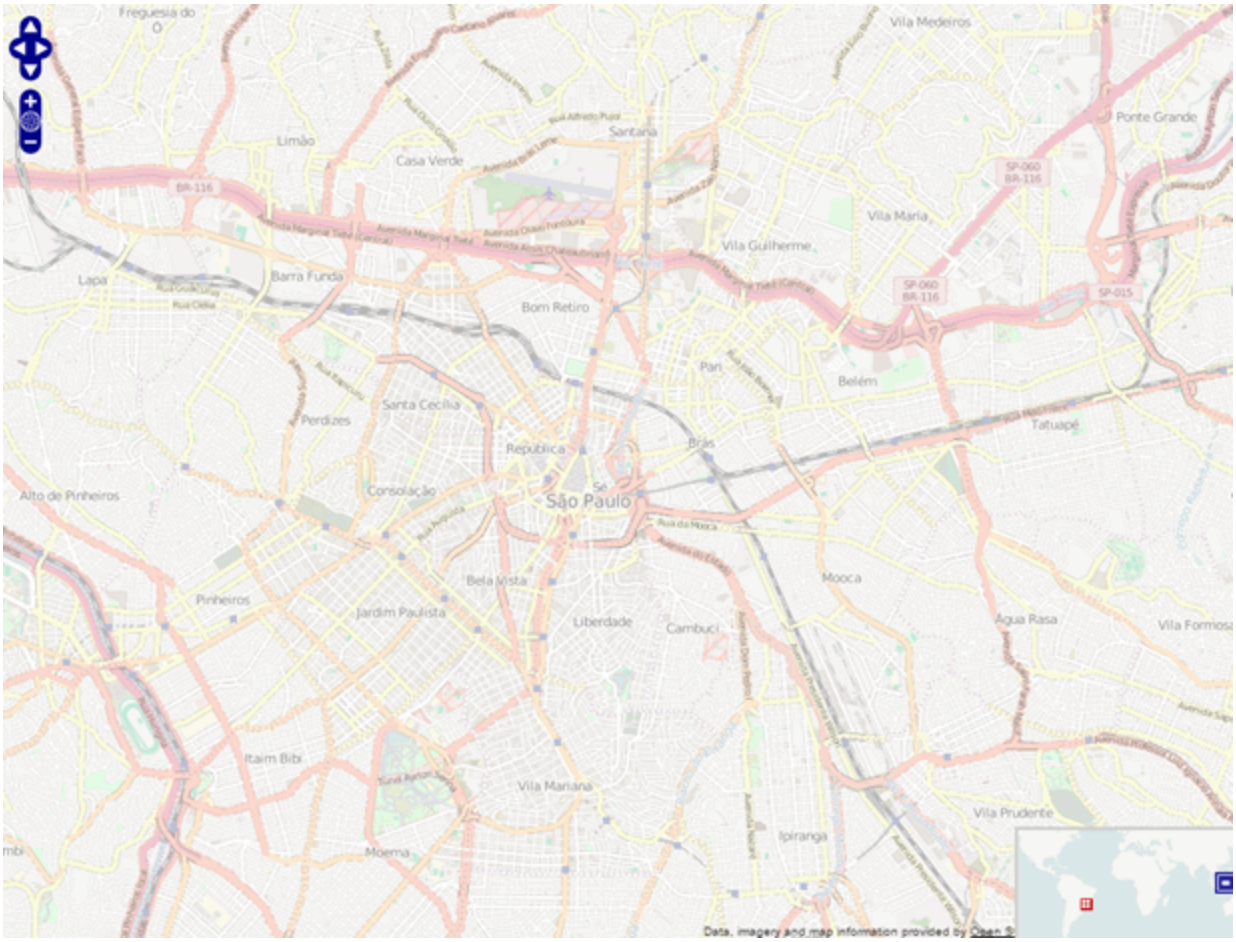


- Floorplan — The floorplan map displays the location of APs in a floorplan you configure. Using information about the size and composition of the building, this map provides an overview of the coverage of wireless APs.



- Geographic — The Geographic map shows a global or regional view where network locations are shown geographically. This map is useful for networks spread across large geographical areas or as a top-level map used to organize multiple networks in different locations.

NOTE: The geographic map type is hosted by OpenStreetMap on an external server. For users with security concerns or if access to third-party servers is prohibited, use the topology map type.



After you create a map, you can then make it a site. Sites allow you to set a default configuration for devices added to your network.

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

How to Perform a Search Using Maps

Using ExtremeCloud IQ Site Engine Maps, you can easily search for wireless and wired clients, access points (APs), and devices in a number of ways. Maps are configured in various places on the **Network** > **Devices** tab in ExtremeCloud IQ Site Engine.

Performing a Search

To search for a wireless client, an AP, a device, or a wired client:

1. Launch ExtremeCloud IQ Site Engine.
2. In the **Search** > **Network** box, select **Advanced** .
3. Enter the MAC Address, IP Address, hostname, user name, AP serial number or ExtremeControl custom field information in the open **Search** box.
4. Press **Enter**.

The Search Result field displays the paths for all the maps that include the client or device you searched, if that client or device is included in multiple maps. If the client or device you searched is included in only one map, that map opens as a result of the search.

You can also search for specific wireless clients, access points, devices, and wired clients from different locations in ExtremeCloud IQ Site Engine.

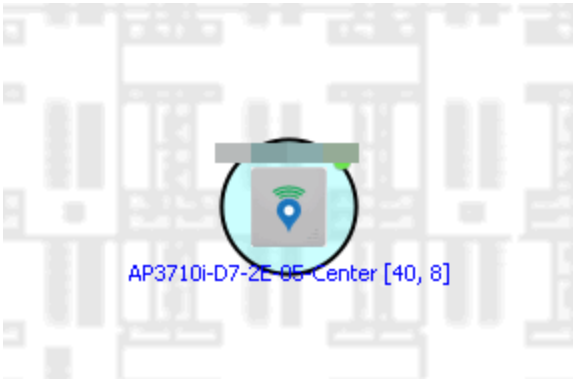
Finding a Wireless Client

From the Search Field on the Network Tab

1. Launch ExtremeCloud IQ Site Engine and select the **Network > Devices** tab.
2. Select Sites from the left-panel drop-down list.
3. Select the map or map navigation tree.
4. Enter the MAC Address, IP Address, hostname, user name, AP serial number or ExtremeControl custom field information in the **Search** field at the far right of the **Devices** window.
5. Press **Enter**.

The search uses RSS-based (Received Signal Strength) location services to locate the wireless client and display the approximate location of the client on the map.

The map opens with the AP centered on the map, with a circle showing the possible area where the client is located. If that information is not available, a square is drawn around the AP last associated with the client.



From the Wireless Tab

To locate a wireless client from the Wireless tab:

1. Launch ExtremeCloud IQ Site Engine.
2. Select **Wireless > Clients.**
3. Select a client in the Clients view.
4. Right-click and select **Search Maps**.
5. The map opens centered on the AP, with a circle showing the possible area where the client is located.
6. Mouse over the client icon to see a tooltip with client information.

NOTE: Tooltip information is based on current data from the wireless domain unless the client icon displays a clock in the center. In that case, the tooltip information is based on historic data from the Wireless > Clients page.

Radius Distance Calculation

The following distance calculation defines the radius of the circle displayed around the wireless client located on the map.

Path loss per meter in free space =
L1 = 20 * log (10) (f) - 28

where:

- [f] is the frequency in MHz
  (Uses Source SNMP MIB dot11ExtSmtCurrentChannel
  or if that value is 0, uses MIB dot11ExtSmtCurChanSelectedByAP)
- [L1] is the path loss on distance of 1 meter

Radial distance for location =
d(RSS,n) = 10 ^(pTx - RSS - L1)/(10*n)

where:

- [n] is the coefficient for the environment
- [pTx] is the transmit power (dB)
- [RSS] is the Received Signal Strength
- [d] is the distance in meters

Finding an Access Point

From the Wireless Tab

1. Launch ExtremeCloud IQ Site Engine.
2. Select **Wireless** > **Access Points.**

3. Right-click an AP in the table.
4. Select **Maps > Search Maps**.
5. If a map contains the AP, the map opens with the AP centered on the map.

From the Reports Page

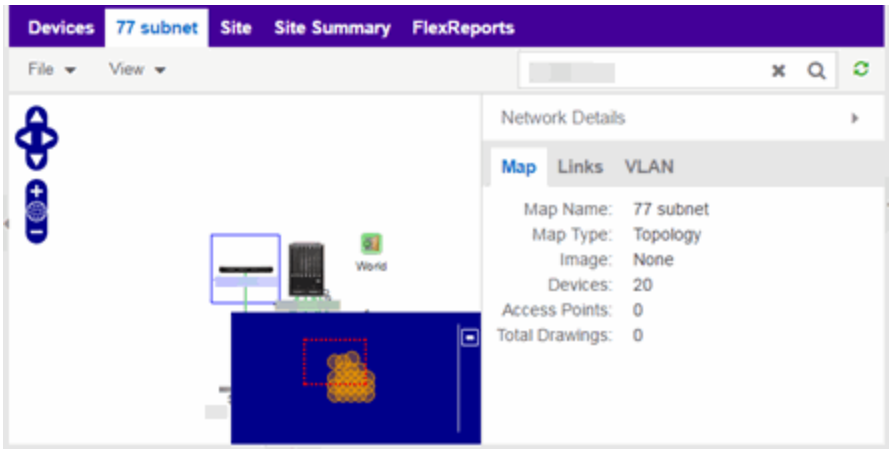
1. Launch ExtremeCloud IQ Site Engine.
2. Select the **Wireless** tab.
3. On the **Reports** tab, select the APs Summary from the **APs Summary** drop-down list.
4. Right-click an AP in the table.
5. Select **Maps > Search Maps**.
6. If a map contains the AP, the map opens with the AP centered on the map.

Finding a Device

From the Network Page Search Field

1. Launch ExtremeCloud IQ Site Engine and select the **Network > Devices** tab.
2. Select Sites from the left-panel drop-down list.
3. Select the map or map navigation tree. Select the **Map** tab in the **Devices** window.
4. Enter an IP address or hostname for the device in the **Network** tab **Search** box
5. Press **Enter**.

The search locates a device added to a map. The map centers on the device. The screen shot below shows the results for a search on a specific IP address.



Finding a Wired Client

From the Network Tab Search Field

1. Launch ExtremeCloud IQ Site Engine and select the **Network > Devices** tab.
2. Select Sites from the left-panel drop-down list.
3. Select the map or map navigation tree.
4. Enter the MAC Address, IP Address, hostname, or user name in the **Network** tab **Search** box.
5. Press **Enter**.

The search locates a wired client if the client is Access Control authenticated and is connected to a switch added to a map. The map centers on the wired client.

From the Control Tab

1. Launch ExtremeCloud IQ Site Engine.
2. Select **Control** > **End-Systems.**
3. Right-click an end-system in the table and select **Search Maps**.
4. If the end-system is connected to a switch added to a map, the map opens with the end-system centered on the map.

For information on related topics:

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

How to Import Maps

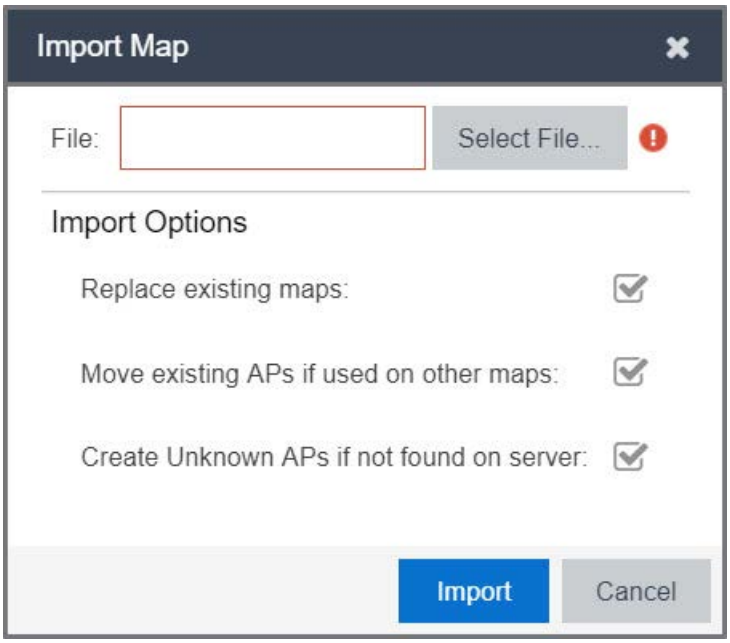
The ExtremeCloud IQ Site Engine Maps lets you import saved maps of devices and wireless access points (APs) from your local drive or network, and configure the behavior of the imported maps.

In order to edit maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

Importing a Map

To import a saved map:

1. Right-click a map in the left-panel Groups/Maps Navigation Tree and select **Maps** > **Import Map**.
   The Import Map window opens.



2. Select the **Select File** button to navigate to the map on your local drive or network.
3. Configure your import options to determine the behavior of maps being imported:
    a. Select the **Replace existing maps** checkbox to replace existing maps in ExtremeCloud IQ Site Engine with maps you import with the same name.
    b. Select the **Move existing APs if used on other maps** checkbox to move APs currently located on another map in ExtremeCloud IQ Site Engine to the map being imported.
    c. Select the **Create Unknown APs if not found on server** checkbox for APs located on the map being imported that are not found on the ExtremeCloud IQ Site Engine server.
4. Select **Import**.

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

How to Create Links Between Devices and Maps

Using the ExtremeCloud IQ Site Engine Maps feature, you can link your network devices and wireless access points (APs) on a map. You can also use this feature to add links between maps.

In order to edit maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

Creating a Manual Link Between Devices

To manually create links between devices on a map:

1. Right-click one of the devices to which you are adding the link.
2. Select **Create Link**.

   The Create a Manual Link window displays.
3. Expand the device in the **Name** column of the From Port section of the window and select the port to which the link connects.
4. Select the other device to which the link connects in the **Select Device** drop-down list.
5. Expand the device in the **Name** column of the To Port section of the window and select the port to which the link connects.
6. Select **OK** to add the link to the map.

NOTES: The **Link State** for a manual link is derived from the **Status** of the ports to which it connects.

Delete a manual link via the Link Details window by double-clicking the link in the map.

Adding Map Links

Map links display the name of the map and an aggregated alarm/device status for the linked map. Double-click on the link to go to the linked map.

For example, the following map link lets you jump to the Second Floor map. The link is green, indicating there are no devices with alarms on the Second Floor map.



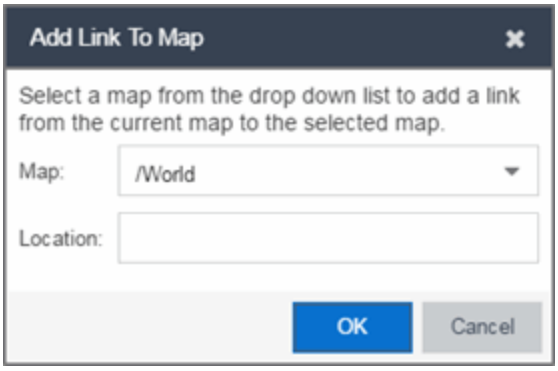
The following map link lets you jump to the First Floor map. The link is red, indicating there is an alarm for a device on the First Floor map.



Use the following steps to add a link to a map.

1. In the Maps navigation tree, right-click on the map from which you want to link and select **Maps** > **Edit Map** or select **File** > **Edit** button in the map properties panel.
2. The map's property panel opens in Edit mode. Select **File** > **Add** > **Map Link**.

3. The **Add Link to Map** window opens.



4. From the **Map** drop-down list, select the map to which you want to link.
5. Enter information in **Location** about the location to which the link connects and select **OK**.
6. The map link is added to the map and can be repositioned, if desired.
7. Select the **Save** button to save the map and close the properties panel.

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

How to Set the Map Scale

You can use the ExtremeCloud IQ Site Engine Maps feature to set the scale of a map of devices or wireless access point (APs) in your network.

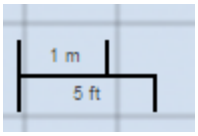
In order to edit maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

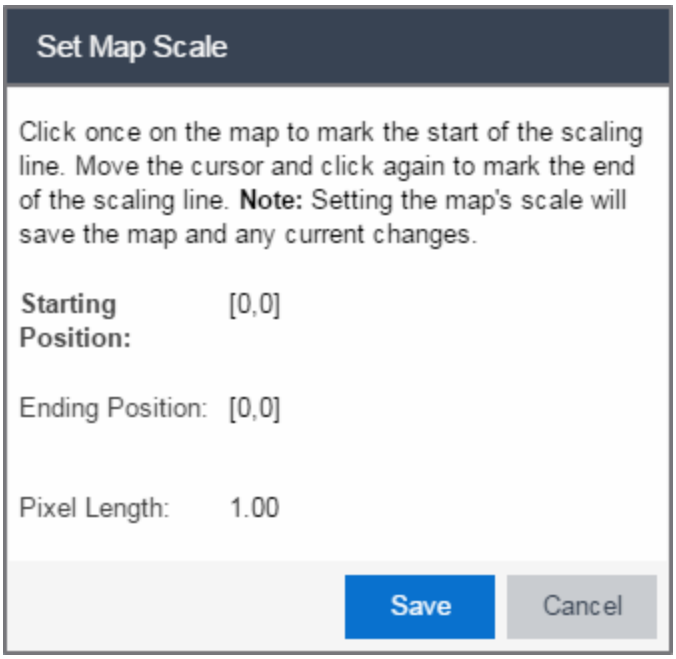
Setting the Map Scale

The map scale appears in the lower left corner of a map and can be changed to accurately reflect your map image.

Use the following steps to set the scale for a map.

1. In the Maps page's navigation tree, right-click on the map and select **Maps** > **Edit Map** or select the **File** > **Edit** button in the map properties panel.
2. Select the map scale in the map's footer panel to open the Set Map Scale window. (Users can access the Set Map Scale window from the Tools menu.)





3. To set the scale, you must measure something in the map using a scaling line, and then set the measurement for the line. For example, in an office floor plan, measure a scaling line on the opening of an office. If you know the office doors are 33 inches wide, enter that as the scaling line measurement.
    a. Select on the map to mark the start of the scaling line. Move the cursor and select again to mark the end of the scaling line.
    b. Enter the line length and units.
4. Select **Save**. The map scale is automatically adjusted and the map is saved.

- ExtremeCloud IQ Site Engine Maps
- Advanced Map Features

Endpoint Locations

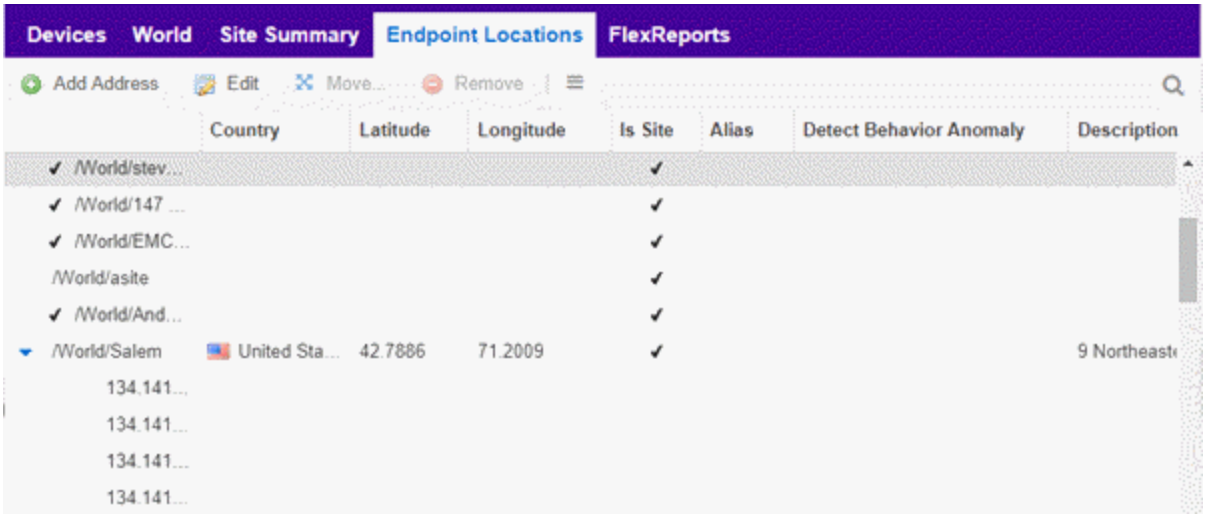
Use the **Endpoint Locations** tab to view and define the geographical locations of sites and subnet addresses in your network. When the geographical locations are defined, flows on the **Application Flows** tab display geographical information depending on the device on which the flow is observed.

To access the **Endpoint Locations** tab, navigate to **Network > Devices** and select **Sites** in the left-panel. The **Endpoint Locations** tab displays in the right panel.

IMPORTANT: To map existing locations to sites, access the **Devices** tab and select a site. Select the **Endpoint Locations** tab in the right-panel. Locations that are not yet associated with a site contain a broken link icon ( ) icon. Right-click the location, select Assign to Site, and select a site from the drop-down list.

Select the **Add Address** button at the top of the table to add an additional address to the table. Select the **Edit** button to modify a selected address of a site in the table. Select the **Move** button to move an address to a different site in the drop-down list. Select the **Remove** button to delete a selected address or site from the table. These options are also accessible when you right-click an address in the table.

Select the **Menu** ( ) button to import or export the Endpoint Locations table to a CSV report.



The following columns are displayed in the Endpoint Locations table:

Tracked
: This column displays the name of the sites or the IP Address/Mask of the items in the table. If an item in the table has a check mark to the left of the site name, it is a Tracked Site. Right-click any site to either add or remove the site from your Tracked Sites list.

Country
: The country in which a site is located.

Longitude
: A site's longitude location, written in decimal degrees.

Latitude
: A site's latitude location, written in decimal degrees.

Is Site
A check mark in this column indicates that the selected item in the table is a site and not an address. A blank in this column indicates the location is orphaned (which may result from an upgrade from a previous version of ExtremeAnalytics).

Alias
An alternate name for a site or a specific subnet of the site.

Description
A description of the site or orphaned location.

For information on related topics:

- Network Tab
- Sites Tab

Restart Devices

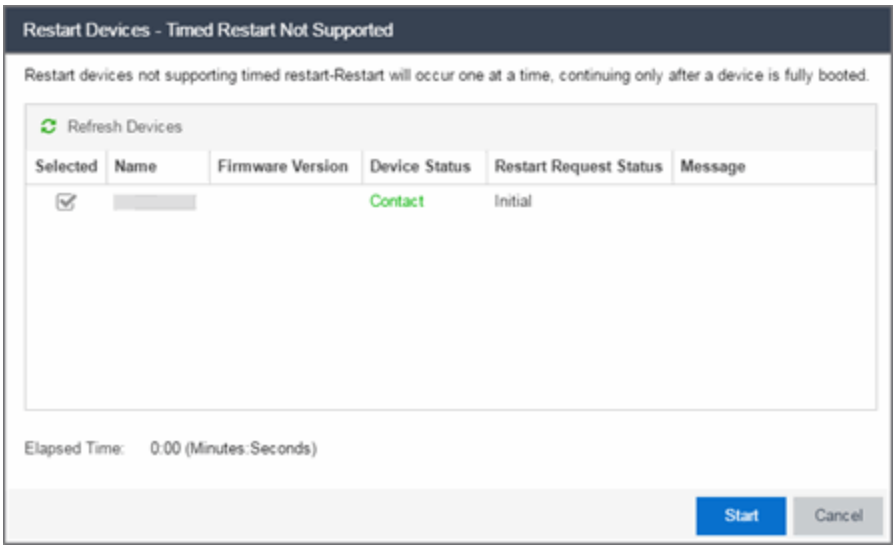
Use this window to restart a device. Devices can be restarted manually, or scheduled at a future date and time, if a timed restart is supported by the device. The window varies depending on the devices you select to restart:

- Timed Restart Not Supported
- Timed Restart Supported

You can access the Restart Devices window from the **Network** tab by selecting the **Menu** icon or right-clicking a device in the table and selecting **More Actions** > **Restart Device**.

Timed Restart Not Supported

To restart a device, select it in the list by selecting the **Selected** checkbox, and select **Start**.



Refresh Devices
: Select the **Refresh Devices** button to update the fields in this window as the restart process is taking place.

Selected
: Select this check box to indicate the devices you are restarting.

Name
: The names of the devices.

Firmware Version
: The firmware version of the devices. If the purpose of the device restart is to upgrade the firmware version, this value changes when the device restart is complete (update the field by selecting **Refresh Device**).

Device Status
The connection status between ExtremeCloud IQ Site Engine and the devices.

Restart Request Status
The time in the restart process during which the devices indicate they are restarting.

Message
Additional information about the devices.

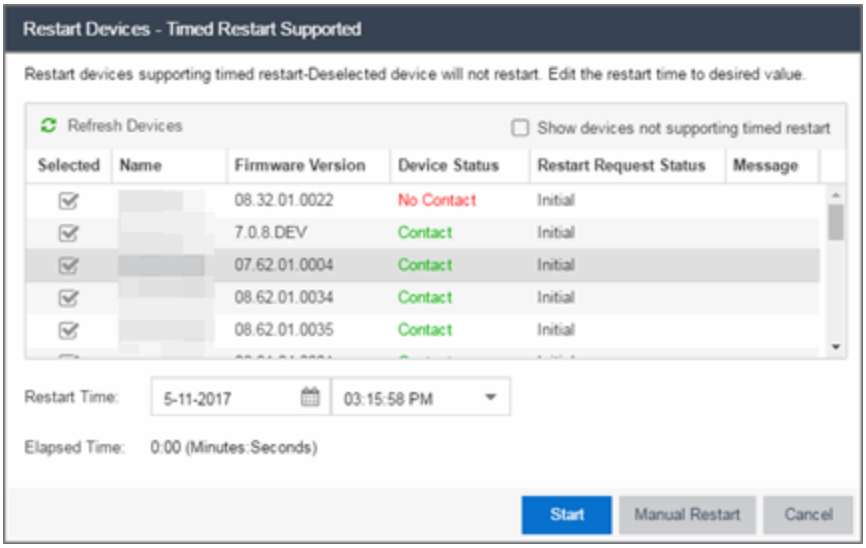
Elapsed Time
The time elapsed since the restart began.

Start
Select **Start** to restart the device.

Close
Select **Close** to exit the **Restart Devices** window without restarting the devices.

Timed Restart Supported

Devices that support Timed Restart allow you to set up your restart operation with a time delay, so that the actual device restarts take place at a later time. This lets you schedule restarts for a time when the network is least busy.



The window for these devices contains additional fields.

Refresh Devices
Select the **Refresh Devices** button to update the fields in this window as the restart process is taking place.

Selected
Select this check box to indicate the devices you are restarting.

Name
The names of the devices.

Firmware Version
The firmware version of the devices. If the purpose of the device restart is to upgrade the firmware version, this value changes when the device restart is complete (update the field by selecting **Refresh Device**).

Device Status
The connection status between ExtremeCloud IQ Site Engine and the devices.

Restart Request Status
The time in the restart process during which the devices indicate they are restarting.

Message
Additional information about the devices.

Elapsed Time
The time elapsed since the restart began.

Start
Select this button to schedule the device restart now, or at the time selected in the **Restart Time** field.

Close
Select this button to exit the **Restart Devices** window without restarting the devices.

Show devices not supporting timed restart
Select this check box to display devices you selected on the **Network** tab for which you can not schedule a restart.

Restart Time
Select the date and time when the devices restart.

Fabric

The ExtremeCloud IQ Site Engine Fabric technology is a solution to manage your domains seamlessly and interdependently across both physical and virtual servers, storage, and networks. It is designed to be highly efficient, flexible enough to adapt to your network's varying traffic volume, and easily maintained with minimal intervention. You can provision Fabric functionality on the **Sites** tab in ExtremeCloud IQ Site Engine.

For additional information about Fabric functionality, see the *Configuring Fabric Basics and Layer 2 Services on the VOSS Operating System Software VSP 8600* guide for the latest VSP 8600 release.

ExtremeCloud IQ Site Engine's fabric solution consists of two major components:

- Fabric Manager — A virtual engine that provides ExtremeCloud IQ Site Engine with fabric topology information and allows you to configure fabric functionality on your fabric-enabled devices.
- Fabric Tab — The tab within ExtremeCloud IQ Site Engine that allows you to view and configure the fabric functionality on your devices.

NOTE: Beginning with ExtremeCloud IQ Site Engine version 8.5.5, the Ubuntu Operating System has upgraded to version 18.04.5 for the Fabric Manager.

The Fabric Manager engine must be installed and running on your network for the **Fabric** tab in ExtremeCloud IQ Site Engine to receive and display fabric topology information.

Once the Fabric Manager engine is running in ExtremeCloud IQ Site Engine, the **Fabric** tab on the **Devices** tab displays information about the fabric topologies currently configured on your devices.

NOTES: The following device types support fabric functionality:

ERS35xx with firmware version 5.3.7 and later, ERS36xx with firmware version 6.2.0 and later, ERS48xx with firmware version 5.12.0 and later, ERS49xx with firmware version 7.6.0 and later, ERS59xx with firmware version 7.6.0 and later, VSP7024 with firmware version 10.4.6 and later, VSP4xxx with firmware version 6.1.3 and later, VSP7xxx with firmware version 6.1.3 and later,VSP8xxx with firmware version 6.1.3 and later

For minimum requirements, see ExtremeCloud IQ Site Engine Configuration and Requirements.

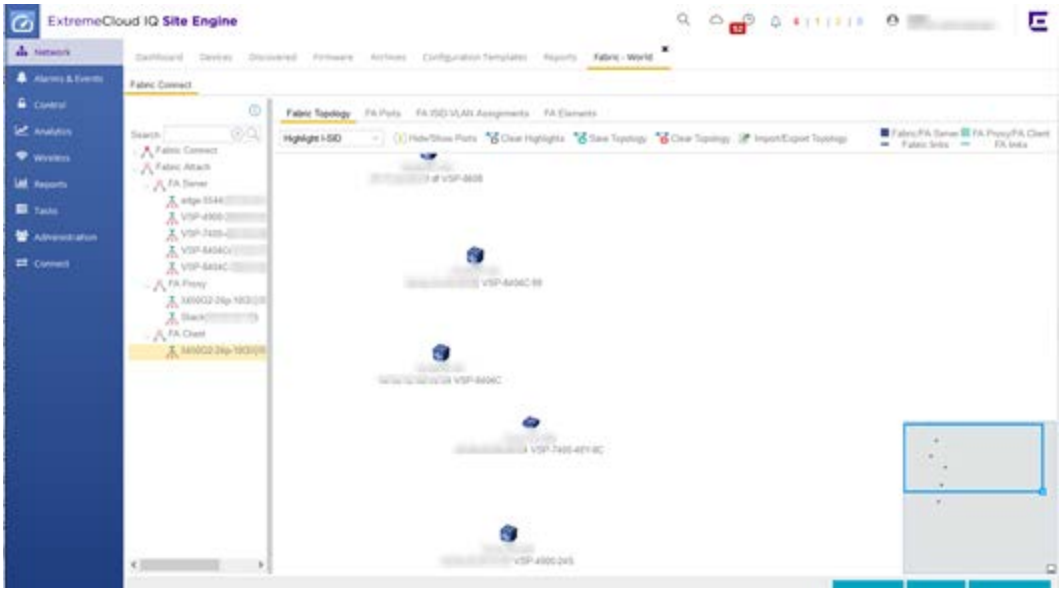
Accessing Fabric in ExtremeCloud IQ Site Engine

After adding the Fabric Manager engine in ExtremeCloud IQ Site Engine, view the fabric topologies configured on your devices on the **Fabric** tab.

To access the **Fabric** tab:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Right-click a site in the left-panel tree.
4. Select **More Views** > **Fabric Topology** from the menu.

   The **Fabric** tab opens.



Fabric Tab

The **Fabric** tab includes three sub-tabs:

- Fabric Topology — Displays the fabric topologies configured on your fabric-enabled devices.
- FA Ports — Displays the ports on which fabric is configured.
- FA ISID-VLAN Assignments — Allows you to view Virtual Extensible LANs (VXLANs) that tunnel Layer 2 traffic over a Layer 3 network in the fabric topologies you configure.

For information on related topics:

- Services
- Service Summary
- Fabric Connect
- Fabric Assist

Fabric Manager Installation (Legacy)

Install the Fabric Manager virtual machine (VM) to enable Fabric Manager in ExtremeCloud IQ Site Engine.

Pre-Installation

The Fabric Manager is distributed in a deployable VMware-based .OVA template, which is similar to the other ZTP+ (Zero Touch Provisioning Plus)-based engines (for example,ExtremeControl).

The Fabric Manager supports two initial configuration modes for ExtremeCloud IQ Site Engine discovery and registration:

- DHCP Mode
- Static Mode

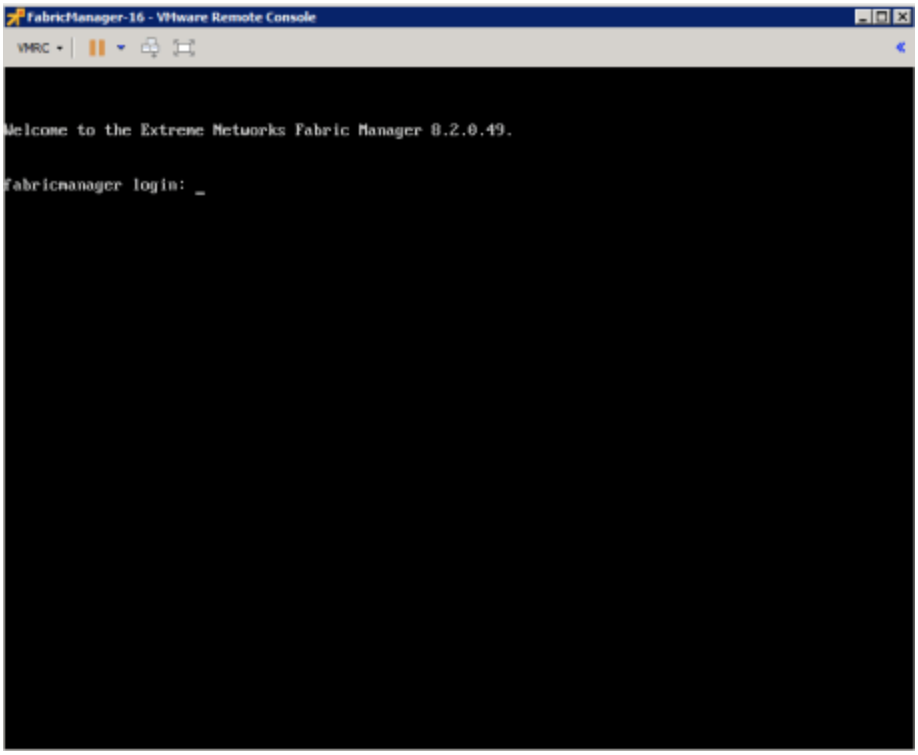
The DHCP mode is the default configuration mode during the Fabric Manager VM's initial startup. Use the static mode when providing a predefined set of networking configurations.

Fabric Manager Installation Static Mode

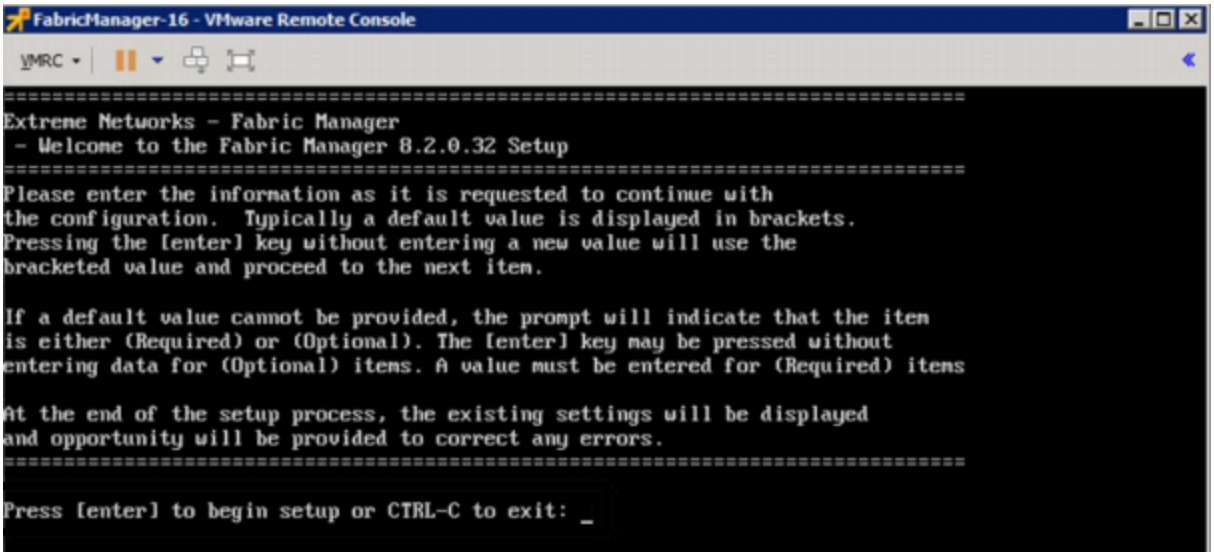
Fabric Manager begins installation in DHCP mode by default. Switch to static mode at any time during the initial installation by pressing the ENTER key.

Use the following instructions to install Fabric Manager in static mode:

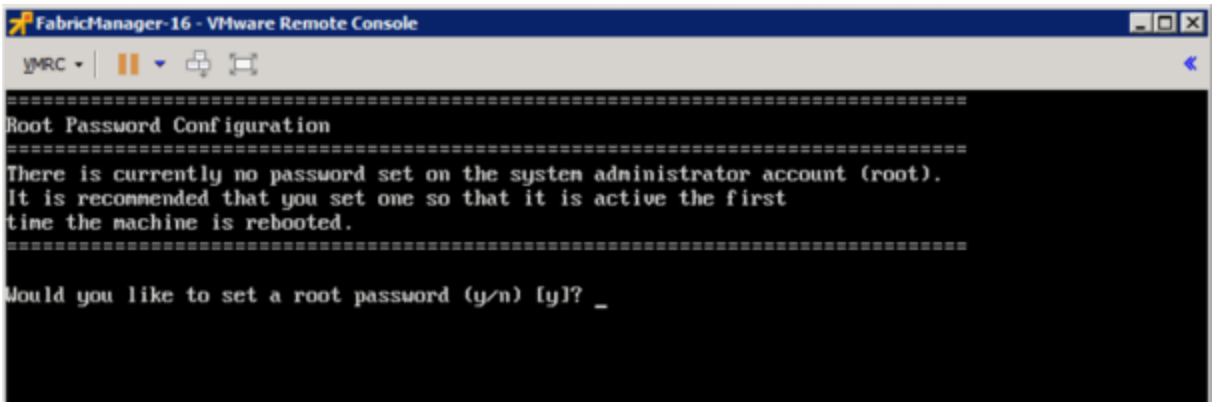
1. In the Console tab of the vSphere client, login as root with no password and press **Enter**.



2. Follow the installation process to complete installation of static mode:
    a. Begin the set-up.

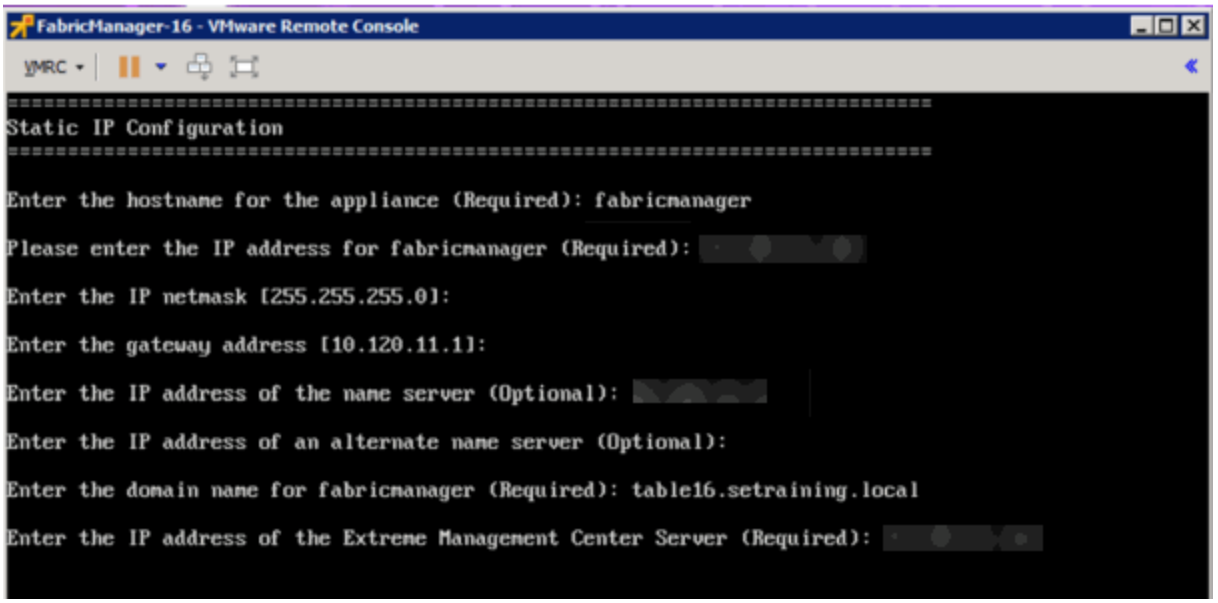


b. Set a root password by entering `y`.



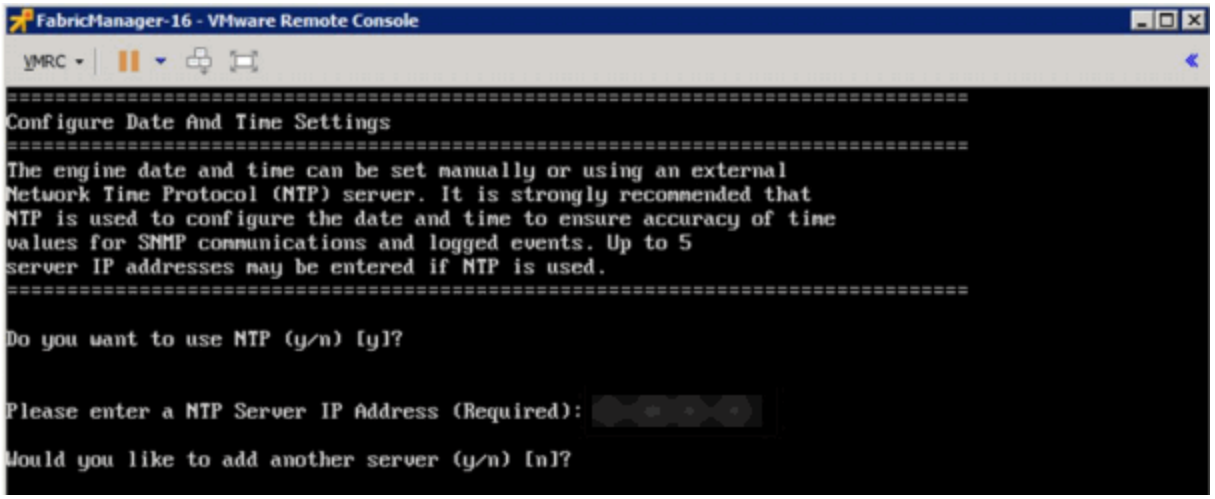
c. Enter and re-type a UNIX password at the next prompt.

The Static Configuration screen opens.



d. Enter a hostname.
e. Enter the IP address for the VM engine.
f. Enter the default IP Network netmask address.
g. Enter the default Gateway address.
h. Enter the IP address of the name server.
i. Enter the domain name specific to the table.
j. Enter the ExtremeCloud IQ Site Engine server IP address.

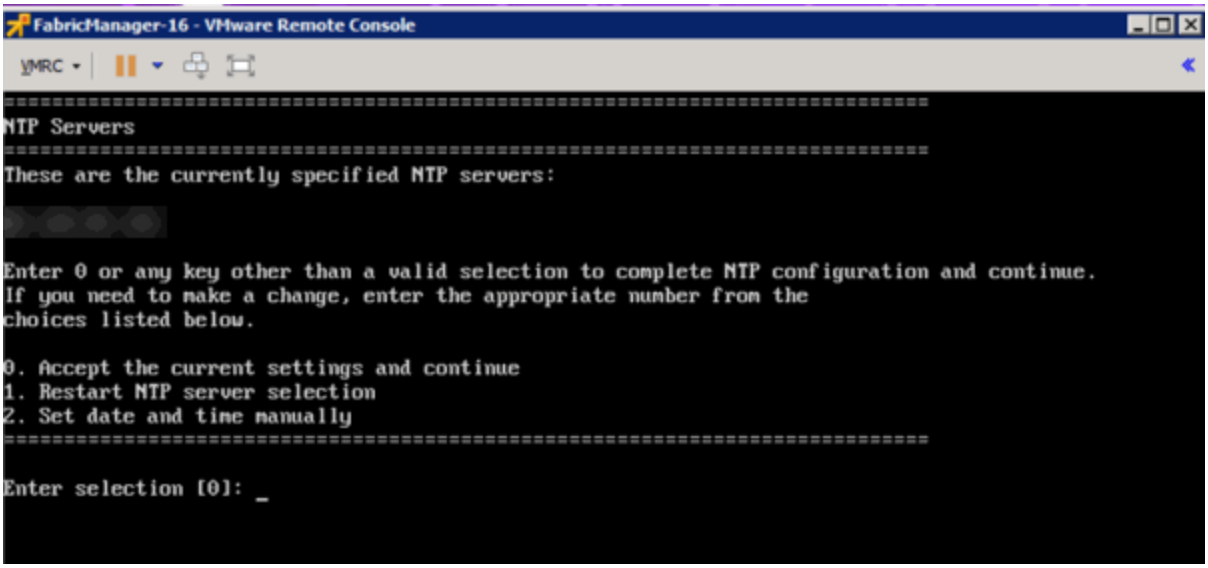
The Date and Time Configuration screen opens.



k. Enter `y` at the next prompt to use NTP (Network Time Protocol).

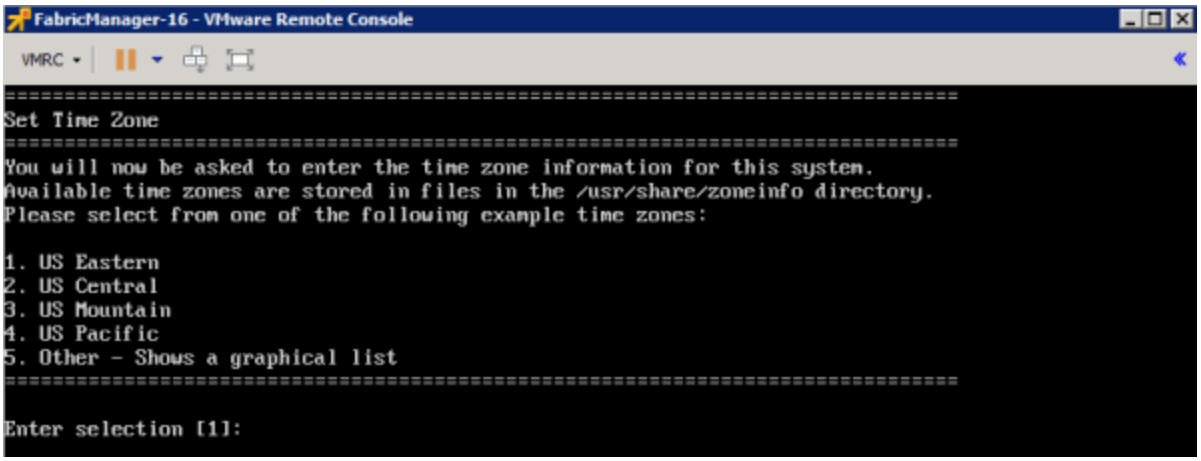
l. Enter the NTP Server IP Address.

m. Enter `n` at the next prompt to skip adding another NTP server. This is optional.



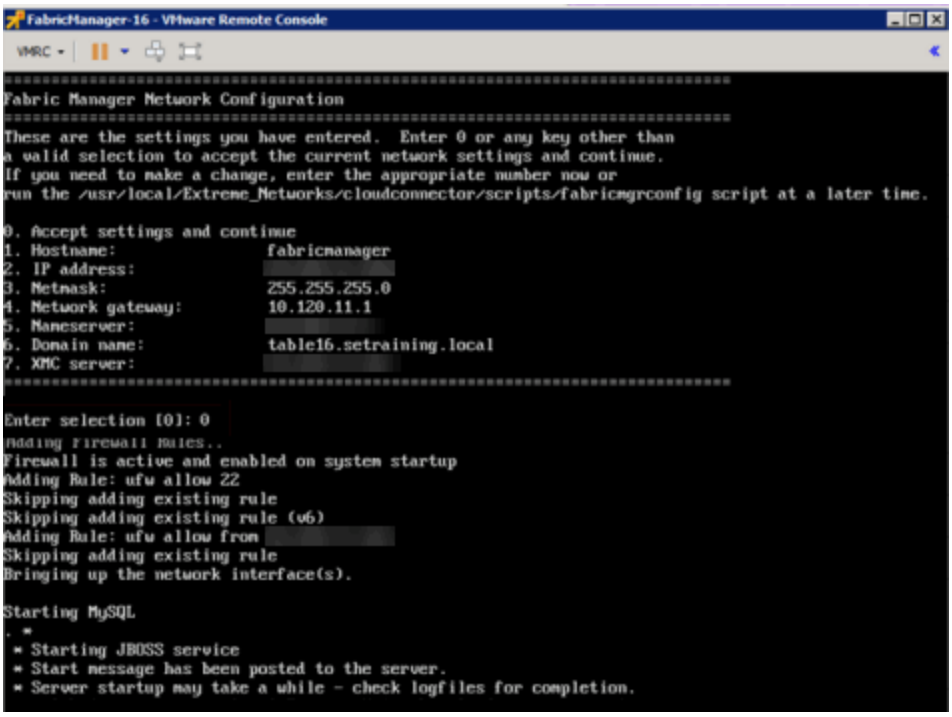
n. Enter the default `0` and accept the current settings and continue.

o. Select the correct Time Zone for your network.



p. Enter the number that corresponds to your time zone.

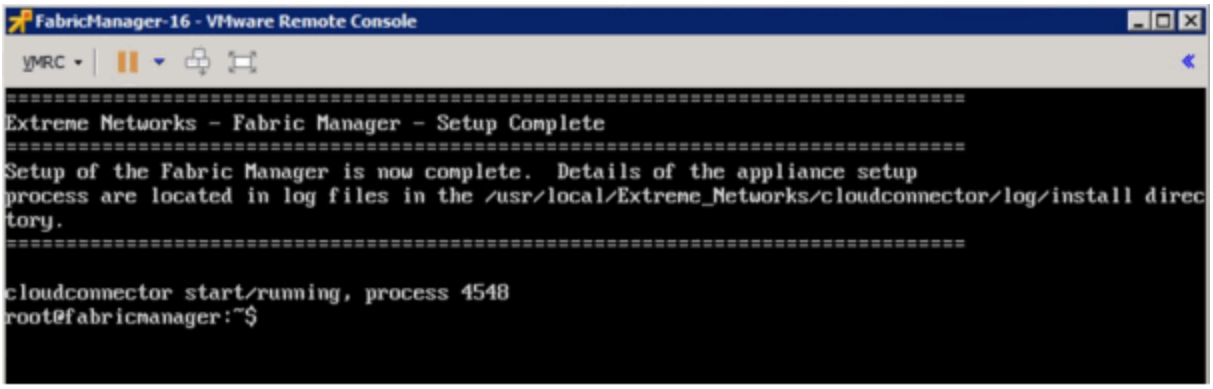
The Fabric Manager Network Configuration screen displays a summary of the configuration options you selected.



q. Enter `0` to confirm all the selections displayed are correct.

To modify any selection, enter the corresponding number of the item you want to change.

r. A Setup Complete message displays when installation is complete.



Adding Fabric Manager to ExtremeCloud IQ Site Engine

After you install the Fabric Manager virtual machine (VM), you can add it to ExtremeCloud IQ Site Engine and enable it via ZTP+ (Zero Touch Provisioning Plus) functionality.

NOTE: You need to upgrade the firmware in ExtremeCloud IQ Site Engine to add and launch the Fabric Manager engine.

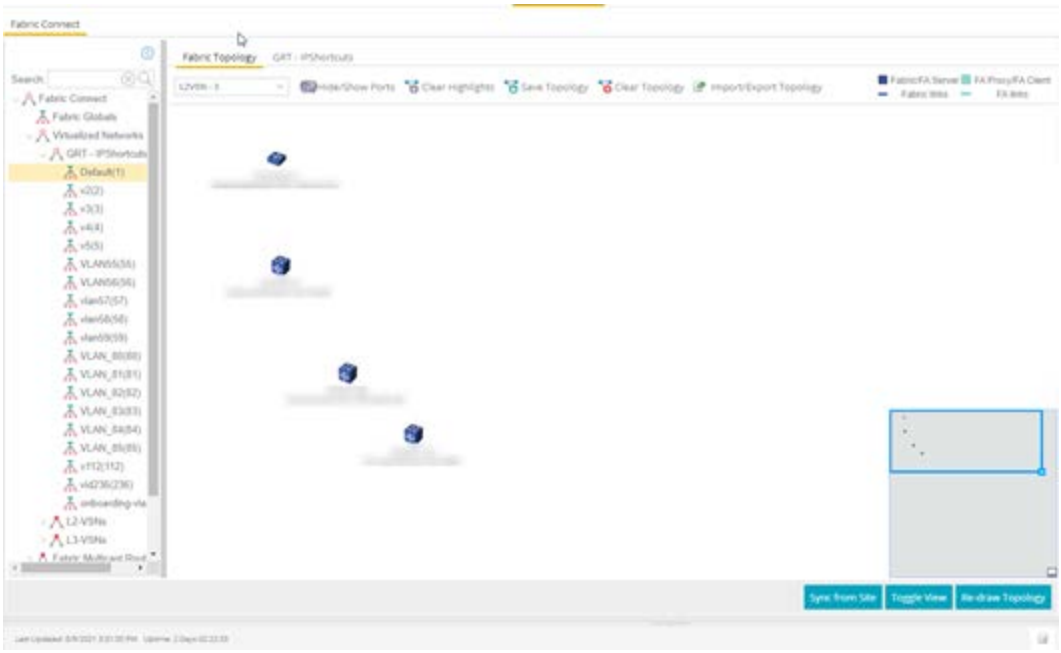
- How to Upgrade Firmware in ExtremeCloud IQ Site Engine
- Fabric Manager ZTP+ Configuration in ExtremeCloud IQ Site Engine
- ExtremeCloud IQ Site Engine Fabric

Fabric Connect

ExtremeCloud IQ Site Engine's **Fabric Connect** within the Fabric Manager engine displays your network's fabric technology and extended fabric functionality. Fabric Connect uses Fabric Topology templates that allow you to view and to configure SPBm (Shortest Path Bridging), based L2 and L3 Virtual Services Networks (VSNs), as well as IP-shortcut based VSNs. The Fabric Attach extends Fabric technology functionality to network elements or hosts that are not SPB-capable.

The Fabric Connect tab allows you to view topologies with the fabric-enabled sites in your network. Select the **Toggle View** button to display fabric services for individual devices.

NOTE: Fabric Connect uses Fabric Topology templates that define the topologies, services and service applications that comprise the Fabric Topology. Create the topology and service definitions via the **Sites** tab before you assign the Fabric Connect Topology to a site and access the **Fabric Connect** tab.



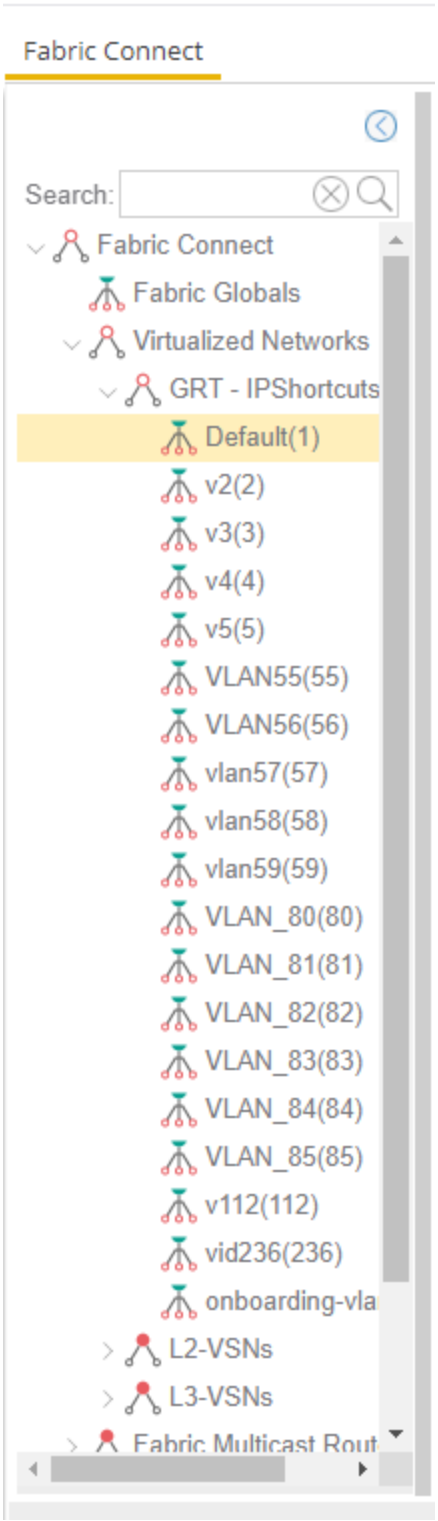
The Fabric Connect tab is divided into two sections: the left-panel tree view and a Fabric Topology right-panel map view.

Left-Panel Tree

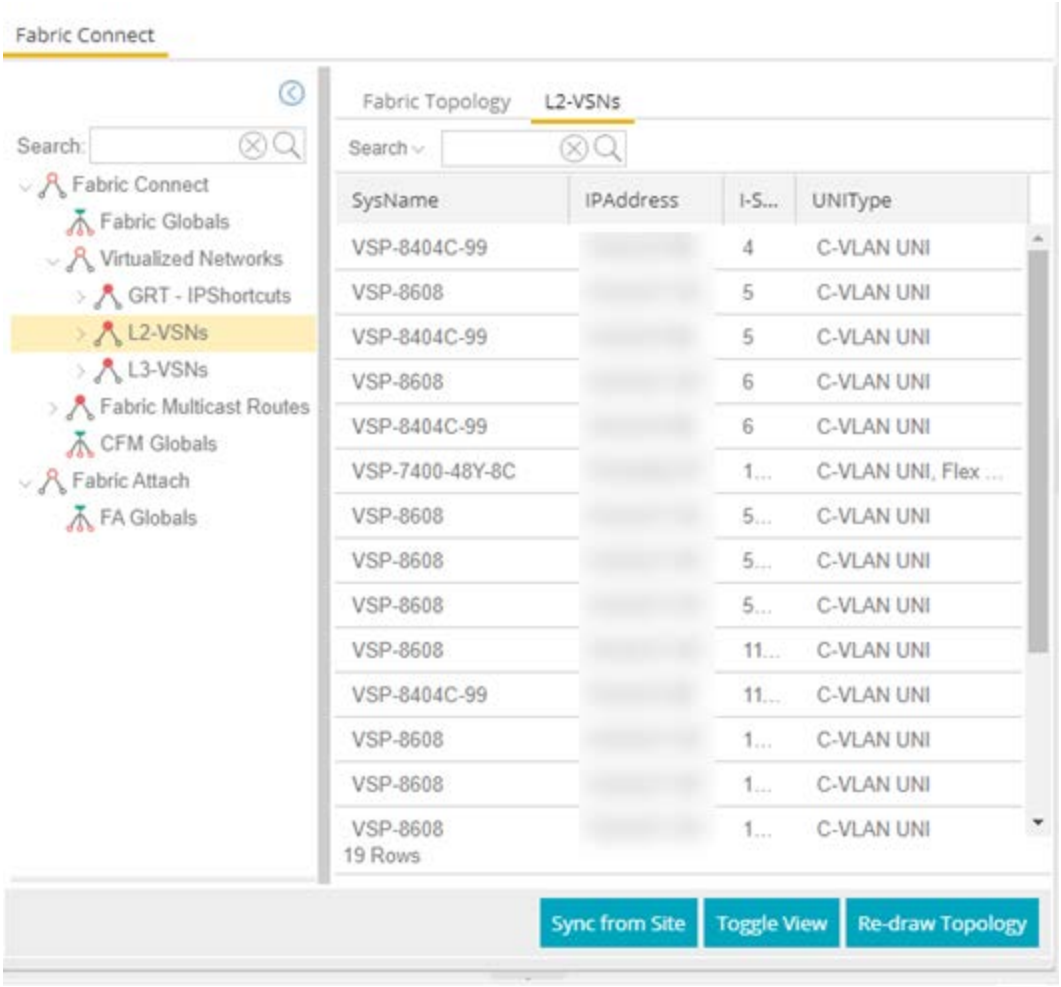
Beginning in version 26.11.10, ExtremeCloud IQ Site Engine supports two Fabric technology infrastructures: Fabric Connect and Fabric Attach (FA). The left-panel tree includes Fabric Connect and Fabric Attach folders that expand to display all fabric services you have configured in your network.

Fabric Connect Folder

Select the Fabric Connect tab to display the fabric topologies configured on the devices in the site.



Select a service in the Fabric Connect folder to open a fabric topology map and a service name tab in the right panel. The map displays the devices enabled with the services you selected and the service name tab displays a table with details about that service.



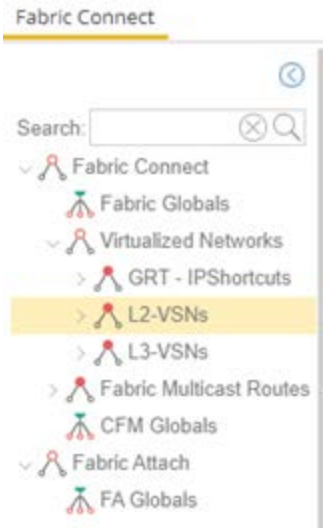
Select the **Toggle View** button to display Fabric Connect fabric services for individual devices.

Fabric Attach Folder

The Fabric Attach (FA) extends Fabric technology functionality to network devices that are not SPB-capable. The Fabric Attach tab displays global, server and proxy capable services for your network and devices.

NOTE: You can enable Fabric Attach on the following switches:

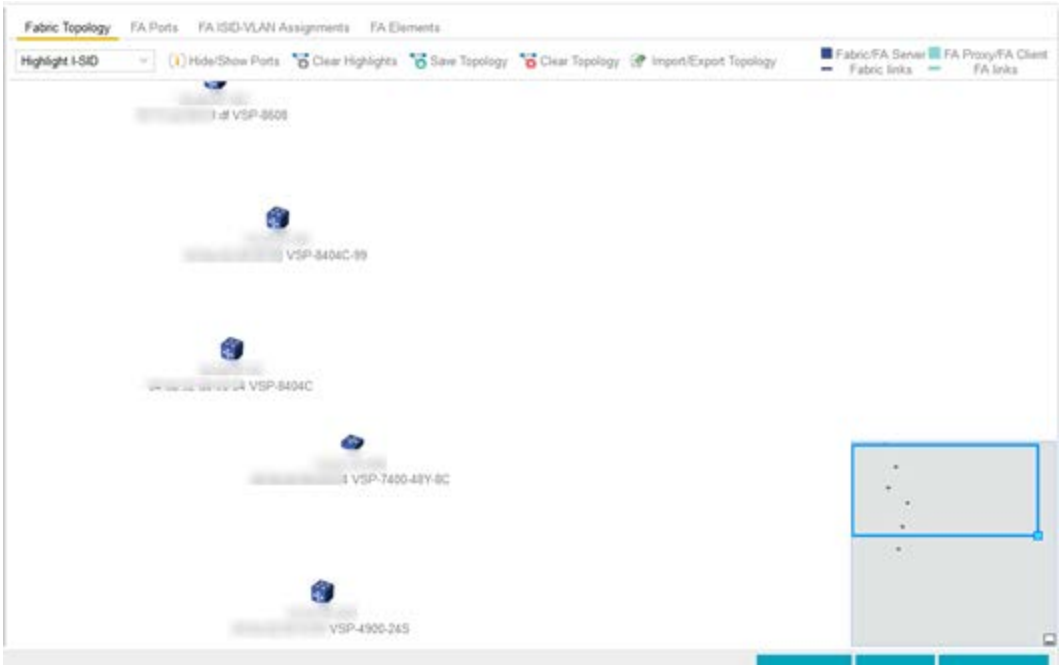
FA Server — for Fabric Engine, ERS 49xx v5.9.2 and later, ERS 4850 v5.9.2 and later, and ERS 59xx series devices; FA Proxy (client proxy) — for ERS 35xx, ERS 48xx, ERS 49xx, ERS 55xx, ERS 56xx, ERS 59xx, and VSP 70xx series devices; FA Standalone Proxy (client proxy) — for ERS 35xx, ERS 48xx, ERS 55xx, ERS 56xx, ERS 59xx, and VSP 70xx series devices



Select a service in the Fabric Attach folder to open a fabric topology map and a VSN tab in the right panel. The map displays the devices enabled with the service you selected and the VSN Home tab displays a table with details about the VSNs enabled on the site. Select the **Toggle View** button to display Fabric Attach services for individual devices.

Right-Panel Topology Map

The Fabric Topology panel includes the **Fabric Topology** tab that displays a topology map of the fabric-enabled sites or devices in your network. You can use the topology map to gain a high-level view of your network, or to view detailed information about devices and links in the topology. Drag your device icons in the topology map to rearrange the map. Additionally, you can modify and save your map layouts in the Fabric Topology tab.



Topology Tab Tools

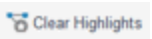
The Fabric Topology tab includes the following tools:

Fabric Service 

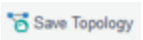
Lists fabric services in your network. Select a service from the drop-down list to display it in the topology map.

Hide/Show Ports

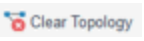
Use to hide or display fabric enabled ports in your network.

Clear Highlights 

Use to clear existing highlights on the topology map.

Save Topology 

Use to save your topology map.

Clear Topology 

Use to remove the devices in your topology map.

Color Legend 

The types of fabric services are coded by colors in the topology map.

Topology Tab Buttons

The Fabric Topology tab also includes the following buttons that allow you to further manipulate the fabric service and topology data:

Sync From Site
Use to copy the fabric service configuration for the site to all the devices in the map.

Toggle View
Select to display fabric topology, services and tables for individual devices.

Re-draw Topology
Select to display an alternate topology arrangement.

Help
Select to access ExtremeCloud IQ Site Engine help.

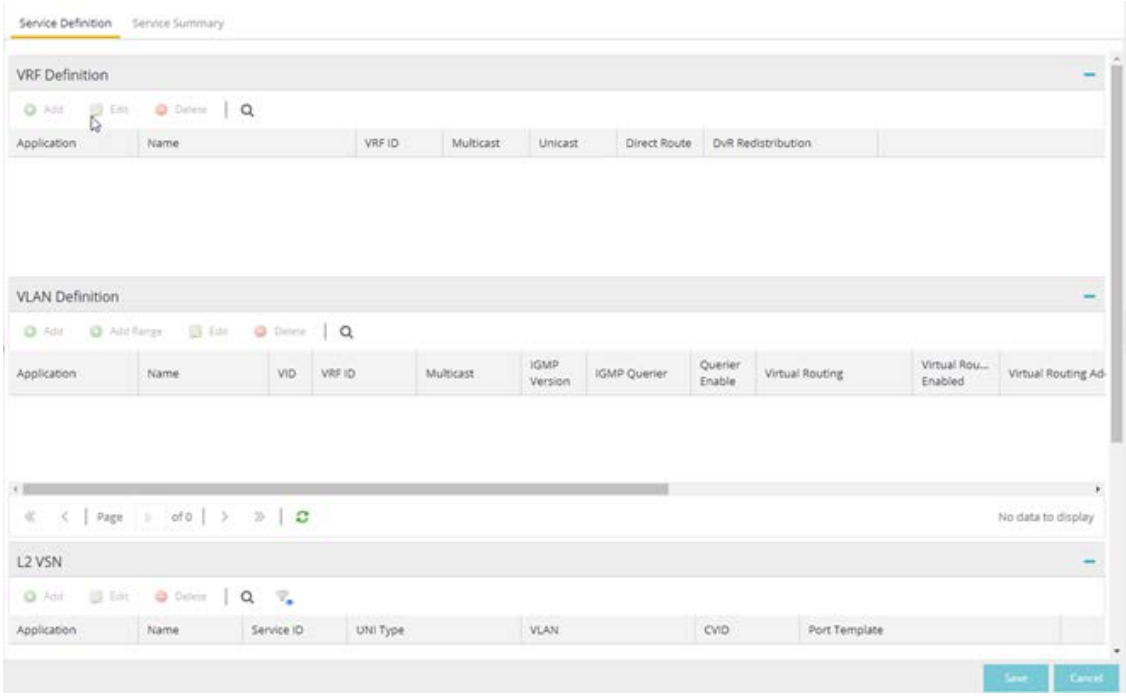
For information on related topics:

- Services
- Service Summary
- Sites
- Devices
- Fabric Assist

Services

The **Services** tab displays virtual routing and forwarding functionality configured as part of a service application, the virtual local area networks defined for the service application, as well as all of the services included in a service application or all of the services included in a service definition, depending if you select a service application or a service definition in the left-panel, respectively.

The **Services** tab is included in the **Sites** tab.



The Services tab includes three tables:

- **VRF Definition** — Create and configure VRF (Virtual Routing and Forwarding) definitions for the service application. VRFs allow for networking paths to be segmented without using multiple devices.
- **VLAN Definition** — Create and configure VLAN (Virtual Local Area Network) definitions for the service application.
- **L2 VSN** — Configure the L2 Virtual Services Networks (VSNs).
- **L3 VSN** — Configure the L3 Virtual Services Networks (VSNs).

VRF Definition

The VRF Definition table allows you to configure virtual routing and forwarding definitions included as part of the service.

Name
The name of the VRF definition.

VRF ID
The ID number assigned to the VRF definition.

Multicast
Select to indicate the service sends IP packets to a group of recipients on the network.

Unicast
Select to indicate the service sends IP packets to a single recipient on the network.

Direct Route
Select to indicate the service sends IP packets directly to another device without going through a third device.

VLAN Definition

The VLAN Definition table allows you to configure virtual local area network definitions included as part of the service.

Name
The name of the VLAN definition.

VID
The ID number assigned to the VLAN.

VRF ID
The ID number assigned to the VRF definition.

Multicast
Indicates the service sends IP packets to a group of hosts on the network.

IGMP Version
Indicates which version of IGMP is utilized on the port (Version 1 or Version 2).

IGMP Querier
The address of the IGMP Querier. This feature is used when there is no multicast router in the VLAN to originate the queries.

Querier Enable
Indicates whether an IGMP Query is enabled.

Virtual Routing
Displays the version of VRRP the default gateway is using:

- **NONE** — Virtual routing is not configured on the VLAN.
- **VRRPv2** — VRRP version 2 is configured on the VLAN. VRRP version 2 only supports IP addresses in IPv4 format.
- **VRRPv3** — VRRP version 3 is configured on the VLAN. VRRP version 3 supports IP addresses in both IPv4 and IPv6 formats.
- **DvR –** DvR functionality is configured on the VLAN.

NOTE: Virtual Routing is only supported on Fabric Engine devices.

Virtual Routing Enable
Indicates whether virtual routing is enabled for the VLAN.

Virtual Routing Address

The IP address for the virtual routing interface. The Virtual Routing address must be in the same subnet as the VLAN subnet address.

VRRP ID

An identifier devices use to determine peer devices that participate in a virtual routing interface.

VRRP Priority

A value used by VRRP peers to determine the role of each of the devices in the VLAN. The default value is **100**. The device with the largest value is assigned the role of Master. For example, in a VLAN with two routers, one with a **VRRP Priority** of **200** and one with a **VRRP Priority** of **100**, the router with a **VRRP Priority** of **200** becomes the Master. In the event of identical priority numbers, the devices use the MAC address to determine priority.

VRRP Backup Master

This option determines if the backup router is able to forward traffic independently outside of the VLAN (enabled), or must forward the traffic to the Master router before it is forwarded outside of the VLAN (disabled).

VRRP Advertisement Interval

Indicates frequency (in seconds) that protocol packets are sent from the virtual router in the VLAN.

VRRP Hold Down Timer

Indicates the amount of time (in hundredths of a second) that the backup router waits for the primary router to respond before it becomes the primary router.

DHCP Snooping

Indicates whether DHCP snooping is enabled for the VLAN. DHCP Snooping is a Layer 2 security feature, that provides network security by filtering untrusted DHCP messages received from the external network causing traffic attacks within the network. DHCP Snooping is based on the concept of trusted versus untrusted switch ports. Switch ports configured as trusted can forward DHCP Replies, and the untrusted switch ports cannot. DHCP Snooping acts like a firewall between untrusted hosts and DHCP servers.

ARP Inspection

Indicates whether ARP inspection is enabled. Dynamic ARP Inspection (DAI) is a security feature that validates ARP packets in the network. Without DAI, a malicious user can attack hosts, switches, and routers connected to the Layer 2 network by poisoning the ARP caches of systems connected to the subnet, and intercepting traffic intended for other hosts on the subnet. DAI prevents these attacks by intercepting, logging, and discarding the ARP packets with invalid IP to MAC address bindings. The switch dynamically builds the address binding table from the information gathered from the DHCP requests and replies when DHCP Snooping is enabled. The switch pairs the MAC address from the DHCP request with the IP address from the DHCP reply to create an entry in the DHCP binding table. When you enable DAI, the switch filters ARP packets on untrusted ports based on the source MAC and IP addresses seen on the

switch port. The switch forwards an ARP packet when the source MAC and IP address matches an entry in the address binding table. Otherwise, the switch drops the ARP packet.

NOTE: **DHCP Snooping** must be enabled to use **ARP Inspection**.

Service Application Name

The **Service Application Name** table displays all of the services included in a service application or all of the services included in a service definition, depending if you select a service application or a service definition in the left-panel, respectively. The Services tab is included in the **Sites** tab.

Services are created within service applications. You can include multiple services within an application. Service applications are then included within service definitions. You can also include multiple service applications within a service definition. A service definition that includes a complete set of services is then assigned to a site, which configures the fabric-enabled devices within that site.

The **Services** tab is only configurable when you select a service application. The services displayed when selecting a service definition are read-only.

L2 VSN

Name
The name of the Layer 2 service.

Service ID
The I-SID, which is the system-defined ID number assigned to the fabric service.

UNI Type
The User-Network-Interface (UNI) of the fabric service. The following interface types are available:

- **Switched** — A VLAN-ID and a port (VID, port) mapped to a Layer 2 VSN I-SID. With UNI type, VLAN-IDs can be reused on other ports and mapped to different ISIDs.
- **Transparent** - A physical port maps to a Layer 2 VSN I-SID (all traffic through the port, 802.1Q tagged or untagged, ingress and egress maps to the I-SID).

  NOTE: All VLANs on a Transparent Port UNI interface now share the same single MAC learning table of the Transparent Port UNI I-SID.

- **CVLAN** — a platform customer VLAN-ID.

VLAN
The customer VLAN-ID of the associated CVLAN UNI type.

CVID
Specifies the customer VLAN ID of the associated switched UNI port.

Management Service

Defines is the L2 VSN is used for switch management purposes.

AutoSense Service Type

Defines if the L2 VSN service is auto-assigned by the switch-level AutoSense detection. The following types are available:

- **AP Untagged** — If the AutoSense feature detects Access Point, then this service is automatically assigned to the port.
- **Camera Untagged** — If the AutoSense feature detects Camera then this service is automatically assigned to the port.
- **Voice Untagged** — If the AutoSense feature detects a VoIP device then this service is automatically assigned to the port.
- **Voice Tagged** — If the AutoSense feature detects a VoIP device then this service is automatically assigned to the port.
- **Proxy Switch Auth Tagged —** If the AutoSense feature detects a Fabric Attach switch capable of authenticating (ERS devices) then this service is automatically assigned to the port.
- **Proxy Switch No Auth Untagged —** If the AutoSense feature detects a Fabric Attach switch is not capable of authenticating (Switch Engine devices) then this service is automatically assigned to the port.
- **Proxy Switch Auth & Proxy Switch No Auth —** If the AutoSense feature detects any physical Fabric Attach switch (ERS/EXOS/Switch Engine device) then this service is automatically assigned to the port.
- **Data Untagged** — If the AutoSense feature does not detect a device type then this service is automatically assigned to the port.
- **None** — AutoSense is not related to this L2VSN service.

NOTE: Each AutoSense Service Type can only be used once on a switch. The switch cannot use two different service IDs with the same AutoSense Service Type.

AutoSense Service CVID

The AutoSense Service CVID value defines the 802.1q VLAN tag sent from the switch to the device. If the **AutoSense Service Type** is **Voice Tagged** or **Proxy Switch Auth Tagged** or **Proxy Switch Auth & Proxy Switch No Auth** then AutoSense Service CVID must be defined. The value range is 1-4094.

Port Template

If the **UNI Type** is **Switched** or **Transparent** you can select from the Global Port templates to define the purpose of the port.

L3 VSN

Name
The name of the Layer 3 service.

Service ID
The I-SID, which is the system-defined ID number assigned to the service.

VRF
Select the virtual routing and forwarding definition included as part of the service.

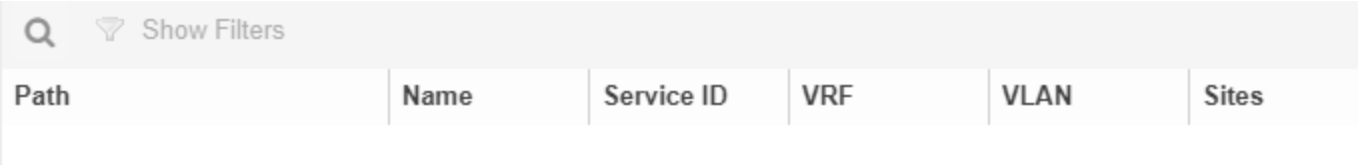
Multi Cast
Select to indicate that the service sends IP packets to a group of hosts on the network.

Unicast
Select to indicate that the service sends IP packets to a single recipient on the network.

Direct Route
Select to indicate that the service sends IP packets directly to another device without going through a third device.

Service Summary

The **Service Summary** tab displays a summary of the fabric services you create and the sites to which they are assigned.



Path
The path to the Service Application in which the service is located.

Name
The name of the fabric service included in the service application or definition.

Service ID
The I-SID, which is the system-defined ID number assigned to the service.

VRF
The ID number assigned to the VRF definition.

VLAN
The ID number assigned to the VLAN.

Sites
The site to which the fabric service is assigned.

- Services
- Fabric
- Sites

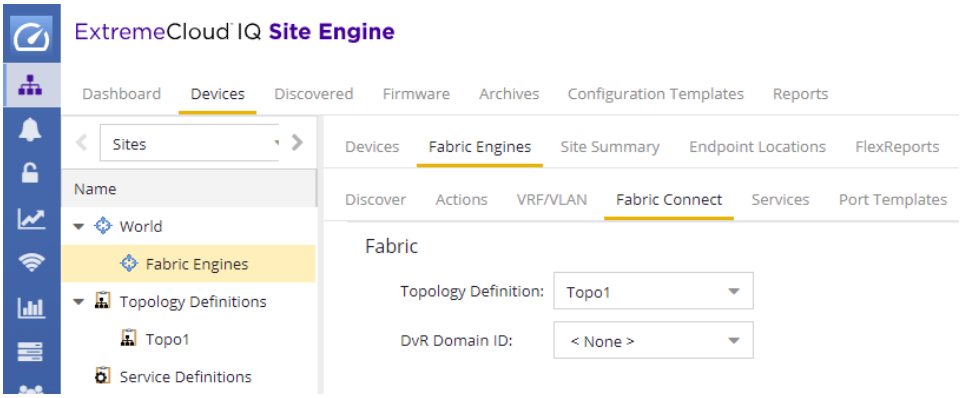
Applying Fabric Services

When you have created and configured your fabric topology, service and service application services, you can apply them to sites within your network. When fabric topology and services have been assigned to a site, they cannot be deleted.

NOTE: Services not assigned to a service definition (where NONE has been selected) can be deleted from a site after they have been assigned to that site.

Applying a Fabric Topology to a Site

1. Open the **Network > Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Select a site in the left-panel tree.
4. Select the site name tab in the **Devices** sub-tab.

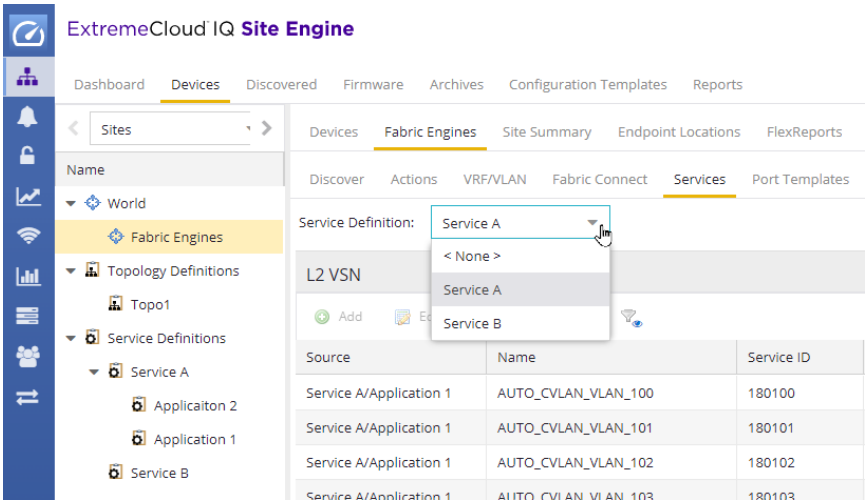


5. Select the **Fabric Connect** tab.
6. Select the topology you want to apply to the site from the **Topology Definition** drop-down list.
7. Select the DVR Domain from the **DVR Domain** drop-down list.
8. Select **Save**.

NOTE: Only one Fabric Topology and one DVR Domain can be assigned a site in ExtremeCloud IQ Site Engine.

Applying a Service Application to a Site

1. Open the **Network > Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Select a site in the left-panel tree.
4. Select the site name tab in the **Devices** sub-tab.
5. Select the **Services** tab.
6. Select the service definition you want to apply to the site from the **Service Definition** drop-down list. The service application details that you configured to the service definition display in the L2 VPN and L3 VPN tables.



7. Select **Save** to apply the services to the site.

Applying Fabric to Port Templates

The Port Templates Configuration window enables you to configure ports with a Fabric role. When complete, you can apply the Port Templates configuration to a device.

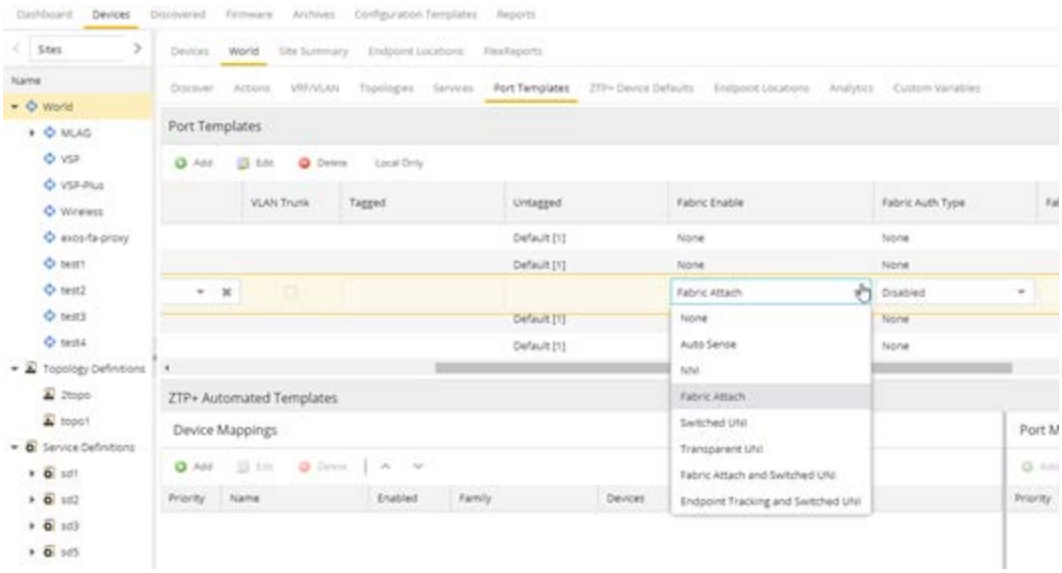
ExtremeCloud IQ Site Engine supports the following Fabric roles:

- None
- NNI
- Fabric Attach

- Switched UNI
- Transparent UNI
- Fabric Attach and Switched UNI

NOTE: The Fabric Attach (FA) and Switched UNI (S-UNI) option means that the port is configured for both features, but only one feature is active at any one time. The mode is determined by which mapping request the port receives first (FA or S-UNI). Ports receive mapping requests via LLDP TLVs.

The following screen capture shows the Port Templates window, which you can access from either the World view or from a specific Site.



Use the following steps to configure fabric to a port template:

NOTE: Port templates for which you configure Fabric Enable values must be configured as Global port templates. To create a Global port template, select the World site and select **Global** from the **Source** drop-down list.

1. Open the **Network > Devices** tab.
2. Select **World** or a specific Site, and then the **Port Templates** tab.
3. Select a template, and then the Edit (Edit) button.
4. Under Fabric Enable, select a fabric mode.
5. Under Fabric Auth Type, select an authentication type.
6. Under Fabric Auth Key, select an authentication key if available.
7. Select **Save**

Applying Fabric to Ports

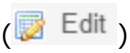
The Port Configuration window enables you to edit the fabric information about the ports on a device.

ExtremeCloud IQ Site Engine supports the following Fabric roles:

- None
- NNI
- Fabric Attach
- Switched UNI
- Transparent UNI
- Fabric Attach and Switched UNI

NOTE: The Fabric Attach (FA) and Switched UNI (S-UNI) option means that the port is configured for both features, but only one feature is active at any one time. The mode is determined by which mapping request the port receives first (FA or S-UNI). Ports receive mapping requests via LLDP TLVs.

Use the following steps to configure fabric to a port:

1. Open the **Network > Devices** tab.
2. Select **Devices**.
3. Select the **Menu** icon (☰) or right-click on a device.
4. Select **Configure**.
   The Configure Device window opens.
5. Select **Ports**.
6. Select a port, and then the Edit (

) button.
7. Under Fabric Enable, select a fabric mode.
8. Under Fabric Auth Type, select an authentication type.
9. Under Fabric Auth Key, select an authentication key if available.
10. Select **Save**.

Applying Fabric Services to a Device

After you have applied fabric topologies and services to a site, you can also apply the fabric services to devices assigned to that site.

Applying Fabric Topology to a Device

1. Open the **Network > Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Right-click a site in the left-panel tree.
4. Select **Configure Device** from the drop-down list. The **Configure Device** window opens.
5. Select the **Fabric Connect** tab.
6. Select the **Sync from Site** button to populate the tab with the fabric topology details you applied to the site. The topology details you applied to the site will be applied to the device, as long as the device you have selected is assigned to the same site.
7. To populate the tab manually, select the **Enable Fabric** checkbox.
8. Select a **Fabric Role** from the drop-down list.
9. Enter a system ID number in the **System ID** field.
10. Enter a nickname in the **SPBM Nickname** field.
11. Check the **Multicast** checkbox, if needed.
12. Check the **IP Shortcuts** checkbox, if needed.
13. Enter the system name in the **System Name** field.
14. Select the **Enforce Preview** button.

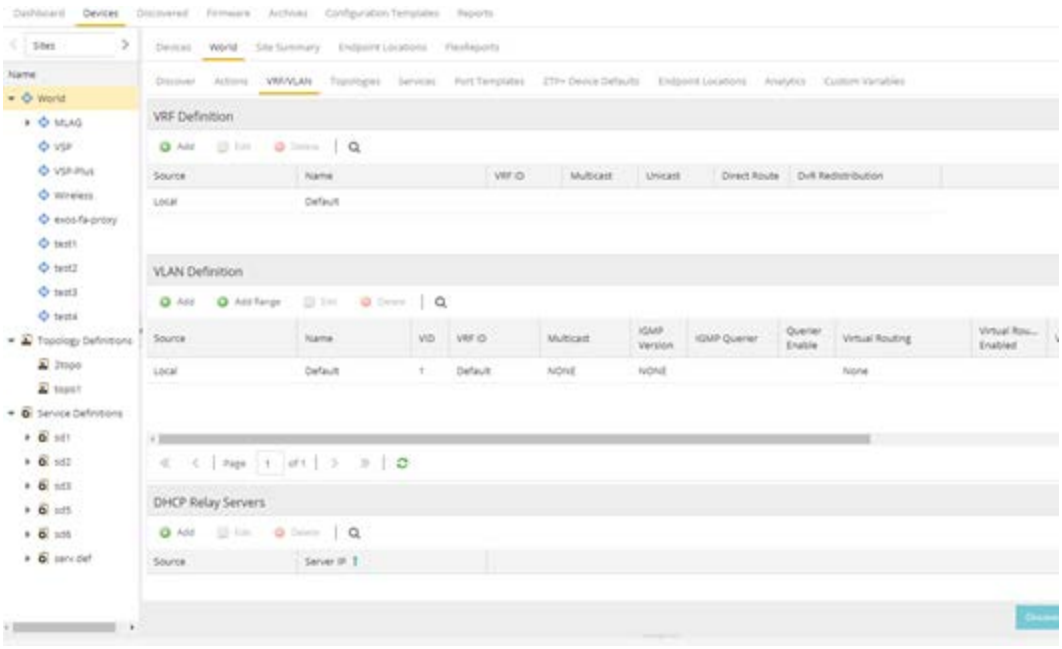
Applying Fabric Services to a Device

1. Open the **Network > Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Right-click a site in the left-panel tree.
4. Select **Configure Device** from the drop-down list. The **Configure Device** window opens.
5. Select the **Services** tab. The service details that you configured to the site display in the L2 VPN and L3 VPN tables.
6. Select the **Sync from Site** button to populate the tab with the fabric service details you applied to the site. The service details you applied to the site will be applied to the device, as long as the device you have selected is assigned to the same site.
7. Select the Add (Add) button to add an L2 VSN or L3 VSN service to the device.
8. Select the Edit (Edit) button to edit service details that were populated from the site.
9. Select the **Enforce Preview** button.

NOTE: The L3VPN table is disabled when the device is set as a DVR Leaf node.

Adding and Deleting VRF Definitions

1. Open the **Network > Devices tab**.
2. Select **Sites** from the left-panel tree drop-down list.
3. Right-click a site in the left-panel tree.
4. Select **Configure Device** from the drop-down list. The **Configure Device** window opens.
5. Select the **VRF/VLAN** tab.



The top table on the **VRF/VLAN** tab in the **Configure Device** window displays read-only VRF details you applied to the site. You can add a new VRF to the device.

1. Select the Add (Add) button.
2. Enter the name of a VRF in the **Name** field.
3. Enter the ID number in the **VRF ID** field.
4. Select **Update** to add the VRF to the device.
5. Select the **Enforce Preview** button.

You can delete a VRF from the **VRF/VLAN** tab.

1. Select a VRF in the table.
2. Select the **Delete** (Delete) button.
3. Select **Yes** to remove the VRF.

Adding and Deleting VLAN Definitions

1. Open the **Network > Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Right-click a site in the left-panel tree.
4. Select **Configure Device** from the drop-down list. The **Configure Device** window opens.
5. Select the **VRF/VLAN** tab.

   The middle table on the **VRF/VLAN** tab in the Configure Device window displays read-only VLAN details you applied to the site. You can add a new VLAN to the device.

   1. Select the Add (Add) button.
   2. Enter the name of a VLAN in the **Name** field.
   3. Enter the ID number in the **VLAN ID** field.
   4. Select **Update** to add the VLAN to the device.
   5. Select the **Enforce Preview** button.

   You can delete a VLAN from the **VRF/VLAN** tab.

   1. Select a VLAN in the table.
   2. Select the **Delete** (Delete) button.
   3. Select **Yes** to remove the VLAN.

Enforcing the Fabric Configurations

After you enforce previews on the **Fabric Connect**, **Services**, and **VRF/VLAN** tabs, use the **Compare Device Configuration** window to enforce the configurations to the device. Additionally, the **VLAN Definition** tab allows you to enforce the **VLAN** and **Ports** fabric configurations.

Enforcing Fabric Connect

1. Select **Enforce Preview** on the **Fabric Connect** tab in the **Configure Device** window.
2. The **Compare Device** window opens.
3. Select the Fabric Connect Enforce Option.
4. Select **Enforce**.

Enforcing Fabric VRF

1. Select **Enforce Preview** on the **VRF/VLAN** tab in the **Configure Device** window.
2. The **Compare Device** window opens.
3. Select the **VRF/VLAN** tab.
4. Select **Enforce**.

Enforcing Fabric Services

1. Select **Enforce Preview** on the **Services** tab in the **Configure Device** window.
2. The **Compare Device** window opens.
3. Select the Services Enforce Option.
4. Select the **L2 VPN** tab.
5. Select **Enforce**.
6. Select the **L3 VPN** tab.
7. Select **Enforce**.

Enforcing Fabric VLAN

1. Select **Enforce Preview** on the **VLAN** tab in the **Configure Device** window.
2. The **Compare Device** window opens.
3. Select the VLAN Definition Enforce Option.
4. Select **Enforce**.

Enforcing Fabric Port

1. Select **Enforce Preview** on the **Ports** tab in the **Configure Device** window.
2. The **Compare Device** window opens.
3. Select the Ports Enforce Option.
4. Select **Enforce**.

Fabric Manager ZTP+ Configuration (Legacy)

Fabric Manager is a resilient, scalable, and highly efficient network management application that allows your network domains to operate interdependently, efficiently, and with minimal intervention. Fabric Manager allows you to monitor the fabric topology and service applications on your network.

Fabric Manager is deployed as a separate virtual machine (VM) in ExtremeCloud IQ Site Engine, and is enabled via ZTP+ (Zero Touch Provisioning Plus) functionality.

General Network Configuration

Fabric Manager supports two initial configuration modes for ExtremeCloud IQ Site Engine discovery and registration: DHCP mode and Static mode. DHCP is the default configuration mode.

Use the Static mode when providing a predefined set of networking configurations.

Use the DHCP mode so the engine can communicate with the ExtremeCloud IQ Site Engine server. The following DHCP settings and DNS mapping of **extremecontrol** are for when Fabric Manager is installed in DHCP Mode:

- The DHCP Server needs to return a DNS Server and Domain Name to the ZTP+ device. It is the default mode of configuration during the Fabric Manager VM's initial bootup cycle.
- The DNS Server needs to map the name **extremecontrol.<*domain-name*>** to the IP address of the ExtremeCloud IQ Site Engine server.

Once ExtremeCloud IQ Site Engine and the ZTP+ device are pre-configured, you can add the site definition to the ExtremeCloud IQ Site Engine database. For information, see How to Add Fabric Manager.

For information on related topics:

- Sites
- Profiles
- Add Device
- Edit Device
- Devices

How to Add Fabric Manager (Legacy)

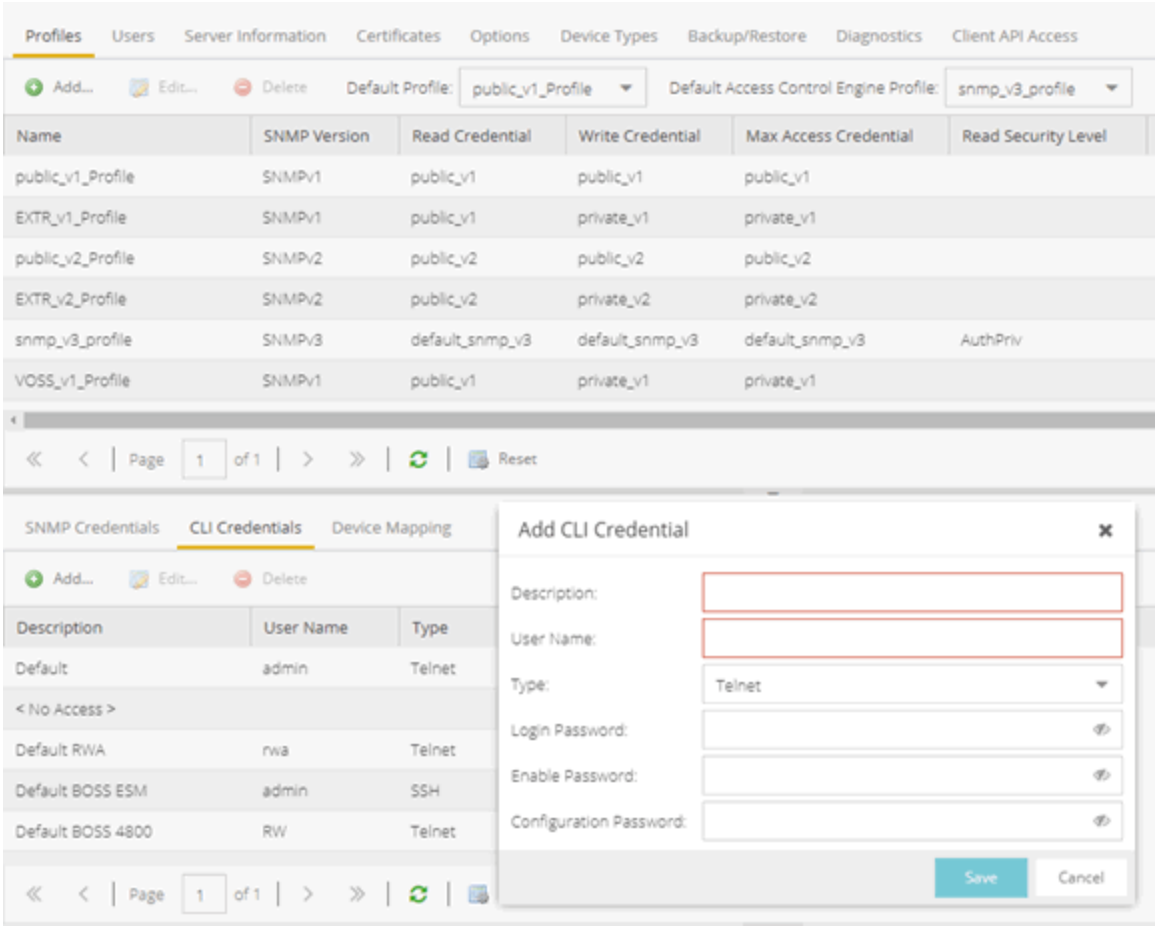
Once you install the Fabric Manager virtual machine (VM), you can add it to ExtremeCloud IQ Site Engine and enable it via ZTP+ (Zero Touch Provisioning Plus) functionality.

Adding Fabric Manager to ExtremeCloud IQ Site Engine

Prior to adding the Fabric Manager engine, you must create an Administration Profile for the Fabric Manager with CLI credentials. Fabric Manager uses the Administrator Profile as an additional user account.

Add CLI Credentials

1. Launch ExtremeCloud IQ Site Engine.
2. Open the **Administration > Profiles** tab.
3. In the bottom panel, select the **CLI Credentials** tab.

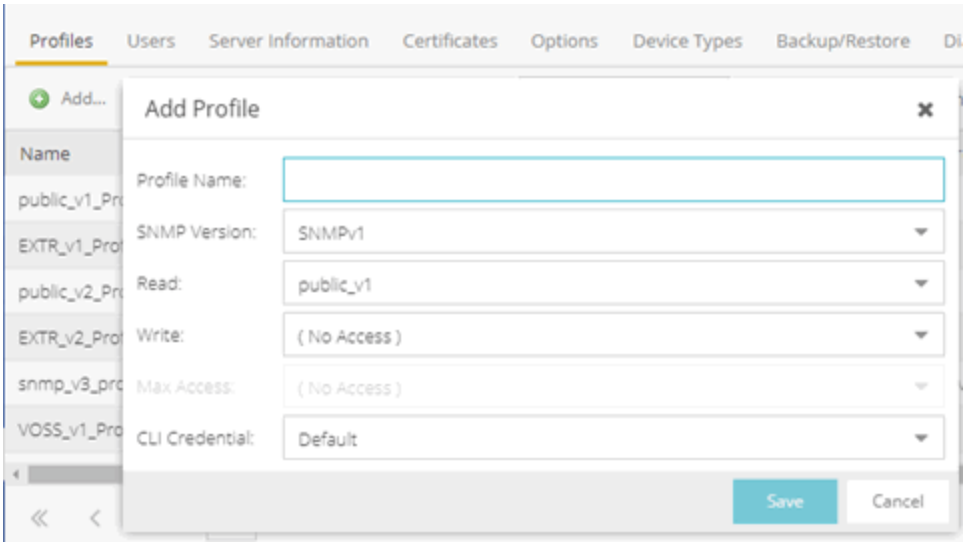


4. Select the **Add** button (Add) to open the **Add CLI Credential** window.
5. Enter a name for the CLI Credential in the **Description** field.
6. Enter **root** in the **User Name** field.
7. Select **SSH** from the **Type** drop-down list.
8. Enter a password in the **Login Password** field.
   This password must be the same password that you provided in Step 2b of the Fabric Manager Installation Static Mode topic.
9. Enter a password in the **Enable Password** field.

10. Enter a password in the **Configuration Password** field.
11. Select **Save**.

Create Administration Profile

1. At the top of the **Profiles** tab, select the **Add** button (Add) to open the **Add Profile** window.



2. In the **Profile Name** field, enter a name for this profile.
3. In the **SNMP Version** field, select **SNMPv1**.
   Fabric Manager does not use SNMP; the SNMP credentials here are just placeholders.
4. In the **Read** field, select **Ping Only**.
5. In the **Write** field, select either **No Access** or **Ping Only**.
6. In the **CLI Credential** field, select the same CLI Credential that you created in Step 4 of the Add CLI Credentials topic.
7. Select **Save**.

Add Administration Profile to the Fabric Manager engine

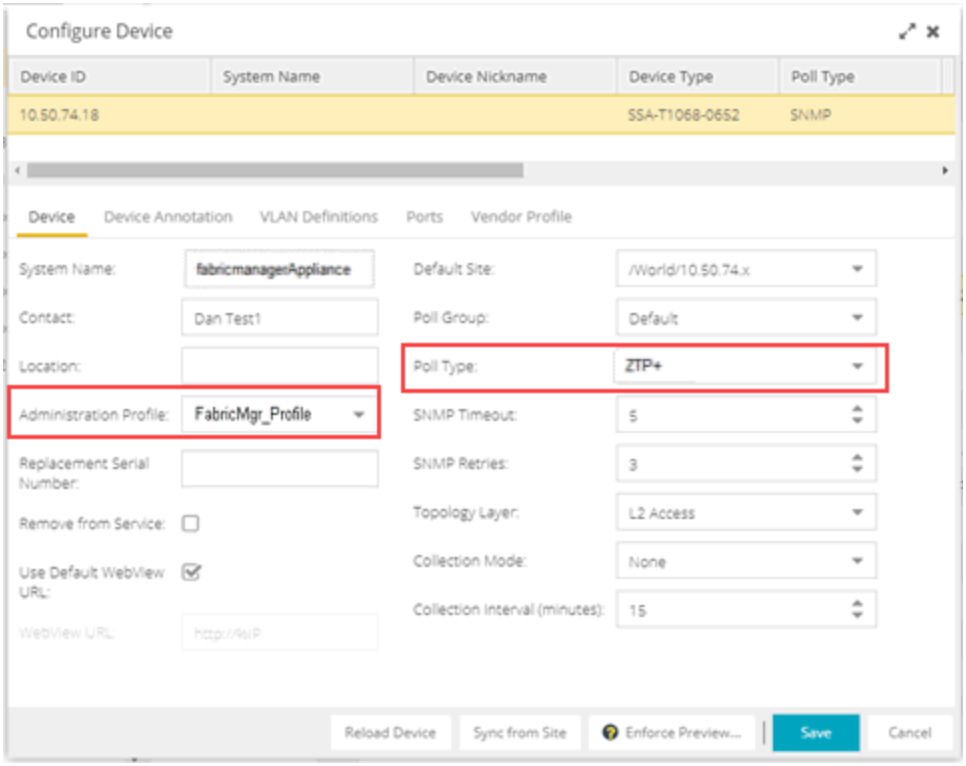
1. Open the **Network** > **Discovered** tab in ExtremeCloud IQ Site Engine.

NOTE: The Fabric Manager appears as a device on the **Discovered** tab. It is listed with a **Status** of **ZTP+ Pending Edit**, indicating the configuration needs to be edited before adding it to the ExtremeCloud IQ Site Engine server.

---

2. Right-click the new Fabric Manager file and select **Configure Devices** tab from the drop-down list.

   The **Configure Device** window opens.



3. Select the profile you created from the **Administration Profile** drop-down list.
4. Select **ZTP+** from the **Poll Type** drop-down list.
5. Select the **ZTP+ Device Settings** tab in the **Configure Device** window.
6. Configure the fields on the **ZTP+ Device Settings** tab to determine how the Fabric Manager is managed by ExtremeCloud IQ Site Engine using ZTP+ functionality.

ZTP+ Discovery

Once the ZTP+ discovery process is complete, the Fabric Manager engine is added to the ExtremeCloud IQ Site Engine database and moves from the **Network** > **Discovered** tab to the **Network** > **Devices** tab. The ZTP+ discovery process may take up to five minutes to complete.

NOTES: If you did not select **Automatically Add Devices** on the **Site** tab, the Fabric Manager engine remains on the **Discovered** tab with a **Status** of **ZTP+ Complete**. Select the file, select the **Add Devices** button (the **Add Device** window appears), and select the **Add** button to add the device to the ExtremeCloud IQ Site Engine database.

> In the event a configuration is not correctly transmitted to the switch or if connectivity is lost during any part of this process, the file resets and allows the process to restart.

The Fabric Manager engine **Status** (displayed on the Discovered tab) is now **ZTP+ Staged**, indicating ExtremeCloud IQ Site Engine will push the configuration to the device the next time the device contacts ExtremeCloud IQ Site Engine.

When ExtremeCloud IQ Site Engine pushes the configuration to the Fabric Manager engine, the **Status** is **ZTP+ Complete**.

- ExtremeCloud IQ Site Engine Fabric
- Fabric Connect

Fabric Topology Definition on the Sites Tab

Use the **Fabric Topology Definition** tab to create a fabric topology definition, configure fabric topology settings, and review fabric topology paths and sites. You can also rename or delete a fabric topology definition.

Create a Topology Definition

You can create a Topology Definition on the **Sites** tab in ExtremeCloud IQ Site Engine. After you create topology definitions, you can add them to sites in your network to build a fabric topology map.

To create a topology definition:

1. Access the **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Navigate to **Topology Definitions** in the left-panel tree.
4. Right-click **Topology Definitions**.
5. Select **Create Topology Definition**.

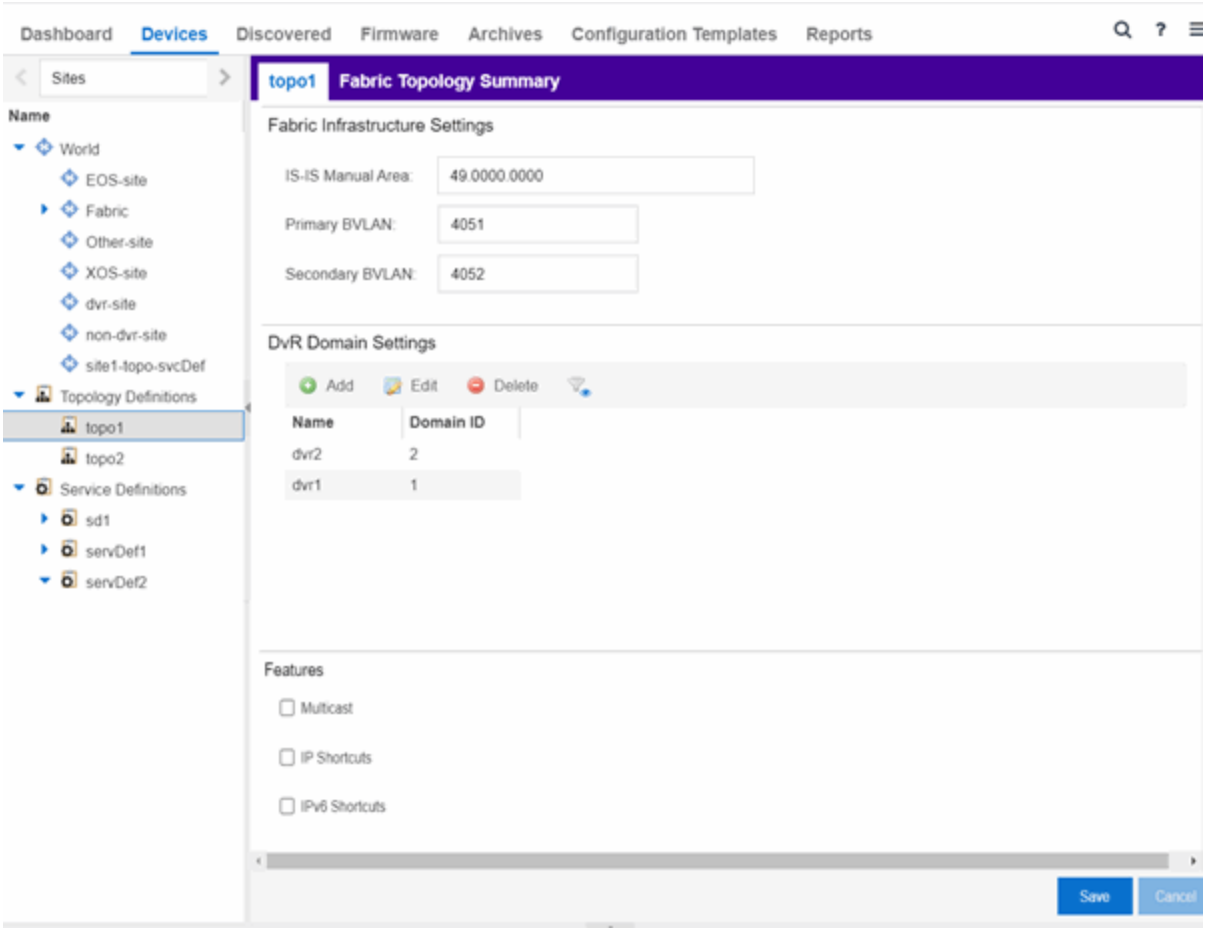
   The **Create Topology Definition** window opens.
6. Enter a name in the **Name** field.
7. Select **Fabric Connect** from the **Fabric Type** drop-down.
8. Select **OK** to create the topology definition.

Configure a Topology Definition

After the topology definition is created, it is available in the **Sites tab** left-panel tree. Select it to open a new right panel that includes the Fabric Name tab and a Fabric Summary tab.

Fabric Name Tab

Use the **Fabric Name** tab to configure the topology definition.



The Topology Definition tab includes the following sections:

Fabric Infrastructure Settings

The following fields are included in the Fabric Infrastructure Settings section:

- ISIS Manual Area - Use a xx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx format (1-13 bytes).
- Primary BVLAN - Enter the Primary Backbone VLAN (BVLAN).
- Secondary BVLAN - Enter the Secondary BVLAN.

DvR Domain Settings

The following fields are included in the DvR Domain Settings section:

- Name - The Domain name assigned to the DvR Domain. Select the down arrow to open the drop-down list to access sort, hide columns and search filter functionality for the domain name column.

- Domain ID - The identifying number assigned to the DvR Domain. Select the down arrow to open the drop-down list to access sort, hide columns and numeric filter functionality for the Domain ID column.

You can also Add, Edit, or Delete DvR Domain settings.

Features

The following fields are included in the Features section:

- Multicast - Select the check box to configure to distribute data to multiple recipients.
- IP Shortcuts - Select the check box to enable IPv4 Shortcuts for the topology definition.
- IPv6 Shortcuts - Select the check box to enable IPv6 Shortcuts for the topology definition.

Select **Save** to save the topology definition settings you selected.

After the topology definition is created and configured, you can apply it to a site within your network. After fabric topologies have been assigned to a site, they cannot be deleted.

Fabric Summary tab

The Fabric Summary tab lists any fabric topologies you have created and the sites to which they are assigned.

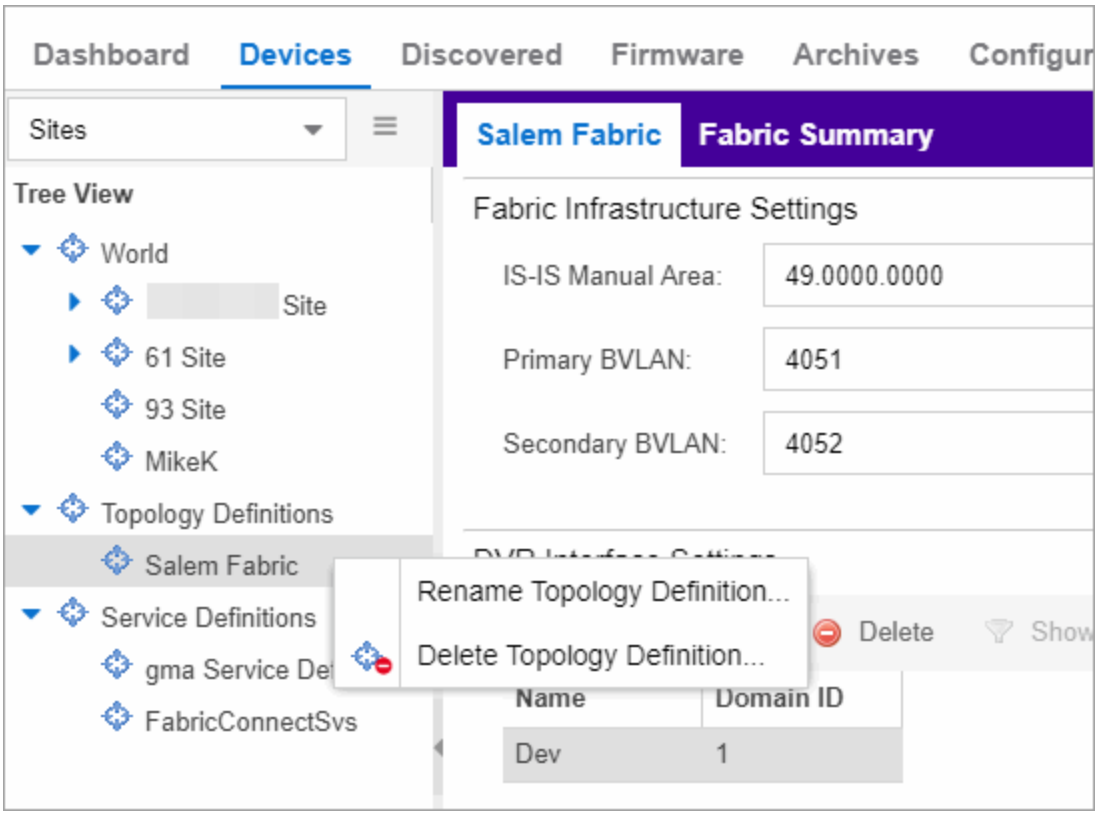
Rename a Topology Definition

After a topology definition has been created and configured, you can change or modify its name.

To rename a topology definition:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Expand **Topology Definitions** in the left-panel.

4. Right-click the topology definition you are renaming.



5. Select **Rename Topology Definition**.
6. Enter a new name in the **Name** field.
7. Select **OK** to change the topology name.

Delete a Topology Definition

After a topology definition has been created and configured, you can delete it; however, a topology definition cannot be deleted if it has been assigned to a site.

To delete a topology definition:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Expand the **Topology Definitions** in the left-panel.
4. Right-click the topology definition you are deleting.
5. Select **Delete Topology Definition**.
6. Select **Yes** to delete the topology definition you selected.

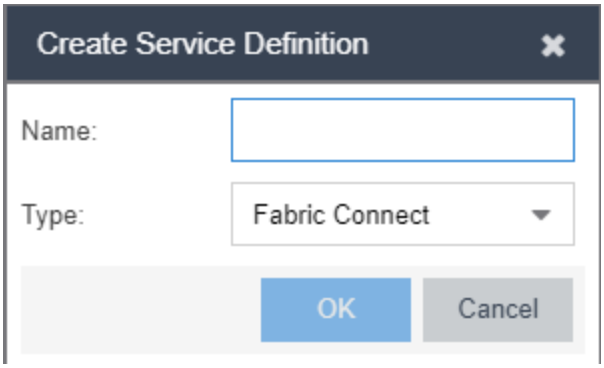
How to Create a Fabric Service Definition

You can create a service definition in the **Sites tab** in ExtremeCloud IQ Site Engine. Service definitions display information configured in service applications definitions. When created, service definitions are added to sites in your network and are used to build a fabric topology map.

Create a Service Definition

To create a service definition:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Select **Service Definitions** in the left-panel.
4. Right-click **Service Definitions**.
5. Select **Create Service Definition**.



   The **Create Service Definition** window opens.
6. Enter a name in the **Name** field.
7. Select **Fabric Connect** from the **Type** drop-down list.
8. Select **OK** to create the service definition.

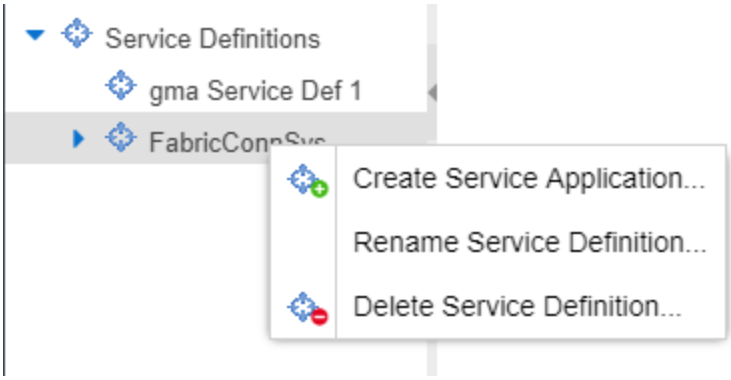
After the service definition is created and configured, you can apply it to a site within your network. When fabric services have been assigned to a site, they cannot be deleted.

Service Definition Panel

After the service definition is created, it is available in the left-panel tree. Select it to open a new right panel that includes a **Services** tab and a **Service Summary** tab.

Rename a Service Definition

After a service definition has been created and configured, you can change or modify its name.

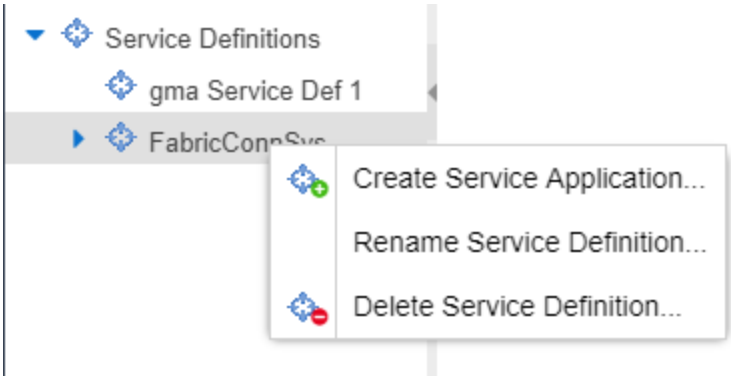


To rename a service definition:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Expand **Service Definitions** in the left-panel.
4. Right-click the service definition you are renaming.
5. Select **Rename Service Definition**.
6. Enter a new name in the **Name** field.
7. Select **OK** to rename the service definition.

Delete a Service Definition

When a service definition has been created and configured, you can delete it; however, a service definition or any of its associated service applications cannot be deleted if it has been assigned to a site.



To delete a service definition:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Expand **Service Definitions** in the left-panel.
4. Right-click the service definition you are deleting.
5. Select **Delete Service Definition**.
6. Select **Yes** to delete a service definition.

For information on related topics:

- Services
- Fabric
- Sites
- Devices

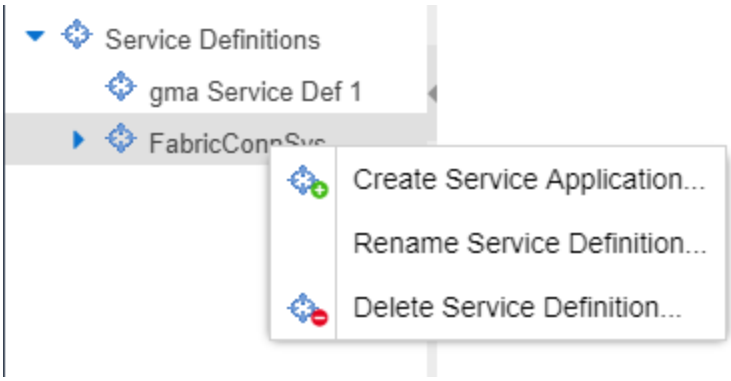
How to Create a Service Application

You can create a service application via the **Sites** tab in ExtremeCloud IQ Site Engine. Service definitions display information from service applications. When created, service applications are added to sites in your network and are used to build a topology map.

Create a Service Application

To create a service application:

1. Access the **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Expand **Service Definitions** in the left-panel.
4. Right-click the service definition in which you want to create the service application.



5. Select **Create Service Application**.

   The **Create Service Application** window opens.
6. Enter a name in the **Name** field.
7. Select **OK**.
8. Select the newly created service application.
9. Use the Services tab and a Service Summary tab to configure the service application.

The service application is created. After the service application is created and configured, you can apply it to a site within your network. After services have been assigned to a site, they cannot be deleted.

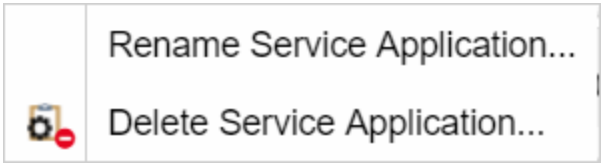
NOTE: A Service Application must have the same fabric type as its associated Service Definition. For example, if a Service Definition is created with Fabric Connect type, it can only have Service Applications of Fabric Connect type. Currently, Fabric Connect is the only fabric type available.

After the service application is created, it is available in the left-panel tree and a new right panel opens that includes a Services tab and a Service Summary tab.

Rename a Service Application

To change the name of a service application:

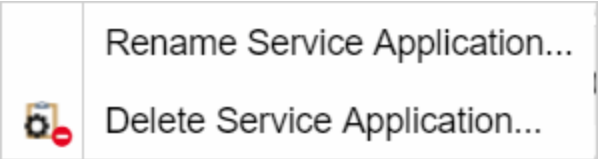
1. Open the **Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Expand **Service Definitions** in the left-panel.
4. Right-click the service application you are renaming.



5. Select **Rename Service Application**.
6. Enter a new name in the **Name** field.
7. Select **OK** to change the name of the service application.

Delete a Service Application

You can delete all user-defined service applications, unless the service application or any of its associated service definitions are assigned to a site.



To delete a service application:

1. Open the **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Expand **Service Definitions** in the left-panel.
4. Right-click the service application you are deleting.
5. Select **Delete Service Application**.
6. Select **Yes** to delete the service application.

For information on related topics:

- Services
- Fabric
- Sites
- Devices

Upgrading Fabric Manager (Legacy)

Use the following procedure to upgrade your version Fabric Manager.

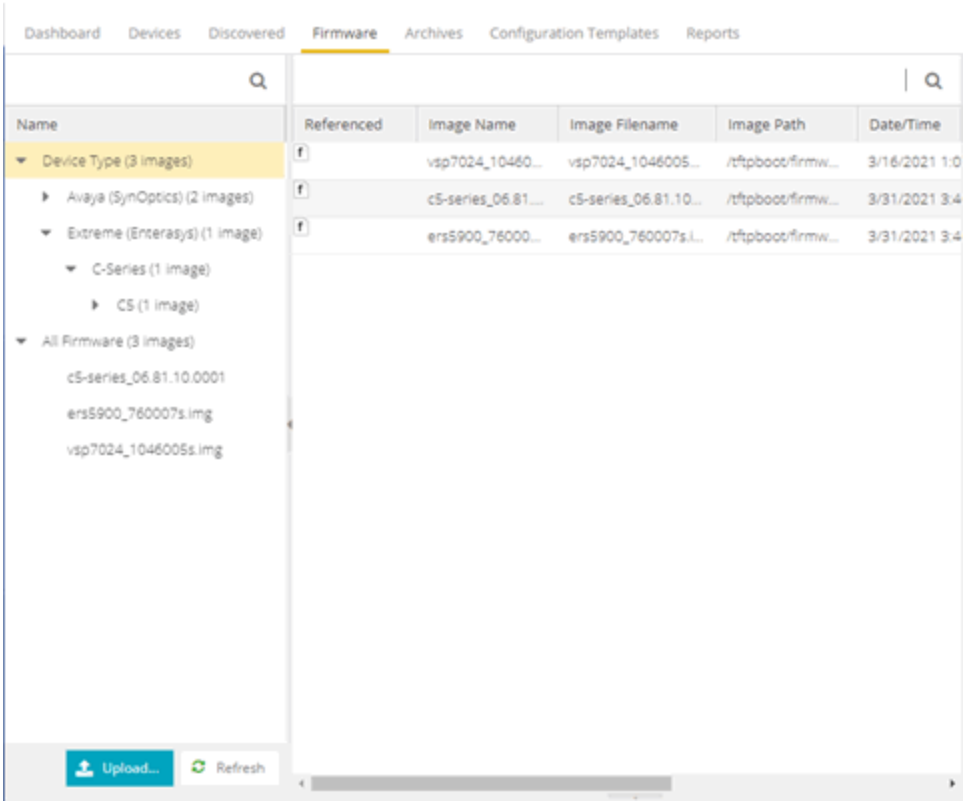
Prerequisites

- Upgrade ExtremeCloud IQ Site Engine to the later version before you upgrade Fabric Manager to the corresponding build number.
- Ensure that both the current and target ExtremeCloud IQ Site Engine and Fabric Manager build numbers are the same.
- Download the latest upgrade bundle from the Extreme Networks software download Portal.
- Change **Login Information** from **Anonymous** to appropriate SCP credentials in the SCP Server Properties section in the **Administration** > **Options** > **Inventory Manager** > **File Transfer** tab.

NOTE: After you deploy Fabric Manager and then register with ExtremeCloud IQ Site Engine, only the user credential associated with the Fabric Manager profile has SSH login access.

Upgrade Procedure

1. Open the **Network** tab in ExtremeCloud IQ Site Engine.
2. Select the **Firmware** tab.

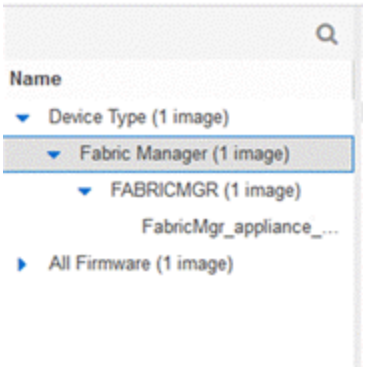


3. On the left panel, select **Upload** .
4. In the Directory field, select the **SCP** radio button and select **Upload**.

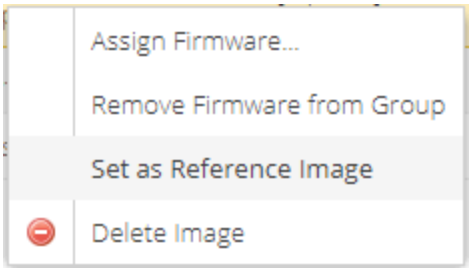


5. Select on **Drop files here or select to browse** and select the previously downloaded upgrade bundle.
6. Select the **Upload** button to initiate the bundle upload to the ExtremeCloud IQ Site Engine server.

   Once the upload is completed successfully, if not previously added after selecting the **Refresh** button, a new entry appears under Device Type called Fabric Manager.

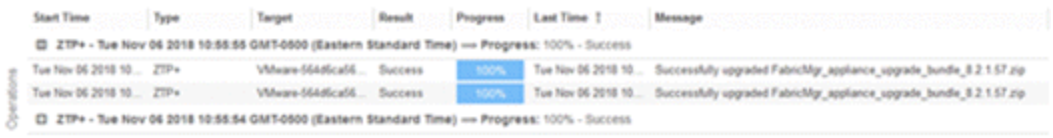


7. Navigate through the newly added Device type until you see the bundle image listed.
8. Right-click the bundle listed on the main panel and select **Set as Reference Image**.

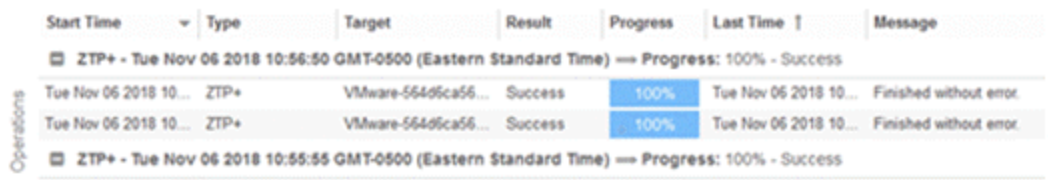


This step sets this image bundle as the Reference upgrade image for Fabric Manager. The upgrade process to get triggered by default can take **up to five minutes** depending on the poll interval set on ExtremeCloud IQ Site Engine.

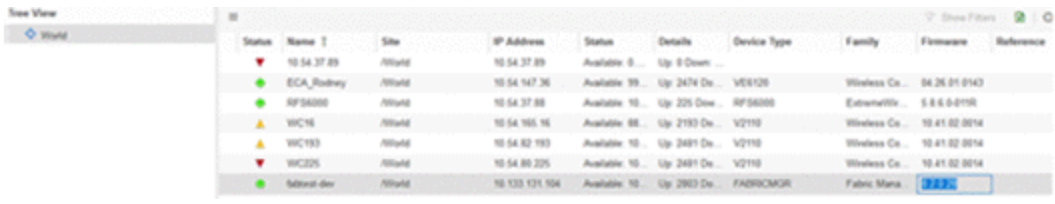
9. Open the **Operations** log on ExtremeCloud IQ Site Engine and wait until a log of type 'ZTP+' with the message `Successfully upgraded FabricMgr_appliance_upgrade_bundle_<version_number>.zip` appears.



This is followed by a message `Finished without error` to indicate the upgrade operation has been completed by the ZTP+.



10. When the upgrade is complete, the details on Fabric Manager are updated to the latest version.



Post Upgrade Steps

1. Ensure that the same user credential associated with the Fabric Manager profile has SSH login access.
2. Navigate to the previously added and referenced upgrade image and un-reference it by right selecting the bundle and then selecting **Unset as Reference Image**.

- ExtremeCloud IQ Site Engine Fabric
- Fabric Connect

Fabric Assist

The purpose of Fabric Assist is to help you set up your Fabric Connect network as quickly as possible. It will also eliminate the need to perform manual operations repetitively.

Fabric Assist helps you to migrate your existing VLAN-centric network to a Fabric Connect network. Fabric Assist accomplishes the migration by enhancing VLAN provisioning using the following features:

- VLAN Trunk Mode – Identifies a port as a VLAN trunk and automatically adds all the device VLANs as tagged.
- VLAN Range - Imports many VLANs to the device instead of manually adding and editing one entry at a time.
- Layer 2 VSN Service Creation - Automatically maps VLAN entries to Layer 2 VSNs.
- VLAN Pruning - Prevents the unnecessary configuration of VLANs that have no egress.
- Import to Service Definition - Enables you to import a device's active configuration into a Service Application, which you can then use as a configuration template for other devices managed by ExtremeCloud™ IQ Site Engine.

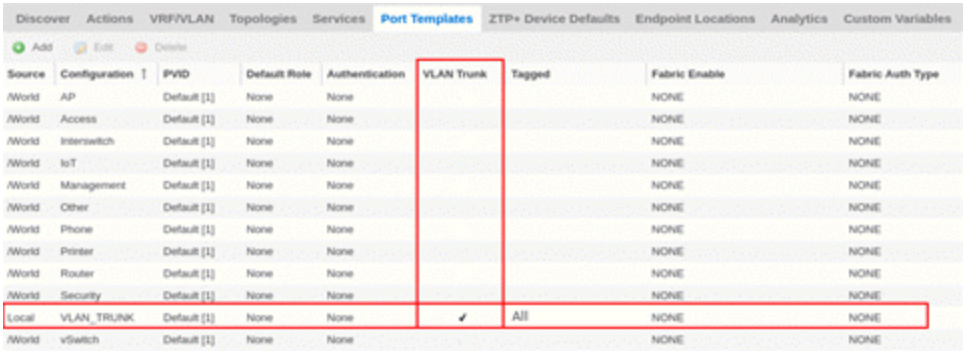
IMPORTANT: With the VLAN Trunk Mode and Layer 2 VSN Service Creation features, you can provision VLAN trunk ports and Layer 2 VSNs automatically. Do not use these features if the device is running **Fabric Attach**. Fabric Attach dynamically makes equivalent configuration changes, and if Fabric Assist is enabled, it will change those settings to static on the device.

For information on related topics:

- Provision VLAN Trunks Automatically
- How to Edit a Port Template
- Add a Range of VLANs at the Device Level
- Add a Range of VLANs at the Site Level
- Add a Range of VLANs at the Service Definition Level
- Enable Fabric Assist
- Fabric Assist L2 VSN Considerations

VLAN Trunk Mode

VLAN Trunk mode enables you to configure a port as a VLAN trunk and add all the VLANs on the port as tagged. This configuration happens automatically when you select one box in the VLAN Trunk column.



- **Trunk ports** link to other switches, as opposed to access ports that link to end devices.
- **Tagged ports** pass traffic for multiple VLANs, as opposed to untagged ports that accept traffic for only a single VLAN.

The VLAN Trunk column is available on the **Ports** and **Port Templates** tabs. This feature enables you to configure VLAN Trunks on an individual port or map the template to multiple ports.

IMPORTANT: With the VLAN Trunk Mode feature, you can provision VLAN trunk ports automatically. Do not use this feature if the device is running **Fabric Attach**. Fabric Attach dynamically makes equivalent configuration changes, and if Fabric Assist is enabled, it will change those settings to static on the device.

Configuring VLAN Trunks on a Port

At the **Ports** level, you can configure the VLAN trunk property *only* if no port template is assigned to that port. Then you can enable VLAN Trunk to attach all VLANs created at the device level.

NOTE: To edit a port that is bound to a port template, you must change the Port Template type to <Use Local Settings >. For more information, see How to Edit a Port Template.

You can update the port data on a port with VLAN Trunk enabled. However, you cannot modify the tagged and untagged areas of this port. All VLANs shown in the VLAN Definition window are Tagged, and no VLAN will be included under Untagged.

The Ports dialog updates automatically when you make VLAN definition changes such as adding or deleting VLANs. Changes that you make to VLANs at the site or service level also result in updates to the Ports dialog.

Fabric Assist makes the following behavioral changes when you upgrade Extreme Management Center to Release 8.4 (and later) and during the Device Discovery process. The Port Template Inheritance feature compares the Port Template and the configuration for each port of each device.

- If the port configuration matches the attributes defined by the assigned Port Template, the assigned Port Template type will remain assigned to that port.
- If the port configuration differs from the attributes defined by the assigned Port Template, the assigned Port Template type changes to <Use Local Settings> for that port.

Reload Device behaves the same as Device Discovery, except that the Port Template Inheritance feature compares the *previously assigned* Port Template with the actual configuration for the port on the device.

Configuring VLAN Trunks on a Port Template

After you check VLAN Trunk at the Port Templates level, Fabric Assist does the following:

- Automatically provisions tagged VLANs for this template.
- Disables the editors for the Tagged column and for all Fabric-related fields, such as Fabric Enable, Fabric Auth Type, and Fabric Auth Key.
- Changes the Tagged field to display **All**.
- Changes the Fabric Enable field to display **NONE**.

When you map a VLAN trunk port template to a port, Fabric Assist imports all the VLAN settings, including the VLAN Trunk property, from the template to the port. All the VLANs in the device grid will be tagged to this port.

NOTE: Changes made to VLANs at the site or service level have no effect on the port template.

For information on related topics:

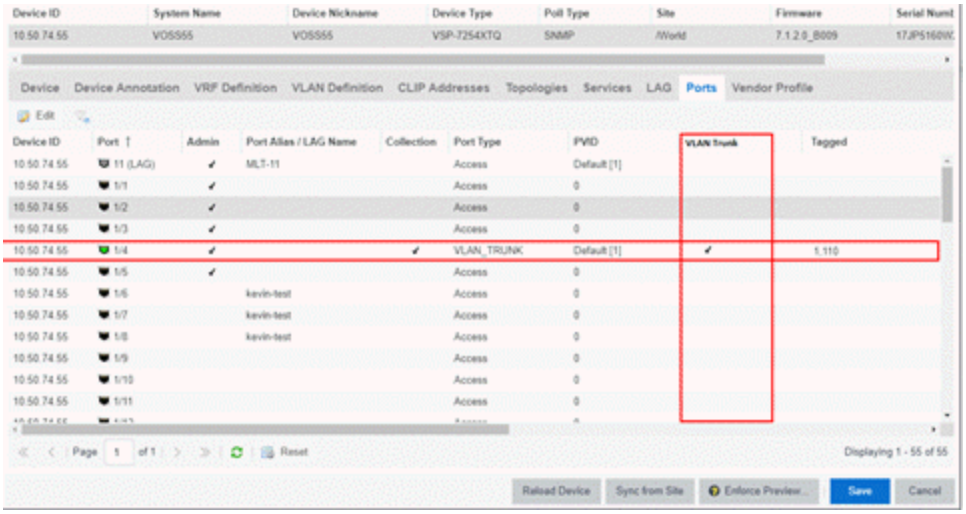
- Provision VLAN Trunks Automatically
- How to Edit a Port Template

Provision VLAN Trunks Automatically

You can provision trunks at the Ports level or at the Port Templates level.

To Provision VLAN Trunks at the Ports Level:

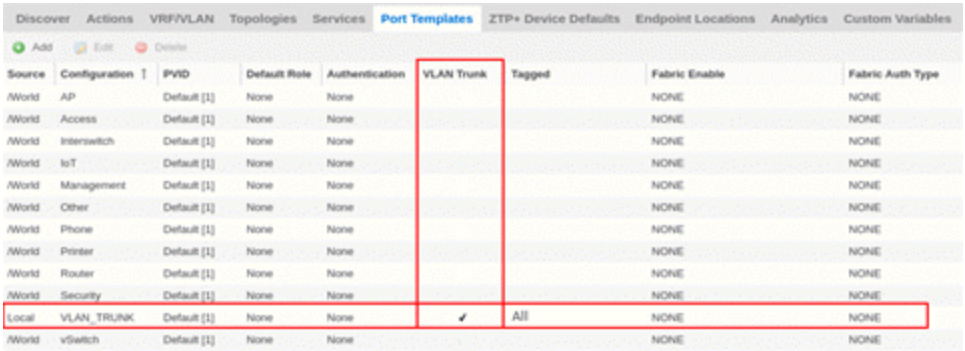
1. Open **Devices > Devices**.
2. Right-click on a specific device, and then select **Configure**.
   The system displays the **Configure Device** dialog.
3. In the Configure Device dialog, select **Ports**.



4. Select  Edit .
5. Select a port, and then check **VLAN Trunk**.
6. Select **Save**.

To Provision VLAN Trunks at the Port Templates Level:

1. Open **Devices > World**.
2. Select **Port Templates**.
   The system displays the **Port Templates** dialog.



3. Select Edit .
4. Select a port, and then check **VLAN Trunk**.
5. Select **Save**.

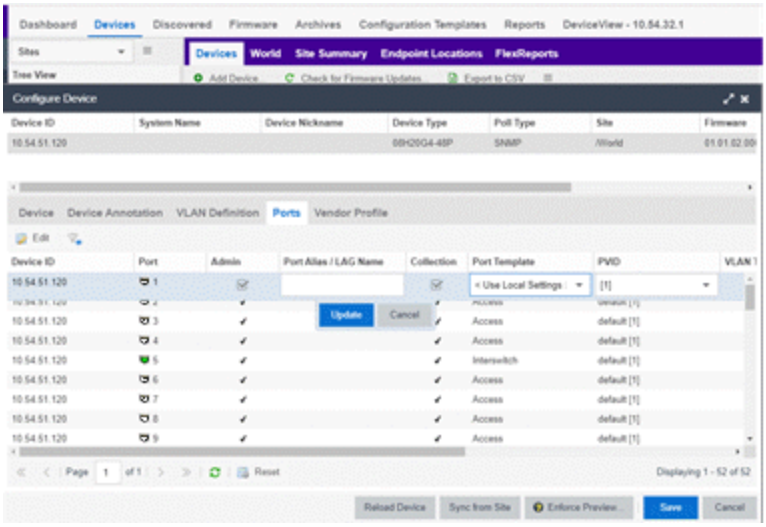
Edit a Port Template

You cannot edit all the fields for a port that is bound to a template. If you want to edit all the fields, you must change the Port Template type to **<Use Local Settings>**. This Port Template type value is available only in the Device Port grid.

NOTE: Ports that have a Port Template type of **<Use Local Settings>** will not inherit any settings from any defined Port Template.

To edit a Port Template:

1. Open **Devices > Devices**.
2. Right-click on a specific device, and then select **Configure**.
   The system displays the **Configure Device** dialog.
3. In the Configure Device dialog, select **Ports**.
4. In the Port Template drop-down column, select **<Use Local Settings>**.



VLAN Range

VLAN Range makes it easy to add many VLANs to a device. To add VLANs in a group, instead of manually adding and editing one entry at a time, provide the VID range, Name prefix, and VRF ID for all

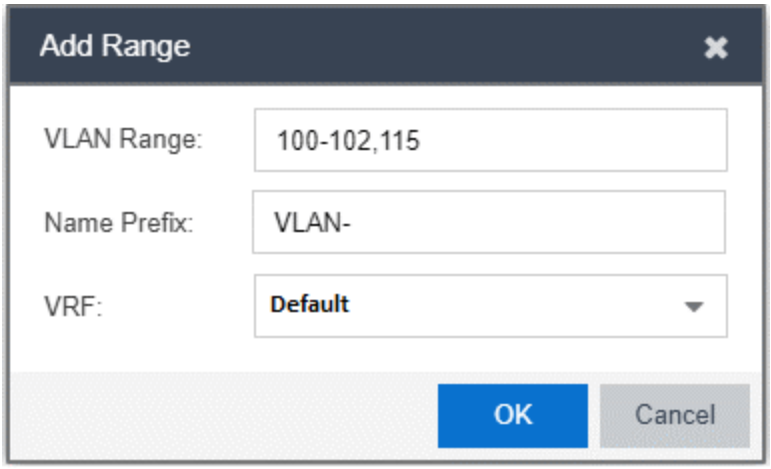
newly imported VLANs.

You can provision VLANs from three different levels (device, site, service definition):

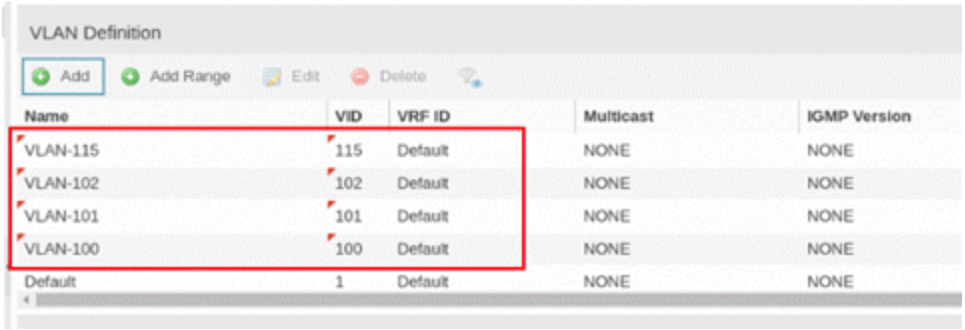
- **Device Level** – Use this level to configure a VLAN on an individual device.
- **Site Level** – Use this level to configure VLANs for all the devices that belong to a site.
- **Service Definition Level** – Use this level to configure VLANs on a Service Definition, which serves as a container for shared configurations. You can assign a Service Definition to a site, which then applies all the contained configurations to all the devices that belong to that site.

In the VLAN Definition window for the above levels, select Add Range to specify the following:

- Comma-separated list of VLAN ranges
- Prefix that is used for the auto generated VLAN names
- VRF



When you select OK, Fabric Assist creates the specified VLANs and displays them in the corresponding VLAN Definition window (device, site, or service definition).



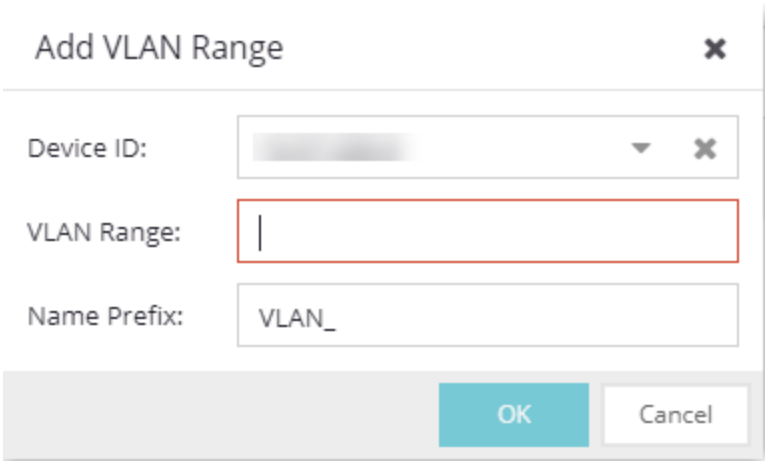
For information on related topics:

- Add a Range of VLANs at the Device Level
- Add a Range of VLANs at the Site Level
- Add a Range of VLANs at the Service Defiinition Level
- VLAN Pruning

Add a Range of VLANs at the Device Level

To configure a range of VLANs that apply to a specific device only:

1. Open **Devices > Devices**.
2. Right-click on a specific device, and then select **Configure**.
   The system displays the **Configure Device** dialog.
3. In the Configure Device dialog, select the **VLAN Definition** tab.
4. Select Add Range.



5. For **Device ID**, select the device where you want to create the VLANs.
6. For **VLAN Range**, enter the range of VLAN IDs using a comma to separate them. You can use a dash to enter consecutive IDs such as 1-10.
7. For **Name Prefix**, enter a name for the prefix that all the created VLANs will use. The format is <prefix>-<vlanId>).
8. For **VRF**, select **Default**.
   The default value of the VRF field will be resolved to the default VRF for the selected device. If you select multiple devices, the default value will be Default.

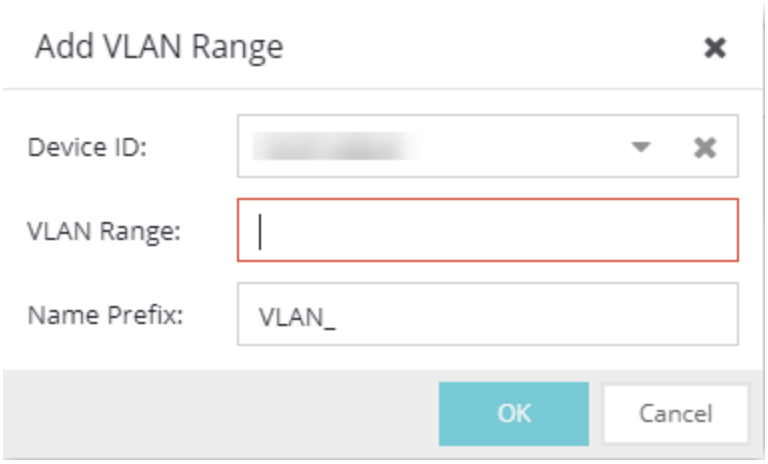
NOTE: If the selected device does not support VRFs, the VRF field does not display.

9. Select **OK**.

Add a Range of VLANs at the Site Level

To configure a range of VLANs that apply to all devices that belong to the site:

1. Open **Devices > Tree View**.
2. Expand **World**, and then select a site.
3. In the VLAN Definition window, select Add Range.



4. For **VLAN Range**, enter the range of VLAN IDs using a comma to separate them. You can use a dash to enter consecutive IDs such as 100-102.
5. For **Name Prefix**, enter a name for the prefix that all the created VLANs will use. The format is <prefix>-<vlanId>).
6. For **VRF**, select **Default**.

> **NOTE:** If the selected device does not support VRFs, the system hides the VRF field .

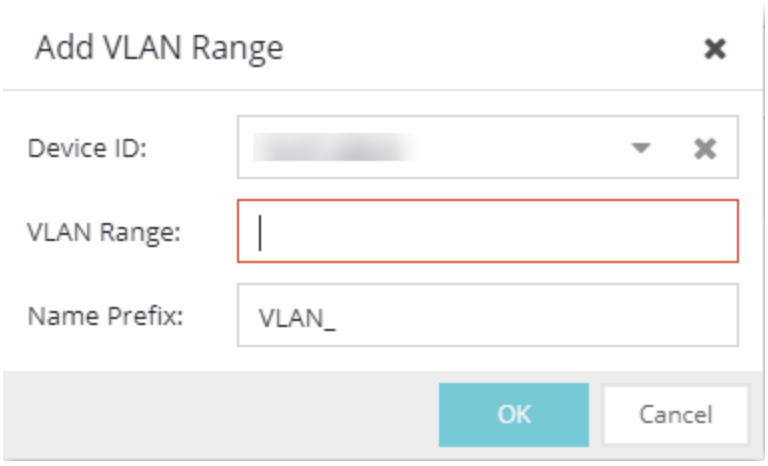
7. Select **OK**.

Add a Range of VLANs at the Service Definition Level

To configure a range of VLANs in a Service Definition, which you can then assign to one or more sites:

1. Open **Devices > Tree View**.
2. Expand **Service Definition**, and then select a service application.

3. In the VLAN Definition window, select Add Range .



4. For **VLAN Range** , enter the range of VLAN IDs using a comma to separate them. You can use a dash to enter consecutive IDs such as 100-102.
5. For **Name Prefix**, enter a name for the prefix that all the created VLANs will use. The format is <prefix>-<vlanId>).
6. For **VRF**, select **Default**.

NOTE: If the selected device does not support VRFs, the system hides the VRF field .

7. Select **OK**.

Layer 2 VSN Service Creation

In Layer 2 Virtual Services Network (L2 VSN) functionality, a VLAN is mapped to a Service ID and becomes a customer VLAN (C-VLAN). C-VLANs are bridged over the Fabric Connect core infrastructure using the shortest path topology learned using IS-IS.

IMPORTANT: With the Layer 2 VSN Service Creation feature, you can provision Layer 2 VSNs automatically. Do not use this feature if the device is running **Fabric Attach**. Fabric Attach dynamically makes equivalent configuration changes, and if Fabric Assist is enabled, it will change those settings to static on the device.

Enhanced Validation

Validation ensures consistency between service applications within a service definition. However, validation is done only when you save the entire service definition. This delay is problematic, because you can lose all the manual edits made since the last save.

Fabric Assist performs validation as soon as you enable it. This enhanced validation is at a more granular level within the service definition than validation without Fabric Assist. It also ensures that the Service ID Range does not overlap with existing L2 VSN services in other service applications within the same service definition. The row editor widgets for each grid within the Service Application panel (VRF Definition, VLAN Definition, L2 VSN, and L3 VSN) also perform this enhanced validation when you select the corresponding Update button.

For information on related topics:

- Fabric Connect
- Fabric Assist

Enabling Fabric Assist

You can enable or disable Fabric Assist at the Service Definitions level only.

Service definitions contain groups of service application templates that you can apply to fabric-enabled devices. When you map a service definition to a site, the service applications are shared by the fabric-enabled devices within the site.

To enable the automatic creation of L2 VSN services, you must enter a Service ID Offset in the L2 VSN dialog.

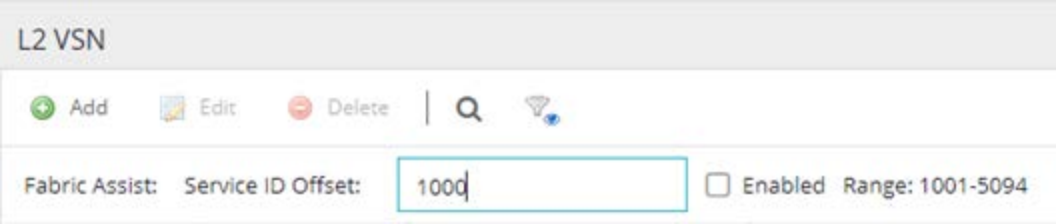


After you configure a valid offset, the Fabric Assist Enabled check box becomes available to check. When checked (enabled), Fabric Assist automatically creates a corresponding C-VLAN entry for every VLAN that is not already mapped to an existing L2 VSN C-VLAN entry. Fabric Assist also creates an L2 VSN C-VLAN entry for any new VLANs created in the service application.

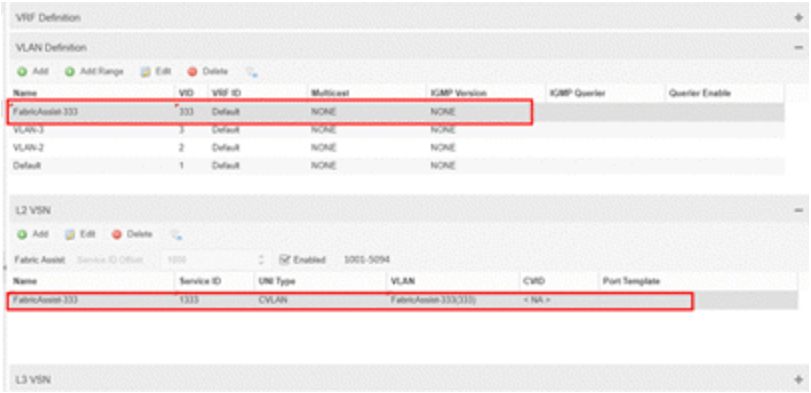
NOTES:

- The Service ID Offset determines the L2 VSN Service ID Range, which is from the offset value to the offset plus 4094.
- A valid Service ID Offset cannot contain the Service ID for an existing L2 VSN that falls within the Service ID Range.
- When enabled, Fabric Assist disables the Service ID Offset field and the Edit and Delete buttons to prevent any changes to L2 VSN services.

Fabric Assist displays the Service ID Range. For example, if the Service ID Offset is **1000**, the Service ID Range will be from 1001 to 5094.



Fabric Assist displays the L2 VSN configuration information, including the Service ID, in the service application window. Any changes to Fabric Assist go into effect when you save the service definition.



Fabric Assist L2 VSN Considerations

- The following rules apply to service applications within the same service definition:
  - Service applications can have the same Service ID Offset because VLANs cannot be reused between service applications in the same service definition.
  - Service applications with different Service ID Offsets are valid as long as the Service ID Ranges do not overlap within the service definition.

- When Fabric Assist is enabled, you can manually create L2 Switched or Transparent UNI services, but you can no longer manually create L2 VSN C-VLAN services through the Service Application dialog.
- If you do not want a VLAN to have a service, create that VLAN at the site level. L2 VSNs that are created by Fabric Assist are based only on the VLANs in the service application window.
- If you want to modify Fabric Assist, you must disable Fabric Assist by clearing the L2 VSN **Enabled** check box.

IMPORTANT: Any C-VLAN entries that Fabric Assist created are automatically deleted from the L2 VSN window when you disable Fabric Assist.

VLAN Pruning

If a VLAN has no tagged egress or untagged egress, there is no need for Fabric Assist to process it. VLAN Pruning prevents VLANs with no egress from being enforced to a device.

To enable VLAN Pruning, check **Enable Pruning** in either the device VLAN Definition window or the site VLAN Definition window.



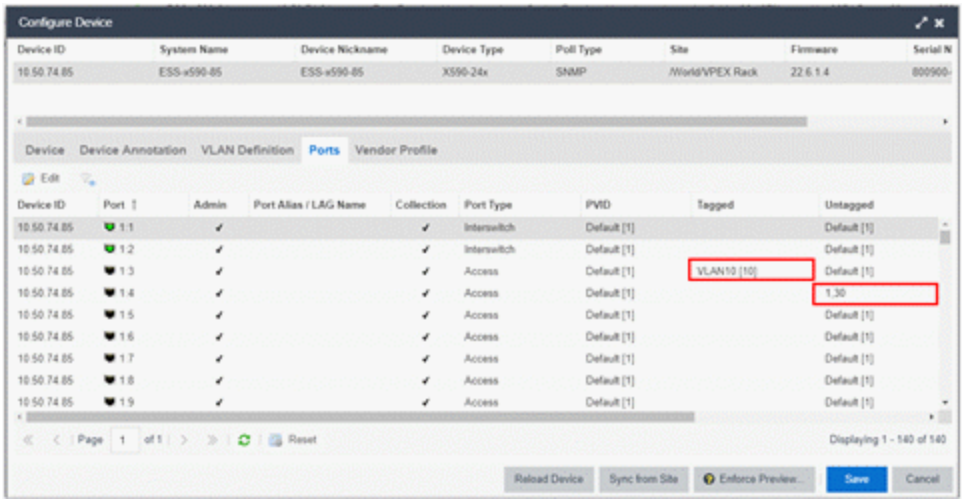
Devices inherit VLAN definitions configured in a site or inherited from a service application that is mapped to a site. Devices in a site also inherit the Enable Pruning value from the site:

- When VLAN Pruning is *not enabled*, the inherited VLANs are created on the devices during an enforce operation unless you manually exclude them.
- When VLAN Pruning is *enabled*, only the VLANs with tagged or untagged egress on the device are enforced.

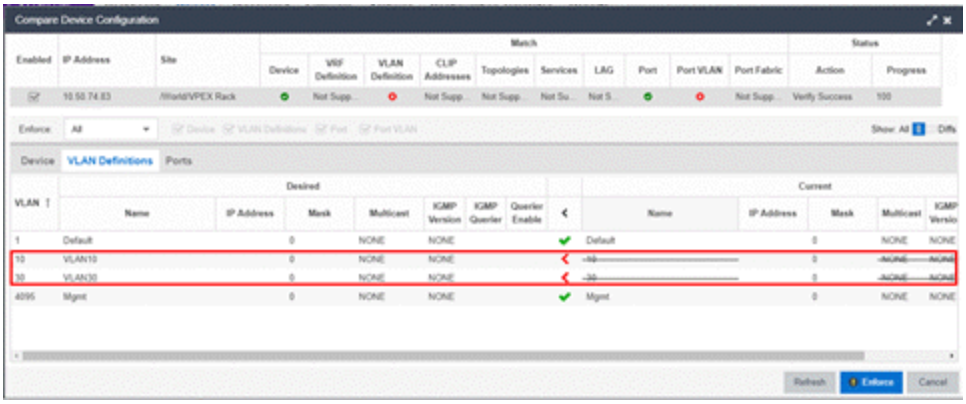
The device VLAN Definition window shows all inherited VLANs so that you can configure tagged or untagged egress on ports. VLAN pruning takes place when you launch the enforce preview. The Enforce Preview window shows only the VLANs that have egress configured on the device.

For example, the following figure shows the VLANs that a device inherited from a site:

- tagged egress on VLAN10
- untagged egress on VLAN30
- no egress configured on VLAN20



In the Enforce Preview window, Fabric Assist creates only VLAN10 and VLAN30 on the device.



For information on related topics:

- VLAN Trunk Mode
- Fabric Assist

Import to Service Definition

The Import to Service Definition feature enables you to import a device's active configuration into a Service Application. With this feature, you can select a device that uses a **golden configuration** and use that as the basis for a configuration template. Then you can apply the Service Application to other devices managed by ExtremeCloud IQ Site Engine.

Importing configurations enable you to have the same VLAN configuration in the core of your network as you have on the edge devices without having to manually enter in that configuration. However, this depends upon the device type that ExtremeCloud IQ Site Engine will import from the device into the Service Application.

- For ExtremeXOS/Switch Enginedevices, ExtremeCloud IQ Site Engine provides **VLAN provisioning support** so only the VLANs from the device will be imported into the Service Definition.
- For Fabric Engine devices, ExtremeCloud IQ Site Engine provides **Fabric Connect provisioning support** so the VRFs, VLANs, Layer 2 Services, and Layer 3 Services will be imported into the Service Definition.

You can also use this feature to assist you in bringing new platforms online, as you integrate those devices into an existing network, or transition out older devices from their network.

For information on related topics:

- Fabric Assist

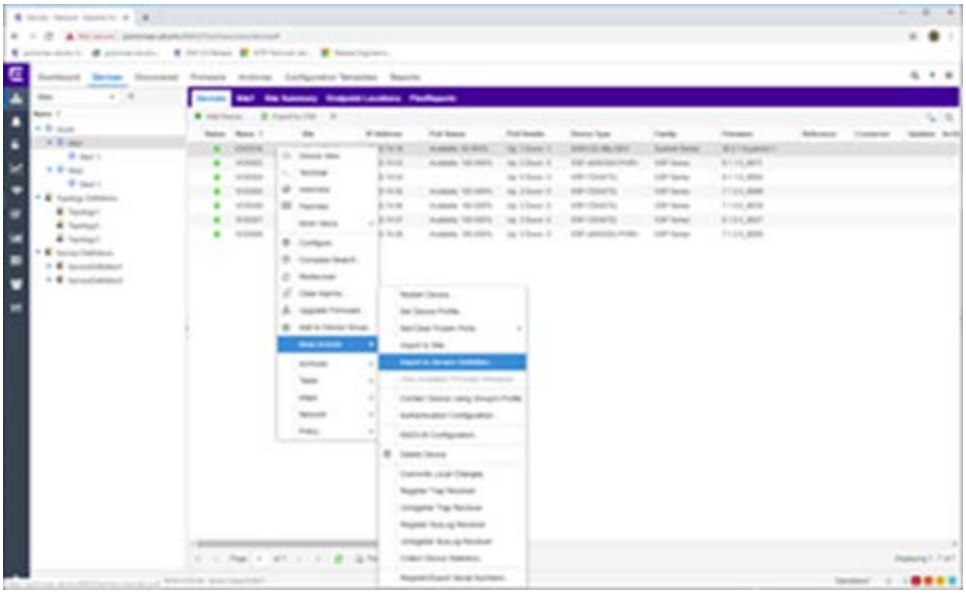
Prerequisites

Before you begin the import process, you must do the following:

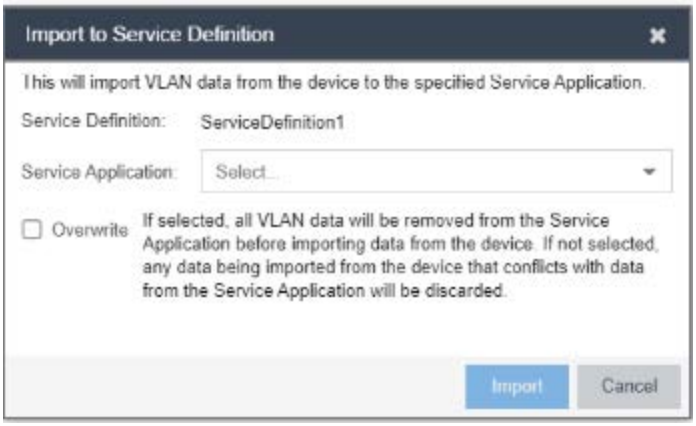
- Identify the target Service Definition and Service Application(s) that you want to import into. If the Service Definition and Service Application(s) have not already been created, you must create them before the import process begins.
- Assign the Service Definition to the Site that contains the device being imported from. If the site does not have a Service Definition assigned to it, the **Import to Service Definition** option on the More Actions menu will not be available.

Import a Configuration to a Service Definition

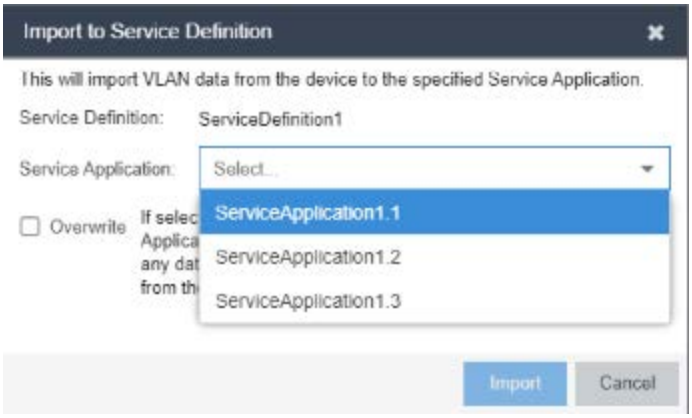
1. Open **Network > Devices > Sites View**.
2. Expand **World**, and then select a site.
3. On the Devices sub-tab, right-click on the device that you want to import from, and then select More Actions > Import to Service Definition.



The system displays the Import to Service Definition dialog.



4. In the **Service Application** field, select the Service Application where you want to import the device's configuration into. The following screen capture shows an example.



5. Consider the following limitations before deciding whether to use the **Overwrite** option.

   The configuration that ExtremeCloud IQ Site Engine imports from the device depends upon the device's capabilities and the ability of ExtremeCloud IQ Site Engine to provision certain features:

   - For devices that ExtremeCloud IQ Site Engine has **VLAN provisioning support** (such as EOS and ExtremeXOS/Switch Engine), only the VLANs from that device will be imported into the Service Definition.
   - For devices that ExtremeCloud IQ Site Engine has **Fabric Connect provisioning support** (such as Fabric Engine), the VRFs, VLANs, L2, and L3 services will be imported into the Service Definition.

   NOTE: Currently only CVLAN UNI services are supported in Release 8.4. Switched and Transparent UNI support will be added in a future release.

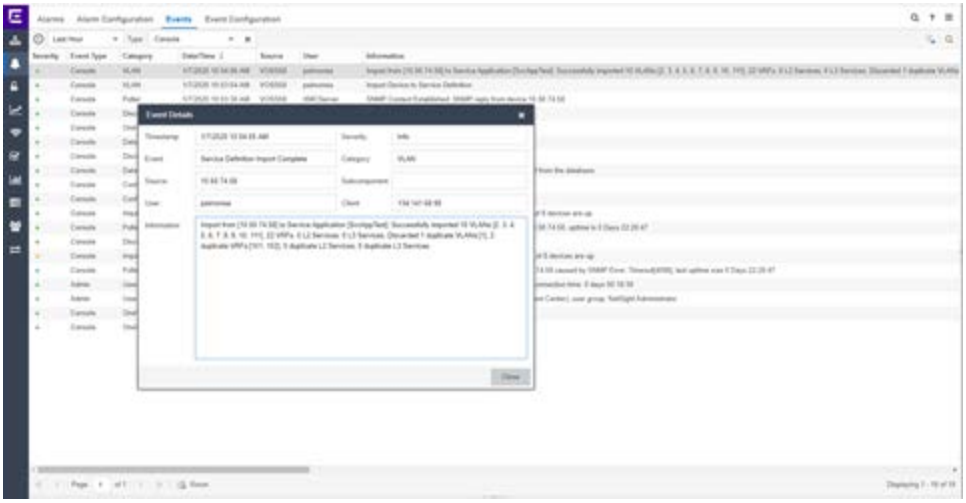
   Select the **Overwrite** check box if you want to remove the Service Application's existing configuration before importing the device's configuration.

   If you do not select Overwrite, the import process merges the device's configuration into the existing Service Application. If there are any conflicts (such as duplicate VLAN IDs) between the Service Application's existing configuration and the device's configuration, the conflicting items are discarded from the import process.

6. Select **Import**.
7. Monitor the progress of the import operation by checking the **Operations** pane at the bottom of the **Devices** window. The following screen capture shows an example.



8. Open **Events** and select the **Console** type. Then double-click on any row in the table to display the **Event Details**, which indicates the status of the import process and whether any configuration items were discarded.



9. Select **Close**.

How to Create an EAPS Domain

This section outlines how to create an EAPS domain, from the **Network** tab.

To create a new EAPS Domain:

1. Launch ExtremeCloud IQ Site Engine.
2. Open the **Network** > **Devices** tab and select a map within the World map navigation tree.
3. Select the EAPS tab in the Network Details section of the window. The EAPS Summary pane opens.
4. Select the **New EAPS Domain** button. The New EAPS Domain wizard opens to the Select Devices window.
5. Highlight the devices to add to the EAPS domain and select the right arrow button to move the devices to the selected device column.

   NOTE: Use the up and down arrows to change the order in which devices are listed.

6. Select **Next >**. The Configure Domain window opens.
7. Enter a **Name** for the EAPS domain.
8. Select the links to add to the EAPS domain in the Available Links section and select the **Add** button.
9. Enter the **Name** and **Tag** of the Control VLAN for the EAPS domain.
10. Select a **Master Node** and **Primary Port** for the EAPS domain from the drop-down menus in the Master Node section of the window.
11. Enter the amount of time, in seconds, for the **Hello** and **Fail** timers.
    - **Hello Timer** — The interval, in seconds, between which polling signals are sent by the master node to detect ring breaks.
    - **Fail Timer** — The amount of time, in seconds, after the master node sends the Hello Timer signal until the master node detects a ring failure if a reply signal is not received. If a ring failure occurs, the switch can respond by either sending an alert or opening the secondary port.

1. Select **Next >**. The Results window opens.
2. Verify the EAPS domain is properly created.

   NOTE: If the EAPS domain is not created correctly, select the **< Back** button to change the values in the New EAPS Domain wizard.

3. Select **Close** to exit the New EAPS Domain wizard. The EAPS domain is created.

For information on related topics:

- Maps
- Network
- How to Create and Edit a VLAN

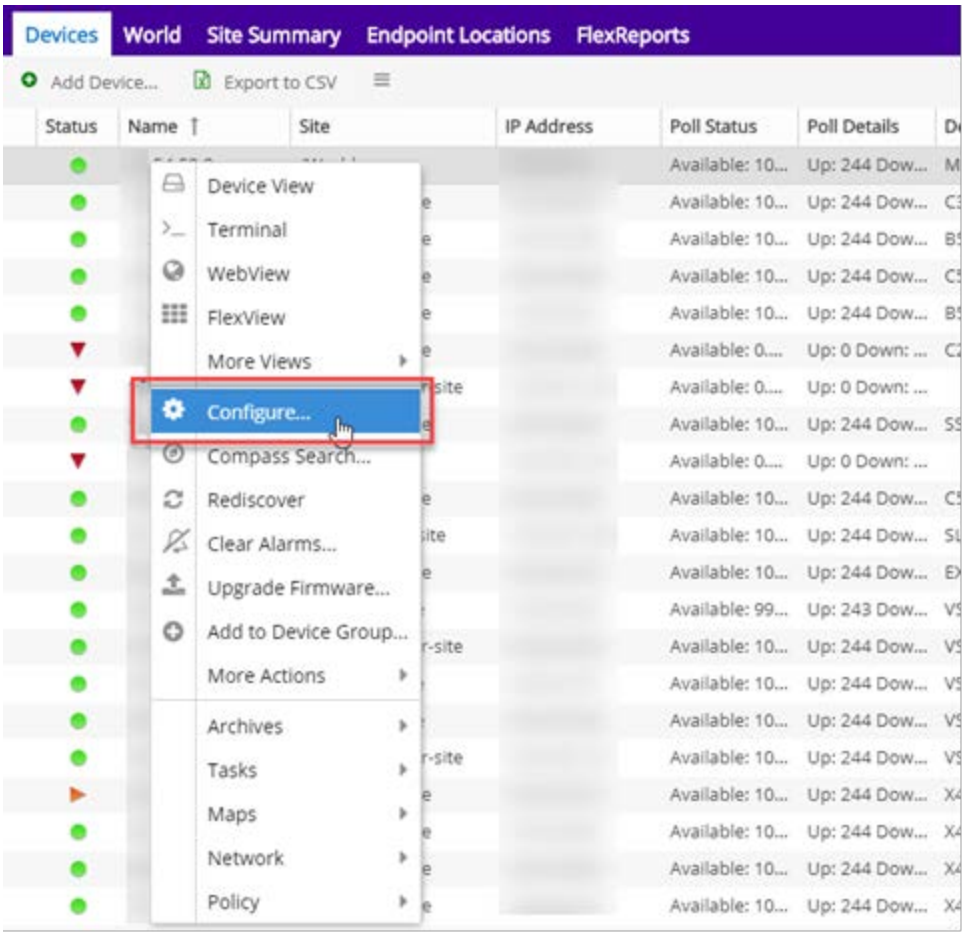
Changing Device Configurations

Changes to device configurations are first staged in ExtremeCloud IQ Site Engine, then enforced to the devices themselves.

To make changes to devices in ExtremeCloud IQ Site Engine:

1. Access the **Network** > **Devices** tab.
2. Use the **Navigation** drop-down menu to select the method by which ExtremeCloud IQ Site Engine organizes devices.
3. Select the **Devices** tab in the right-panel.
4. Select the devices for which you are changing the configuration in the Devices list in the right-panel.

5. Select the **Menu** icon (☰) and select **Configure**.



   The **Configure Device** window opens.

6. Use the Configure Device window, to make changes.
7. Select **Enforce Preview**.

   The **Compare Device Configuration** window opens.

8. Use the **Enforce** drop-down list to verify all of the changes you are enforcing to your devices.
9. Select **Enforce**.

The changes are saved to your devices.

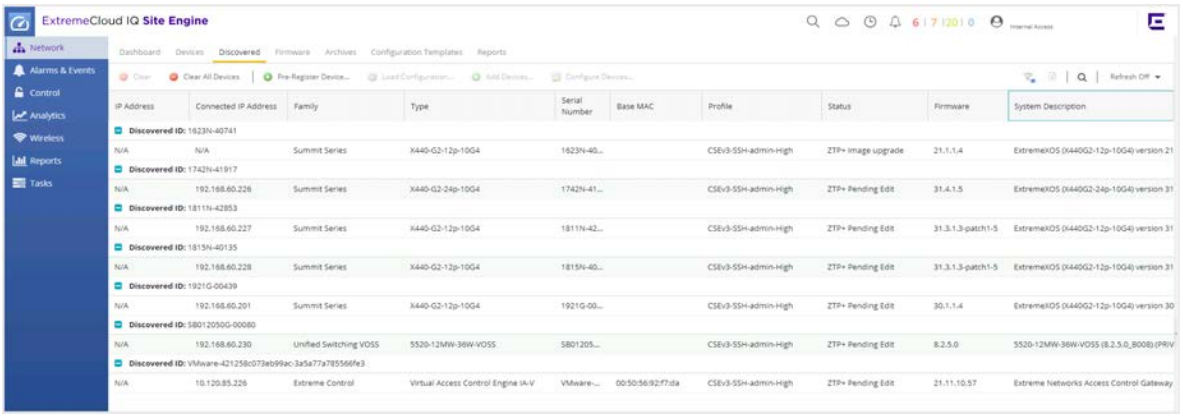
For information on related topics:

- Configure Device
- Compare Device Configuration

Discovered

Use the **Discovered** tab to view devices new to your network not yet added to the ExtremeCloud IQ Site Engine database.

To access the **Discovered** tab open the **Network** tab and select the **Discovered** tab.



Devices appear on the **Discovered** tab when they are:

- Discovered via the **Site** tab and one of the following occurs:
  - The **Automatically Add Devices** checkbox is not selected in the Site Actions section of the tab.
  - The serial number of the device matches:
    - The serial number of another device being discovered.
    - The serial number of a device already in the ExtremeCloud IQ Site Engine database.
  - The serial number is not defined for a device and the base MAC address matches:
    - The base MAC address of another device being discovered.
    - The base MAC address of a device already in the ExtremeCloud IQ Site Engine database.
  - The serial number and base MAC address are not defined for a device and the IP address matches:
    - The IP address of another device being discovered.
    - The IP address of a device already in the ExtremeCloud IQ Site Engine database.
  - The device uses a profile different than those associated with devices that already exist in the ExtremeCloud IQ Site Engine database.

- Discovered using the Pre-Register Device window for your ZTP+ (Zero Touch Provisioning Plus) enabled devices.

  NOTE: ZTP+ functionality is supported on ExtremeXOS/Switch Engine devices on which version 21.1 (or greater) is installed, FastPath devices, Fabric Manager, ExtremeAnalytics engines, and Access Control engines.

- Discovered using a trap to discover a ZTP (Zero Touch Provisioning) enabled device.

  NOTE: ZTP functionality is not identical to ZTP+ functionality.

Device Grouping

ExtremeCloud IQ Site Engine can group devices with data that match another newly discovered device or a device that currently exists in the ExtremeCloud IQ Site Engine database. By default, ExtremeCloud IQ Site Engine grouping in the Discovered View is by the Discovered ID column.

Enable or remove grouping functionality on the **Discovered** tab by selecting the arrow icon in the right-side of a column and selecting or deselecting the **Show in Groups** checkbox, respectively. Additionally, to change the grouping to a column other than Discovered ID, select the **Group by This Field** option in a specific column to group devices based on the criteria of that column.

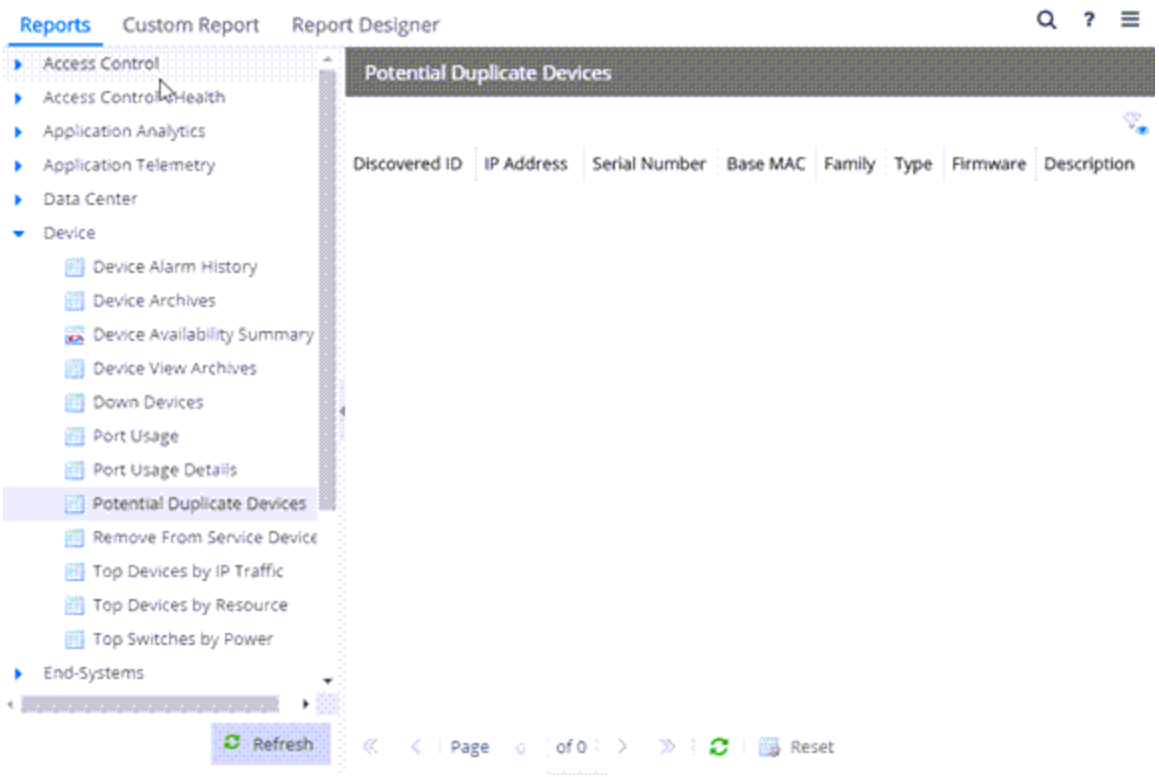
For example, you are adding three devices to ExtremeCloud IQ Site Engine that appear on the **Discovered** tab. All three devices share the same Serial Number, but have different IP Addresses. The Discovered ID column will display the same serial number. Selecting **Group by This Field** in the menu for the **Serial Number** column would group the devices with the same serial number together.

Use the information in the **Status** column to determine which device to add to the ExtremeCloud IQ Site Engine database. You can then clear the remaining devices from the list.

Preventing duplicate devices in ExtremeCloud IQ Site Engine allows you to:

- Avoid unnecessary polling of devices
- Minimize the collection of statistics
- Maximize the efficiency of your device count license
- Ensure there are not multiple configurations of the device in ExtremeCloud IQ Site Engine

The Potential Duplicate Devices report includes information about potential duplicate devices that may already exist in the ExtremeCloud IQ Site Engine database. This report is included in ExtremeCloud IQ Site Engine's Reports > Report Catalog > Device tab.



The following columns are included in the Potential Duplicate Devices report:

Discovered ID
Displays the Serial Number, Base MAC address, or IP Address assigned to discovered devices.

ID
Displays the device's ID number.

Name
Displays the name of the device.

Site
Displays the site in which the device resides.

IP Address
Displays the device's IP address.

Serial Number
Displays the serial number assigned to the device.

Base MAC
Displays the device's MAC address.

Family
Displays the device's device family.

Type
Displays the device's device type.

Firmware
Displays the device's current firmware version.

Poller Name
Displays the type of poll used by the trap engine to poll the device.

Profile Name
Displays the profile the device is using for its administrative SNMP and CLI credentials.

Description
Displays a description of the device.

OID
Displays the SNMP sysObjectId OID.

For instructions about how to discover devices and add them to the ExtremeCloud IQ Site Engine database, see How to Discover Devices in ExtremeCloud IQ Site Engine.

Columns

The columns on the **Discovered** tab display the details about the devices available to be added to the ExtremeCloud IQ Site Engine database.

IP Address
The **IP Address** column displays the IP address assigned to the discovered device.

Discovered ID
The **Discovered ID** column displays the Serial Number, Base MAC address, or IP Address assigned to discovered devices, which is used to group potential device duplicates. If devices are potential duplicates, ExtremeCloud IQ Site Engine groups potential devices first by Serial Number, then by Base MAC address, then by IP address. When the **Show in Groups** checkbox is selected and the Discovered ID column is set as the Group by this Field for the view, ExtremeCloud IQ Site Engine groups those devices so potential duplicates are displayed. Select the device to add it to ExtremeCloud IQ Site Engine, so it appears in the Device View, maps, and other areas of ExtremeCloud IQ Site Engine.

For example, if you added two devices to ExtremeCloud IQ Site Engine, ExtremeCloud IQ Site Engine first attempts to group the devices by a shared Serial Number. If there is no serial number, ExtremeCloud IQ Site Engine attempts to group the devices by a shared Base MAC address. If the values for both the Serial Number and the Base MAC address are blank, ExtremeCloud IQ Site Engine then attempts to group devices by a shared IP address.

Connected IP Address
The **Connected IP Address** column displays the IP address a ZTP+-enabled device used to communicate with ExtremeCloud IQ Site Engine.

Family

The **Family** column displays the series of devices to which a device belongs, known as a device family in ExtremeCloud IQ Site Engine.

Type

The **Type** column displays the device type, when the discovery determines it in ExtremeCloud IQ Site Engine. If ExtremeCloud IQ Site Engine does not have enough information to determine the device type, the type column is blank.

Serial Number

The **Serial Number** column displays the serial number of the device.

Base MAC

The **Base MAC** column displays the MAC address of the device.

Source

The **Source** column displays the source of the functionality that added the device to the **Discovered** tab in ExtremeCloud IQ Site Engine. For example, the **Source** column displays ZTP+ when the device has been added by ZTP+ functionality. The **Source** column also displays subnet details for devices added to the **Discovered** tab via Discovery functionality.

Site Path

The **Site Path** column shows the site to which the device is assigned. To change the site, select the **Add Devices** button for devices with a Status of **New,** the **Edit Devices** button for devices with a Status of **Exists,** or the **Configure Device** view for devices discovered via ZTP+, and use the **Default Site** drop-down list in the Device section of the window to select an existing site.

WARNING:

When changing the **Default Site** you are prompted to Import Site Configuration to the device.

If you select Yes to Import Site Configuration:

- The existing VLAN Definition, Ports, and ZTP+ Device Settings assigned are overwritten on the device.
- Any applicable Automated Port Templates from the selected site are assigned to the relevant ports on the device.

You can create new sites on the **Network** > **Devices** tab.

Profile

The **Profile** column displays the profile the device is using for its administrative SNMP and CLI credentials. To change the profile, select the **Add Devices** button for devices with a Status of **New**, the **Edit Devices** button for devices with a Status of **Exists**, or the **Configure Device** view for devices discovered via ZTP+, and use the **Admin Profile** drop-down list in the Device section of the window to select an existing profile.

You can create new profiles on the **Administration** > **Profiles** tab.

Status

The **Status** column indicates whether the device exists in the ExtremeCloud IQ Site Engine database.

- **Exists** — The device already exists in the ExtremeCloud IQ Site Engine database with the same Profile.
- **Exists [<Profile Name>]** — The device already exists in the ExtremeCloud IQ Site Engine database with a different Profile, followed by the name of the device profile currently used by the device in the database.
- **Matches [SN:<#########>]** <list of matching IPs> — The serial number of the device matches the serial number(s) of devices currently in the ExtremeCloud IQ Site Engine database, followed by the device IP Address(es) in the database which match the Serial Number.
- **Matches [MAC:<#########>]** <list of matching IPs> —The serial number of the device is blank and the Base MAC address of the device matches the Base MAC address of device(s) currently in the ExtremeCloud IQ Site Engine database (displayed as part of the Status), followed by the IP address(es) currently used by the devices in the database.
- **New** — The device is discovered by ExtremeCloud IQ Site Engine, but it has not yet been added to the ExtremeCloud IQ Site Engine database.
- **ZTP+ Registered** — The ZTP+-enabled device is registered in ExtremeCloud IQ Site Engine.
- **ZTP+ Staged** — The configuration is staged in ExtremeCloud IQ Site Engine for the ZTP+-enabled device .
- **ZTP+ Complete** — The ZTP+-enabled device is configured successfully in ExtremeCloud IQ Site Engine and is ready to be added to the ExtremeCloud IQ Site Engine database.
- **ZTP+ Pending Edit** — The configuration of the ZTP+-enabled device is not complete and ExtremeCloud IQ Site Engine is waiting for edits.
- **ZTP+ Pending Configuration** — The ZTP+-enabled device is ready to be configured in ExtremeCloud IQ Site Engine.
- **ZTP+ Unknown** — The ZTP+-enabled device is in an unknown state.

- **ZTP+ Configuration Error** — The ZTP+-enabled device is not correctly configured. See the Event log for additional details.
- **ZTP+ Certificate Error** — The ZTP+-enabled device is not correctly configured. See the Event log for additional details.
- **ZTP+ Script Error** — The ZTP+-enabled device is not correctly configured. See the Event log for additional details.
- **ZTP+ RMA Starting** — ExtremeCloud IQ Site Engine is starting the RMA process for the ZTP+-enabled device (**Remove from Service** is selected on the **Device** tab in the **Configure Device** window).
- **ZTP+ RMA Complete** — The RMA process is complete for the ZTP+-enabled device (**Remove from Service** is selected on the **Device** tab in the **Configure Device** window).
- **ZTP+ Image Upgrade** — ExtremeCloud IQ Site Engine is upgrading the firmware image for the ZTP+-enabled device.
- **ZTP+ RMA Failed** — The RMA process did not complete successfully for the ZTP+-enabled device (**Remove from Service** is selected on the **Device** tab in the **Configure Device** window).

Details
: The **Details** column shows whether the profile is acceptable for the device as configured on the **Site** tab in the **Profiles** list. If the **Reject** checkbox is selected for the profile on the **Site** tab, ExtremeCloud IQ Site Engine does not successfully discover the device using that profile, even if the SNMP credentials in the profile are successful. This is to prevent ExtremeCloud IQ Site Engine from discovering devices using less secure profiles. For ZTP+-enabled devices, the **Details** column displays details about the devices' ZTP+ status.

Firmware
: The **Firmware** column shows the version number of the firmware or boot PROM image.

Connector
: The **Connector** column displays the connector version running on the ZTP+ device.

System Description
: The System Description displays the MIB-II sysDescr OID.

Object ID
: The **Object ID** column displays the SNMP sysObjectId OID.

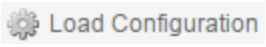
First Seen
: The **First Seen** column displays the date and time the device first appeared in the **Discovered** tab.

Last Seen
: The **Last Seen** column displays the date and time the device last communicated with the ExtremeCloud IQ Site Engine server.

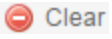
Times Seen
: The **Times Seen** column displays the number of times the device communicated with the ExtremeCloud IQ Site Engine server.

Toolbar Buttons

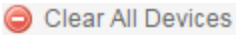
The toolbar at the top of the tab allows you to perform various tasks on the devices on the **Discovered** tab.

Load Configuration 

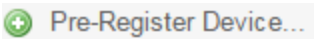
: Select to open the Load a configuration on a Discovered Device window, which allows you to use a saved configuration for an existing device on a ZTP (zero touch provisioning) enabled device.

Clear 

: Select to remove the currently selected device from the **Discovered** tab.

Clear All Devices 

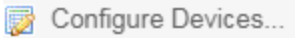
: Select to remove all devices listed on the **Discovered** tab.

Pre-Register Device 

: Select to open the Pre-Register Device window, where you can pre-configure a ZTP+ (zero touch provisioning plus) enabled device so when you add it to ExtremeCloud IQ Site Engine, the configuration occurs automatically.

Add Devices 

: Opens the Add Selected Devices window, where you can configure newly discovered devices and add them to the ExtremeCloud IQ Site Engine database.

Configure Devices 

: Opens the Configure Device window, where you can edit the configuration for a device.

Filters
: Use the filter functions to view, modify, apply, or remove filters from a table column. You can filter multiple columns in a table.

Export to CSV 
: Select to export all of the data in the table to a .CSV file. The exported data displays with any sorting, filtering, and searching applied.

Search 
: Select to open a search box into which you can enter search parameters. The data in the table filters to display devices that match your search entry.

Load Configuration on a Discovered Device

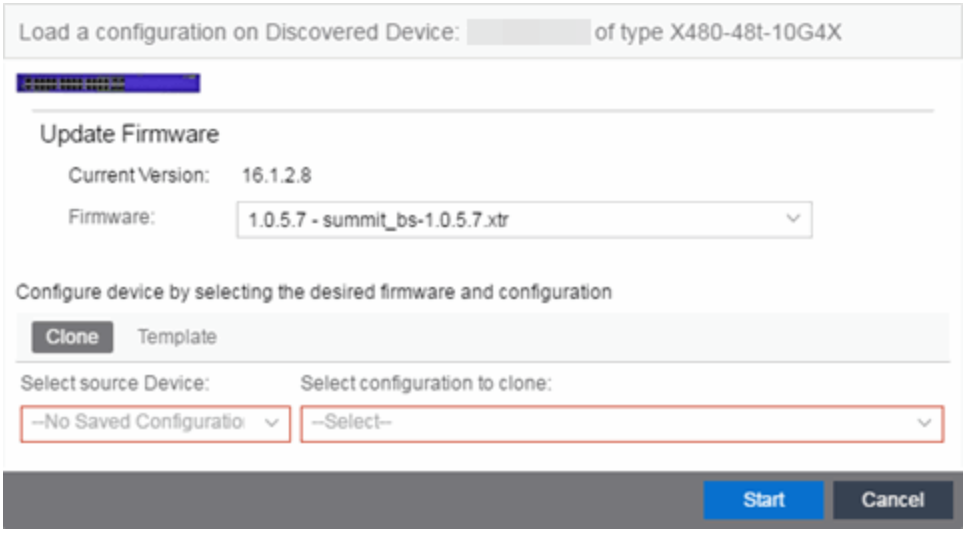
Use this window to use a saved device configuration on a device you are adding to ExtremeCloud IQ Site Engine. Devices to which you load a saved configuration must have ZTP (Zero Touch Provisioning) enabled.

This window is accessible by selecting the **Load Configuration** button or by right-clicking an existing device and selecting **Load Configuration** on the **Network** > **Discovered** tab.

The window contains two tabs, depending on the type of configuration you are loading on the new device:

- **Clone** — A configuration currently used on an existing device copied to the new device.
- **Template** — A configuration saved to ExtremeCloud IQ Site Engine as a template.

Clone



Current Version
: Displays the current version of firmware installed on the device.

Firmware
: Use the drop-down list to select a new firmware version to install on the device.

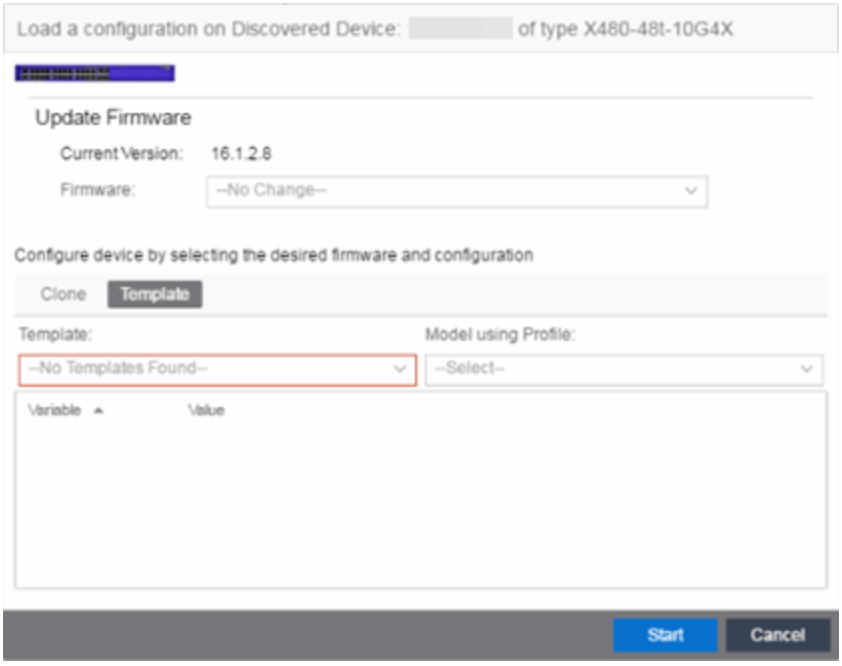
Select source Device
: Use the drop-down list to select a device currently added to ExtremeCloud IQ Site Engine from which to copy the device configuration.

Select configuration to clone
: Use the drop-down list to select the configuration on the device listed in the **Select source Device** drop-down list that is being cloned to the new device.

Start
: Select the **Start** button to copy the configuration from the selected device to the new device.

Cancel
: Select the **Cancel** button to close the window without copying the configuration.

Template



Current Version
: Displays the current version of firmware installed on the device.

Firmware
: Use the drop-down list to select a new firmware version to install on the device.

Template
: Use the drop-down list to select a device configuration template saved to ExtremeCloud IQ Site Engine.

Model using Profile
: Use the drop-down list to select the profile to use when modeling the template on the new device.

Start
: Select the **Start** button to copy the configuration from the selected device to the new device.

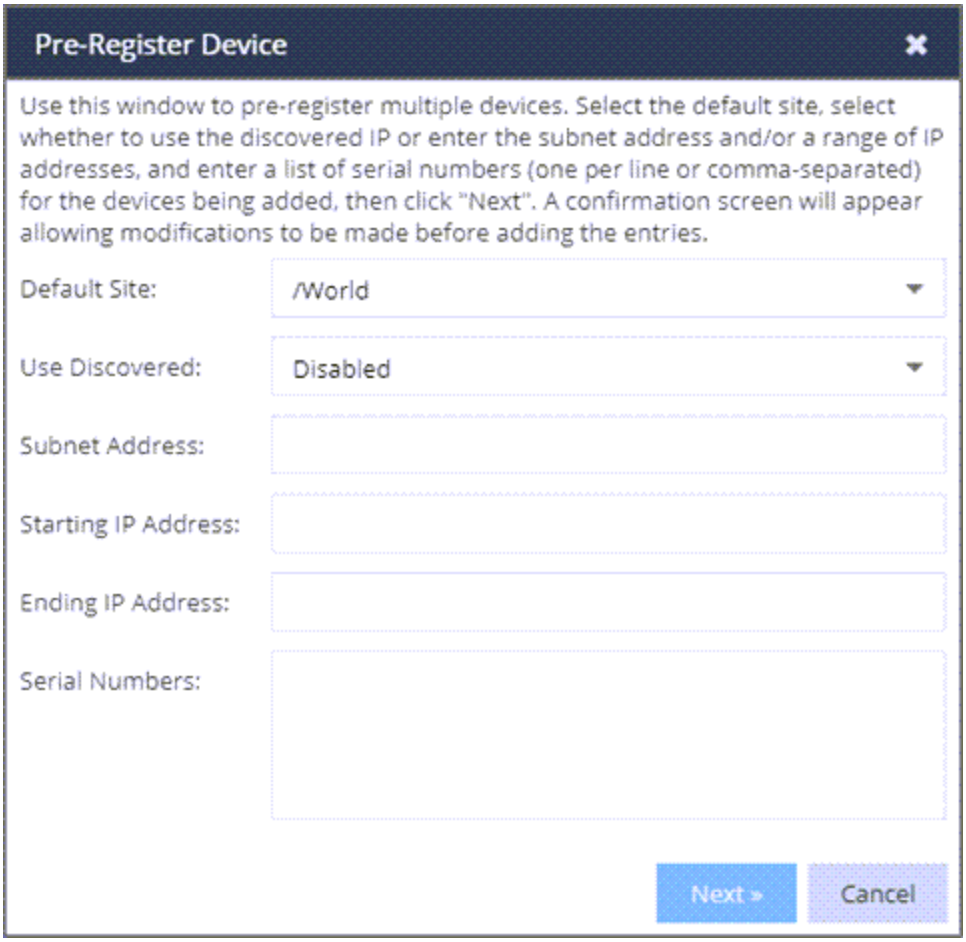
Cancel
: Select the **Cancel** button to close the window without copying the configuration.

Pre-Register Device

Use this window to add multiple ZTP+ enabled devices to ExtremeCloud IQ Site Engine.

The **Pre-Register Device** window is accessible on the **Network** > **Discovered** tab by selecting the **Pre-Register Device** button.

Pre-Register Device Window



Default Site

The site to which the devices are to be added. If the site has ZTP+ Device Defaults configured, those values are populated in the **Pre-Register Device Window** when you select the site from the Default Site menu.

Use Discovered

Use the **Use Discovered** drop-down list to add the IP address or IP address and management interface the device uses when it contacts ExtremeCloud IQ Site Engine via ZTP+. Then, enter the Serial Number for the Discovered IP address.

Subnet Address

If you do not use the **Use Discovered** option, enter the device's IP subnet address (IPv4 or IPv6) in this field. The subnet must be separated from the IP address by a slash (/). Use either the mask bit notation (for example, /24), or the dotted-decimal notation (for example, /255.255.255.0.).

Starting IP Address

If you do not use the **Use Discovered IP**, you must add a range of at least two IP Addresses. Enter the first IP Address (IPv4 or IPv6) in your range of addresses in this field. The starting IP Address must be within the subnet address you specified. It must not match the ending IP Address.

Ending IP Address

If you do not use the **Use Discovered IP**, you must add a range of at least two IP Addresses. Enter the last IP Address (IPv4 or IPv6) in your range of addresses in this field. The ending IP Address must be within the subnet address you specified. It must not match the starting IP Address.

Serial Number

Enter the manufacturer-assigned serial numbers of the devices being added, separated by commas. You can also enter each serial number on its own line.

Next

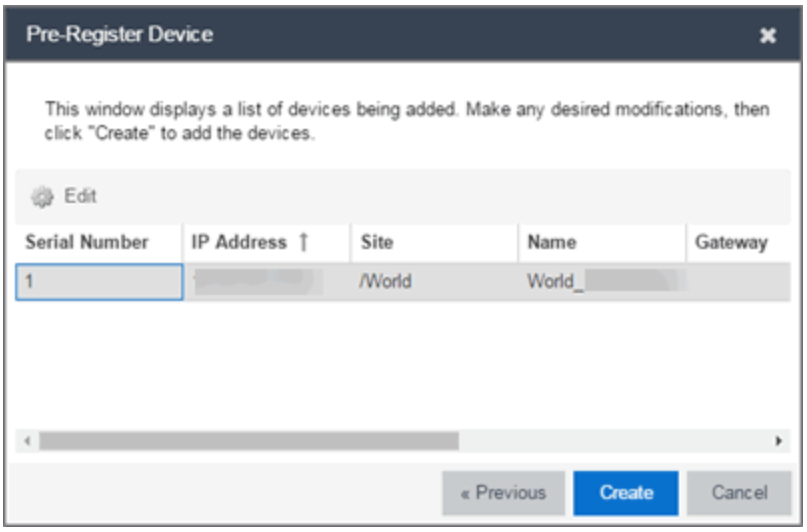
Select the **Next** button to open a confirmation window allowing you to verify the device information entered. Although it is recommended you enter device information in the site's **ZTP+ Device Defaults** window, you can also use this window to enter the Gateway, Domain Name, and DNS Server information for each device you are adding.

Cancel

Select the **Cancel** button to close the window with no devices added to the **Discovered** tab.

Pre-Register Device Confirmation Window

Use this window to confirm device information and supply any additional required information before adding devices to the **Discovered** tab in ExtremeCloud IQ Site Engine.



Serial Number

The serial number of the device. It is very important, especially for ZTP+-enabled devices, that the serial number entered here matches the device's serial number.

Use Discovered IP

Select to use discovered IP Address. You can also edit the discovered IP Address for a specific device.

IP Address

The device's IP address. The subnet mask is also displayed after the /.

Site

The site to which the device is to be added. To change the **Site**, use the Configure Device window.

Name

The name assigned to the device. The default **Name** includes the **Site** to which the device is assigned, followed by the device's Serial Number.

NOTE: If you are Pre-Registering Fabric Manager devices, the **Name** must be in hostname format (only ASCII a-z, digits 0-9 and hyphen -).

Gateway

Enter the IP address of the switch's default gateway. If a device is ZTP+-enabled, the site's ZTP+ Device default gateway displays.

Domain Name

Enter a value in the **Domain Name** field to configure the domain name on the devices being discovered. If a device is ZTP+-enabled, the site's ZTP+ Device default domain name displays.

DNS Server

Enter a DNS server address for the devices being discovered. If a device is ZTP+-enabled, the site's ZTP+ Device Default DNS Server displays.

NTP Server
Enter the NTP server address for the devices being discovered, if the devices are using an NTP server.

Create
Select the **Create** button to add the devices listed to the **Discovered** tab.

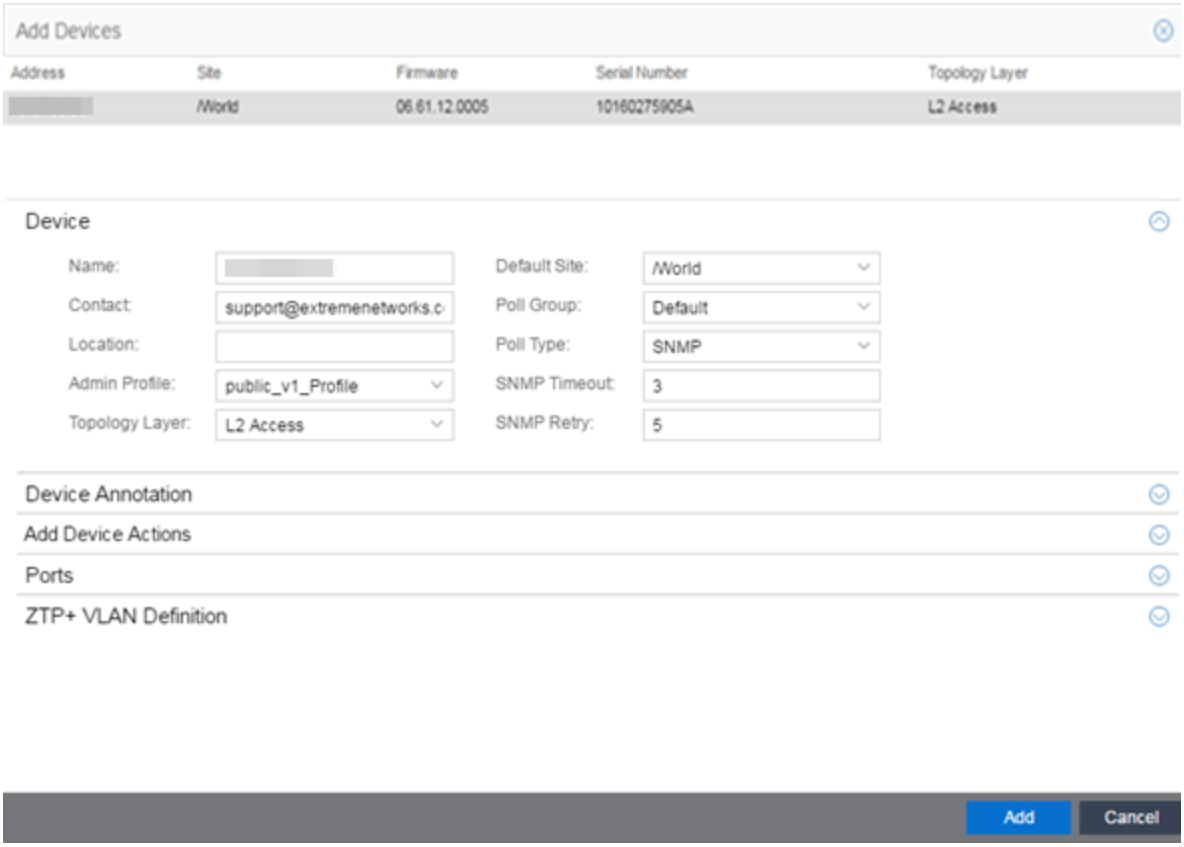
Add Devices

Use this window to configure a newly discovered device before you add it to the ExtremeCloud IQ Site Engine database. From this window you can configure basic information about the device, the device annotation, configure actions for the device, and add or remove ports for the device.

NOTE: When adding an ExtremeXOS/Switch Engine device in ExtremeCloud IQ Site Engine, enter the following commands in the device CLI:

```
configure snmpv3 add community "private" name "private" user "v1v2c_rw"
configure snmpv3 add community "public" name "public" user "v1v2c_rw"
enable snmp access
enable snmp access snmp-v1v2c
disable snmp access snmpv3
```

This window is accessible by selecting the **Add Devices** button or by right-clicking an existing device and selecting **Add Devices** on the **Network** > **Discovered** tab.



If you selected multiple devices to add, they are listed at the top of the window by IP address.

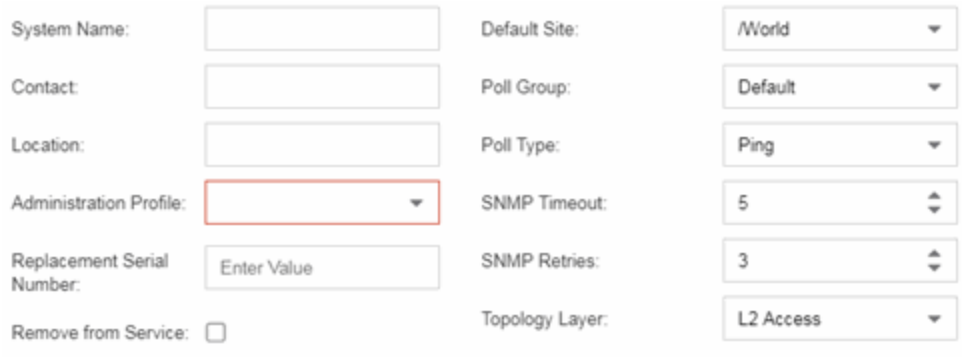
When you first open the window, only the Device section is expanded. Select a section heading to expand that section.

The Add Device window contains the following sections:

- Device
- Device Annotation
- Add Device Actions
- Ports
- ZTP+ VLAN Definition

Device

The Device section displays basic information about the device.



Name

The name by which the device is known.

Contact

Allows you to specify contact information for the person maintaining the device.

Location

The physical location of the device.

Admin Profile

Use the drop-down list to select the access Profile that gives the Discover tool administrative access to the devices you wish to discover. To create or edit a profile, open the **Administration** > **Profiles** tab.

Topology Layer

The layer and networking attributes for the device.

Default Site

Use the drop-down list to select the map to which the device is associated.

Poll Group

Use the drop-down list to select a Poll Group for the discovered devices. ExtremeCloud IQ Site Engine provides three distinct poll groups (defined in the Options > **Status Polling** tab) that each specify a unique poll frequency. When you save newly discovered devices to the database, they are polled with the poll group specified here. If you save discovered devices that already exist in the database, the poll group specified here overwrites the poll group currently being used in the database.

NOTE: Poll Group is not used if you set the Poll Type to **Not Polled**. To use Poll Group, select a Poll Type other than Not Polled.

Poll Type

Use the drop-down list to select the Poll Type used to discover devices: SNMP, Ping or Not Polled. When SNMP is specified, the SNMP version (SNMPv1 or SNMPv3) is determined by the Profile specified for the IP Range. If the Profile is set to Ping Only, the Poll Type must be set to Ping.

NOTE: On a Windows platform, device operational status cannot be determined for devices with their Poll Type set to Ping unless you are logged on and running ExtremeCloud IQ Site Engine as a user with Administrative privileges.

SNMP Timeout

The amount of time (in seconds) that ExtremeCloud IQ Site Engine waits before re-trying to contact the device. The value for this setting must be between 3 and 60 seconds.

The value entered in this field overrides the default entered in the SNMP Advanced view in the **Administration** > **Options** tab.

NOTE: When SNMP requests are redirected through the server, all SNMP timeouts are extended by a factor of four (timeout X 4) to allow for the delays incurred by redirecting requests through the server.

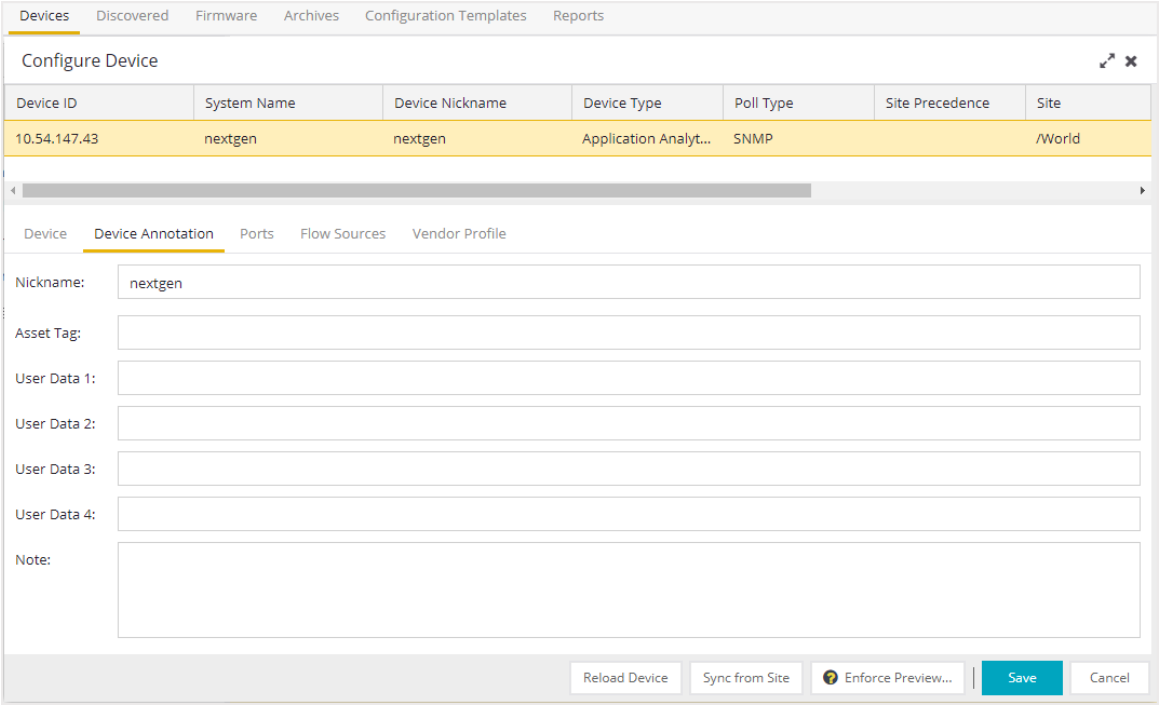
SNMP Retry

The number of attempts ExtremeCloud IQ Site Engine makes to contact a device after an attempt at contact fails. The value for this setting must be between 1 and 60 tries.

The value entered in this field overrides the default entered in the SNMP Advanced view in the **Administration** > **Options** tab.

Device Annotation

The Device Annotation section allows you to add user-defined information about the device.



Nickname

The user-defined nickname for the selected device. This is the name for this device that appears in the device tree in the left panel when **nickname** is selected in the **How to Display Devices in Tree** menu option in the OneView options menu in the **Administration** > **Options** tab.

User Data

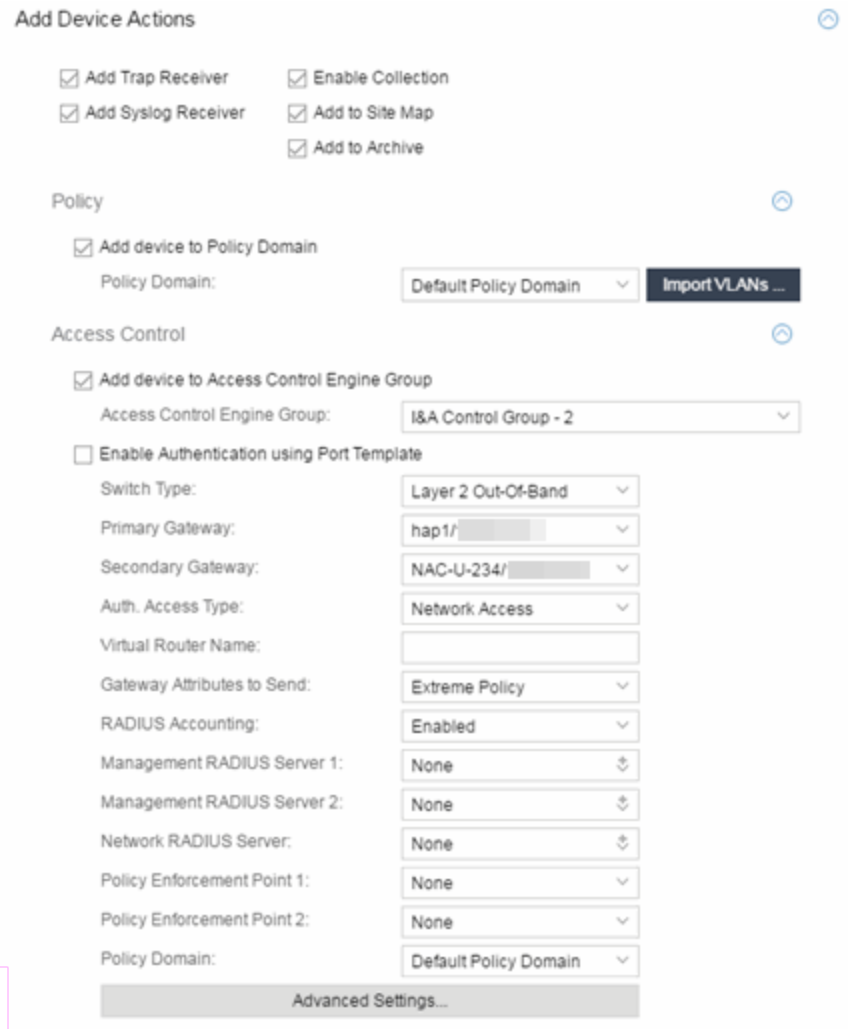
The user-defined information displayed in the devices table in the **User Data** columns.

Notes

Additional user-defined information displayed in the devices table in the **Notes** column.

Add Device Actions

The Add Device Actions section indicates the actions taken by the device upon being discovered.



Add Trap Receiver

Select this checkbox if you want the devices being discovered to receive trap information it sends to ExtremeCloud IQ Site Engine.

Add Syslog Receiver

Select this checkbox to configure the devices being discovered to receive information it sends to the syslog.

Enable Collection

Select this checkbox to collect device statistics on the device being discovered you can use in ExtremeCloud IQ Site Engine reports.

Add to Site Map

Select this checkbox to add the devices being discovered to the map, as well as its parent site, that is associated with the currently accessed site. Selecting the check box also adds the devices to the map specified on the site's Add Action tab.

Add to Archive

Select this checkbox to create an archive, which saves the configurations of the devices being discovered in the **Network** > **Archives** tab.

Policy

Add device to Policy Domain

Select this checkbox to add the device to a policy domain you create on the **Policy** tab. When the checkbox is selected, use the Policy Domain drop-down list to select the policy domain to which the device is added.

Select the **Import VLANs** button to import the VLAN definitions from the policy selected in the Policy Domain drop-down list.

Access Control

Add device to Access Control Engine Group

Select this checkbox to add the device to an Access ControlEngine Group you create on the **Access Control** tab. When the checkbox is selected, use the **Access Control Engine Group** drop-down list to select the engine group to which the device is added.

Enable Authentication using Port Template

Select this checkbox to allow users to authenticate using a port template, configured on the **Site** tab.

Switch Type

Use the drop-down list to select the type of switch you are adding:

- **Layer 2 Out-Of-Band** — A switch that authenticates on layer 2 traffic via RADIUS to an out-of-band Access Control engine.
- **Layer 2 Out-Of-Band Data Center** — A switch within a data center where virtualization and mobility are a factor. If an end-system changes location but does not move to a different Access Control engine, Access Control removes the end-system authentication from their prior port/switch. This allows VMs that quickly move from one server to another and then back again to still have their location updated in ExtremeCloud IQ Site Engine, because only one authenticated session is allowed per end-system in ExtremeCloud IQ Site Engine.
- **Layer 2 RADIUS Only** — In this mode, ExtremeCloud IQ Site Engine does not require any information from the switch other than the end-system MAC address (from Calling-Station-Id or User-Name). The NAS-Port does not need to be specified. If the switch supports RFC 3576, you can set the Reauthentication Behavior in the Advanced Switch Settings window. IP resolution and reauthentication may not work in this mode.
- **VPN** - A VPN concentrator being used in an ExtremeControl VPN deployment. In this case, you should specify one or more Policy Enforcement Points below. If you do not

specify a Policy Enforcement Point, then ExtremeCloud IQ Site Engine is unable to apply policies to restrict access after the user is granted access.

Primary Engine

Use the drop-down list to select the primary Access Control Engine for the selected switches. If load balancing has been configured for the engine group, the ExtremeCloud IQ Site Engine server determines the primary and secondary engines at Enforce, and this field displays **Determined by Load Balancer**.

Secondary Engine

Use the drop-down list to select the secondary Access Control Engine for the selected switches. If load balancing has been configured for the engine group, the ExtremeCloud IQ Site Engine server determines the primary and secondary engines at Enforce, and this field displays **Determined by Load Balancer**.

NOTE: To configure additional redundant Access Control Engines for each switch (up to four), use the Display Counts option in the Display Options panel (Administration > Options > Access Control).

Auth. Access Type

Use the drop-down list to select the type of authentication access allowed for these switches. This feature allows you to have one set of switches for authenticating management access requests and a different set for authenticating network access requests.

WARNING: Access Control uses CLI access to perform configuration operations on Fabric Engine devices. ExtremeControl uses SNMP and CLI access to perform configuration operations on Switch Engine devices based on the firmware version.

- Enabling an Auth type of "Any Access" or "Management Access" can restrict access to the switch after an enforce is performed. Make sure that an appropriate administrative access configuration is in place by assigning a profile such as "Administrator Access Control Profile" to grant proper access to users. Also, verify that the current switch CLI credentials for the admin user are defined in the database that ExtremeCloud IQ Site Engine authenticates management login attempts against.
- Switching from an Auth type of "Any Access" or "Management Access" back to "Network Access" can restrict access to the switch after an enforce is performed. Verify that the current switch CLI credentials for the admin user are defined locally on the switch.

- **Any Access** - the switch can authenticate users originating from any access type.
- **Management Access** - the switch can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- **Network Access** - the switch can only authenticate users that are accessing the network via the following authentication types: MAC, PAP, CHAP, and 802.1X. If

RADIUS accounting is enabled, then the switch also monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. If there are multiple sessions for a single end-system, the session with the highest precedence displays to provide the most accurate access control information for the user. The Access Control authentication type precedence from highest to lowest is: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.

- **Monitoring - RADIUS Accounting** - the switch monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. ExtremeCloud IQ Site Engine learns about these session via RADIUS accounting. This allows ExtremeCloud IQ Site Engine to be in a listen mode, and to display access control, location information, and identity information for end-systems without enabling authentication on the switch. If there are multiple sessions for a single end-system, the session with the highest precedence displays to provide the most accurate access control information for the user. The Access Control authentication type precedence from highest to lowest is: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.
- **Manual RADIUS Configuration** - ExtremeCloud IQ Site Engine does not perform any RADIUS configurations on the switch. Select this option if you want to configure the switch manually using the **Policy** tab or CLI.

Virtual Router Name

Enter the name of the Virtual Router. The default value for this field is **VR-Default**.

WARNING: For ExtremeXOS/Switch Engine devices only. If ExtremeCloud IQ Site Engine has not detected and populated this field, enter the Virtual Router Name carefully. Incorrectly entering a value in this field causes the RADIUS configuration to fail, which is not reported when enforcing the configuration to the switch.

RADIUS Attributes to Send

Use the drop-down list to select the RADIUS attributes included as part of the RADIUS response from the Access Control engine to the switch. You can also select Edit RADIUS Attribute Settings from the menu to open the RADIUS Attribute Settings window where you can define, edit, or delete the available attributes.

RADIUS Accounting

Use the drop-down list to enable RADIUS accounting on the switch. RADIUS accounting can be used to determine the connection state of the end-system sessions on the Access Controlengine, providing real-time connection status in ExtremeCloud IQ Site Engine.

Management RADIUS Server 1 and 2

Use the drop-down list to specify RADIUS servers used to authenticate requests for administrative access to the selected switches. Select from the RADIUS servers you have configured in ExtremeCloud IQ Site Engine, or select New or Manage RADIUS Servers to open the Add/Edit RADIUS Server or Manage RADIUS Servers windows.

Network RADIUS Server

This option lets you specify a backup RADIUS server to use for network authentication requests for the selected switches. This allows you to explicitly configure a network RADIUS server to use if there is only one Access Control engine. (This option is only available if a Secondary Engine is not specified.) Select from the RADIUS servers you have configured in ExtremeCloud IQ Site Engine, or select New or Manage RADIUS Servers to open the Add/Edit RADIUS Server or Manage RADIUS Servers windows.

Policy Enforcement Point 1 and 2

Select the Policy Enforcement Points used to provide authorization for the end-systems connecting to the VPN device you are adding. The list is populated from the N-Series, S-Series, and K-Series devices in your Console device tree. If you do not specify a Policy Enforcement Point, then Access Control is unable to apply policies to restrict end user access after the user is granted access.

Policy Domain

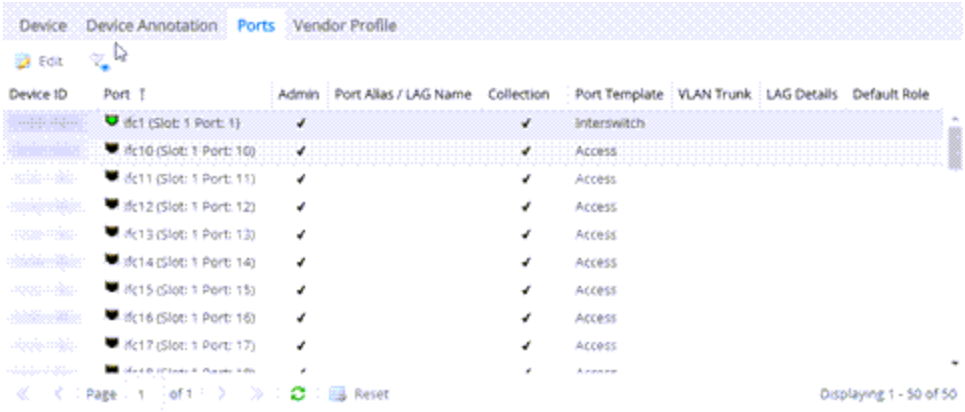
Use this option to assign the switch to a policy domain and enforce the domain configuration to the switch. The switch must be an Extreme Networks switch.

Advanced Settings

Select the Advanced Settings button to open the Advanced Switch Settings window.

Ports

The Ports section of the Add Selected Device window allows you to enter information about the ports on a device. Select the **Add** button to add a new port to the list. Select the **Delete** button to remove a device from the list.



Name

Enter the name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

Alias

Shows the alias (ifAlias) for the interface, if one is assigned.

Configuration

Use the drop-down list to determine the purpose of the port:

- **Access** — Select this option if the port connects to user end-systems.
- **Interswitch** — Select this option if the port is used to connect to other switches.
- **Management** — Select this option if the port is used to manage network traffic with ExtremeCloud IQ Site Engine.

Policy

The policy assigned to the selected port.

Add

Select the **Add** button to add the device to the ExtremeCloud IQ Site Engine database with the current configuration.

Cancel

Select the **Cancel** button to close the window without adding the device to the ExtremeCloud IQ Site Engine database.

ZTP+ VLAN Definition

The ZTP+ VLAN Definition section allows you to configure VLANs on the device you are adding. To add a VLAN, select the **Add** button. You can remove a VLAN by selecting the **Delete** button.



Name

Displays the name of the VLAN.

VID

Indicates the VLAN ID for the VLAN. A unique number between 1 and 4094 that identifies a particular VLAN. VID 1 is reserved for the Default VLAN.

Dynamic Egress

Indicates if the associated dynamic egress setting for the VLAN (Enable or Disable) is written to the device(s) when you enforce.

Protocol Filter

Indicates the VLAN uses an X-Pedition Protocol Filter.

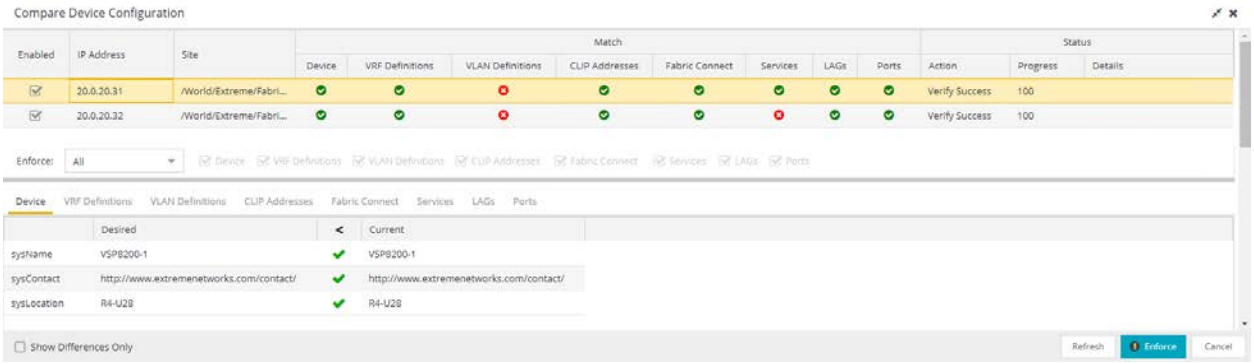
Management
Indicates which VLAN the ExtremeXOS/Switch Engine device uses for Management and assigns the device IP to that VLAN.

Always Write to Device(s)
Indicates if the VLAN is written to the device whether or not it is being used in a rule or role.

Device Configuration Enforce Preview

This window allows you to preview changes you make to a device configuration and then enforce them to the device.

To access this window, select **Enforce Preview** in the **Configure Device** window.



The Compare Device Configuration window is divided into three sections:

- Device Details
- Enforce Options
- Device Configuration Detail Table

Device Details

The top of the window displays a list of the devices you selected to verify. Select a device in the table at the top of the window to display the configuration for that device in the Device Configuration Detail table at the bottom of the window.

The data in this section is divided into **Match** and **Status** columns:

Match Column

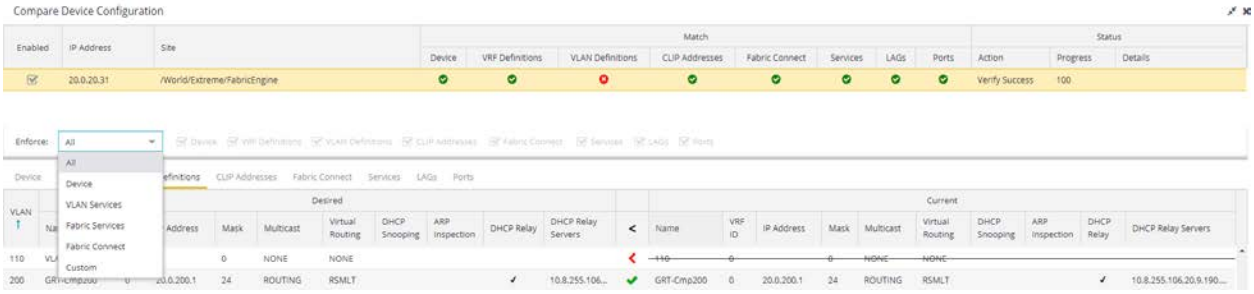
Devices on which the current configuration matches the desired configuration display a check icon (✔), while devices on which differences are detected display a red x (✖).

Status Column

The Status column displays the details of the status of the configuration matches in the Match column.

Enforce Options

The Enforce Options section of the window enables you to push the changes you made to the device, view and compare the changes to the current



Select an option from the **Enforce** drop-down list to push the changes you make to the device or the specific service you select. Your selection from the drop-down list displays the changes to the configurations that are being pushed to the device in the Device Configuration Detail Table at the bottom of the window.

NOTES: Device is the default option for the Enforce Options window.

Use Enforce to verify whether the settings you want to configure on the device require other settings to also be set on the device. The Enforce fails if the other required settings are not configured for the changes you want to make.

The following options are included in the **Enforce** drop-down list:

All

To push configuration changes to multiple components of the device, select **All**. The Device, VRF Definitions, VLAN Definitions, CLIP Address, Topology, Services, LAGs, and Ports tabs in the Device Configuration Detail table become available for you to view the changes and compare them to the current configuration.

Device

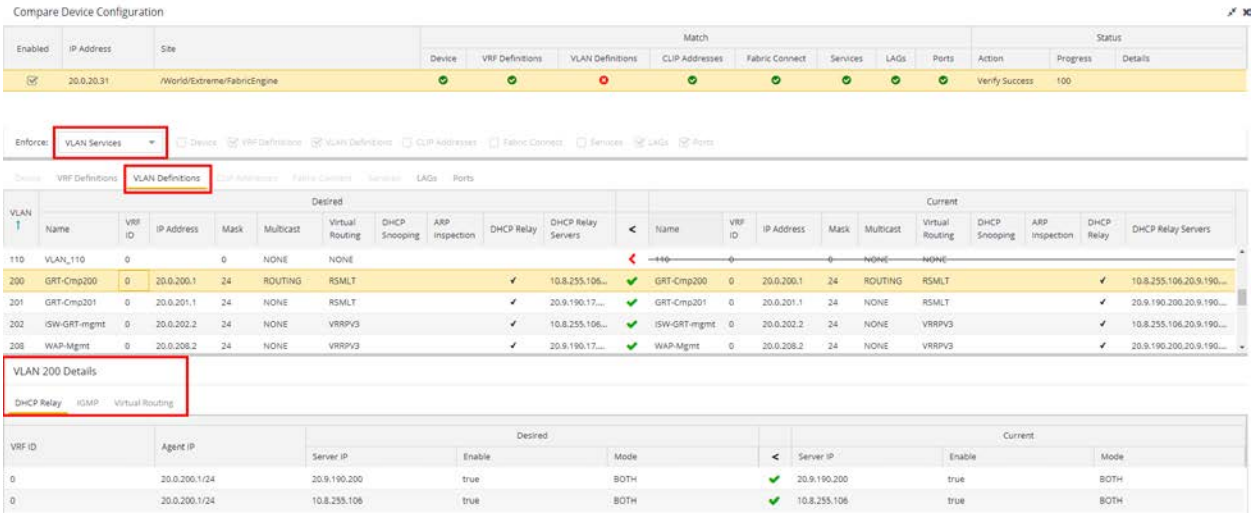
To view configuration changes to the device, select **Device**. The Device tab in the Device Configuration Detail table becomes available for you to view the changes and compare them to the current configuration.

VLAN Services

To push configuration changes to the VLAN, select **VLAN Services**. The VRF Definitions, VLAN Definitions, LAGs, and Ports tabs in the Device Configuration Detail table become available for

you to view the changes and compare them to the current configuration.

In addition, the VLAN Details grid opens at the bottom of the Device Configuration table. The grid provides additional details about the changes you made to the VLAN:



The VLAN Details grid includes the following tabs:

DHCP Relay
Displays details of changes you've made to the DHCP relay servers enabled for the VLAN.

IGMP
Displays changes you've made to the IGMP assigned to the VLAN.

VRRP
Displays changes to the state of the virtual router interfaces assigned to IPs in the VLAN.

Fabric Services
To push configuration changes to Fabric Services on the device, select **Fabric Services**. The VRF Definitions, VLAN Definitions, CLIP Addresses, Services, LAGs, and Ports tabs in the Device Configuration Detail table become available for you to view the changes and compare them to the current configuration.

Fabric Topology
To view the configuration changes to the fabric topology, select **Fabric Topology**. The Fabric Connect tab in the Device Configuration Detail table becomes available for you to view the changes and compare them to the current configuration.

Custom
The **Custom** option enables you to select which tabs to display in the Device Configuration Detail table. Use the check boxes to the right of the **Enforce** button to select the tabs you want to include in the table.

NOTE: Device is the default option for the Enforce Options window.

IMPORTANT: When performing an enforce on the following options, ExtremeCloud IQ Site Engine validates your changes:

- All
- VLAN Services
- Fabric Services
- Fabric Connect

An error displays if you are attempting to enforce changes that are not valid for the device.

Device Configuration Detail Table

The Device Configuration Detail table includes several tabs:

- Device
- VRF Definitions
- VLAN Definitions
- CLIP Addresses
- Fabric Connect
- Services
- LAGs
- Ports

The configurations are separated into two columns on each tab:

- The Desired column shows the configuration you are saving to the device on the next enforce.
- The Current column shows the configuration currently on the device.

A check mark between the columns (✔) indicates the Current configuration matches the Desired configuration.

A left arrow icon () indicates the configurations do not match. Selecting it copies the Current configuration to the Desired configuration so no configuration change is made when enforcing the device.

Device

The **Device** tab displays any changes to basic information about the device.

sysName
The name by which the device is known.

sysContact
Allows you to specify contact information for the person maintaining the device.

sysLocation
The physical location of the device.

VRF Definitions

The **VRF Definitions** tab displays any changes to the configuration of VRFs on the device.

Name
Displays the name of the VRF.

Multicast
Select to indicate the service sends IP packets to a group of hosts on the network.

Unicast
Select to indicate the service sends IP packets to a single recipient on the network.

Direct Route
Select to indicate the service sends IP packets directly to another device without going through a third device.

Default Gateway
Enter the IP address of the switch's default gateway. If a device is ZTP+-enabled, the site's ZTP+ Device default gateway displays.

VLAN Definitions

The **VLAN Definitions tab** displays the changes to the configuration of VLANs on the device.

VLAN
A unique numerical identifier of the VLAN.

Name
Displays the name of the VLAN.

VRF ID
Displays the ID number of the VRF associated with the VLAN.

IP Address
Displays the IP address associated with the VLAN.

NOTE: IP Address provisioning is only supported on Fabric Engine devices.

Mask
Displays the IP/subnet mask.

Secondary IPs

Displays the secondary IP addresses associated with the VLAN.

NOTE: Secondary IP Address provisioning is only supported on Fabric Engine devices.

Multicast

Indicates the service sends IP packets to a group of hosts on the network.

IGMP Version

Indicates which version of IGMP is utilized on the port (Version 1 or Version 2).

IGMP Querier

The address of the IGMP Querier. This feature is used when there is no multicast router in the VLAN to originate the queries.

Querier Enable

Indicates whether an IGMP Query is enabled.

Virtual Routing

Displays the version of VRRP the default gateway is using:

- **NONE** — Virtual routing is not configured on the VLAN.
- **VRRPv2** — VRRP version 2 is configured on the virtual router. VRRP version 2 only supports IP addresses in IPv4 format.
- **VRRPv3** — VRRP version 3 is configured on the virtual router. VRRP version 3 supports IP addresses in both IPv4 and IPv6 formats.
- **DvR –**DvR is configured on the VLAN. There are several requirements that must be met to configure DvR on a VLAN, including:
  - The VLAN must have an IP address and prefix.
  - The DvR IP address must be IPv4.
  - The DvR IP address must fall within the VLAN's subnet.
  - The DvR IP address cannot be reused across multiple VLANs on the device.
  - The VLAN must have an L2VSN associated with it.
  - If the VLAN is using on a non-zero VRF ID, the VLAN must also have:
    a. An L3VSN associated with the VRF.
    b. The VRF must have the unicast option enabled.
  - Devices participating in DvR as controllers must have non-zero IPv4 ISIS Source Addresses.
  - Devices participating in DvR must have IPv4 Shortcuts and Multicast enabled.
- **RSMLT** — Routing Redundancy Method is configured on the VLAN. RSMLT requires that a Virtual IST is configured. If the device is not configured as a vIST pair, **RSMLT** can be

selected, but the feature is not active. Once the vIST is configured, RSMLT becomes active.

NOTES:

Virtual Routing is only supported on Fabric Engine devices.

Fabric Enginedevices support a new "dvr-one-ip" feature in the 8.2 release that allows you to share an IP address between a VLAN and its DvR interface. ExtremeCloud IQ Site Engine currently does not support the "dvr-one-ip" feature and cannot read or enforce configurations of this type. Configure Fabric Engine device IP addresses on VLANs and their DvR interfaces through the **VLAN Definitions** tab.

Virtual Routing Enable
Indicates whether virtual routing is enabled for the VLAN.

Virtual Routing Address
The IP address for the virtual router. The Virtual Routing address must be in the same subnet as the VLAN subnet address.

VRRP ID
An identifier devices use to determine peer devices that participate in a VRRP (Virtual Routing Redundancy Protocol) virtual routing interface.

VRRP Priority
A value used by VRRP peers to determine the role of each of the devices in the VLAN. The default value is **100**. The device with the largest value is assigned the role of Controller. For example, in a VLAN with two routers, one with a **VRRP Priority** of **200** and one with a **VRRP Priority** of **100**, the router with a **VRRP Priority** of **200** becomes the Controller. In the event of identical priority numbers, the devices use the MAC address to determine priority.

VRRP Backup Master
This option determines if the backup router is able to forward traffic independently outside of the VLAN (enabled), or must forward the traffic to the Controller router before it is forwarded outside of the VLAN (disabled).

VRRP Advertisement Interval
Indicates frequency (in seconds) that protocol packets are sent from the virtual router in the VLAN.

VRRP Hold Down Timer
Indicates the amount of time (in hundredths of a second) that the backup router waits for the primary router to respond before it becomes the primary router.

DHCP Snooping
Indicates whether DHCP snooping is enabled for the VLAN. DHCP Snooping is a Layer 2 security feature, that provides network security by filtering untrusted DHCP messages

received from the external network causing traffic attacks within the network. DHCP Snooping is based on the concept of trusted versus untrusted switch ports. Switch ports configured as trusted can forward DHCP Replies, and the untrusted switch ports cannot. DHCP Snooping acts like a firewall between untrusted hosts and DHCP servers.

ARP Inspection

Indicates whether ARP inspection is enabled. Dynamic ARP Inspection (DAI) is a security feature that validates ARP packets in the network. Without DAI, a malicious user can attack hosts, switches, and routers connected to the Layer 2 network by poisoning the ARP caches of systems connected to the subnet, and intercepting traffic intended for other hosts on the subnet. DAI prevents these attacks by intercepting, logging, and discarding the ARP packets with invalid IP to MAC address bindings. The switch dynamically builds the address binding table from the information gathered from the DHCP requests and replies when DHCP Snooping is enabled. The switch pairs the MAC address from the DHCP request with the IP address from the DHCP reply to create an entry in the DHCP binding table. When you enable DAI, the switch filters ARP packets on untrusted ports based on the source MAC and IP addresses seen on the switch port. The switch forwards an ARP packet when the source MAC and IP address matches an entry in the address binding table. Otherwise, the switch drops the ARP packet.

NOTE: **DHCP Snooping** must be enabled to use **ARP Inspection**.

DHCP Relay

Indicates whether a Dynamic Host Configuration Protocol relay server is enabled for the VLAN. A DHCP relay receives and converts a DHCP broadcast message to dynamically assign an IP address to a device on the network.

DHCP Relay Servers

The IP addresses of the DHCP relay servers for the VLAN.

NOTE: Select **Manage** to open the **Manage DHCP Relay Servers** window, where you can add or delete DHCP relay servers.

CLIP Addresses

Use the **CLIP Addresses** tab to view changes to IPv4 and IPv6 CLIP Addresses on your device.

Device ID

The ID address of the device to which the CLIP address is assigned.

CLIP Interface

The interface ID for the CLIP address.

IP Version

Indicates the IP Address: IPv4 or IPv6

IP Address

The IP address associated with the selected interface (VLAN, BROUTER or MGMT).

Prefix Length

Displays the number of digits that comprise the IP Address prefix. Prefix length for IPv4 Addresses is between 8 and 30 digits, and the prefix length for IPv6 addresses is between 8 and 128 digits

Fabric Connect

The **Fabric Connect** tab displays changes to the Fabric Connect features to devices in your network.

Topology Definition

Displays the Topology Definition that applies to the device. The Topology Definitions available in the drop-down list are configured in the **Topology Definition** tab.

- **None** - No Fabric Connect configuration on the device. If you select **None** for a device that is configured for Fabric Connect, that configuration is removed.
- **Local** - The Fabric Connect configuration is configured locally and not by ExtremeCloud IQ Site Engine.
- **Disabled** - The Fabric Connect configuration is applied to the device, but ISIS is disabled, which allows the user to take a device out of service without removing all its configuration.
- **Service Definition** - The Service Definition that has been applied to the site to which the device is assigned.

SPBM Instance

The system-defined identifier for the Fabric Connect configuration on the device. The default value is 1.

Secondary BVLAN

The Secondary Backbone VLAN. This information is configured on the **Sites > Topology Definition** tab.

Primary BVLAN

The Primary Backbone VLAN. This information is configured on the **Sites > Topology Definition** tab.

Nickname Server Prefix

This is the 1-byte "x.y" portion of the larger "1.23.45" nickname format. This field can be edited when **Nickname Server Enable** is selected and the **Topology Definition** is Local, Disable, or a user-defined topology definition.

Nickname Server Enable

This enables the Nickname Server on a Fabric Engine device. You can enable this function when **Topology Definition** is set to Local, Disable, or a user-defined topology definition, and **SPBM Nickname Dynamic Allocation** is set to Dynamic.

Nickname
A value that other fabric devices use to identify the device. The SPBM nickname must be unique within the fabric.

Multicast Enable
The check box is selected if Multicast is enabled for the device.

ISIS System Name
The system name of the device.

ISIS System ID
The system-defined fabric service identifier assigned to the device. The default is the MAC address for the device.

ISIS IP Source Address (V6)
The IPv6 address the device uses to transmit ISIS traffic to other fabric devices. The address must be unique within the fabric.

ISIS IP Source Address
The IPv4 address the device uses to transmit ISIS traffic to other fabric devices. The address must be unique within the fabric.

ISIS Manual Area
The IS-IS Manual Area in xx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx format (1-13 bytes). This information is configured on the **Sites > Topology Definition** tab.

IPv6 Shortcuts
The check box is selected if IPv6 Shortcuts are enabled for the device.

IPv4 Shortcuts
The check box is selected if IPv4 Shortcuts are enabled for the device.

Enable RSMLT Edge Support
Select this option to use the RSMLT Edge.

Enable Fabric Attach
The check box is selected if Fabric Attach functionality is supported.

Enable Fabric
Select this option to use the SPBM fabric.

DvR Role
Displays the DvR Role from the drop-down list:

- None - DvR (Distributed Virtual Routing) is not configured on the device.
- Controller - Indicates the device is one of the main devices participating in the DvR virtual routing interface.
- Leaf - Indicates the device is one of several edge devices within the DvR domain.

- Global Backbone - Indicates the device is a standard Fabric Connect device that and does not run the DvR protocol, but will learn routes from DvR controllers in the fabric.

DvR Domain ID
Displays the identifying number for the DvR domain.

Services

The **Services** tab displays the services created within service applications and configured on the device. Use this tab to add new services to the device. Services may be inherited from a service definition or may be configured locally on the device.

L2 VSN

Source
Indicates the service definition and service application from which the service is inherited.

Device ID
Indicates the IP address of the device on which the service is used.

Origin
Indicates how the service is created.

Name
The name of the Layer 2 service.

Service ID
The ID number of the fabric service.

VLAN
The VLAN to which the fabric service is associated.

L3 VSN

Source
Indicates the service definition from which the service is inherited.

Name
The name of the Layer 3 service.

Service ID
The ID number assigned to the service.

VRF
Select the VRF to which the service is associated.

LAGs

Use the **LAG** tab to configuration changes to LAGs and MLAGs (also known as MLTs and SMLTs, respectively). A LAG combines multiple network connections to increase the throughput beyond that

of a single connection. An MLAG allows a device to send network traffic to two switches to improve network diversity, while only managing a single logical interface.

Source
Indicates the location from which the LAG is inherited. The LAG can be inherited from a site, locally configured on the device itself, or can be excluded.

NOTE: Selecting **Exclude** indicates you are excluding an inherited configuration. LAG configurations locally defined on the device and are not cannot be excluded. You can only select **Exclude** for configurations inherited from a Site (or a Service Application).

IP Address
Displays the IP address of the LAG.

Type
Displays the type of LAG, either LAG or MLAG.

LAG ID
Displays a system-defined ID number for the LAG.

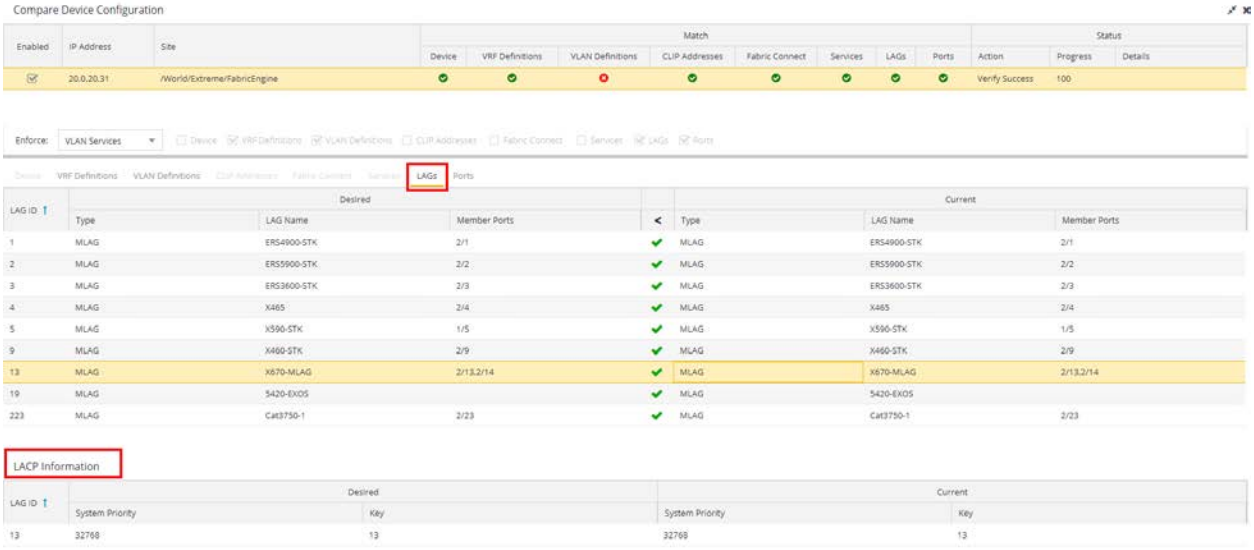
Name
Displays a user-defined name for the LAG.

Member Ports
Displays the ports that are included in the LAG.

Aggregatable Type
Indicates whether the LAG is static or dynamic:

- Static — the LAG is static.
- LACP — the LAG is dynamic via LACP.

The LACP Information grid opens at the bottom of the Device Configuration table:



The LACP Information grid displays the following tabs, separated into Desired and Current columns:

System Priority

Displays the LACP priority, which ExtremeCloud IQ Site Engine uses to determine the probability network traffic uses the LAG. Valid values are between 1 and 65,535. The lower the value entered, the higher ExtremeCloud IQ Site Engine prioritizes the LAG.

Key

Displays the LACP key, which the LAG uses to ensure it only pairs with properly configured endpoints.

Ports

The **Ports** tab displays any changes to the configuration of ports on the device.

Port

The name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

Alias

Displays the alias for the port, if one is assigned.

PVID

The port's VLAN assignment. Possible values are 1 through 4094.

Tagged

The port is added to the list with the egress state set to Tagged (frames are forwarded as tagged).

Untagged

The port is added to the list with the egress state set to Untagged (frames are forwarded as untagged).

Fabric Enable

Indicates the fabric functionality is enabled on the port.

ExtremeCloud IQ Site Engine can extend FA functionality to ExtremeXOS/Switch Engine devices and provision them as FA Proxy devices. Select "Fabric Attach" or "" from the drop-down list to enable the port on a Fabric Engine device (acting as FA Server) to connect to an ExtremeXOS/Switch Engine device (acting as FA Proxy).

- **Fabric Attach** - Enable Fabric Attach server functionality on the port of a Fabric Engine device acting as a Fabric Attach server) to connect to an ExtremeXOS/Switch Engine device (acting as a Fabric Attach proxy).
- **Fabric Attach and Switched UNI** - Enable Fabric Attach server functionality on the port of a Fabric Engine device acting as a Fabric Attach server) to connect to an ExtremeXOS/Switch Engine device (acting as a Fabric Attach proxy). When selecting this option, the port is configured for both features, but only one feature is active at any one time.
- **Auto Sense** - Select **Auto Sense** on the port of a Fabric Engine device to enable the port to automatically sense and configure automatically sense and configure the appropriate Fabric settings for the port. These settings include the following:
  - PVID
  - VLAN Trunk
  - Tagged
  - Untagged
  - Fabric Mode
  - Fabric Auth Type
  - Fabric Auth Key
  - Fabric Connect Drop STP-BPDU
  - BPDU Guard
  - Authentication

NOTE: If **Fabric Enable** is **Auto Sense** the Fabric settings listed above are not configurable.

Fabric Auth Type

If **Fabric Enable** is **Fabric Attach** or **NNI**, this defines the type of authentication the device uses for the port to communicate with the other ISIS devices to secure those services.

Fabric Auth Key

Indicates the fabric authentication key used for the port.

Span Guard

Select to enable Span Guard, which allows the device to shut down a network port if it receives a BPDU (bridge protocol data unit). Enable this feature on network edge ports to prevent rogue STA-aware devices from disrupting the existing Spanning Tree.

SLPP

Indicates Simple Loop Prevention Protocol (SLPP) is enabled on the port. SLPP provides active protection against Layer 2 network loops on a per-VLAN basis. If an SLPP packet is received, the port is disabled for the amount of time configured in the **SLPP Timer** field.

NOTE: If **SLPP** is enabled, **SLPP Guard** is not available.

SLPP Guard

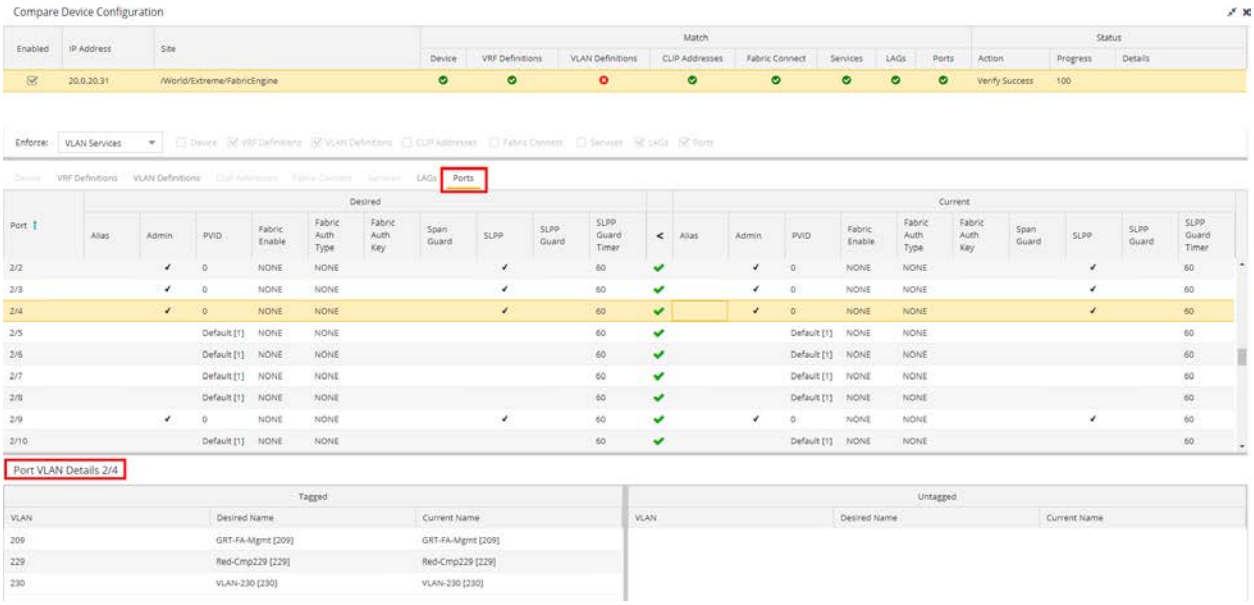
Indicates whether SLPP Guard is enabled on the port. Use SLPP Guard to provide additional loop protection to protect wiring closets from erroneous connections. SLPP Guard requires **SLPP** to be enabled. SLPP detects loops in an SMLT network. Because SMLT networks disable Spanning Tree (STP), Rapid Spanning Tree (RSTP), or Multiple Spanning Tree Protocol (MSTP) for participating ports, SLPP Guard provides additional network loop protection, extending the loop detection to individual edge access ports. SLPP Guard can be configured on MLT or LAG ports. If the edge switch with SLPP Guard enabled receives an SLPP-PDU packet on a port, SLPP Guard operationally disables the port for the configured timeout interval in the **SLPP Guard Timer** field and appropriate log messages and SNMP traps are generated. If the disabled port does not receive any SLPP-PDU packets after the configured timeout interval expires, the port automatically re-enables and generates a local log message, a syslog message, and SNMP traps, if configured.

NOTE: If **SLPP Guard** is enabled, **SLPP** is not available

SLPP Guard Timer

Indicates the amount of time after receiving an SLPP packet before the port is re-enabled.

The Port VLAN Details grid opens at the bottom of the Device Configuration table:



The Port VLAN Details grid displays desired and current ports, separated into **Tagged** and **Untagged** columns.

Select **Enforce** to save your changes to the device.

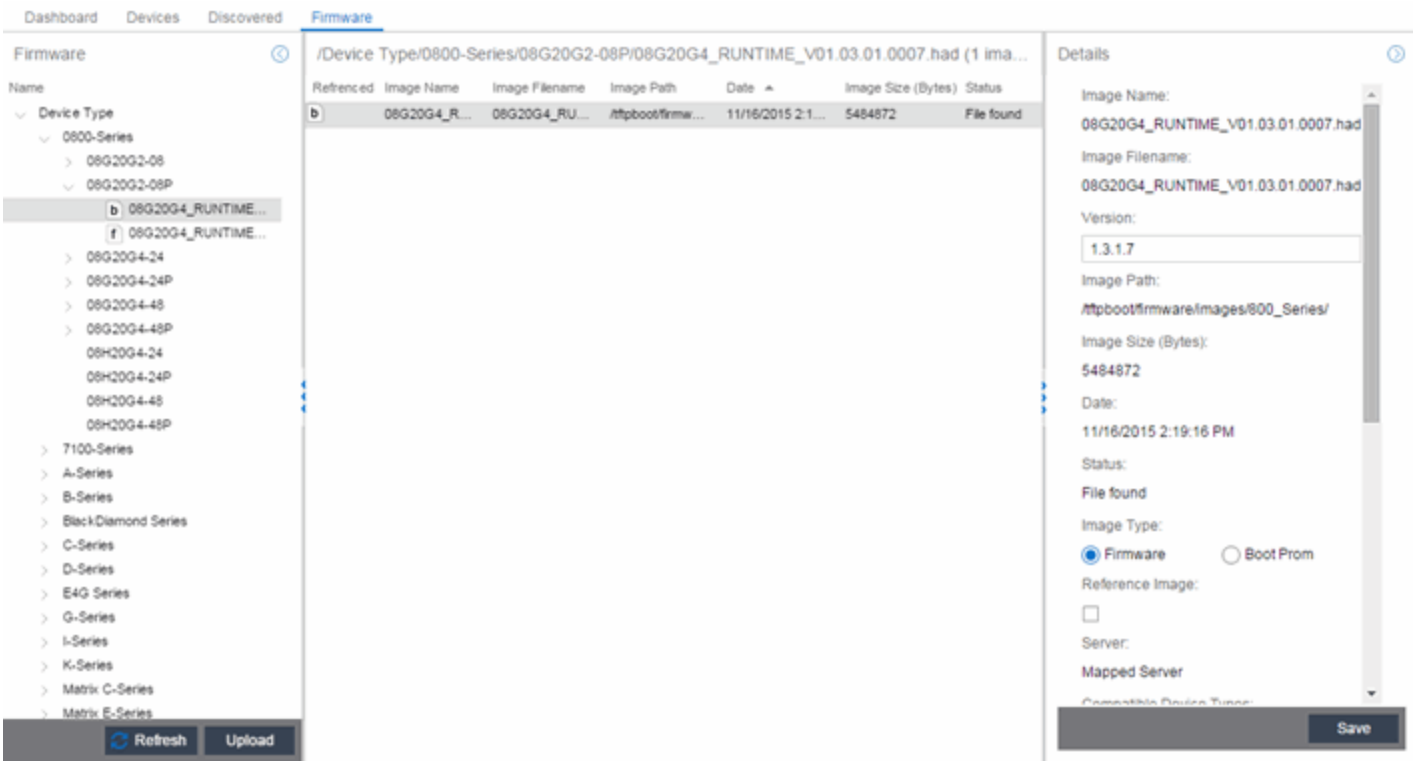
Firmware

The **Firmware** tab allows youto upload firmware and boot PROM images to ExtremeCloud IQ Site Engine and assign them to the devices on your network.

To access the **Firmware** tab, open the **Network** tab and select the **Firmware** tab.

The tab is divided into three sections:

- Firmware Tree
- Device Type Images Section
- Details Section



Firmware Tree

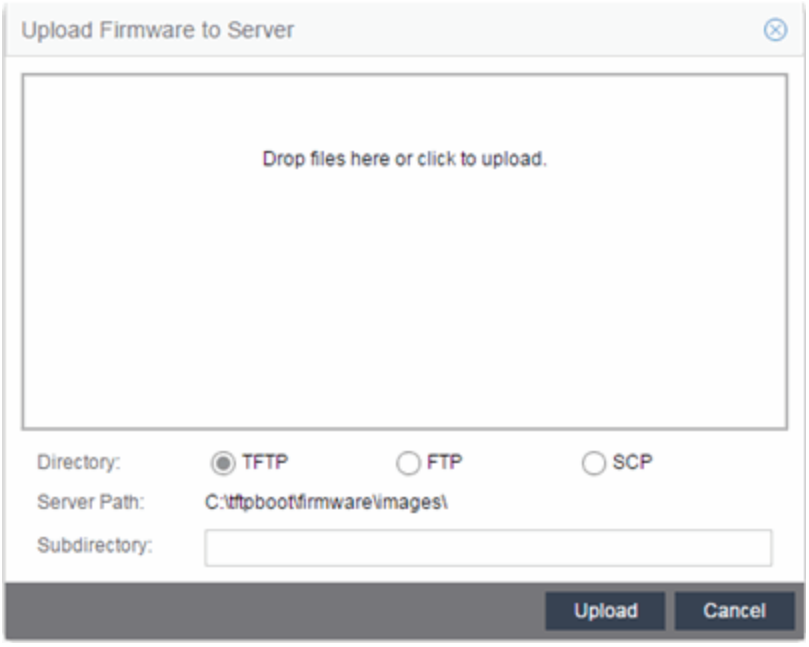
The **Firmware** tree in the left panel displays firmware and boot PROM images grouped according to product family and device type. It provides pre-defined firmware groups and automatically organizes the images stored in your firmware directory under the appropriate group when you perform a firmware discovery or refresh. The Unknown folder contains images that ExtremeCloud IQ Site Engine could not correlate to a device type.

Name

The **Name** navigation tree lists the product families and device types to which you can assign the firmware or boot PROM image.

Upload

Select the **Upload** button to open the Upload Firmware to Server window from which you can save image files to the ExtremeCloud IQ Site Engine server. This allows anyone with access to ExtremeCloud IQ Site Engine to download the image file to a device.



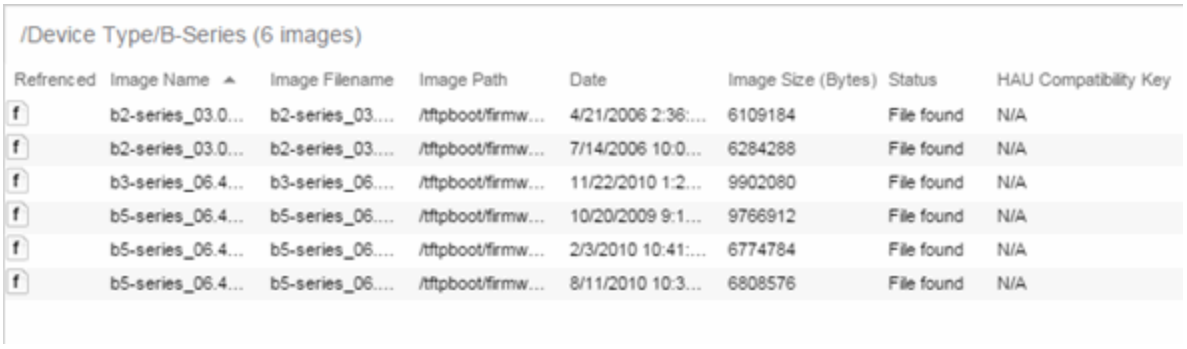
For additional information on how to upload a firmware or boot PROM image, see How to Upgrade Firmware.

Refresh

Select the **Refresh** button to synchronize the images displayed in the Firmware left-panel with the firmware and boot PROM images on the ExtremeCloud IQ Site Engine server. Selecting this button checks for any firmware and boot PROM images saved in the Firmware Directory Path (configured on the **Administration** > **Options** > **Inventory Manager** tab) on the ExtremeCloud IQ Site Engine server and adds or removes images from the Firmware left-panel in ExtremeCloud IQ Site Engine to match.

Device Type Images Section

The Device Type Images section displays the firmware and boot PROM images that match the device type selected in the Firmware left-panel. To save a firmware or boot PROM image to a device, select it from the list and save the image to the device in the Details section of the **Firmware** tab.



Referenced

Firmware or boot PROM images set as a reference image display a reference icon (f) or boot PROM (b) in this column. A reference image is the image you designate as the preferred image for a specific binary family of devices. To set a reference, select a firmware or boot PROM image in the table or the tree, right-click and select **Set as Reference Image** from the menu. The image is set as a reference for all device types with which it is compatible. (If the Set as Reference Image option is not available, make sure that the selected image has been assigned to appropriate device types.).

NOTE: The ratio of devices on which firmware you define as a reference image is installed to the total number of devices is available as a ring chart in the Impact Analysis dashboard.

Image Name

The name of the image as it is displayed in the left-panel Firmware tree. The maximum length of the displayed name is 50 characters. Longer names are truncated to the 50-character maximum with a (2), (3), and so on, appended if there are multiple images with the same name.

Image Filename

The full filename of the firmware or boot PROM image as it appears in your firmware images directory.

Image Path

The path to the location where the image file is stored.

Date

The date of the firmware or boot PROM image as reported by the file system.

Image Size

The file size of the firmware or boot PROM image in bytes.

Status

Indicates the status of the image file in the firmware directory: **File Found** or **File Not Found**. If the image is a user-defined firmware record, this column displays **User-Defined File**.

HAU Compatibility Key

This column displays the HAU Compatibility Key, if one is detected on the firmware image. The HAU Compatible column (in the Assignments table) displays whether the firmware image and the device are HAU compatible. HAU (Highly Available Upgrade) is a feature on certain devices that allows firmware to be upgraded with minimal (if any) downtime. HAU is configured using the device CLI or by creating a FlexView in Console (ethsyHauSystemHauMode). When the device HAU status is set to "If Possible" or "Always" mode, ExtremeCloud IQ Site Engine performs the upgrade using this feature, if the HAU firmware key on the current firmware and the key on the newly selected firmware are compatible.

The following table explains the upgrade procedure for HAU devices:

HAU Mode on Device	New Image HAU Compatible?	Upgrade Procedure
Never	Yes	Standard Upgrade
Never	No	Standard Upgrade
If Possible	Yes	HAU
If Possible	No	Standard Upgrade
Always	Yes	HAU
Always	No	Upgrade Fails

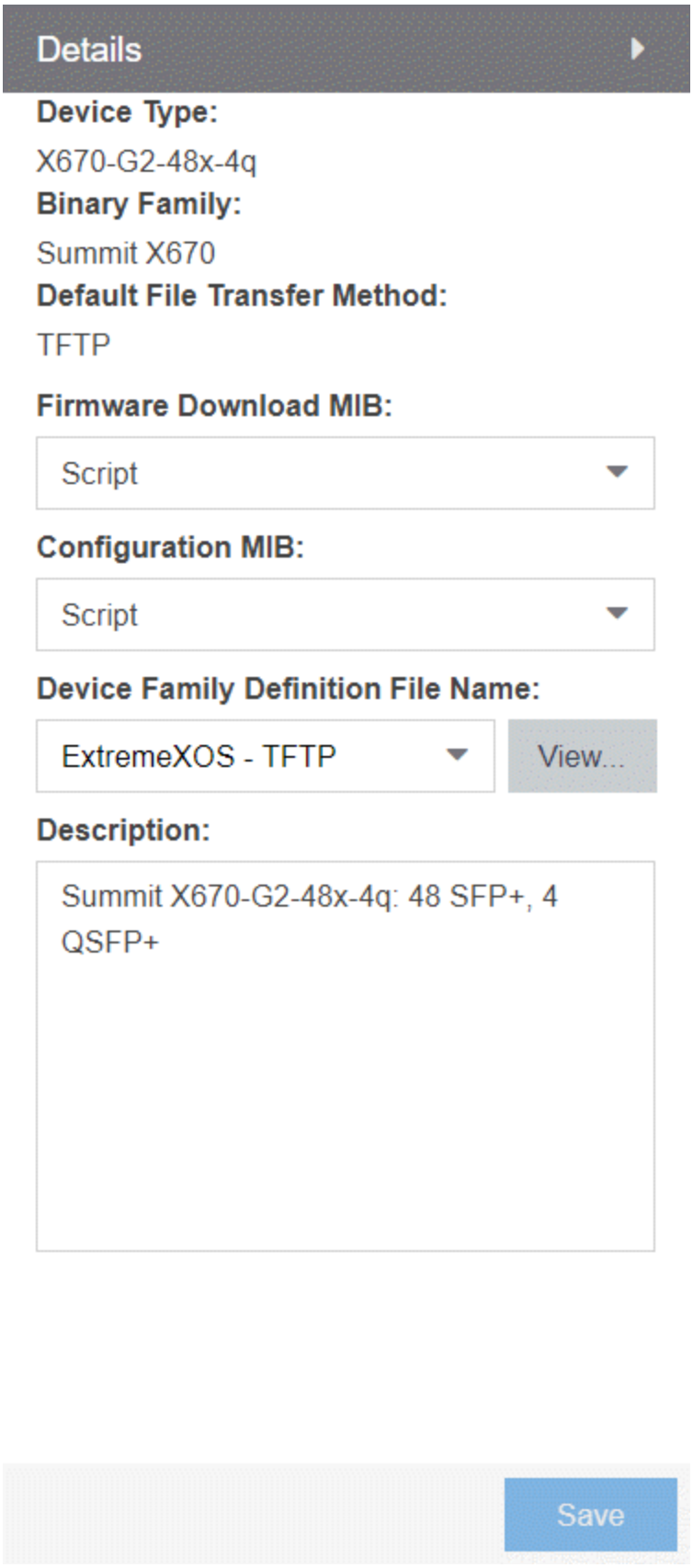
NOTE: Firmware images that were discovered with a NetSight version prior to 4.4 need to be removed from ExtremeCloud IQ Site Engine (right-click the image on the **Firmware** tab and select **Delete Image**) and then rediscovered in order to populate the compatibility key field.

Details Section

The Details right-panel displays additional information about a device type or a firmware or boot PROM image, depending on what you select in the left-panel or in the Device Type Images section of the window.

Device Type Details

Selecting a device type in the Firmware Tree left-panel opens the details for that device in the Details right-panel.


Details
Device Type:
X670-G2-48x-4q
Binary Family:
Summit X670
Default File Transfer Method:
TFTP
Firmware Download MIB:
Script
Configuration MIB:
Script
Device Family Definition File Name:
ExtremeXOS - TFTP
View...
Description:
Summit X670-G2-48x-4q: 48 SFP+, 4 QSFP+
Save

Device Type
The device's model number or hardware type.

Binary Family
The binary family to which the device type belongs. Device types in the same binary family share the same firmware image.

Default File Transfer Method
The default file transfer method for this device type. To set the default file transfer method for a device type, right-click on a device type in the Firmware Tree left-panel and select **Default File Transfer Method**. You can also set the default file transfer method for groups of devices of the same series by right-clicking on the device type's parent folder and selecting **Default File Transfer Method**.

Firmware Download MIB
The Firmware Download MIB supported by this device type. If the device type supports more than one Firmware Download MIB, use the drop-down list to select the desired MIB. In addition to a list of MIBs, other menu options include:

- **Auto Discover** — ExtremeCloud IQ Site Engine reads the Firmware Download MIB on the first device of this device type that you add or import and displays it here. ExtremeCloud IQ Site Engine then uses that MIB to perform firmware and boot PROM downloads on all devices of this device type.
- **Disabled** — Firmware download functionality is not allowed for this device type.

Configuration MIB
The Configuration MIB supported by this device type. If the device type supports more than one Configuration MIB, use the drop-down list to select the desired MIB. In addition to a list of MIBs, other menu options include:

- **Auto Discover** — ExtremeCloud IQ Site Engine reads the Configuration MIB on the first device of this device type that you add or import and displays it here. ExtremeCloud IQ Site Engine then uses that MIB to perform archive operations on all devices of this device type.
- **Disabled** — Archive functionality is not allowed for this device type.
- **Script** — Allows the archive functionality to be executed through the use of a script. This option is used for third-party devices that do not support the required SNMP MIBs.

Device Family Definition File Name
Select the file containing the scripts you are using if **Script** is selected for **Firmware Download MIB** and/or **Configuration MIB**. Include all the scripts and data for each supported ExtremeCloud IQ Site Engine function for specific third-party devices in this file.

ExtremeCloud IQ Site Engine provides sample Definition Files for Extreme, Enterasys, Cisco Systems, and Hewlett Packard devices. Select the **View** button to open the Script Details window, from which you can view the script.

Description

Allows you to enter a description for the device.

Select **Save** to save any changes.

Firmware/boot PROM Image Details

Use this section to edit the version number of the image, the type of image (firmware or boot PROM), and enter a description for the image.

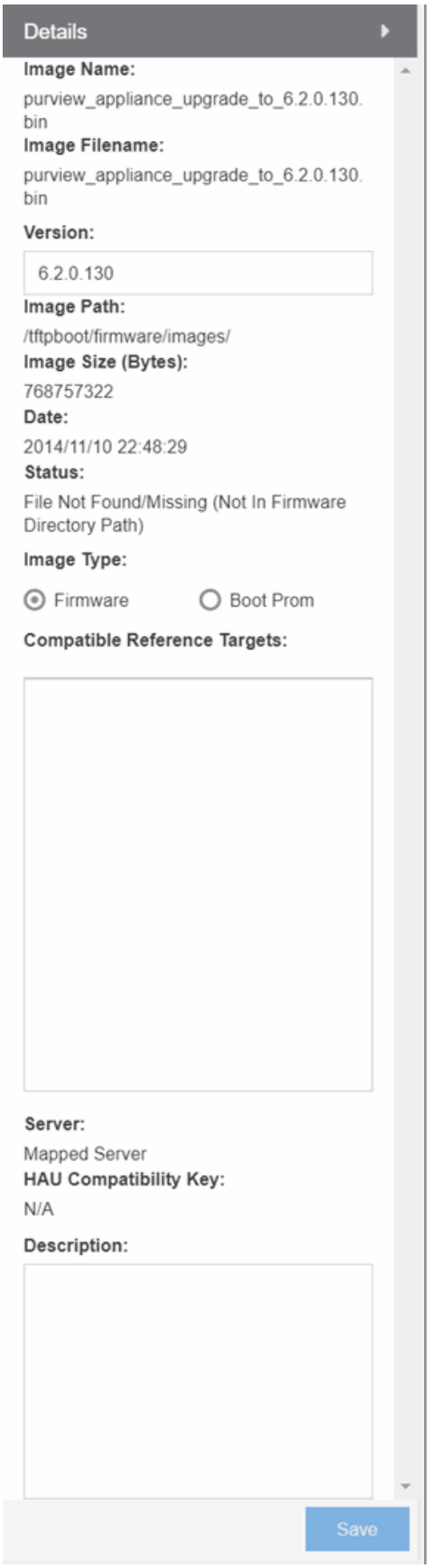

Details
Image Name:
purview_appliance_upgrade_to_6.2.0.130.bin
Image Filename:
purview_appliance_upgrade_to_6.2.0.130.bin
Version:
6.2.0.130
Image Path:
/tftpboot/firmware/images/
Image Size (Bytes):
768757322
Date:
2014/11/10 22:48:29
Status:
File Not Found/Missing (Not In Firmware Directory Path)
Image Type:
Firmware
Boot Prom
Compatible Reference Targets:
Server:
Mapped Server
HAU Compatibility Key:
N/A
Description:
Save

Image Name
The name of the image as it is displayed in the left-panel Firmware tree. The maximum length of the displayed name is 50 characters. Longer names will be truncated to the 50-character maximum with a (2), (3), and so on, appended if there are multiple images with the same name.

Image Filename
The full name of the image as it appears in your firmware images directory.

Version
The version number of the firmware or boot PROM image. If the version number is not available from the image file, and Inventory Manager has not performed a firmware or boot PROM upgrade using this image, this field displays N/A (not available). Enter a version number and select **Save** to manually set a version number for the image.

Image Path
The path to the location where the image is stored.

Image Size (Bytes)
The size in bytes of the image.

Date
The image file date and time as reported by the file system.

Status
The status of the image file: **File Found** or **File Not Found**. This shows whether the image file is still present in the firmware directory. If the image is a user-defined firmware record, this column displays **User-Defined File**.

Image Type
Indicates whether the image is a firmware or boot PROM image. Use the radio buttons to change the designation, if necessary.

Compatible Reference Targets
Displays device types for which the selected firmware is assigned and device types with the selected firmware specified as the Reference Image.

Server
Displays the firmware download server associated with the firmware image. A discovered firmware image accessible by the mapped file transfer server displays **Mapped Server**. A user-defined firmware record displays its associated alternate firmware download server.

Root Directory
Displays the root directory for the firmware download server if the server is an alternate firmware download server and the image is a user-defined firmware record. Otherwise, this field is not displayed.

HAU Compatibility Key
This field displays the HAU Compatibility Key if one is detected on the firmware image. HAU (Highly Available Upgrade) is a feature on certain devices that allows firmware to be upgraded

with minimal (if any) downtime. HAU is configured using the device CLI or by creating a FlexView in Console (ethsyHauSystemHauMode). When the device HAU status is set to "If Possible" or "Always" mode, ExtremeCloud IQ Site Engine attempts to perform an HAU upgrade if the HAU firmware compatibility key is the same for the currently running firmware and the newly selected firmware.

NOTE: Firmware images discovered with a version of ExtremeCloud IQ Site Engine prior to 4.4 need to be removed and rediscovered to populate the compatibility key field.

Description

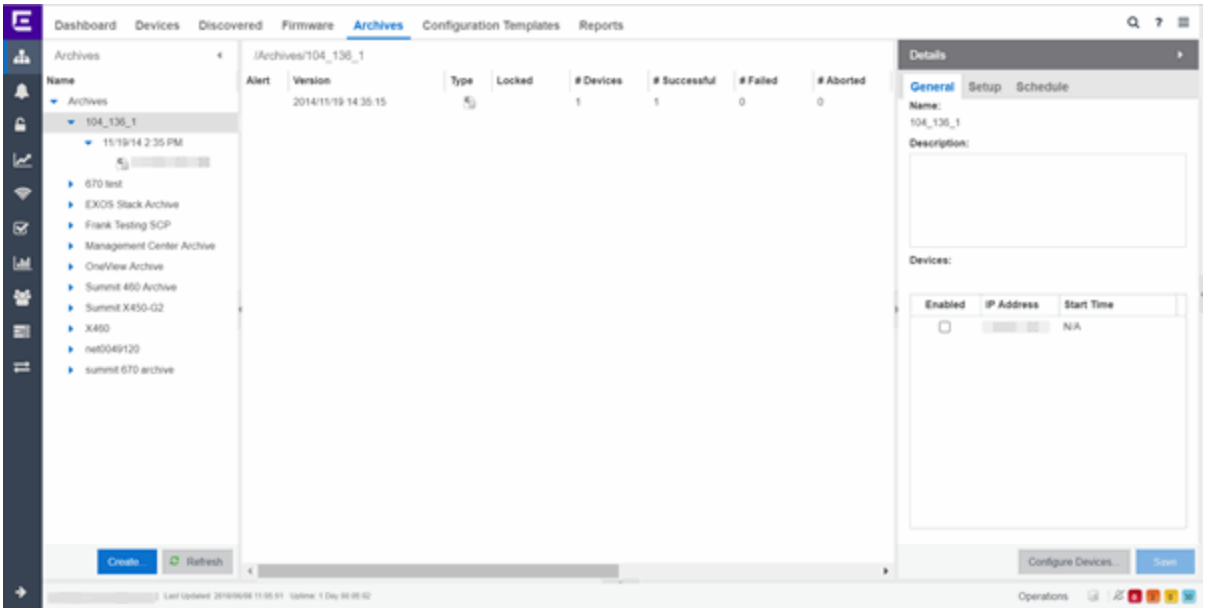
Use this field to add a brief description of the image and any information regarding its use. Select **Save** to save any changes.

Save

Saves any changes you have made to the version or description field.

Archives

The **Archives** tab allows you to create new archives (saved configurations) via the Create Archive window, edit an archive's attributes including devices, schedule, process, and setup, and view all of the archives for a particular device family, or see specific details about an individual archive. Additionally, with an ExtremeCompliance license, you can test your device archives for compliance with industry standards and regulations.



The **Archives** tab contains three panels:

- Archives Navigation Tree — The left-panel of the **Archives** tab contains a navigation tree which organizes your archives by device type:
    - **Archives Folder** — This folder contains all your archive operations.
    - **Archive Name Folder** — This is the name that you gave the archive operation when you created it. This folder contains a list of all the archive versions that have been performed.
    - **Archive Version Folder** — This is the date and time when the archive operation was performed. Each version contains a list of all the individual files that were saved during the archive operation.
    - **Configuration File Icon**  — This icon represents an archived device configuration file.

      Individual files are listed by the IP address of the device whose configuration is saved, followed by the SNMP context, if applicable. Right-click a file in this view and select Create Configuration Template to modify an existing configuration template and create a new configuration template.
    - **Capacity Planning File Icon**  — This icon represents an archived capacity planning file. Individual files are listed by the IP address of the device whose capacity planning data is saved, followed by the SNMP context, if applicable. Right-click a file in this view and select Create Configuration Template to modify an existing configuration template and create a new configuration template.
    - **Both Configuration and Capacity Planning File Icon**  — This icon represents an archived file that includes both device configuration and capacity planning data. Individual files are listed by the IP address of the device whose configuration and capacity planning data is saved, followed by the SNMP context, if applicable.

      Right-click a file in this view and select Create Configuration Template to modify an existing configuration template and create a new configuration template using the **Replace With** feature to insert Custom Variables.
- Archives Main View — The main view of the **Archives** tab displays a table with information related to what you select in the Archives Folder.

  There are four main views available on the **Archives** tab based on what you select in the navigation tree:
    - Archives Folder — Selecting the top-level Archives Folder displays information associated with the device families. This is high level information about each device group family.
    - Archive Name — Selecting a device family in the left-panel shows a table containing all of the archives related to that device family. The information includes the archive type, the number of devices and the ultimate status of the archive process.

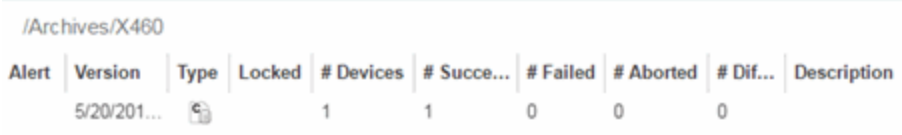
- Archive Version — Selecting the date of an archive in the left-panel provides information about the archive initiated on that date. It shows the firmware version as well as information about the saved file.
- Archive File — Selecting an individual archive file in the left-panel displays two tabs containing specific information about the archive record. The **General** tab contains information identical to that contained in the Archive Date panel. Right-click a file in this view and select Create Configuration Template to modify an existing configuration template and create a new configuration template. The **Custom Variables** tab shows all of the information saved in the archive.

- Details Right-Panel — The Details right-panel contains information related to what you select in the Archives main view. The right-panel displayed depends on what is selected in the main view:
  - Archive Name Right-Panel
  - Archive Version Right-Panel
  - Archive File Right-Panel

The Create Archive button at the bottom of the left-panel opens the Create Archive window, which allows you to create new archives for your devices.

Archive Name

The Archive Name Panel appears when you select an archive name folder in the left-panel of the Archives tab. The main panel displays the archive's versions, the dates and times the selected archive occurred. Right-click an item or items for a menu of options.



Alert

A yellow alert icon in this column signifies one or more of the following:

- ≠ — there is a difference between the saved configuration(s) in this version and previous configurations saved for the device(s).
- ⚠ — a configuration save failed for one or more of the devices in this archive version.

Version

Lists the all the dates and times (archive versions) the archive occurred.

Type
The icon in this column signifies the type of data the archive is configured to save:

- — Device Configuration Data
- — Capacity Planning Data
- — Both Device Configuration and Capacity Planning Data

Locked
A ✓ indicates that the archive version is locked. A locked archive version is not deleted when the maximum number of saved versions for this (as specified in the Create Archive window). To lock and unlock an archive version, right-click the archive version in the left-panel **Archives** tab, and select **Lock/Unlock**.

 # Devices
The number of devices for which this archive version is responsible.

 # Successful
The number of successful configuration saves for the archive version.

 # Failed
The number of configuration saves that failed for the archive version.

 # Aborted
The number of configuration saves aborted for the archive version.

 # Different
The number of saved configurations different from the previous configurations saved for the device(s).

Description
Displays any notes about the version entered into the **Description** field in the Archive Version right-panel, which opens in the right-panel when you select an archive version from the Archive Main panel (the current view) or when you select an archive version folder from the left-panel.

Right-Panel

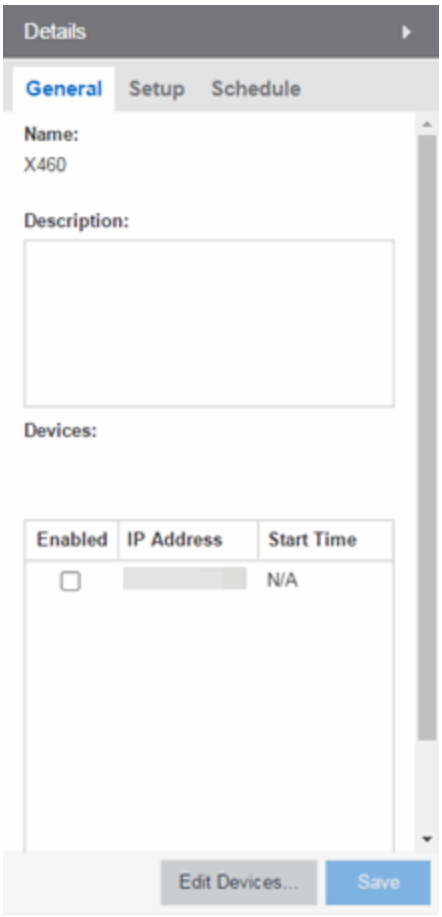
The right-panel varies depending on whether an archive version is selected in the Archive Name main panel table.

- Archive version not selected — Archive Name right-panel is displayed.
- Archive version is selected — Archive Version right-panel is displayed.

Archive Name (Right-Panel)

The Archive Name right-panel appears when you select an archive name folder in the left-panel of the **Archives** tab. It contains three tabs that allow you to edit an archive's attributes including devices, schedule, process, and setup.

General



Name

The name of the archive operation. You cannot change the archive name here. To rename an archive, right-click the archive in the left-panel of the **Archives** tab, and then select **Rename**.

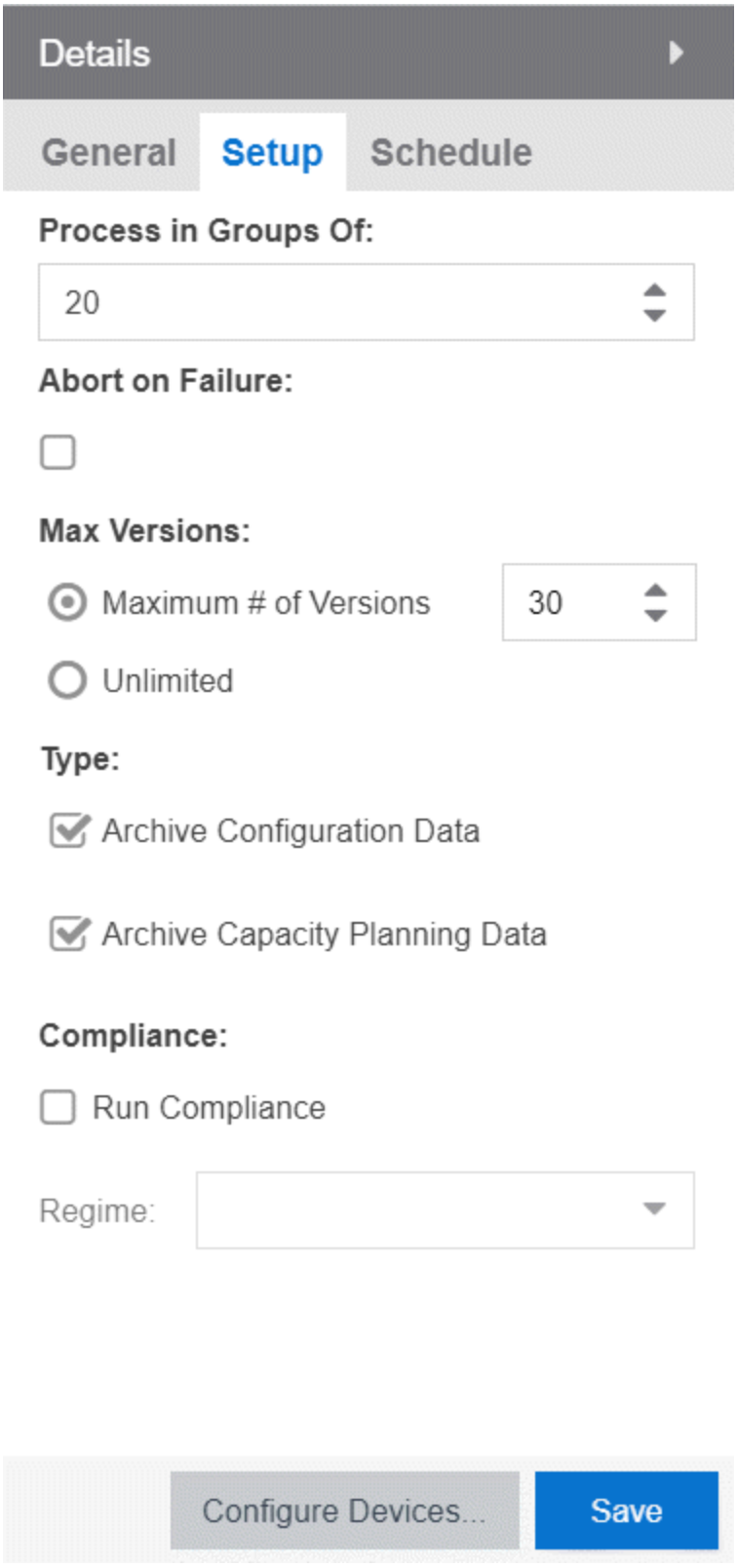
Description

A brief description to help you identify the archive operation.

Devices

Lists the devices selected for the operation. Using the **Enabled** checkboxes, select or deselect the devices you want to archive. To edit this device list, select **Edit Devices**.

Setup


Details
General
Setup
Schedule
Process in Groups Of:
20
Abort on Failure:
Max Versions:
Maximum # of Versions
30
Unlimited
Type:
Archive Configuration Data
Archive Capacity Planning Data
Compliance:
Run Compliance
Regime:
Configure Devices...
Save

Process in Groups Of

The archive is performed simultaneously on the number of devices specified in the **Process in Groups Of** field. Enter the value **1** to perform the operation serially, one device after another.

Abort on Failure

Select this checkbox to stop the archive operation after a failure. This is useful if you are performing an archive operation on multiple devices and you want the operation to stop after a failure on a single device.

Max Versions

Specify the maximum number of versions to save for this archive. This allows you to limit the number of versions saved for each archive. When the maximum number is reached, older versions are automatically deleted. If you specify a number that is less than the current number of saved versions, older versions over the maximum number are automatically deleted the next time the archive is performed. Select **Unlimited** if versions are always retained.

Type

Select the appropriate checkbox for the type of data you wish to archive:

- **Archive Configuration Data** — Create archives (backup copies) of your devices' configurations you can restore to the devices at a later date.
- **Archive Capacity Planning Data** — Create archives of port and FRU information.

Compliance

Select the **Run Compliance** checkbox to perform an ExtremeCompliance audit on the archive using the regime you select in the **Regime** drop-down list.

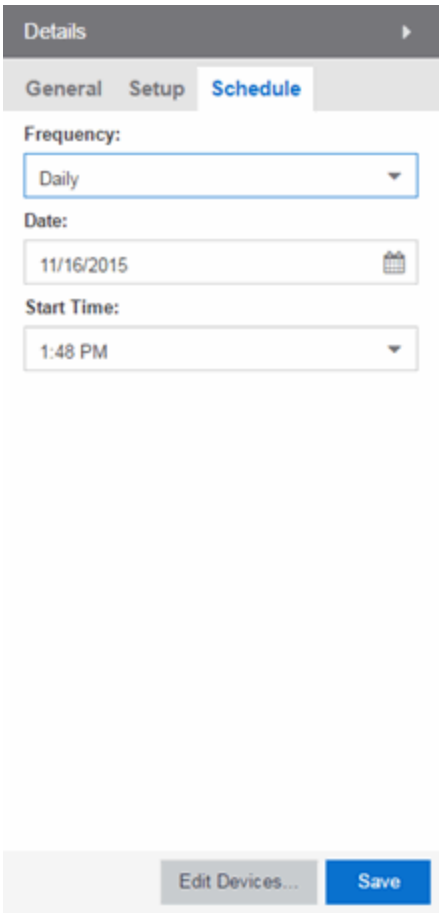
Save

Saves any changes made to the archive attributes. Selecting a Frequency of **Now** performs the archive immediately.

Edit Devices

Opens the Create Archive window where you can select a single group or a list of devices to include in this archive. This allows you to change the devices the archive is performed on.

Schedule



Frequency

Use the drop-down list to select the frequency with which you want the archive performed: **Never**, **Now**, **Once**, **Daily**, **Weekly**, or **On Start Up**. The Never option lets you create an archive operation without actually performing it. The Now option lets you perform an immediate archive.

Date

Use the drop-down list to select the month you want the archive to start. A calendar corresponding to the selected month is displayed. Select the desired starting day by selecting the calendar. You can use the arrows on either side of the drop-down list to change the month, and change the year by entering a new year in the text field.

Start Time

Set the starting time for the operation and select AM or PM. (This field is grayed out if you select the **Never** or **Now** frequency.)

Archive Version

The Archive Version panel appears when you select an archive version folder in the left-panel of the **Archives** tab. The archive version is the date and time that an archive operation occurs. The panel displays a table showing the individual configurations saved for this archive version, listed by device IP address. Right-click an item or items in the table for a menu of options.



Alert

A yellow alert icon in this column signifies one or more of the following:

- ≠ — Difference between this saved configuration and the previous configuration saved for the same device.
- ⚠ — Configuration save failed.

To acknowledge an alert and place a check mark on the alert icon, right-click the icon and select Acknowledge Alert from the menu.

IP Address

Lists the individual devices (by device IP address) whose configuration files are saved by this version of the archive operation.

Firmware Version

Shows the firmware version for this device at the time of the save operation.

File Status

The status of the config file: File Found or File Not Found/Missing. File Not Found/Missing indicates that ExtremeCloud IQ Site Engine can no longer find the config file (it is deleted or moved) or the archive operation did not include saving device configuration data. Check the Description field for more information.

File Time Stamp

The date and time of the configuration creation.

File Size

The size of the saved configuration in bytes.

Description

When a configuration file is saved, it is automatically compared to the previously saved configuration file for the same device. This field displays a message regarding that comparison. It also displays information pertaining to any alert icon displayed in the Alert column. If the archive did not include a device configuration save, this field displays "Device archived without configuration file." Rest your cursor on the field to display a tooltip of the complete description.

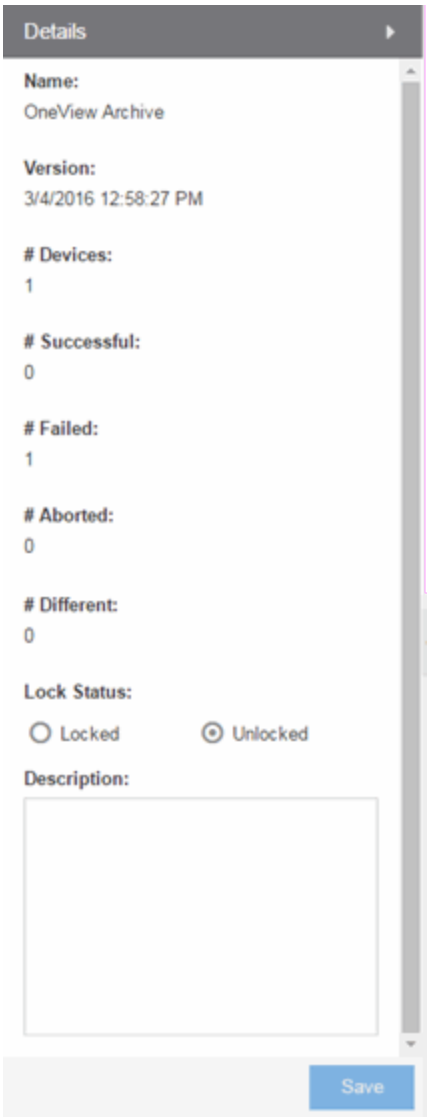
Right-Panel

The right-panel varies depending on whether an archive configuration is selected in the Archive Version main panel table.

- Archive configuration not selected — Archive Version right-panel is displayed.
- Archive configuration is selected — Archive Configuration right-panel is displayed.

Archive Version (Right-Panel)

The Archive Version right-panel appears when you select an archive version in the left panel of the **Archives** tab or in the table in the Archive Name panel. The archive version is the date and time that an archive operation was performed. This panel displays information about the version, including the number of successful and failed saves for that version.



Name

The name of the archive operation.

Version

The date and time of the archive version creation.

 # Devices

The number of devices included in this archive version.

 # Successful

The number of successful saves for the archive version.

 # Failed

The number of failed saves for the archive version.

 # Aborted
The number of aborted saves for the archive version.

 # Different
The number of saved configurations different from the previous configurations saved for the device(s).

Lock Status
Whether the version is locked or not locked. A locked archive version is not deleted when the maximum number of saved versions for this archive (as specified in the Create Archive window) is reached. To lock and unlock an archive version, right-click the archive version in the left-panel of the **Archives** tab or in the table on the Archive Name panel and select **Lock/Unlock**.

Description
Use this field to add additional notes about the version and save them using the **Save** button.

Save Button
Saves any changes you made to the panel.

Archive File

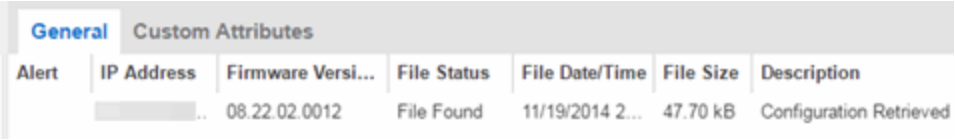
The Archive File panel appears when you select an archive configuration file in the left-panel of the **Archives** tab. It contains information about specific archive configurations.

Information is contained in two tabs:

- General
- Custom Attributes

General Tab

The **General** tab shows basic information about the configuration file created by the archive process.



Alert
A yellow alert icon in this column signifies one or more of the following:

- ≠ — Difference between this saved configuration and the previous configuration saved for the same device.
- ⚠ — Configuration save failed.

To acknowledge an alert and place a check mark on the alert icon, right-click the icon and

select Acknowledge Alert from the menu.

IP Address
Lists the individual devices (by device IP address) whose configuration files were saved by this version of the archive operation.

Firmware Version
Shows the firmware version for this device at the time of the save operation.

File Status
The status of the config file: File Found or File Not Found/Missing. File Not Found/Missing indicates that ExtremeCloud IQ Site Engine can no longer find the config file (it is deleted or moved) or the archive operation did not include saving device configuration data.

File Time Stamp
The date and time of the configuration creation.

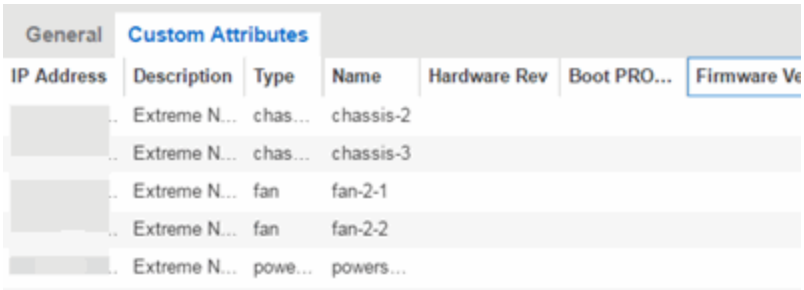
File Size
The size of the saved configuration in bytes.

Description
When a configuration file is saved, it is automatically compared to the previously saved configuration file for the same device. This field displays a message regarding that comparison. It also displays information pertaining to any alert icon displayed in the Alert column. If the archive did not include a device configuration save, this field displays "Device archived without configuration file." Rest your cursor on the field to display a tooltip of the complete description.

Custom Attributes Tab

The **Custom Attributes** tab displays a table of attribute information about the selected device(s). The information you see depends on the device type(s) selected; some devices support one attribute but not another. If a device returns multiple values for an attribute, each value is on a separate row. If a device does not support any of the attributes, the **Custom Attributes** tab for that single device is blank.

Custom Attribute tabs for device groups only display devices that support one or more of the attributes. Devices configured with an SNMP context display separate entries for each context.



Description
A description of the module or component.

Type
A description of the module or component type.

Name
The name of the module or component.

Hardware Version
The current hardware version of the device.

BootPROM Version
The current version of Boot PROM installed in the module.

Firmware Version
The current firmware version installed in the module.

Serial Number
A unique number assigned to the module or component by the manufacturer.

Manufacturer
The manufacturer of the module or component.

Model Name
The model number of the module or component type.

Asset Tag
A unique asset number assigned to the module or component for inventory tracking purposes.

Field Replaceable
Whether or not the manufacturer considers the component to be field replaceable (true or false).

Legacy Devices

SSR Hardware Attributes

Slot Number
The slot number in the chassis where the module resides.

Status
The current status of the module: online or offline.

Type
The physical module type.

Description
A description of the module.

Number of Ports
The number of physical ports on the module.

Version
The module version.

Memory
The system memory size available on the module, reported in megabytes (MB).

E5 and E6/E7 Power Supply and Fan Attributes

Power Supply Number
The number of the power supply.

Power Supply Type
The power supply type: ac-dc, dc-dc, or highOutput.

Fan State
The state of the fan: Installed and Operating, Installed and Not Operating, or Not Installed.

Power Supply State
The state of the power supply: Installed and Operating, Installed and Not Operating, or Not Installed.

Power Supply Redundancy
Whether the power supply is redundant or not.

RoamAbout Radiocard and Base MAC Address Attributes

Card Type
The type of PC card inserted in the Access Point.

Versions
The hardware and firmware versions for the PC card.

Station Name
The wireless station name sent out as part of the beacon messages. Valid only when a DS card is inserted in the Access Point.

Base MAC Address
The physical layer address assigned to the interface through which ExtremeCloud IQ Site Engine is communicating.

Vertical Horizon Attributes

Number in Stack
The total number of switches present on this system.

Number of Ports
The total number of ports present on this system.

Firmware Version
The current firmware version installed in the device.

BootPROM Version
The current version of Boot PROM installed in the device.

CPU
The name of the device's processor (Central Processing Unit).

Power Status
Indicates whether the device is using internal power, redundant power, or both.

Expansion Slot 1
The type of expansion module in slot 1.

Expansion Slot 2
The type of expansion module in slot 2.

Role in System
Indicates whether the device is controller, backup master, or agent in the system.

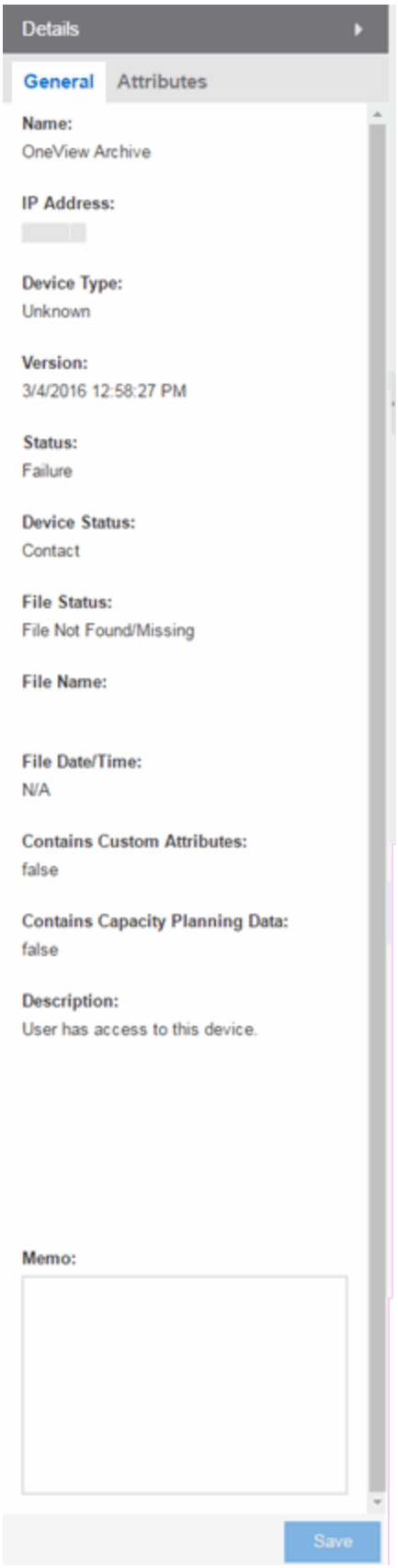
ELS Serial Number Attribute

Serial Number
A unique number assigned to the device by the manufacturer.

Archive File (Right-Panel)

The Archive File right-panel appears when you select an archive configuration in the left panel of the **Archives** tab or in the table in the Archive Version panel. Each configuration you select contains an icon that identifies the type of data that it contains: device configuration data device configuration data ( ) (an individual .cfg config file), capacity planning data ( ), or both device configuration and capacity planning data ( ). The Archive Configuration right-panel contains two tabs that display information about the saved data.

General


Details
General
Attributes
Name:
OneView Archive
IP Address:
Device Type:
Unknown
Version:
3/4/2016 12:58:27 PM
Status:
Failure
Device Status:
Contact
File Status:
File Not Found/Missing
File Name:
File Date/Time:
N/A
Contains Custom Attributes:
false
Contains Capacity Planning Data:
false
Description:
User has access to this device.
Memo:
Save

Name
The name of the archive operation.

IP Address
The IP address of the device whose data is saved, followed by the SNMP context, if applicable.

Device Type
The device's model number or hardware type.

Version
The date and time the archive operation occurred.

Status
The status of the operation: Success or Failure.

Device Status
The status of the device when the archive operation occurred: Contact or No Contact.

File Status
The status of the config file: File Found or File Not Found/Missing. File Not Found/Missing indicates that ExtremeCloud IQ Site Engine can no longer find the config file (it is deleted or moved) or the archive operation did not include saving device configuration data. Check the Description field for more information.

File Name
The path and filename for the saved configuration. For archive operations configured to archive only capacity planning data (and not configuration data), this column is blank.

File Time Stamp
The date and time of the creation of the configuration file. For archive operations configured to archive only capacity planning data (and not configuration data), this column is blank.

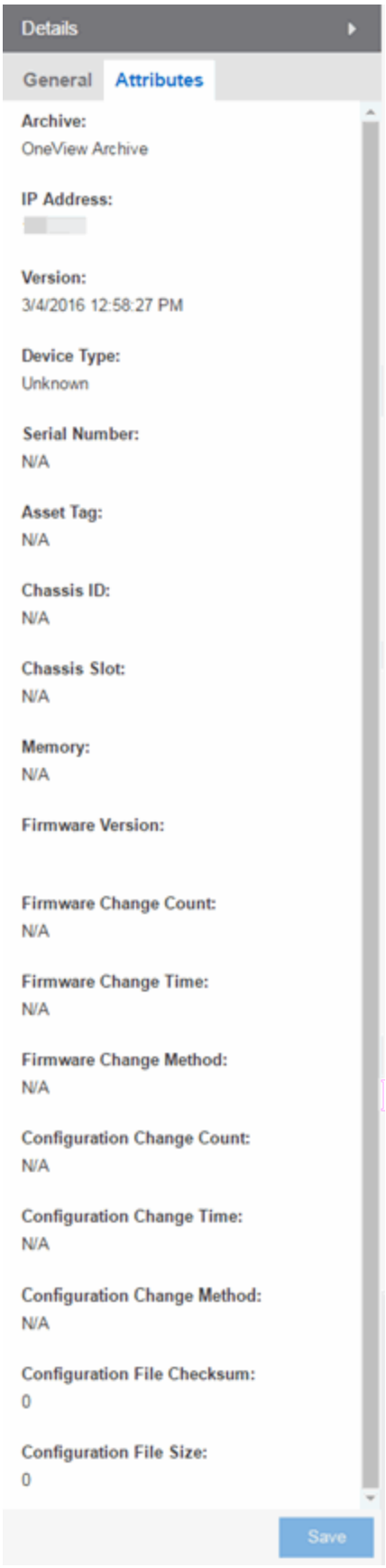
Contains Custom Attributes
Indicates whether the archive contains the device's custom attributes. If the device type does not support custom attributes or if the archive did not complete successfully, this field displays **No**.

Contains Capacity Planning Data
Indicates whether the device's port and FRU information are saved in the archive.

Description
When a configuration file is saved, it is automatically compared to the previously saved configuration file for the same device. This field displays a message regarding that comparison. For archive operations configured to archive only capacity planning data (and not configuration data), this column displays a Warning message stating that the ability to archive configuration data is disabled for this archive.

Memo
Use this field to add additional notes about the configuration and save them using the **Save** button.

Attributes


Details
General
Attributes
Archive:
OneView Archive
IP Address:
Version:
3/4/2016 12:58:27 PM
Device Type:
Unknown
Serial Number:
N/A
Asset Tag:
N/A
Chassis ID:
N/A
Chassis Slot:
N/A
Memory:
N/A
Firmware Version:
Firmware Change Count:
N/A
Firmware Change Time:
N/A
Firmware Change Method:
N/A
Configuration Change Count:
N/A
Configuration Change Time:
N/A
Configuration Change Method:
N/A
Configuration File Checksum:
0
Configuration File Size:
0
Save

Archive
The name of the archive operation.

IP Address
The IP address of the device whose data is saved, followed by the SNMP context, if applicable.

Version
The date and time that the archive operation occurred.

Device Type
The device's model number or hardware type.

Serial Number
A unique number assigned to the device by the manufacturer.

Asset Tag
A unique asset number assigned to the device for inventory tracking purposes.

Chassis ID
The ID assigned to the chassis where the device resides (if applicable). This is usually a serial number or MAC address, depending on the chassis type.

Chassis Slot
The slot number in the chassis where the device resides. N-Series devices and devices that do not reside in a chassis, display a value of N/A.

Memory
The device's total installed local memory, DRAM (Dynamic Random Access Memory), reported in megabytes (MB).

Firmware Version
The firmware version installed in the device at the time of the configuration save.

Firmware Change Count
The number of successful firmware image downloads. Devices that do not support the *enterasys-configuration-change-MIB* display N/A (Not Available).

Firmware Change Time
The date and time of the last successful firmware image download. Devices that do not support the *enterasys-configuration-change-MIB* display N/A (Not Available).

Firmware Change Method
The method used to cause the last firmware change (e.g. SNMP, Telnet, Local Management (LM), Command Line Interface (CLI)). If the individual user login or the source IP address is available, they are included. Devices that do not support the *enterasys-configuration-change-MIB* display N/A (Not Available).

Configuration Change Count
The number of successful configuration changes. Devices that do not support the *enterasys-configuration-change-MIB* display N/A (Not Available).

Configuration Change Time

The date and time of the last successful configuration change. Devices that do not support the *enterasys-configuration-change-MIB* display N/A (Not Available).

Configuration Change Method

The method used to make the last configuration change (e.g. SNMP, Telnet, Local Management (LM), Command Line Interface (CLI)). If the individual user login or the source IP address is available, they are included. Devices that do not support the *enterasys-configuration-change-MIB* display N/A (Not Available).

Configuration File Checksum

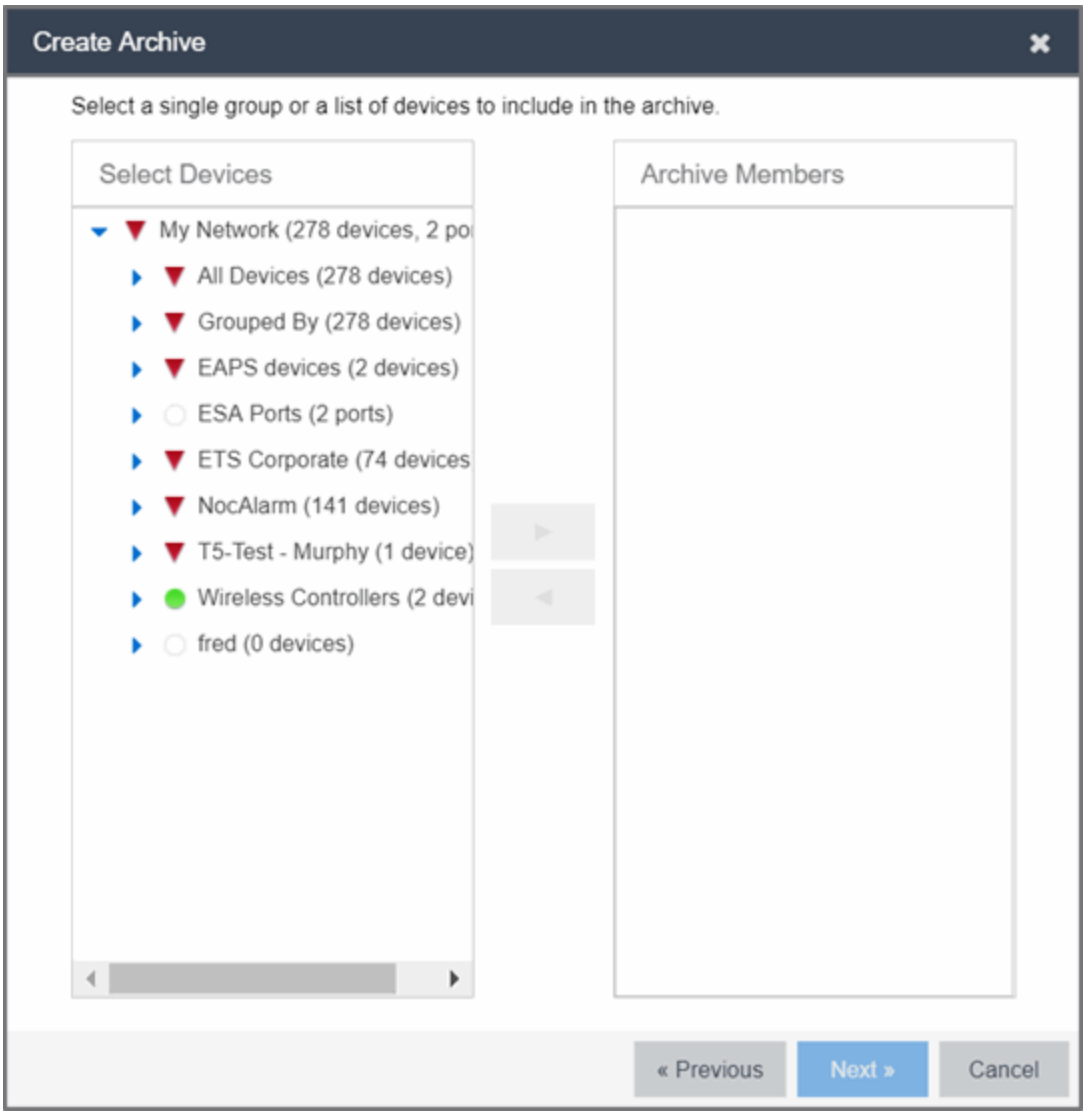
The checksum is a value calculated on the entire file. You can compare this value to values obtained from different archive versions. Any difference in checksum values would indicate a change in the configuration.

Configuration File Size

The size of the saved configuration file in bytes. You can compare this size to the size reported in different archive versions. Any difference in size would indicate a change in the configuration file.

Create Archive

This window lets you edit the device(s) on which to perform the archive. The current archive members are listed when you open the window. Access the window from the **Edit Devices** button in the Archive Name right-panel.



Select Devices

Expand the folders and select a single device, multiple devices, or a single device group. Select the right arrow button **›** to move the devices to the Archive Members list.

Archive Members

Lists the device(s) or device group the on which the archive is performed. To remove a member from the list, select the member and select the left arrow button **‹**.

Right Arrow Button

Select **›** to add the selected device(s) or device group to the Archive Members list.

Remove Button

Select **‹** to remove the selected device(s) or device group from the Archive Members list.

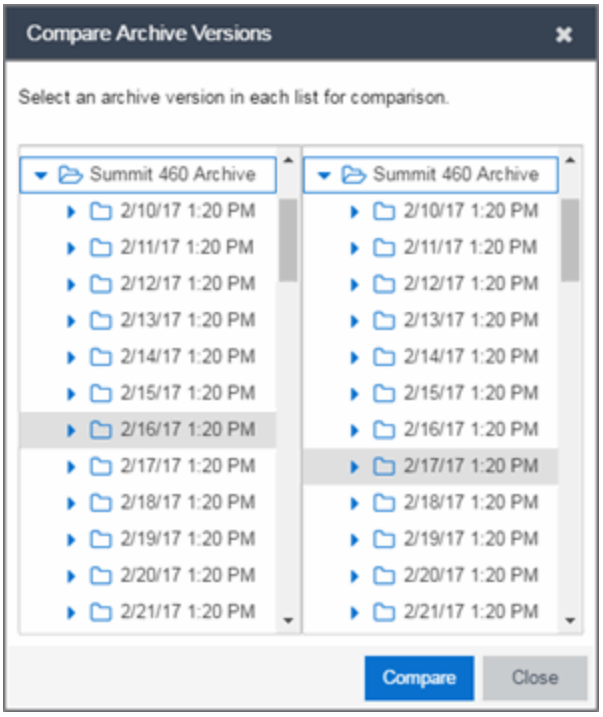
OK

Changes the archive members according to your selections.

Select Archive Versions

This window lets you select two archive versions or configurations to compare in the Compare Archive Versions window. It displays two Archive trees (identical to the Archive tree in the **Archives** tab). Use these trees to select the two archive versions or configuration files you wish to compare. You can compare two individual configurations for the same device, or you can compare two different archive versions (select versions that share common devices).

For information on how to access the window, see How to Compare Archives.



Selection 1

Expand the folders as necessary to select the first version or configuration you wish to compare.

Selection 2
Expand the folders as necessary to select the second version or configuration you wish to compare.

Compare
Performs the comparison and opens the Compare Archive Versions window, where you can view the comparison results.

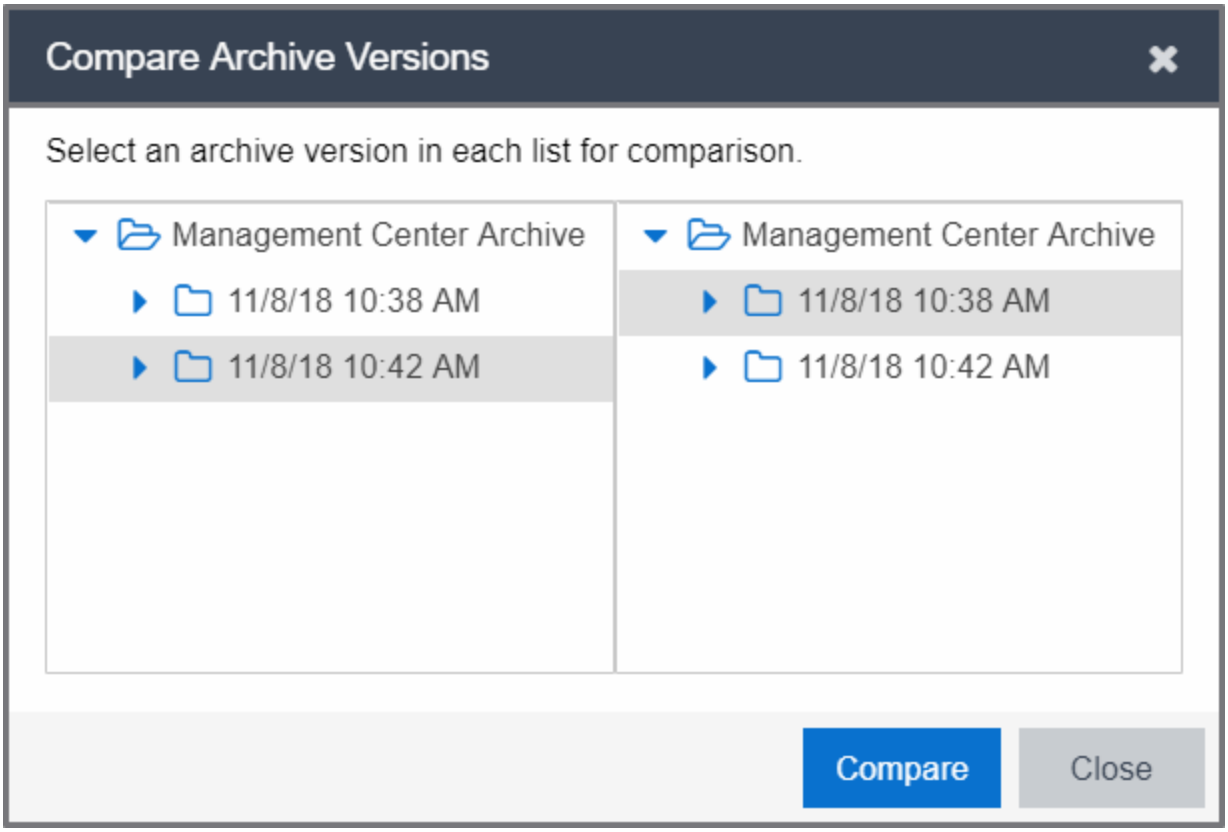
Close
Closes the window.

Compare Archive Versions

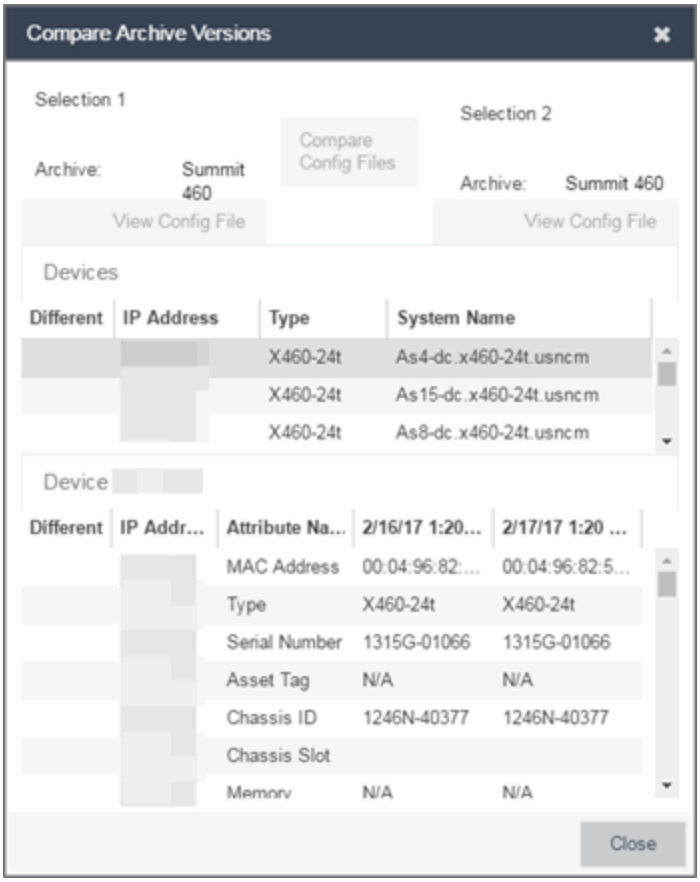
The **Compare Archive Versions** window lets you compare two different archives for the same device and monitor any changes in device attributes. ExtremeCloud IQ Site Engine compares archives using a set group of saved attributes from when the archive occurred.

For information on how to perform a compare archive operation, see How to Compare Archives.

When you first open the **Compare Archive Versions** window, select the two archive versions you are comparing and select **Compare**.



The second window appears. The values for these attributes are displayed in a table with any differences between the values flagged by a yellow **Difference** icon (≠) in the **Different** column.



Selection 1 / Selection 2

Displays the two archive versions you select to compare and gives the total number of devices in common between the two compared versions.

Compare Progress

The bar shows the progress of large compare operations. The **Abort Compare** button allows you to stop a compare operation; any comparisons completed are available for viewing.

In addition, the following buttons are available only for archives that include device configuration data:

- **Compare Config Files** — Opens the Configuration File Compare window and displays the two archived configuration files for the selected device. This option is only available when there are differences between the two configuration files being compared.
- **View Config File** — Opens the Configuration File Viewer and displays the archived configuration file of the selected device. This option is only available when there are no differences between the two config files being compared.

Devices Table

This table lists the devices included in the comparison. If differences were found, the yellow **Difference** icon ( ) displays in the **Different** column. Select the device whose comparison results you wish to see. The results display in the Comparison Results table.

Comparison Results Table

This section displays the results of the comparison for the device selected in the Devices table, with any differences between the two versions flagged by a yellow **Difference** icon ( ) in the **Different** column. For a definition of each attribute, see Archive File right-panel.

Different
A yellow **Difference** icon ( ) in this column signifies a difference between the two attributes.

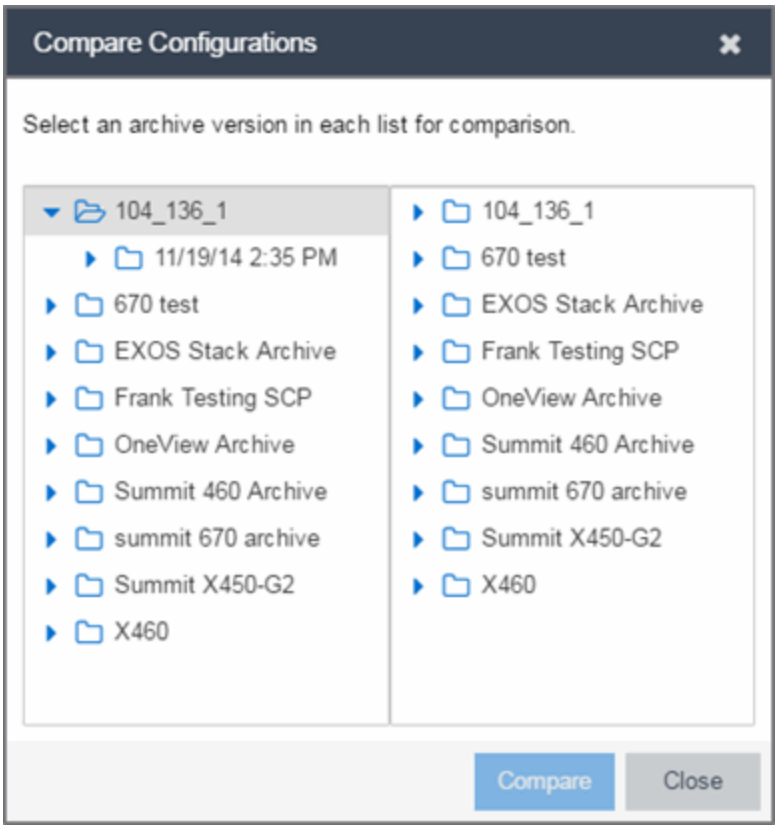
IP Address
Lists the IP address of the device whose attributes are being compared.

Attribute Name
Lists the name of the attribute being compared. For a definition of each attribute, see Archive File right-panel.

Attribute Values
These two columns list the attribute values for the versions being compared.

Compare Configurations

This window lets you select two configuration files to compare in the Configuration File Compare Window. To access the window, right-click a configuration that includes device configuration data (or) in the **Archives** tab tree or main panel, and select **Compare Configuration Files**.



Selection 1

Expand the folders as necessary to select the configuration file you wish to compare. This file displays in the left panel of the Configuration File Compare window.

Selection 2

Expand the folders as necessary to select the second configuration file you wish to compare. This file displays in the right panel of the Configuration File Compare window.

Compare Button

Performs the configuration comparison and opens the Configuration File Compare window, where you can view the comparison results.

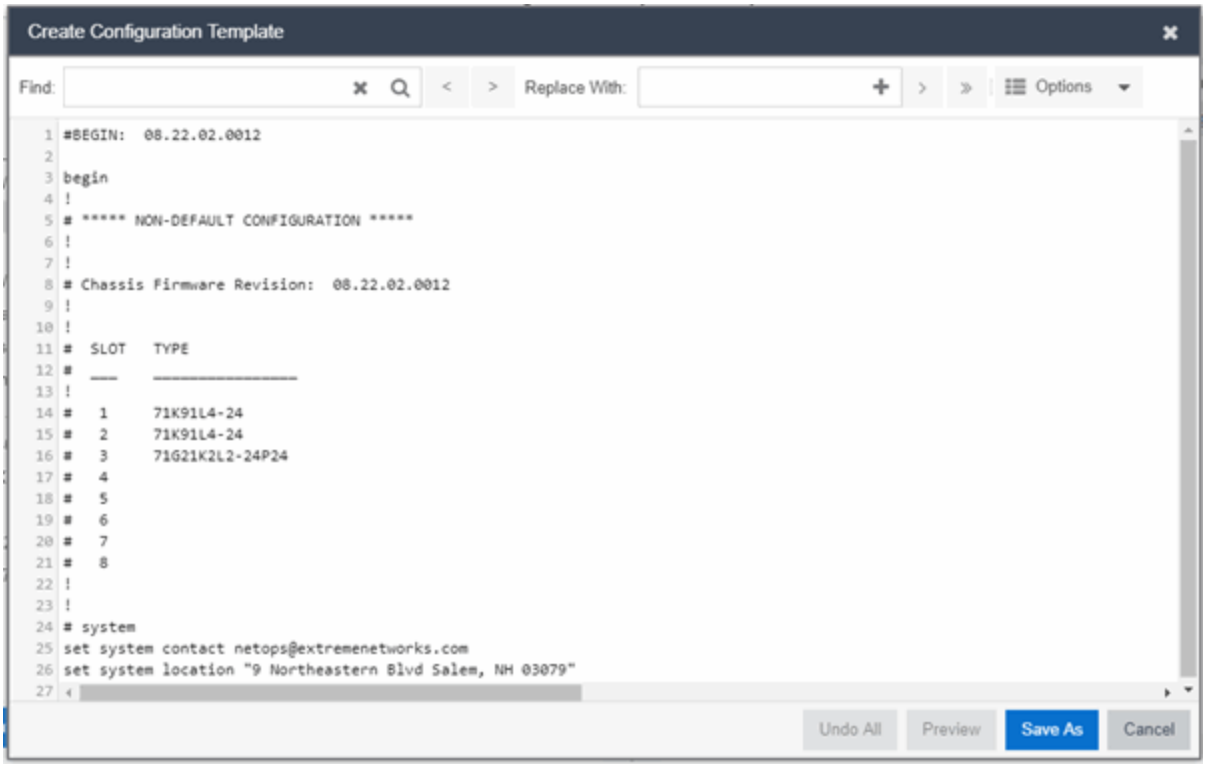
Creating a Configuration Template

Configuration templates contain configuration data for archived devices on a site. The **Create Configuration Template** window lets you view an archived device configuration file and modify it with custom variables to create a new configuration template. The **Network > Configuration Templates** tab displays details about the configuration templates you create.

To create a configuration template:

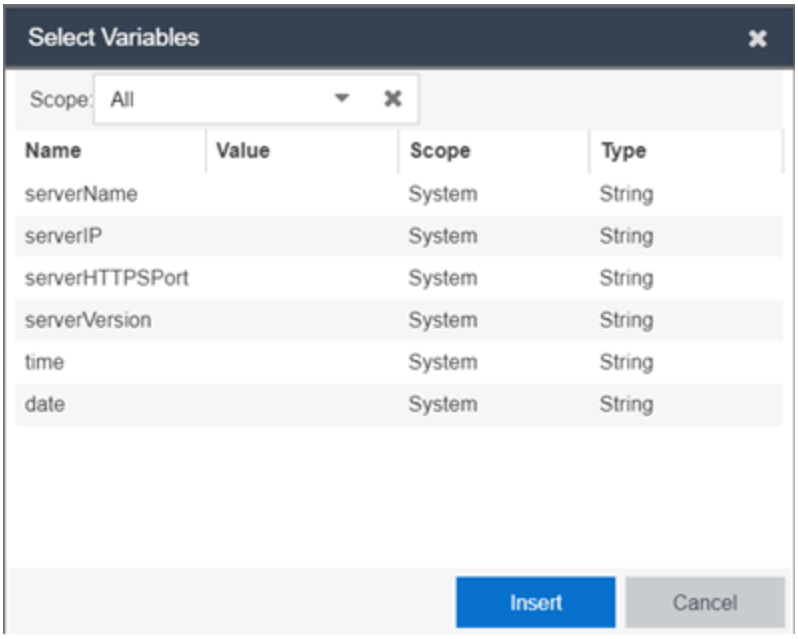
1. Access the **Archives** tab.
2. Right-click an archive file in either the left-panel Archives tree or the **General** tab table and select **Create Configuration Template**.

   The Create Configuration Template window opens.

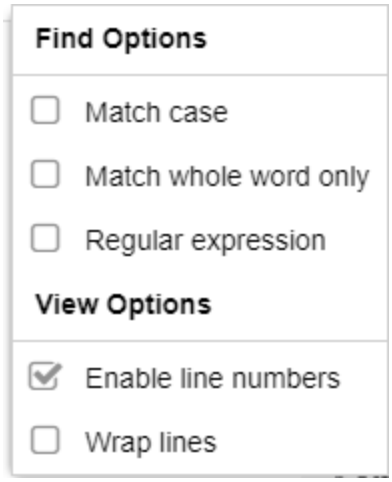


   Archived device configuration file data displays in ASCII format or html format, depending on the device family to which the archived device is assigned.

3. Enter the value you are replacing in the **Find** field. Select the magnifying glass icon (🔍) to highlight all the instances of that value.
4. Enter the new value you are inserting in the **Replace With** field or select the plus icon (+) in the **Replace With** field to open the **Select Variable**s window. Hover over the plus icon (+) to display a tooltip that instructs you to use the % character, then hold the CTRL key and type SPACE to view the variables inline.



5. Select the **Options** button to modify your results. Select from the following drop-down list items:



6. Select the variable you want to include in the configuration file and select the **Insert** button. The variable displays in the **Replace With** field.
7. Select the **>** arrow to replace a single instance and the **>>** to replace all instances with the new variable. To create new variables, use the **Custom Variables** tab.

Undo All

Select the **Undo All** button to undo your unsaved changes.

Preview

Select the **Preview** button to open the **Configuration Template Preview** window to compare the original configuration file with the new configuration template. Changes or deletions to the original file display as red strikethrough text in the left-hand original panel. Additions display as blue strikethrough text in the right-hand latest panel. The window also allows you to do the following:

- Switch the original and latest panels using the **Swap Sides** button
- Identify any discrepancies or errors using the **Search** field
- Save your changes and close the window using the **OK** button

Save As

Select the **Save As** button to save your new configuration template.

Cancel

Select the **Cancel** button to cancel the new configuration template.

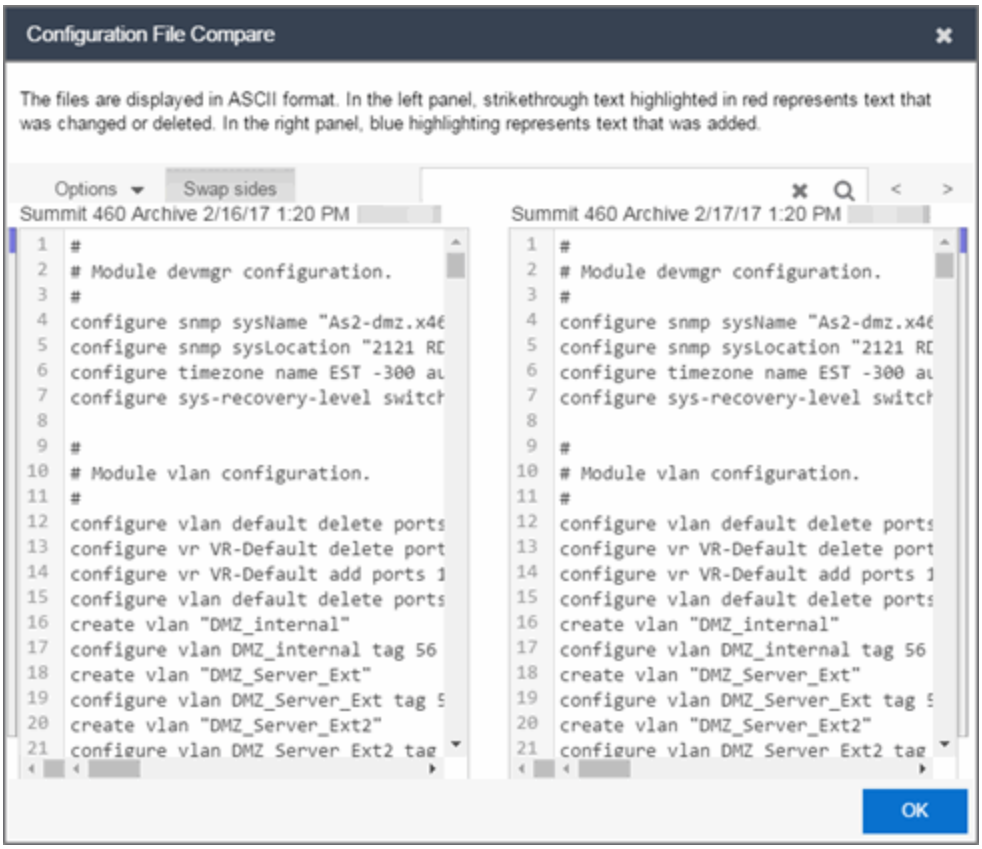
Configuration File Compare

The Configuration File Compare window lets you compare two archived configuration files.

There are several ways to access the window:

- Right-click an archive configuration that includes device configuration data (or) in the **Archives** tab left-panel navigation tree and select **Compare Archives**. The Select Configurations window opens, where you can select the two configurations you want to compare. Select **OK**.
- Right-click on a record in the main panel and select **Compare Configuration Files** from the menu. The Select Configurations window opens, where you can select the two configurations you want to compare. Select **OK**.
- In the Compare Archives window, select the **Compare Config Files** button.

The files are displayed in ASCII format. However, if one or both of the files are in binary, you can display them. Lines highlighted in green represent changed lines. Red highlighting represents added lines.



Search



Use the **Search** box at the top of the window to search for strings of characters in the configuration files.

Clear Search Button

Select this button to clear the search parameters from the **Search** box.

Find Previous Row/Find Next Row Buttons < >

Select these buttons to find the previous or next row that contains search parameters that match what you entered in the **Search** box.

Swap Sides Button Swap sides

Selecting this button switches the sides on which each archive configuration is located.

Options Options

The **Options** drop-down list allows you to configure how information displays in the archive configurations.

- **Enable line numbers** — Select this checkbox to display line numbers to the left of each line in the configuration file.

- **Wrap lines** — Select this checkbox to wrap text in the configuration files, so a horizontal scroll bar is not required to view information.
- **Enable side bars** — Select this checkbox to display a sidebar on the outside of each configuration file indicating your relative position in the file.

OK

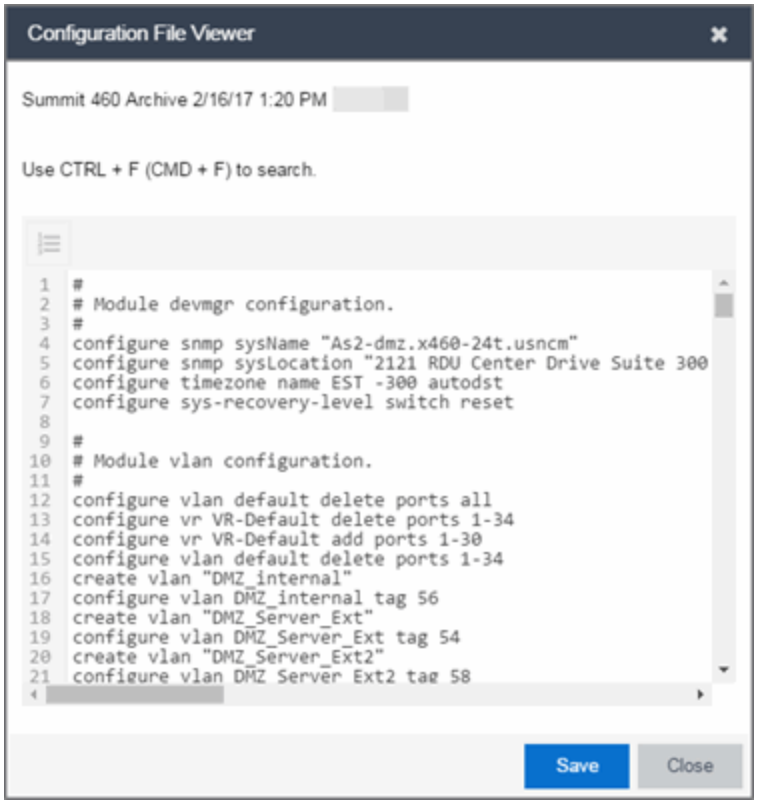
Select the **OK** button to close the Configuration File Compare window and return to the previous screen.

Configuration File Viewer

The Configuration File Viewer lets you view an archived device configuration file. To access the viewer, select a configuration that includes device configuration data (or) in the **Archives** tab left-panel navigation tree or in the main panel, and select **View Configuration File**. You can also open the window by selecting the **View Config File** button in the Compare Archive Versions window.

If the configuration file status is "File Not Found/Missing", then this menu option is not available. The file is displayed in ASCII format. However, if the file is in binary, you can still view it.

You can search the configuration file by pressing **CTRL** + **F** on your keyboard and entering the search parameters in the search box.



Save

Select **Save** to automatically save the configuration file to your default download folder in CFG format.

Close

Select **Close** to exit the Configuration File Viewer window and return to the previous screen.

Create Archive

Use the **Create Archive** window to archive device configuration data and/or capacity planning data. Archiving device configuration data lets you create archives (backup copies) of your network devices' configurations you can restore to the devices at a later date. Archiving capacity planning data lets you store port and FRU information. Create an archive that saves both configuration data and capacity planning data, or create an archive that targets one type of data or the other.

Use the window to perform archives on a single device, multiple devices, or on an entire device group. Because it is useful to archive data on a regular basis, ExtremeCloud IQ Site Engine lets you schedule archives to be performed at a future time, and/or on a routine basis. After you configure an archive's parameters, use that archive on a repeated basis to save new versions of the desired data. For example, you can create an archive that saves your device configurations on a weekly basis, and also create an archive that saves only capacity planning information on a daily basis to monitor what is changing on the network.

TIP: You can set up an email notification based on the event log message that is generated when a configuration change is detected. When the current archive differs from the previously saved archive, ExtremeCloud IQ Site Engine generates an event log message. Using the ExtremeCloud IQ Site Engine **Alarms & Events** tab, you can create an alarm that monitors the log for the text "Configurations Are Different" and define an email to be executed as the specific alarm action.

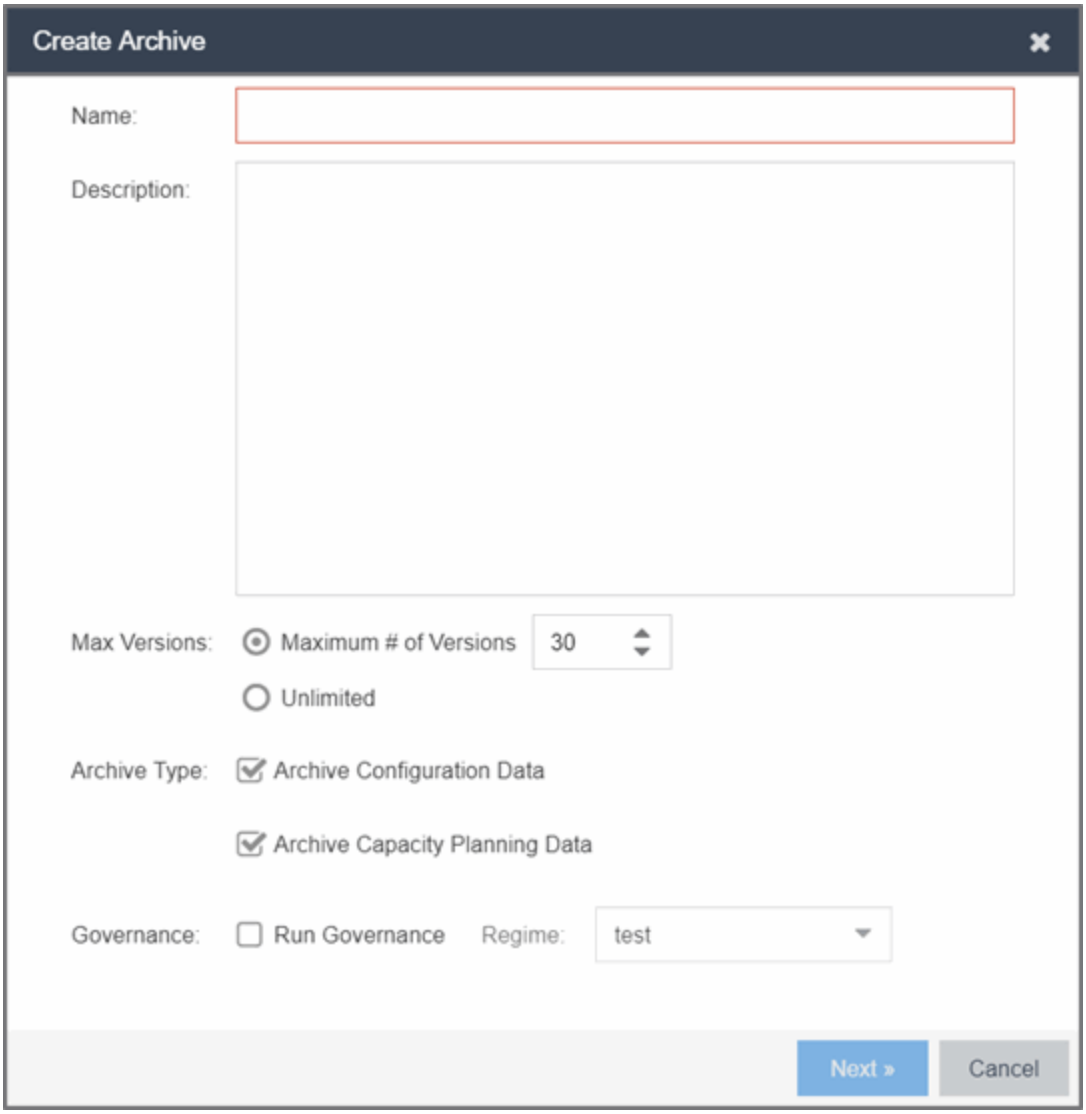
After an archive operation is created, it is listed by name in the left-panel Archives folder. Below the archive name are the archive versions, displayed by the date and time of the creation of the version. Under the versions are individual configurations, listed by the IP address of the device whose data is saved. Each configuration displays an icon that identifies the type of data being saved: device configuration data ( ), capacity planning data ( ), both device configuration and capacity planning data ( ).

To access the window, select the **Create** button from the bottom of the left-panel on the **Network** > **Archives** tab. A TFTP or FTP server must be running to create an archive.

NOTE: When archiving device configuration data on an X-Pedition router, the Startup configuration file is saved.

Archive Name Window

Use this window to name and configure the archive.



Name

Enter a name for the archive operation.

Description

Enter a description *(optional)* of the archive operation.

Archive Setup

Max Versions

If desired, specify the maximum number of versions saved for this archive. This allows you to limit the number of versions saved for each archive. When the maximum number is reached,

ExtremeCloud IQ Site Engine automatically deletes older versions. Otherwise, select **Unlimited** to continue adding archive versions with no limit.

Archive Type

Select the appropriate checkbox for the type of data you wish to archive:

- **Archive Configuration Data** — Create archives (backup copies) of your devices' configurations you can restore to the devices at a later date.
- **Archive Capacity Planning Data** — Create archives of port and FRU information.

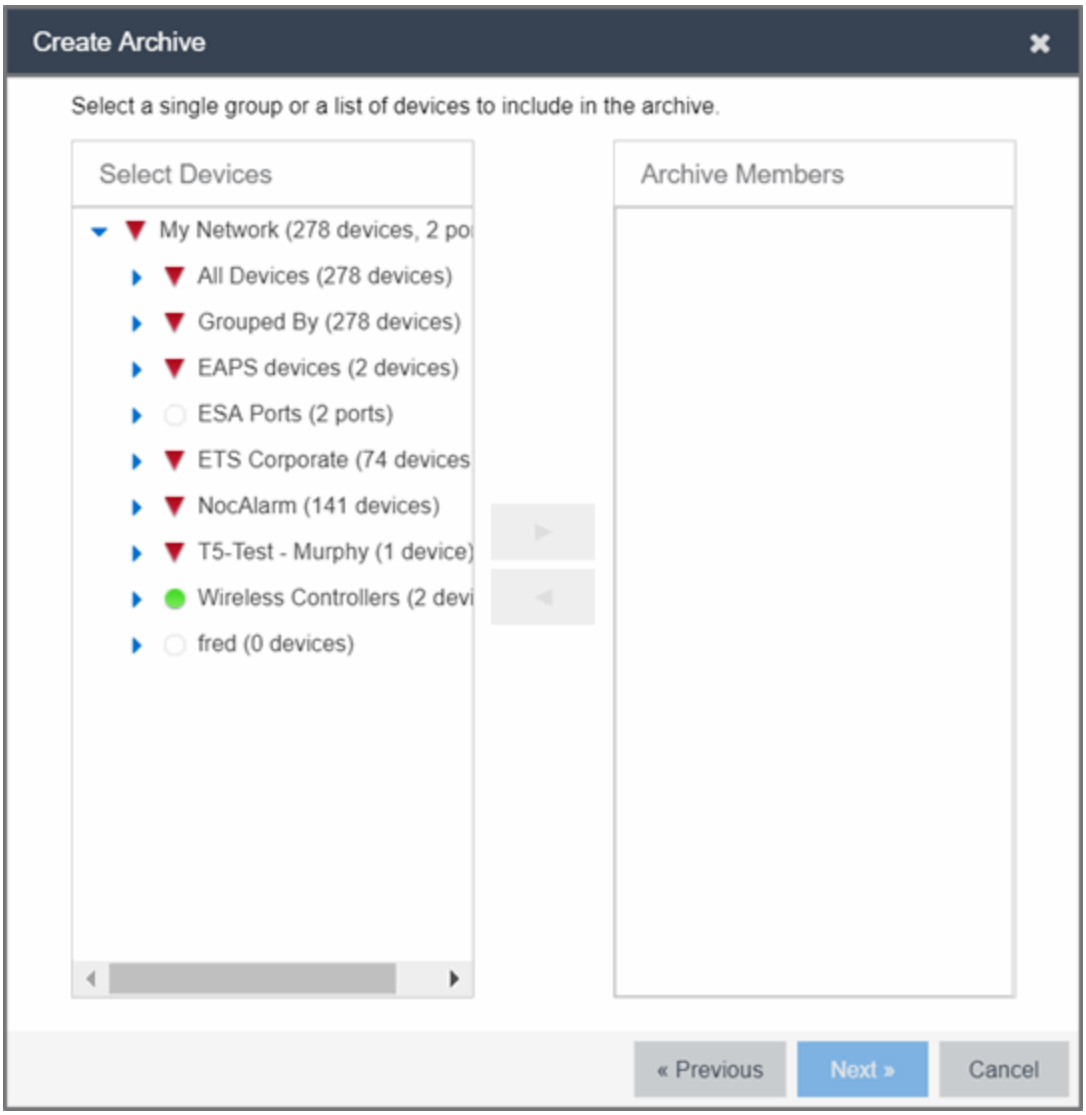
Run Compliance

Select the checkbox to indicate that you want to perform an ExtremeCompliance audit on the device archive. Select the appropriate **Regime** from the drop-down list.

Device Selection Window

Use this window to select the devices to include in the archive.

NOTE: If you select multiple tree nodes representing the same device, but with varying SNMP contexts, an archive save is performed for each context. The context must provide access to the MIBs required for the archive save operation or the archive for that context fails. Perform the archive operation on the device with the default context (switch mode.)



Select Devices

This list displays your current devices as they are listed in the left-panel My Network navigation tree in the **Network** tab. Expand the folders and select the single device, multiple devices, or a single device group to include in the archive. Select the right arrow button **›** to add the devices to the Archive Members list.

Archive Members

The devices you select are listed under Archive Members. To remove a member from the list, select the member and select the left arrow button **‹**.

TIP: If you open the **Create Archive** window from a device or device group in the left-panel, the selected device or device group automatically display under Archive Members.

Right Arrow Button

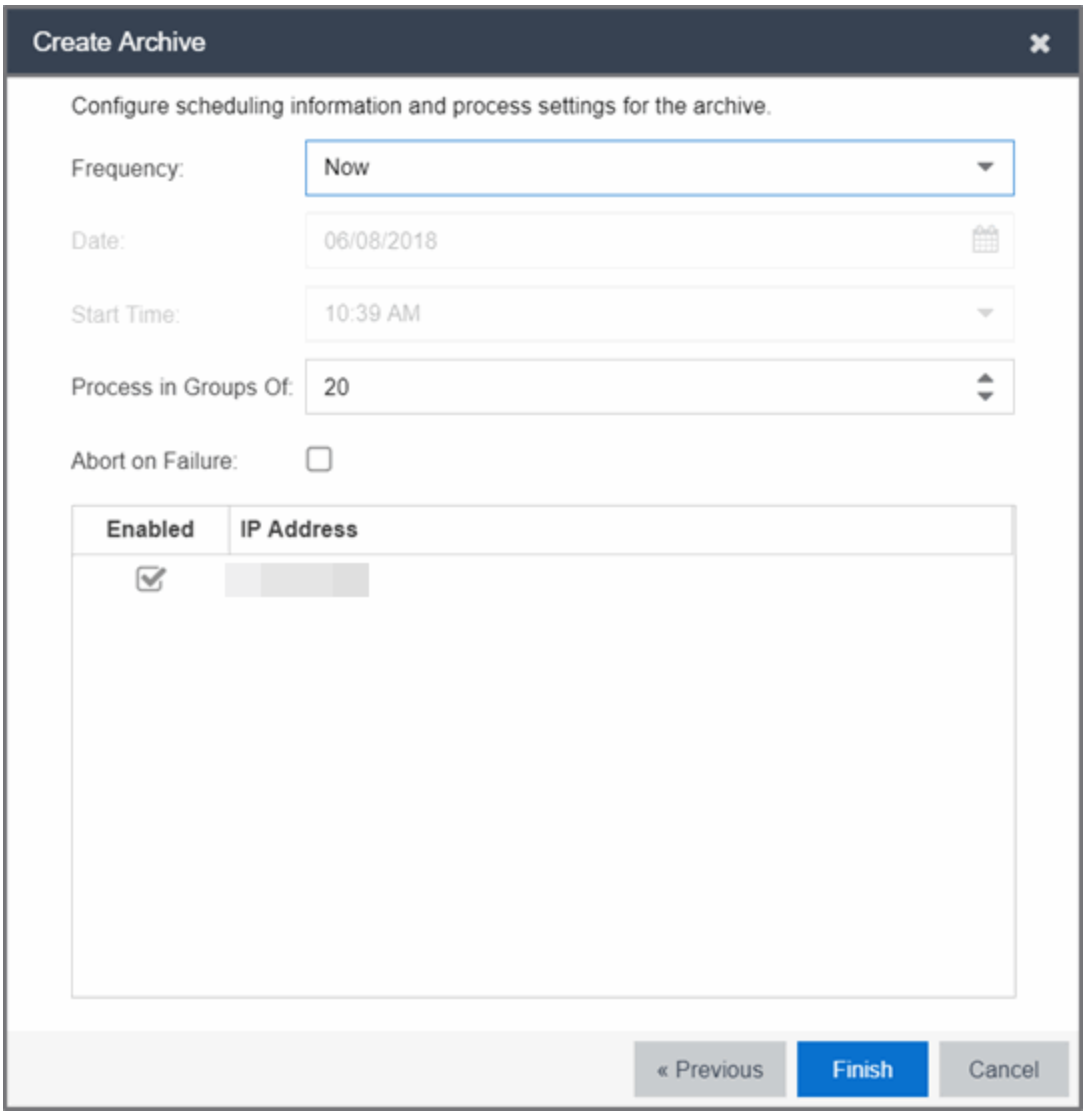
In the Devices tree, select the device(s) or device group you want to archive, and select **›** to add it to the Archive Members list.

Left Arrow Button

Select a device or device group in the Archive Members list, and select **‹** to remove it from the list.

Schedule Window

Use this window to select devices, and configure scheduling information and process settings for the archive. You can schedule a one-time, daily, or weekly archive, or schedule the archive to be performed on server start-up.



Schedule/Process

Frequency

Use the drop-down list to select the frequency with which you want the archive performed: **Never**, **Now**, **Once**, **Daily**, **Weekly**, or **On Server Startup**. The **Never** option lets you create an archive operation without actually performing it. The **Now** option lets you perform an immediate archive.

Date

Use the drop-down list to select the month you want the archive to start. A calendar corresponding to the selected month is displayed. Select the desired starting day by selecting the calendar. You can use the arrows on either side of the drop-down list to change the month, and change the year by entering a new year in the text field. (This field is grayed out if you select **Never** or **Now** as the **Frequency**).

Start Time

Set the starting time for the operation and select AM or PM. (This field is grayed out if you select the **Never** or **Now** for **Frequency**).

Process groups of

The archive is performed in parallel (simultaneously) on the number of devices specified in the **Process groups of** field. Set the value to **1** to perform the operation serially, one device after another.

Abort on failure

Select the **Abort on failure** checkbox to stop the archive operation after a failure. This is useful if you are performing an archive operation on multiple devices and you want the operation to stop after a failure on a single device.

Devices

Selected

Use the **Enabled** checkboxes in this column to select or deselect specific devices to be archived. For example, select a device group in the previous window and then use these checkboxes to deselect individual devices in that group.

IP Address

The IP address of the device you are archiving. Chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.

Finish Button

Creates the archive. The archive is listed by name in the left-panel of the **Archives** tab under the Archives folder, and performed according to its scheduled parameters. You can change the archive's parameters; see Editing an Archive for instructions.

Restore Archive

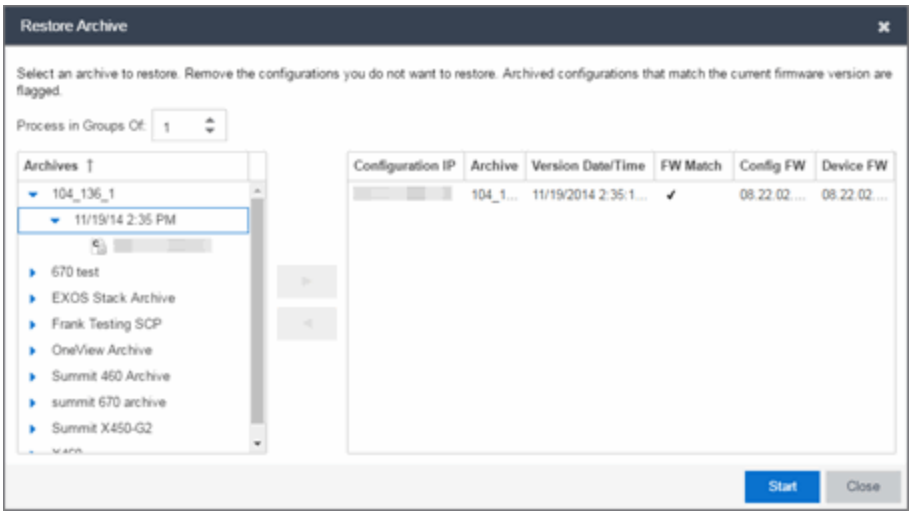
Use the **Restore Archive** window to restore saved (archived) device configuration files to one or more devices. Saved configurations are listed in the left-panel of the **Archive**s tab under the appropriate archive and version. Each configuration displays an icon that identifies the type of saved data: device configuration data ( ), capacity planning data ( ), both device configuration and capacity planning data ( ). Only configurations that include device configuration data (and) are available to be restored.

A configuration can only be restored to a device with the same IP address. This means the device from which an archive is saved and the device to which the archive is restored must be identical. Configurations can be restored to a single device or multiple devices. A TFTP or FTP server must be running to restore a configuration.

To access the window, right-click an archive version or an archive configuration from the left-panel of the **Archives** tab or from the main panel and select **Restore**.

Archive Version Selection Window

Use this window to select an archive version or single configuration to restore. Select the archive version or configuration in the Archives list and select the right arrow button **>** to move it to the restore list. If you select an archive version, use the left arrow button **<** to remove any individual configurations included in the archive version you do not wish to restore.



Archives

This panel displays your current archives as they are listed in the left-panel of the **Archives** tab. Below each archive name are the archive versions, displayed by the date and time the archive occurred. Under the versions are the individual configurations, listed by IP address of the device. Each

configuration displays an icon that identifies the type of saved data: device configuration data ( ), capacity planning data ( ), both device configuration and capacity planning data ( ). Only configurations that include device configuration data (and) are available to be restored.

Expand the folders under the Archives tree and select the archive version or configuration you want to restore. Select the right arrow button **>** to add the configurations to the Configurations to Restore table.

TIPS: If you open the **Restore Archive** window from an archive version or configuration in the left-panel of the **Archives** tab, the selected configuration(s) automatically displays under Configurations to Restore.

Check the FW Match column to see if the current firmware version on the device matches the firmware version on the device at the time of the archive.

Configurations to Restore

Displays the configurations you selected to restore. Select a configuration and use the left arrow button **<** to remove any individual configurations you do not wish to restore.

Configuration IP
The IP address of the device with the saved configuration.

Archive
The name of the archive operation that saved the configuration.

Version Date
The date and time the archive operation occurred.

FW Match
A ✓ indicates the current firmware version installed in the device matches the firmware version installed in the device at the time of the configuration save.

Config FW
The firmware version installed in the device at the time of the configuration save.

Device FW
The current firmware version installed in the device.

Right Arrow Button
In the Archives tree, select the archive version or configuration you want to restore, and select **>** to add it to the Configurations to Restore table.

Left Arrow Button
Select a configuration in the Configurations to Restore table, and select **<** to remove it from the table.

Restore Configurations Window

Use this window to configure restore parameters, initiate the restore operation, and monitor restore progress. Devices that require a restart automatically restart after the restore is complete.

Show all devices/Show only incomplete and failed

When the restore operation starts, the device list table updates with status information for each device. An alert icon (⚠) appears in the Alert column of the table if a restore operation fails for a specific device. Use these radio buttons to show all devices or show only those devices whose restore operations are incomplete or failed.

Device List Table

A list of the devices you selected for your restore operation. When the restore is started, this table updates with status information for the restore operation:

- **Alert** — an alert icon ⚠ appears in the Alert column if a restore operation fails for a specific device.
- **IP Address** — The device's IP address. Chassis that support Distributed Forwarding Engines (DFEs), such as the N-Series, display a single management IP even though there may be multiple DFE modules in the chassis.
- **Configuration** — The name of the configuration file being restored.
- **Status** — The status of the operation for that particular device: **Success** or **Failure**.
- **Operation** — The type of operation performed: Configuration Restore.
- **% Progress** — A progress bar showing the percent completed of the operation.
- **Bytes Trans.** — The number of bytes transferred during the operation.
- **Message** — A message relating to the status of the operation.

Status Summary

When the restore is started, this area updates with status information for the restore operation.

Restore Type

The restore is performed in parallel (simultaneously) on the number of devices specified in the **Process in Groups Of** field. By default, the restores occur in sequential order (**Process in Groups Of**: 1). This is to protect against possible isolation of other devices on the restore list.

CAUTION: Because some devices automatically restart following a restore operation, performing a Restore Type greater than 1 may isolate other devices in the restore list, causing their restores to fail. Use a **Process in Groups Of** value of 1 (perform the restore serially,) unless you know it is safe for the selected network devices to restart simultaneously.

Start Button

Initiates the restore operation. The table at the top of the window and the status area in the bottom left of the window update with status information.

Archive

You can save device configuration data and/or capacity planning data by creating an archive.

Archiving device configuration data lets you create archives (backup copies) of your network devices' configurations you can restore to the devices at a later date. Archiving capacity planning data lets you store port and FRU information. You can create an archive that saves both configuration data and capacity planning data, or you can create an archive that targets one type of data or the other.

You can perform archives on a single device, multiple devices, or on an entire device group. Because it is useful to archive data on a regular basis, ExtremeCloud IQ Site Engine lets you schedule archives to be performed at a future time, and/or on a routine basis. After you configure an archive's parameters, you can use that archive on a repeated basis to save new versions of the desired data. For example, you can create an archive that saves your device configurations on a weekly basis, and also create an archive that saves only capacity planning information on a daily basis to monitor what is changing on the network.

After you create an archive operation, it is listed by name in the left-panel **Archives** tab under the Archives folder. Below the archive name are the archive versions, displayed by the date and time the version was performed. Under the versions are the individual configurations, listed by IP address of the device whose data is saved. Each configuration displays an icon that identifies the type of data being saved: device configuration data ( ), capacity planning data ( ), or both device configuration and capacity planning data ( ).

NOTE: If the device is an X-Pedition router, be aware that when archiving device configuration data, the router's Startup configuration file is saved.

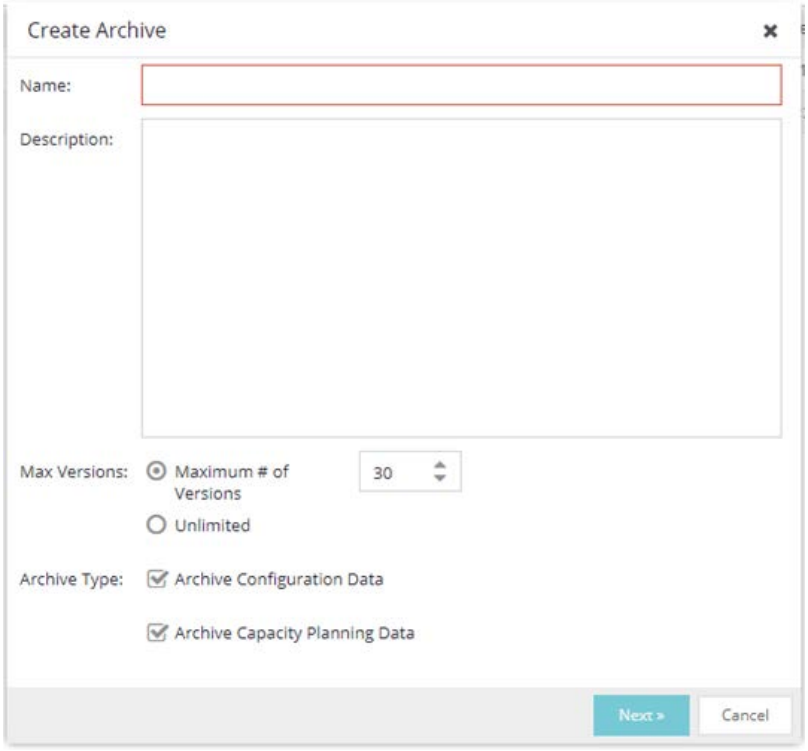
Instructions on:

- Creating an Archive
- Saving a New Archive Version
- Editing an Archive
- Renaming an Archive
- Deleting an Archive

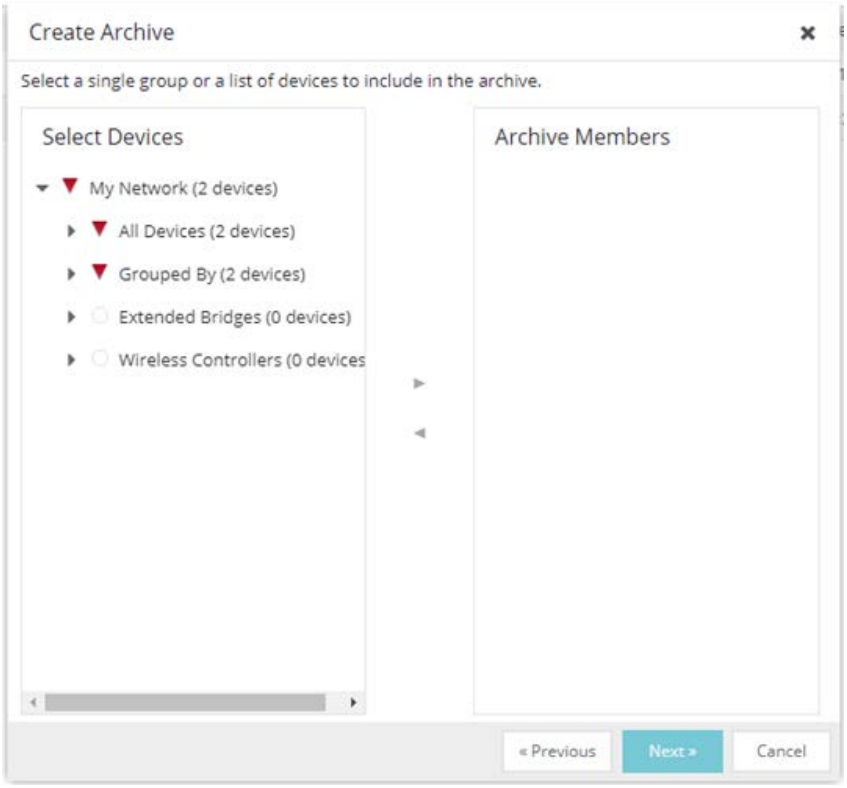
Creating an Archive

Use the **Create Archive** window to archive network configuration data and/or capacity planning data. You can perform archives on a single device, multiple devices, or on an entire device group. You need a running TFTP or FTP server to save a configuration.

1. Select the **Create** button in the left-panel. The **Create Archive** window displays.



2. Enter a name and description *(optional)* of the archive operation.
3. Configure the archive setup:
    a. Specify either the maximum number of versions to be saved for this archive in the **Max Versions** field or select **Unlimited** to retain all archives. Entering a value in the **Max Versions** field allows you to limit the number of versions saved for each archive and when the limit is reached, older versions are automatically deleted.
    b. Select the appropriate checkbox for the type of data you wish to archive:
        - **Archive Configuration Data** — Create archives (backup copies) of your devices' configurations you can restore to the devices at a later date, if needed.
        - **Archive Capacity Planning Data** — Create archives of port and FRU information used to generate reports.
    c. Select **Next**.
    The next **Select Devices** list displays.



4. **Select the Archive Members:**

   a. Expand the folders in the Select Devices list and select the single device, devices, or a device group and select the right arrow button **›** to move the devices to the Archive Members list.

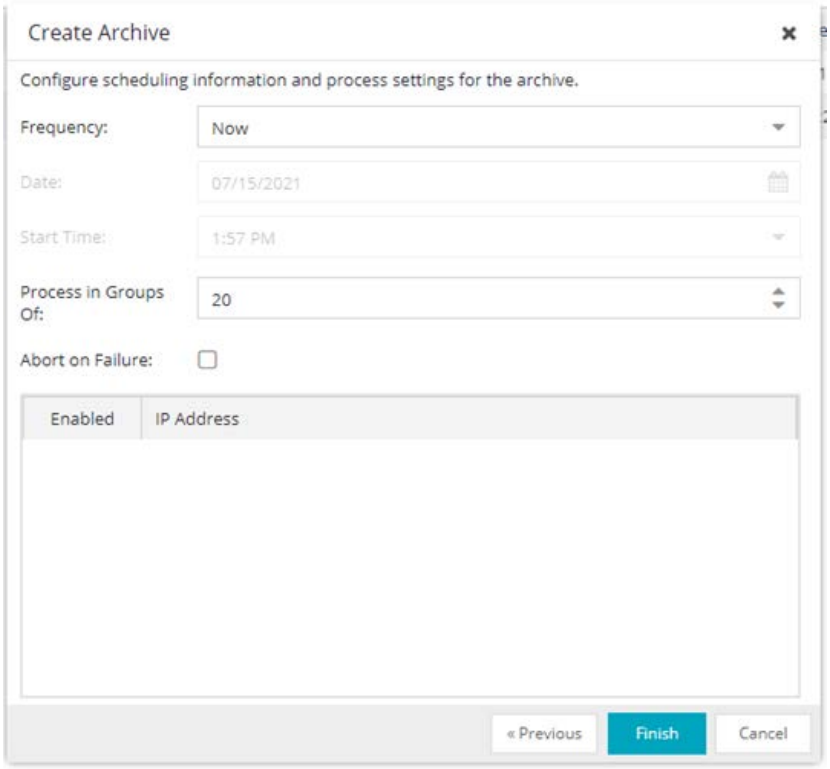
   NOTE: If you select multiple tree nodes representing the same device, but with varying SNMP contexts, an archive save is performed for each context. However, the context must provide access to the MIBs required for the archive save operation or the archive for that context fails. It is recommended you perform the archive operation on the device with the default context (switch mode.)

   b. If you want to remove a member from the Archive Members list, select the member and select the left arrow button **‹**.

   c. Select **Next**.

TIP: If you open the **Create Archive** window from a selected device or device group in the left-panel **Network Elements** tab, the selected items are automatically displayed under Archive Members.

The Configure Scheduling window displays.



5. Select the **Frequency** with which the archive process occurs.
   Note: Scheduled archive tasks can be viewed on the **Tasks > Scheduled Tasks** tab. If you set the frequency for an archive task to On Startup, Now, or Never, the action is not considered scheduled, so the archive cannot be canceled from the **Scheduled Tasks** tab. It can only be set to Never in the **Archives** tab.
6. Select the **Date** to run the archive process and **Start Time** for the archive process.
7. **Configure Process settings for the archive:**
   a. The archive is performed in parallel (simultaneously) on the number of devices specified in the **Process in Groups Of** field. Set the value to **1** to perform the operation serially, one device after another.
   b. Select the **Abort on Failure** checkbox to stop the archive operation after a failure. This is useful if you are performing an archive operation on multiple devices and you want the operation to stop after a failure on a single device.
8. Use the **Enabled** checkboxes to select or deselect devices you are archiving. For example, if you selected a device group in the previous window, you can use these checkboxes to deselect individual devices in that group.
9. Select **Finish** to create the archive. The archive is listed by name in the left-panel of the **Archives** tab under the Archives folder and performed according to its scheduled parameters.

Archive information saved on this tab is shared with ExtremeCloud IQ. You can change the archive's parameters; see Editing an Archive for instructions.

TIP: You can set up an email notification based on the event log message that is generated when a configuration change is detected. When the current archive differs from the previously saved archive, ExtremeCloud IQ Site Engine generates an event log message.

Saving a New Archive Version

After you create an archive, use that archive on a repeated basis to save (stamp) new versions of the desired configurations.

1. With an archive folder selected in the left-panel **Archives** tab, right-click and select **Stamp New Version** from the menu.
2. A new archive version, displayed by the date and time the version is performed, is listed under the archive folder. Under the version are the individual configurations, listed by the IP address of the saved device.

Editing an Archive

After you create an archive, you can edit the archive parameters, including changing the devices on which the archive is performed.

1. Select an archive name in the left-panel of the **Archives** tab.
2. Navigate to the **Details** panel at the far right, which includes the **General, Setup** and **Schedule** tabs.
3. On the **General** tab, edit the archive Description and use the **Enabled** checkboxes in the Devices table to select or deselect devices to be archived, if desired.
4. Select the **Setup** tab.
5. Select the number of devices to archive in parallel (simultaneously) in the **Process in Groups Of** field. Set the value to **1** to perform the operation serially, one device after another.
6. Select the **Abort on Failure** checkbox to stop the archive operation after a failure. This is useful if you are performing an archive operation on multiple devices and you want the operation to stop after a failure on a single device.
7. Specify either the maximum number of versions to be saved for this archive in the **Max Versions** field or select **Unlimited** to retain all archives. Entering a value in the **Max Versions** field allows you to limit the number of versions saved for each archive and when the limit is reached, older versions are automatically deleted.
8. Select the appropriate checkbox for the type of data you wish to archive:
   - **Archive Configuration Data** — Create archives (backup copies) of your devices' configurations you can restore to the devices at a later date, if needed.

- **Archive Capacity Planning Data** — Create archives of port and FRU information.

9. Select the **Run Compliance** checkbox and select a **Regime** to run on the device archive, if necessary.
10. Select the **Schedule** tab.
11. Select the **Frequency** with which the archive process occurs.
12. Select the **Date** to run the archive process and **Start Time** for the archive process.
13. Select **Save**.
    The next time the archive is performed, these new parameters are used.

Renaming an Archive

You can rename an archive.

1. With an archive name selected in the left-panel of the **Archives** tab, right-click and select **Rename** from the menu. The Rename Archive window opens.
2. Enter the new name, and select **OK**.
3. The name of the archive changes in the left-panel tree. All previous versions saved under the old name are available under the new name. The next time the archive is performed, the new name is used.

Deleting an Archive

You can delete an archive, an archive version, or a saved configuration from the **Archives** tab left-panel navigation tree.

1. With an archive name folder, archive version, or archive file selected in the left-panel of the **Archives** tab, right-click and select **Delete** from the menu.
2. A Delete confirmation window opens. Select **Yes** to perform the delete.

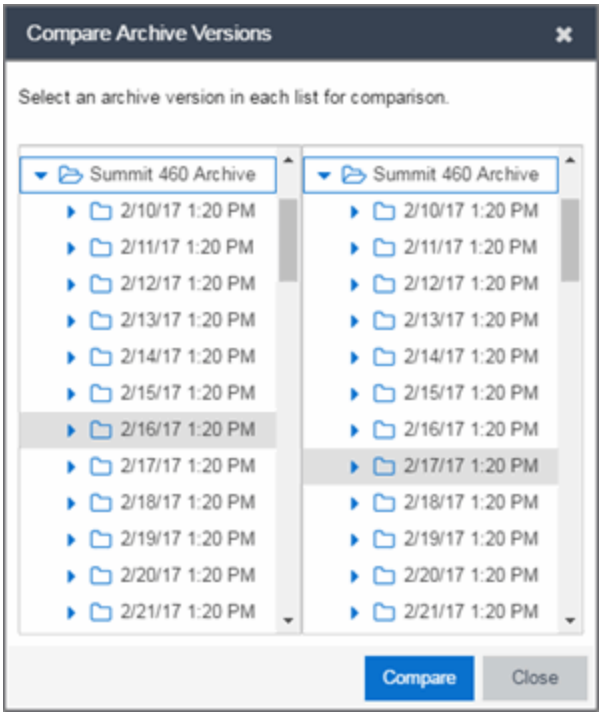
How to Compare Archives

ExtremeCloud IQ Site Engine lets you compare two different archives for the same device and monitor any changes in device attributes. ExtremeCloud IQ Site Engine compares archives using a set group of attributes you saved when the archive was performed. The values for these attributes appear in a table with any differences between the values flagged by a yellow **Difference** icon . Select the configurations you want to compare and use the Compare Archives Versions window to view the comparison results.

1. Access the **Compare Archive Versions** window from the **Archives** tab by right-clicking an archive name, archive version, or configuration file in the left-panel navigation tree or by right-

clicking in the main panel and selecting **Compare Archives**.

2. The **Compare Archive Versions** window displays two Archive trees (identical to the Archive left-panel navigation tree in the **Archives** tab). Expand the folders as necessary to select the two archive versions or configurations you wish to compare. Compare two individual configurations for the same device, or compare two different archive versions (select versions that share common devices). Select the **Compare** button.



Selection 1

Expand the folders as necessary to select the first version or configuration you wish to compare.

Selection 2

Expand the folders as necessary to select the second version or configuration you wish to compare.

Compare

Performs the comparison and opens the Compare Archive Versions window, where you can view the comparison results.

Close

Closes the window.

3. A new **Compare Archive Versions** window opens to display the results of the comparison. The Devices table in the middle of the window displays each device included in the comparison. Any differences between the two versions is flagged by a yellow **Difference** icon

. If there are many devices being compared, a progress bar indicates the progress of the operation. You can stop the compare operation by pressing the **Abort Compare** button.

4. Once the compare operation is complete, select the device in the Summary table whose comparison results you wish to see. The results are displayed in the Device table at the bottom of the window.

In addition, the following buttons are available in the window only for archives that include device configuration data:

- **View Config File** — Opens the Configuration File Viewer and displays the archived configuration file of the selected device. This option is only available when there are no differences between the two configuration files being compared.
- **Compare Config Files** — Opens the Configuration File Compare window and displays the two archived configuration files for the selected device. This option is only available when there are differences between the two configuration files being compared.

How to Restore an Archive

You can restore saved (archived) device configuration files to devices using the Restore Archive window. Saved configurations are listed in the left-panel of the **Archives** tab under the appropriate archive and version. Each configuration displays an icon that identifies the type of data that was saved: device configuration data ( ), capacity planning data ( ), both device configuration and capacity planning data ( ). Only configurations that include device configuration data (and) are available to restore.

You can only restore a configuration to a device with the same IP address. In other words, the device you are restoring *to* must have the same IP address as the device the configuration was originally saved *from*. You can restore configurations to a single device or multiple devices. You must have a TFTP or FTP server running to restore a configuration.

Use these steps to restore a configuration to a device.

1. Right-click an archive version or an archive configuration from the left-panel of the **Archives** tab or from the main panel and select **Restore**. The Restore Archive window displays.
2. **Select the archive version to restore:**
    a. Expand the folders under the Archives tree and select the archive version or configuration you want to restore. Only configurations that include device configuration data (and) can be restored. Select the right arrow button **>**.

b. The Configurations to Restore table lists the configurations. If you select an archive version and want to remove an individual configuration from the list, select the configuration and select the left arrow button **<**.

c. Select **Start**.

TIPS: If you open the **Restore Archive** window from an archive version or configuration in the left-panel of the **Archives** tab, the selected configuration(s) is automatically displayed under Configurations to Restore.

Check the FW Match column to see if the current firmware version on the device matches the firmware version on the device at the time of the archive.

---

3. **Initiate the Restore operation:**

a. Specify the **Restore Type** option. The restore is performed in parallel (simultaneously) on the number of devices specified in the **Process in Groups Of** field. By default, the restores occur in sequential order (**Process in Groups Of**: 1). This is to protect against possible isolation of other devices in the restore list.

CAUTION: Because some devices automatically restart following a restore operation, performing a Restore Type greater than 1 may isolate other devices in the restore list, causing their restores to fail. It is recommended you leave the **Process in Groups Of** value at 1 (perform the restore serially), unless you know it is safe to simultaneously restart the selected network devices.

---

b. Select **Start** to initiate the restore operation. The table at the top of the window and the status area in the bottom left of the screen both update with status information.

c. Review results. An alert icon (⚠) appears in the Alert column of the table if a restore operation fails for a specific device. You can select to show all devices or show only incomplete or failed device archive restorations.

4. Select **Finish** to close the window.

How to Back up, Restore, and Compare Device Configurations

You can back up (archive) and restore device configurations as well as compare two configuration files, using the Network tab in ExtremeCloud IQ Site Engine. The backup operation performs a single configuration archive. The restore operation restores an archived configuration or configuration template to a device. The compare operation compares the last two archived configuration files for a selected device.

NOTES: Configure the path into which configuration files are saved in the **Directory Path** field in Administration > Options > Inventory Manager > Data Storage.

Configure the file transfer settings and login information in the Server Properties section of Administration > Options > Inventory Manager > File Transfer.

All of the operations require that you are using the Archives tab for your archive management.

Device Back up Configuration

To perform a quick device configuration back up from the Devices tab:

1. Select a device in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Archives** > **Backup Configuration**.

   This performs a single configuration archive for the device. You can refer to the ExtremeCloud IQ Site Engine Inventory Event Log to view the archive progress.
4. Open the **Network** > **Archives** tab to view the archive.

NOTES: To perform the backup configuration, you must be a member of an authorization group that has the Inventory Manager > Configuration Archive Management > Archive Restore Wizard capability.

Because the ExtremeCloud IQ Site Engine backup creates a single archive that is not recurring, use the Create Archive button on the **Archives** tab to schedule regular backups of your network device configurations.

Device Restore Configuration

The device restore configuration operation allows you to restore a configuration template or archived configuration to an active device on the network.

1. Select a device in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Archives** > **Restore Configuration**.

   For additional information about restoring a device's configuration, see Restore Device Configuration in ExtremeCloud IQ Site Engine.

Compare Device Configurations

You can compare the last two archived configuration files for a selected device from the **Devices** tab.

1. Select a device in the Device list.
2. Select the **Menu** icon (☰) or right-click in the Devices list.
3. Select **Archives** > **Compare Last Configurations**.

   For additional information about comparing device configurations, see Compare Device Configurations in ExtremeCloud IQ Site Engine.

Configuration Templates

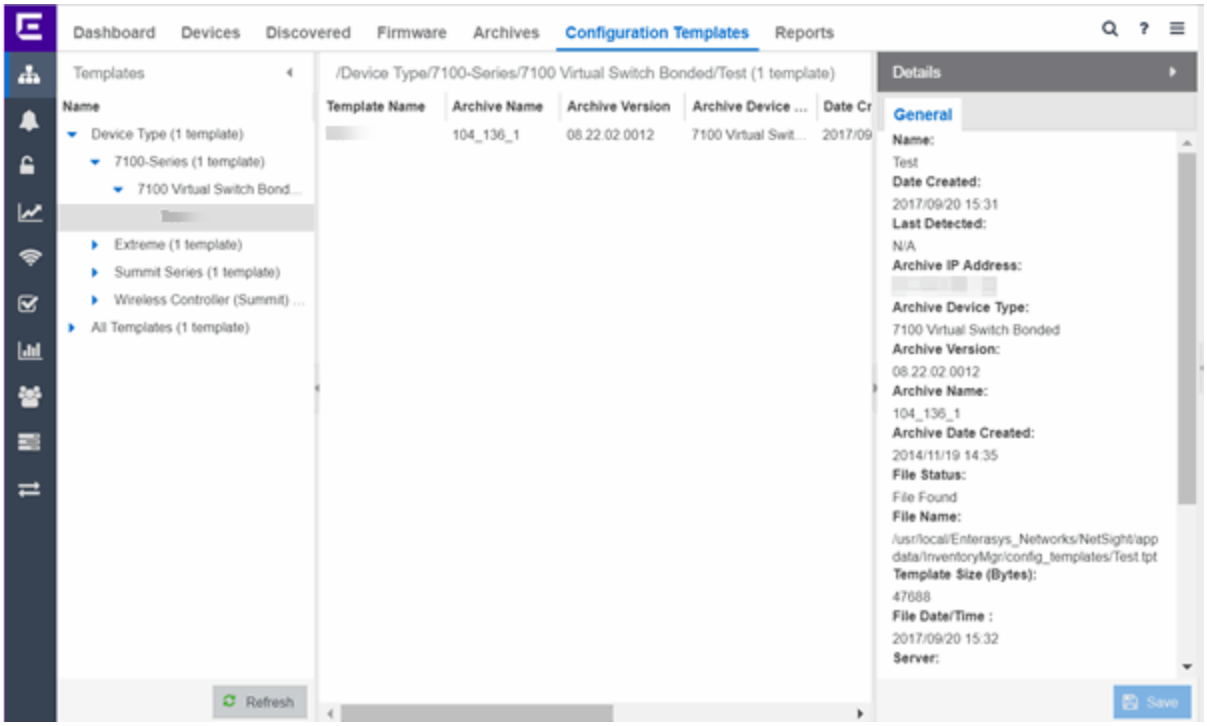
The **Configuration Templates** tab displays configuration templates you create, grouped according to product family and device type. ExtremeCloud IQ Site Engine provides pre-defined template groups and automatically assigns a template to the appropriate group when you create the template. Each template group name is followed by the total number of configuration templates in that group and any subgroups, in parentheses.

Additionally, you can include variables in your configuration templates to serve as placeholders for specific values. ExtremeCloud IQ Site Engine automatically substitutes the values you define on the **Custom Variables** tab into your template.

To access the **Configuration Templates** tab, open the **Network** tab and select the **Configuration Templates** tab.

The tab is divided into three sections:

- Templates Tree
- Templates Table
- Details View



Templates Tree

The Templates tree in the left panel displays configuration templates grouped according to product family and device type. It provides pre-defined template groups and automatically organizes the configuration templates under the appropriate group when you press the **Refresh** button.

Name
: The **Name** navigation tree includes the Device Type Folder and the All Templates folder.

Device Type Folder
: This folder contains pre-defined product family and device type folders.

All Templates Folder
: This folder contains all the configuration templates you create.

Select a template in the All Templates folder or the Device Type folder in the left-panel Templates Tree to display the Templates table and the Details view.

Right-click a template in the Templates table to display the following menu:

- **Assign Template** - Select to open the **Select Device Types** window. Select the device type (s) to which the template is to be assigned. Select the **OK** button to save your selection(s). The template becomes available for the device type(s) you selected.

- **Edit Template** - Select to open the **Edit Configuration Template** window. Follow the same procedure to create a configuration template to edit the template. Select **Save** to save your changes.
- **Rename Template** - Select to open the **Rename Template** window. Enter a new name and select the **OK** button to save the new name to the template.
- **Remove Template From Group** - Select to remove the template you selected in the Templates table from its template group.
- **Delete** - Select to delete the template you selected in the Templates table.

Templates Table

Select a template in the All Templates folder or the Device Type folder in the left-panel Templates Tree to display the Templates table and the Details view.

The Templates table includes the following columns:

Template Name
: The name of the configuration template.

Archive Name
: The name of the archive that was used to create the configuration template.

Archive Version
: The firmware version the device was using when it was archived and used to create the configuration template.

Archive Device Type
: The device type of the archive that was used to create the configuration template.

Date Created
: The date and time the template was created.

File Size (Bytes)
: The size of the template in bytes.

Status
: The status of the template shown as: **File Found** or **File Not Found**. **File Found** indicates the template is still present in the database.

Last Modified
: The date and time the template was last modified.

Right-click a template in the Templates table to display the following menu:

- **Assign Template** - Select to open the **Select Device Types** window. Select the device type (s) to which the template is to be assigned. Select the **OK** button to save your selection(s). The template becomes available for the device type(s) you selected.

- **Edit Template** - Select to open the **Edit Configuration Template** window. Follow the same procedure to create a configuration template to edit the template. Select **Save** to save your changes.
- **Rename Template** - Select to open the **Rename Template** window. Enter a new name and select the **OK** button to save the new name to the template.
- **Remove Template From Group** - Select to remove the template you selected in the Templates table from its template group.
- **Delete** - Select to delete the template you selected in the Templates table.

Details View

The Details view opens when you select a template in the All Templates folder or the Device Type folder in the left-panel Templates Tree.

The following items are included in the Details view General tab:

Name
: The name of the configuration template.

Date Created
: The date and time the template was created.

Last Detected
: The date and time the template was last modified.

Archive IP Address
: The IP Address of the device that was archived to create the configuration template.

Archive Device Type
: The device type of the archive that was used to create the configuration template.

Archive Version
: The firmware version the device was using when it was archived and used to create the configuration template.

Archive Name
: The name of the archive that was used to create the configuration template.

Archive Date Created
: The date and time the archive used to create the configuration template was created.

File Status
: The status of the file shown as: **File Found** or **File Not Found**. **File Found** indicates the template is still present in the database.

File Name
: The name and path for the configuration template.

Template Size
: The size of the template in bytes.

File Date/Time
: The date and time the template was created.

Server
: The ExtremeCloud IQ Site Engine server where the configuration template is located.

Description
: Select in the Description field to add a description of the configuration template, or to modify or edit an existing description. Select **Save** to save your additions or changes.

Alarms and Events

Use the **Alarms & Events** tab to display alarm and event details for all managed devices in the network, with sorting and filtering of relevant information for network troubleshooting and forensics.

Additionally, the **Menu** icon (☰) at the top of the screen provides links to additional information about your version of ExtremeCloud IQ Site Engine.

This Help topic provides information on the following topics:

- Access Requirements
- Alarms
- Alarm Configuration
- Events
    - Event Log Column Definitions
- Event Configuration
- Buttons, Search Field, and Paging Toolbar

Access Requirements

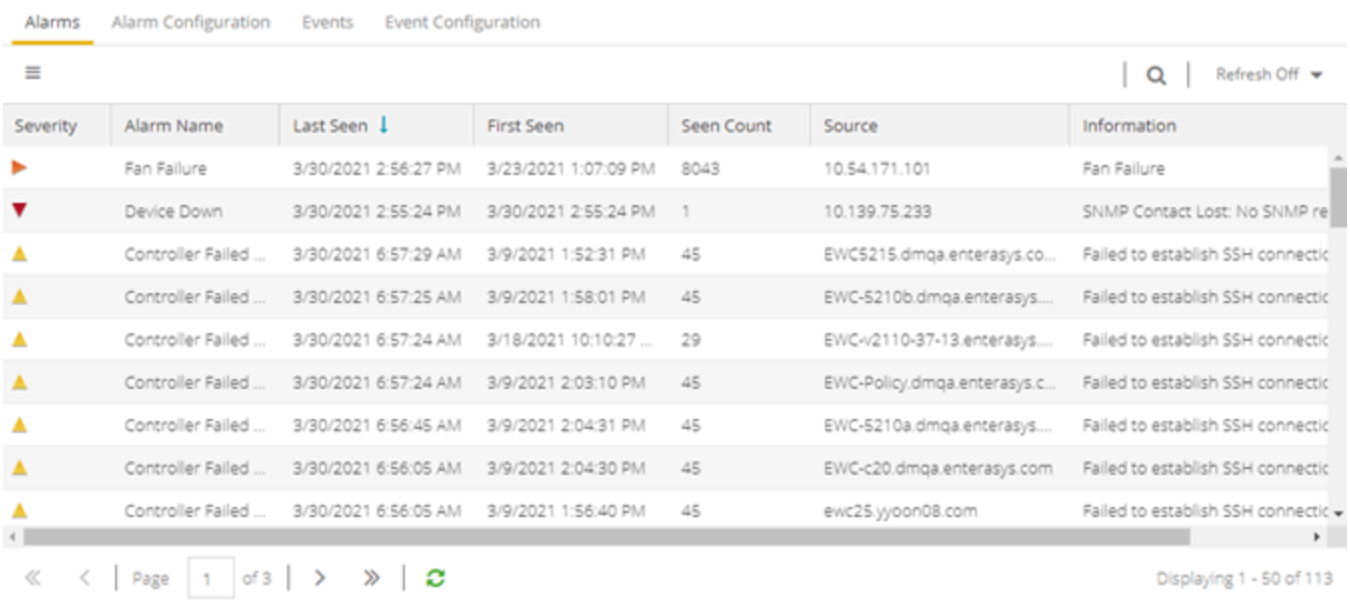
To view the information in the Alarms and Event logs, you must be a member of an authorization group assigned the appropriate ExtremeCloud IQ Site Engine capabilities:

- XIQ-SE OneView > Access OneView
- XIQ-SE OneView > Events and Alarms > OneView Event Log Access
- XIQ-SE OneView > Events and Alarms > OneView Alarms Read Access or Read/Write Access

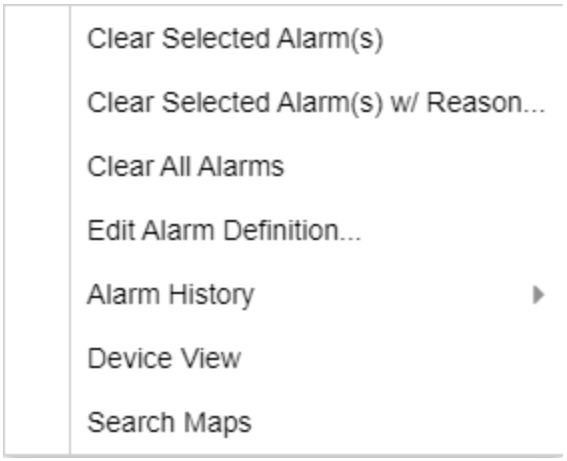
For additional information, see Users and Access Requirements.

Alarms

Use the **Alarms & Events** tab to access the **Alarms** tab that displays the current alarms for the network.



In the **Alarms** tab, right-click on the alarm or select the **Menu** icon (☰) to display several additional functions:

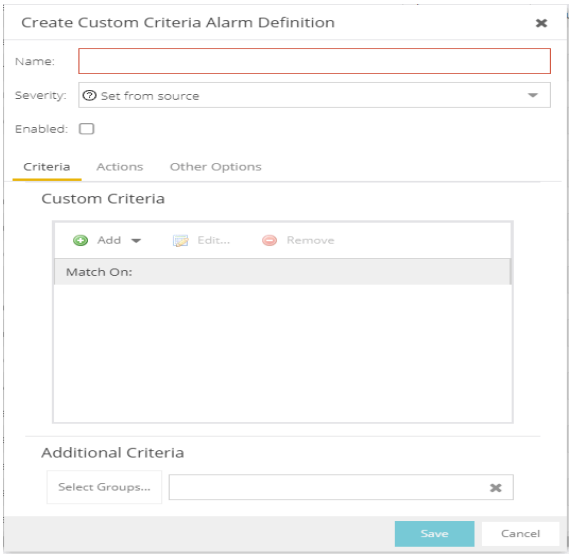


Clear Selected Alarm(s)
Select to clear the selected alarm from the Alarms table.

Clear Selected Alarm(s) w/ Reason
Select to clear the selected alarm or alarms. Supply a reason the alarm(s) cleared, if necessary. which is recorded in the Alarm History.

Clear All Alarms
Select to clear all the alarms in the table.

Edit Alarm Definition
Select to open the alarm in the Alarm Configuration window, from which you can edit the criteria which triggers the alarm. The Create Custom Criteria Alarm Definition window opens:

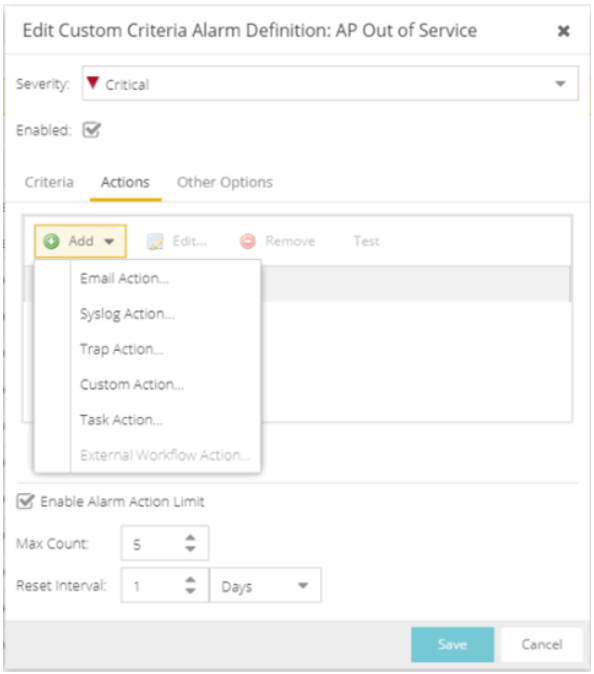


The severity of the alarm displays in the Severity field. Use the drop-down list to change the alarm severity. The Enabled check box indicates if the custom criteria has been enabled.

- Select the **Criteria** tab to open the **Custom Criteria** window, where you can Add, Edit or Remove specific criteria details the alarm.

  Use the Additional Criteria field to add new criteria. Select the **Select Groups** button to open the Alarm Group Section window.

- Select the **Actions** tab to Add, Edit, Remove actions to the alarm definition. Select the Add button to open the Action drop-down list:



The following actions are included on the drop-down list. Select the Override Content check box to change the message content of the action.

- Email Action - Sends an email to email addresses you select
- Syslog Action - Sends a syslog message
- Trap Action - Sends a trap to a remote Trap Receiver. The type of trap being sent to the remote server is determined by the SNMP Credential profile selected. If the profile is V2c or V3 and the 'Use SNMP Informs' is selected, then SNMP informs will be sent instead of SNMP traps.

NOTE: When using SNMPv3 Traps, the Trap Receiver needs to have a v3 user created with the SNMPv3 Trap Server Engine ID to receive the traps.

- Custom Action - Select to add a customized action.
- Task Action - Select to add actions to Workflow tasks.
- External Workflow Action- Select to add actions to a user workflow,

- Select the Other Options tab to clear the conditions of actions for alarms you select.

Alarm History

- Right-click on the alarm or select the **Menu** icon (☰) and select **Alarm History** > **All** to view the Alarm History for all devices.
- Right-click on the alarm or select the **Menu** icon (☰) and select **Alarm History** > **By Source** to view an Alarm History for that device. If the Source includes a subcomponent (such as an interface on the device), then the alarm history is specific to that subcomponent.
- Right-click on the alarm column or select the **Menu** icon (☰) and select **Alarm History** > **By Alarm Name (Devices with Reference Firmware Impact)** to view an Alarm History for a specific alarm.

Device View

Allows you to specify contact information for the person maintaining the device. Additionally, enter a backslash "/" between contacts to create a device group in a tiered tree structure. For example, to move the device into a device group called "John's Devices" within a device group called "Quality Assurance Testing", enter **Quality Assurance Testing/John's Devices** in this field.

Search Maps

Allows you to specify contact information for the person maintaining the device. Additionally, enter a backslash "/" between contacts to create a device group in a tiered tree structure. For example, to move the device into a device group called "John's Devices" within a device group called "Quality Assurance Testing", enter **Quality Assurance Testing/John's Devices** in this field.

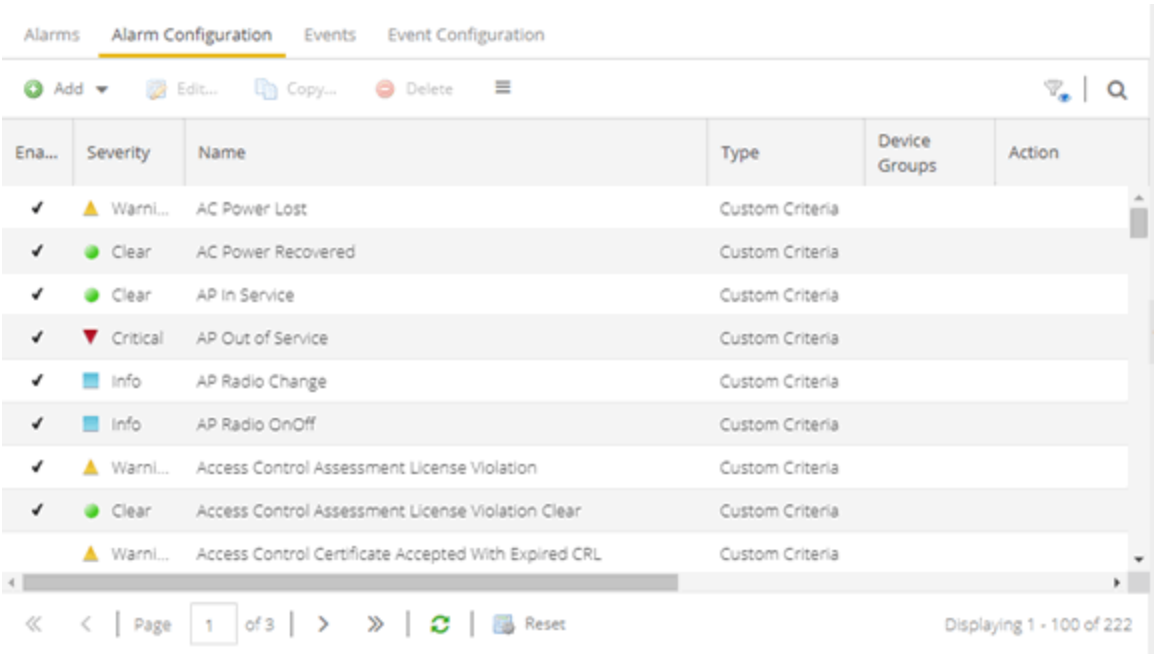
Alarm Summary

Every ExtremeCloud IQ Site Engine page includes a system-wide Alarm Summary in the lower right corner. This indicates the number of current alarms for each severity (Critical, Error, Warning, and Info) present in the entire system. If there are no current alarms, the status displays all zeroes. Select an indicator to open the **Alarms** tab filtered to display the alarms of that severity. An alarm with a slash indicates the alarm is disabled.



Alarm Configuration

Use the **Alarm Configuration** tab in the **Alarms & Events** tab to configure the network alarms that provide status information for a particular problem or condition on a particular network component. Alarms are triggered when event conditions (called a trigger event) occur on your network, and they are tracked until the problem or condition is removed. From the **Alarm Configuration** tab you can also create an alarm definition that detects when the problem or condition is removed and clears the alarm. For example, a Link Down alarm is triggered when a device emits a linkDown trap. Then, when the device emits a linkUp trap, the Link Up alarm automatically clears the Link Down alarm.



Via the **Add** menu, you can:

- Add a new alarm definition, which includes configuring the conditions (criteria) that trigger the alarm, and defining the actions that occur automatically to notify a person or network component about the problem, when the alarm triggers.
- Edit and delete alarm definitions as well as configure email settings for alerts.

ExtremeCloud IQ Site Engine ships with a set of default alarm definitions, which you can use as is, or delete or modify them as desired. Additionally, you can create your own.

Alarm Configuration Column Definitions

Enabled — A check mark in the Enabled column indicates the alarm definition is active. Ignore an alarm definition to ignore your enabled alarms without deleting the definition.

Severity — The icons indicate the seriousness of an alarm definition. This column displays its own specified severity, regardless of the severity of the event or trap that triggered it.

- (question mark) Set from Source — the alarm definition uses the severity level of the trigger event, for example a warning event.
- (Red) Critical — A problem with significant implications.
- (Orange) Error — A problem with limited implications.
- (Yellow) Warning — A condition that might lead to a problem.
- (Blue) Info — Information only; not a problem.
- (Green) Clear — An alarm that clears another alarm (for example, LinkUp).

Name — The name of the alarm definition.

Type — Identifies the type of alarm definition for this row (threshold, trap, or custom criteria).

Device Groups — If desired, you can restrict the alarm definition to devices and port elements in one or more device groups. This column indicates the device group to which the alarm definition is assigned. The alarm definition is only raised on the devices and interfaces in the selected device groups. This allows you to filter alarms to specific devices or important ports.

Action — The actions that occur when an alert is triggered, if any.

Limit Enabled — A checkbox indicates that there is a rate-limit on the alarm's actions.

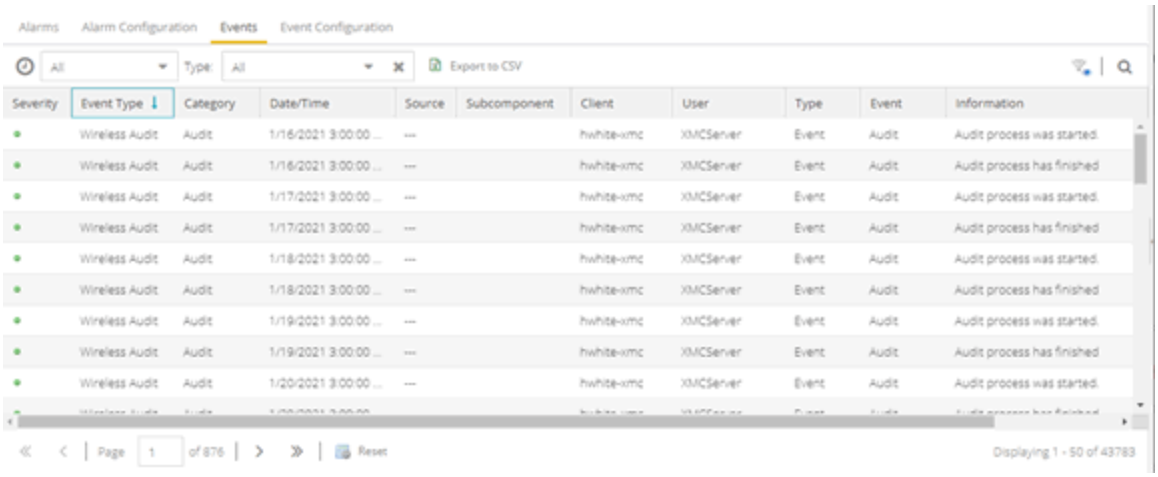
Max Count — If Limit Enabled is checked, this column indicates the number of times an action is performed for this alarm. When the limit is reached, the alarm is still recorded, but no further actions are performed until the Reset Interval expires. If you configure multiple action types, the limit is for the number of times the set of configured actions is performed, not for each individual action. If Limit Enabled is not checked, there is no limit placed on the number of times the action is performed.

Reset Interval — If Limit Enabled is checked, this column displays the length of time from when the first action is triggered until the count is reset. When the count is reset, actions are executed until the Max Count is reached again. If the reset interval is set to "None", then when the alarm limit is reached, the alarm does not reset unless manually reset.

Clearing Alarms — This column displays the **Name** of the alarm that acts to clear the current alarm.

Events

Use the **Events** tab in the **Alarms & Events** tab to access the event log, as well as the event logs for ExtremeCloud IQ Site Engine, legacy applications, and ExtremeControl Audit events and Wireless Audit events. In addition, you can access an event log for ExtremeCloud IQ Site Engine Scheduler events.



Use the drop-down list at the top of the table to filter events based on application:

- Selecting **Console** displays event logs with an **Event Type** of **Admin**, **Console**, and **Wireless**. Selecting Console View displays event logs with an **Event Type** of **Console** only.

  NOTE: Selecting both **Console** and **Console View** displays the event logs with an **Event Type** of **Console** twice.

- The ExtremeCloud IQ Site Engine event logs for ExtremeCloud IQ Site Engine and components (Console, Inventory, Policy, NAC Manager, and Wireless) present the same data as the event logs in the actual applications.
- The Access Control Audit event log provides information on Access Control Registration events such as when a device or user is added during the registration process, or an end-system is added/removed/updated via the registration administration web page.
- The Access Control Engine event log displays engine events.

NOTE: Installed certificates using an MD5 RSA signature algorithm now generate an event in ExtremeCloud IQ Site Engine version 7.

The Wireless Audit event log allows you to view the configuration activity on Wireless Manager.

The ExtremeAnalytics event log displays ExtremeAnalytics engine events as well and ExtremeAnalytics configuration activity.

The Scheduler event log displays events for the scheduled tasks configured via the Tasks tab. The event log includes task execution events and errors.

The Admin event log displays ExtremeCloud IQ Site Engine server and database administrative events, and ExtremeCloud IQ Site Engine user authentication and connection events. (In the legacy Console application, these events are included in the Console event log.)

You can manipulate the table data in several ways to customize the view for your own needs:

- Select the drop-down arrow to open the drop-down list and select an application to include in the Events table.
- Select the column headings to sort column data in ascending or descending order.
- Hide or display different columns by selecting a column heading drop-down arrow and selecting the column options from the menu.
- Select any row in the table to open a window that displays Event Details.

Event Log Column Definitions

Following are definitions of the Event Log table columns:

Severity — Indicates the potential impact of the event or trap. Hold the mouse pointer over a Severity icon to display a tool tip that provides the severity: Alert, Critical, Debug, Emergency, Error, Info, Notice, Warning. For traps, this column shows the Severity as defined in the `trapd.conf` file.

Event Type — Displays the application to which the event or trap is associated.

Category — Shows the category defined in the `trapd.conf` file for traps. For other events, it indicates the source of the information, either a Console Poller, local log, syslog, trap log, Error (java exceptions), etc.

Date/Time — Shows the date and time when an event or trap occurred.

Source — Shows the IP address of the host that was the source of the event or trap. If you want to display the source as a hostname (if available) you can set that option in the Suite-wide Alarm/Event Logs and Tables options.

Subcomponent — If the event or trap can identify a specific subcomponent of a device (or other source) which pinpoints the location of the problem, it is displayed here. One example of a subcomponent is an interface on a device.

Client — Displays the hostname of the source of the event.

User — The user that performed the action that triggered the event.

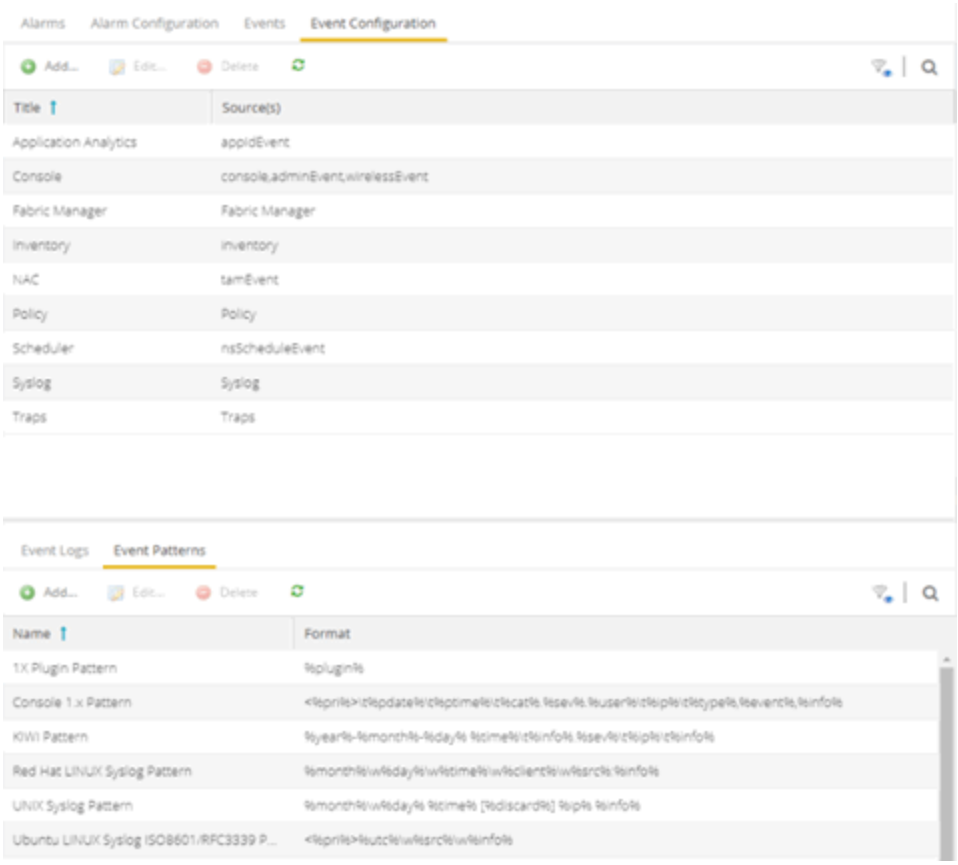
Type — Identifies the type of information for this row (event or trap).

Event — Shows the type of event or trap. For traps, this column shows the name of the event as defined in the `trapd.conf` file.

Information — Shows an summary explanation of the event or trap.

Event Configuration

Use the Event Configuration tab on the Alarms and Events tab to configure the source of information gathered in the event log, the name and location of the log file, and the format of the log pattern.



Buttons, Search Field, and Paging Toolbar

Filter

Use the filter functions to view, modify, apply, or remove filters from a table column. You can filter multiple columns in a table.

Search

The search tool enables you to search for full or partial matches on fields in the table.

Paging Toolbar Page 1 of 2

The paging toolbar provides four buttons that let you easily page through the table: first, previous, next, and last page.

Refresh 

Use the refresh button to update the data in the table.

Reset 

The reset button clears the search field and search results, clears all filters, and refreshes the table.

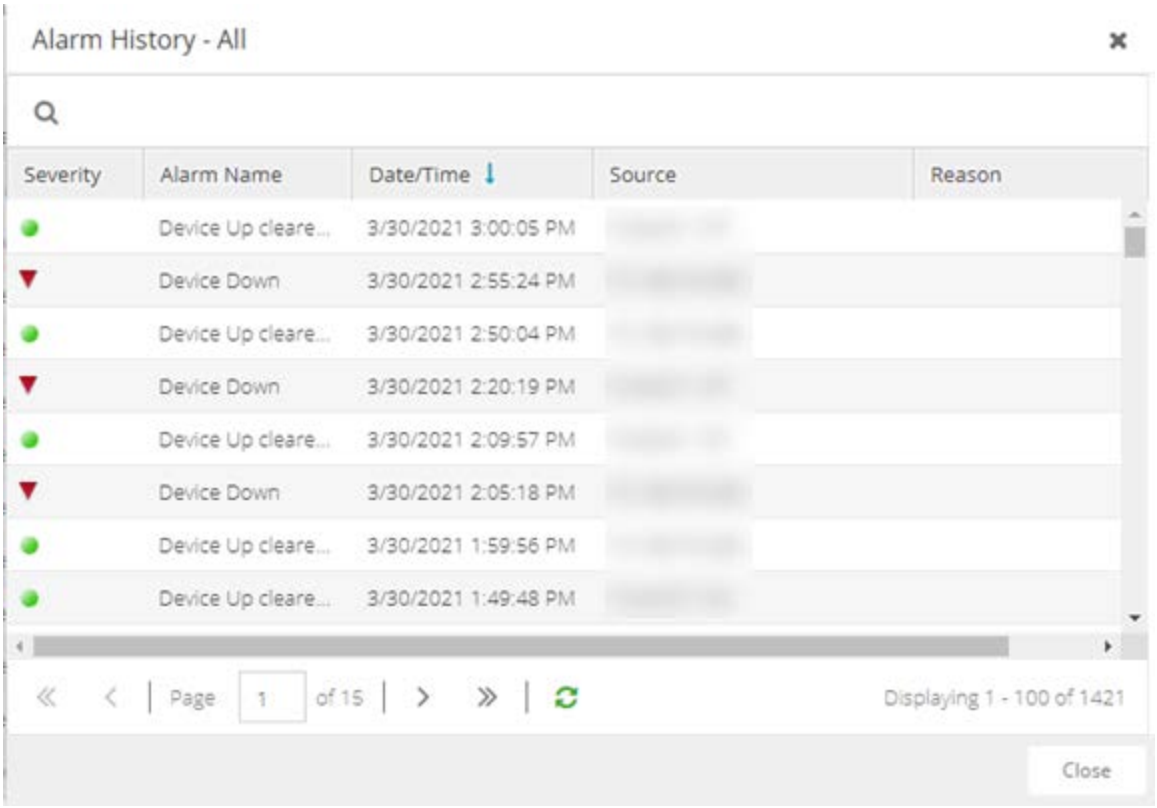
Alarm History

ExtremeCloud IQ Site Engine records alarm information whenever an alarm is raised and whenever an alarm is cleared. The alarm records display in the Alarm History window, allowing you to view information about current and past alarms.

If a triggering event is stored with a selected history record, you can view the event by selecting the View Trigger button. If there is no triggering event, the button is disabled. You can enable an option to preserve alarm triggering events and store them with the alarm history record in the Alarm History section of the Alarm Options (Administration > Options > Alarm).

Use the following instructions to access the Alarm History window from the Alarms tab:

1. Select the alarm in the table for which you want to view the alarm history.
2. Select the **Menu** icon (☰).
3. Select the criteria by which the alarm history is displayed from the **Menu** drop-down list:
    a. Select **Alarm History** > **All** to view the Alarm History for all devices, regardless of the current alarm selection.
    b. Select **Alarm History** > **By Source** to view the Alarm History for that device. If the Source includes a subcomponent (such as an interface on the device), then the alarm history is specific to that subcomponent.
    c. Select **Alarm History** > **By Alarm Name** to view the Alarm History for a specific alarm.



Severity — The icons indicate the seriousness of an alarm definition. This column displays its own specified severity, regardless of the severity of the event or trap that triggered it.

- (question mark) Set from Source — the alarm definition uses the severity level of the trigger event, for example a warning event.
- (Red) Critical — A problem with significant implications.
- (Orange) Error — A problem with limited implications.
- (Yellow) Warning — A condition that might lead to a problem.
- (Blue) Info — Information only; not a problem.
- (Green) Clear — An alarm that clears another alarm (for example, LinkUp).

Alarm Name — The name of the alarm definition.

Date/Time — The date and time the alarm occurred.

Last Seen — The date and time the alarm last occurred.

Source — The IP address and port (if applicable) of the device on which the alarm occurred.

Host Name — The Host Name of the device on which the alarm occurred, if configured.

Subcomponent — The specific component on the device that caused the alarm to occur (for example, a port name).

Reason — The information entered in the **Clear Alarm(s) Reason** window by a user when manually clearing an alarm. To manually clear an alarm from the **Alarms & Events** > **Alarms** tab, select the **Menu** icon (), then select **Clear Selected Alarm(s) w/ Reason**.

Information — Additional details about the alarm.

Cleared Name — The name of the alarm that occurred and is now cleared.

Seen Count — The number of times the alarm occurred on the device.

First Seen — The date and time the alarm first occurred.

Action — The icons indicate the actions performed when the alert occured:

-  — Alarm is raised by ExtremeCloud IQ Site Engine.
-  — Alarm is cleared by a user.
-  — Alarm is cleared automatically by ExtremeCloud IQ Site Engine.

Triggering Event — The event or trap that caused the alarm to occur.

Alarm Limits

To configure alarm action limits on an alarm (in the **Actions** tab of the **Alarm Configuration** window), right-click on an alarm history record and select **Alarm Limits** to open the **Alarm Tracking Information** window. This window displays the configured action limit, the number of times the action has been taken (Total Count), the number of times the action has been taken since the last reset, and the time of the next reset. You can also manually reset the alarm limit count using the **Reset Count** button. This resets the count for only this alarm on only this device or interface.

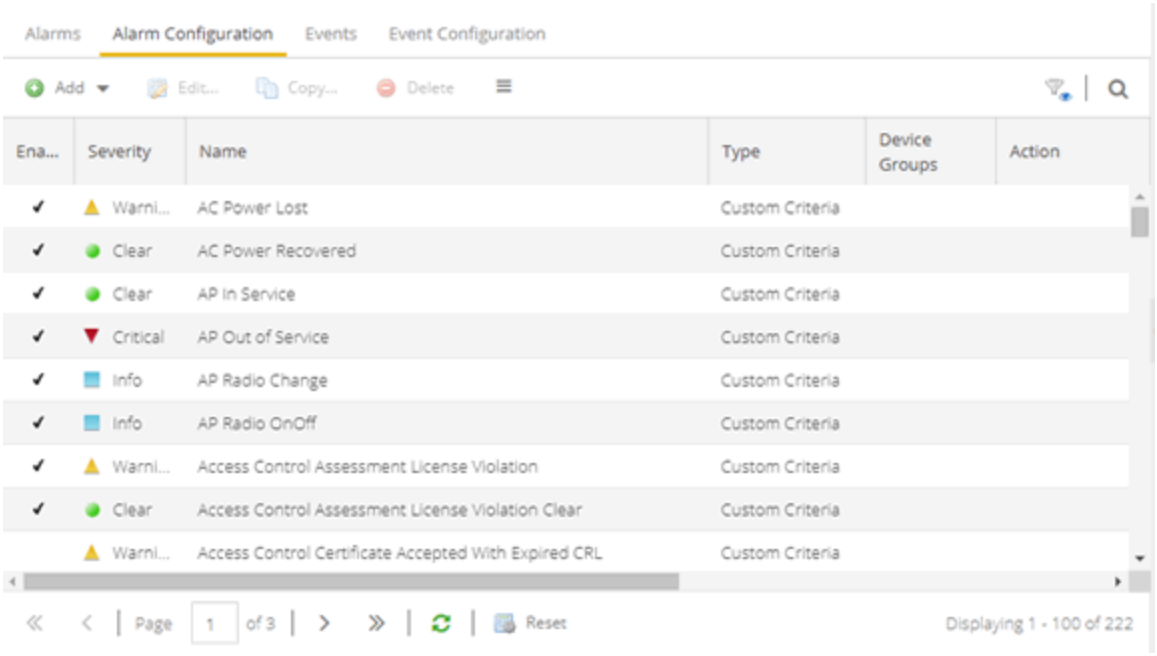
Alarm History Options

Change certain alarm history parameters in the Alarm History section of the Alarm options (**Administration** > **Options** > **Alarm**).

- By default, the alarm history is maintained for 14 days. You can change the number of days in the options.
- By default, a history record is created the first time an alarm is raised on a device or interface, and also when it is cleared. Select **Enable Detailed Alarm History** in **Administration** > **Options** > **Alarm** so that repeat occurrences of an alarm being raised are also recorded.
- You can enable an option to preserve alarm triggering events, so that any triggering events are stored with the alarm history record. If a triggering event is stored with the currently selected history record, you can view the event by selecting the View Trigger button in the Alarm History window. If there is no triggering event, the button is disabled.

How to Configure Alarms

Use the **Alarm Configuration** tab to configure network alarms that provide status information for a particular problem or condition on a particular network device. Alarms are triggered when certain trap or event conditions (called a trigger event) occur on your network, and they are tracked until the problem or condition is removed.



The alarm source, which is the device, interface, or AP that is the source of the trigger event, is considered to have an alarm until the alarm is cleared. You can view alarms and alarm status and clear alarms in the **Alarms & Events** > **Alarms** tab in ExtremeCloud IQ Site Engine. Using the **Alarm Configuration** tab, you can add a new alarm definition, which includes configuring the conditions (criteria) that triggers the alarm, and defining the actions performed to notify a person or network component about the problem, when the alarm is triggered.

You can create an alarm definition that detects a problem or condition and raises an alarm, and create an alarm definition that detects when the problem or condition is removed and clears the alarm. For example, a Device Down alarm is triggered when contact with a device is lost. Then, when contact is established with the device, the Device Up alarm automatically clears the Device Down alarm.

ExtremeCloud IQ Site Engine ships with a set of default alarm definitions, which you can see listed in the **Alarms** tab. You can use these default alarms as is, or enable, disable, delete or modify them, as desired.

This Help topic includes instructions for:

- Defining an Alarm
- Configuring Alarm Actions

- Copying an Alarm
- Disabling Alarms
- Deleting Alarms
- Configuring Email Settings
- Resetting Alarm Action Limits
- Enabling/Disabling All
- Restoring Default Alarms
- Viewing Alarms
- Clearing Alarms

Defining an Alarm

Use the **Alarm Configuration** tab to create new alarm definitions and define their criteria and actions, and to edit the criteria and actions for existing alarms.

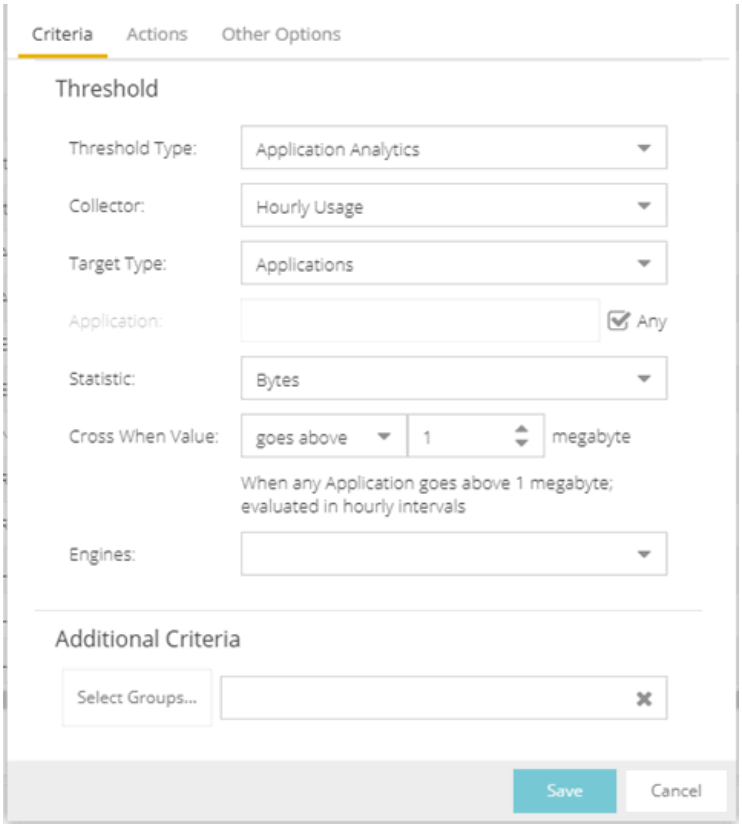
There are six types of alarms, each using different criteria to establish the alarm definition.

- **Custom Criteria Alarm** — Triggers an alarm when very specific criteria you define is met.
- **Flow Alarm** — Flow alarms are used for reporting network traffic flow anomalies detected by the NetFlow flow collector. An alarm triggers when a flow matches criteria you configure.
- **Selected Trap Alarm** — Triggers an alarm when a specific trap occurs. You are able to select from all the Trap IDs available for the devices modeled in the ExtremeCloud IQ Site Engine database.
- **Severity Alarm** — Triggers an alarm when an event or trap occurs to which you assign a specific level of severity. Select an event severity level (Emergency, Alert, Critical, Error, Warning, Notice, or Info) and whether the alarm is triggered by traps, or events, or both.
- **Status Change Alarm** — Triggers an alarm when the operational status for a device changes: **Contact Lost** triggers the alarm when contact with a device is lost, **Contact Established** triggers the alarm when contact is restored, and **Both** triggers the alarm when contact is lost and when contact is restored.
- **Threshold Alarm** — Triggers the alarm when a specified value enters a defined range. For example, when CPU utilization exceeds 80% or when free disk space falls below 100 MB. There are two threshold alarm types: OneView and ExtremeAnalytics. This option is disabled if your ExtremeCloud IQ Site Engine license does not include ExtremeCloud IQ Site Engine features that support threshold alarms (such as device statistics collection) and you do not have an ExtremeAnalytics license.

To create a new alarm definition:

1. Select the **Add** button and select the type of Alarm you are creating from the drop-down list. The **Create Alarm Definition** window opens.
2. Enter a name for your new alarm definition in the **Name** field.
3. Select the appropriate severity level of the alarm definition in the **Severity** drop-down list. The alarm can have its own specified severity regardless of the severity of the event or trap from which it is triggered.
    - (question mark) Set from Source — the alarm uses the severity level of the trigger event, for example a warning event.
    - (Red) Critical — A problem with significant implications.
    - (Orange) Error — A problem with limited implications.
    - (Yellow) Warning — A condition that might lead to a problem.
    - (Blue) Info — Information only; not a problem.
    - (Green) Clear — An alarm that clears another alarm (for example, Device Up).
4. Select the **Enabled** checkbox to activate the alarm definition. You can disable an alarm definition to deactivate it without deleting the definition.
5. Enter the criteria that triggers the alarm. Options in the **Criteria** tab vary depending on the type of alarm you are creating.

    Selected Trap Alarm



a. Select the **Select Traps** button. The Select Traps window opens.

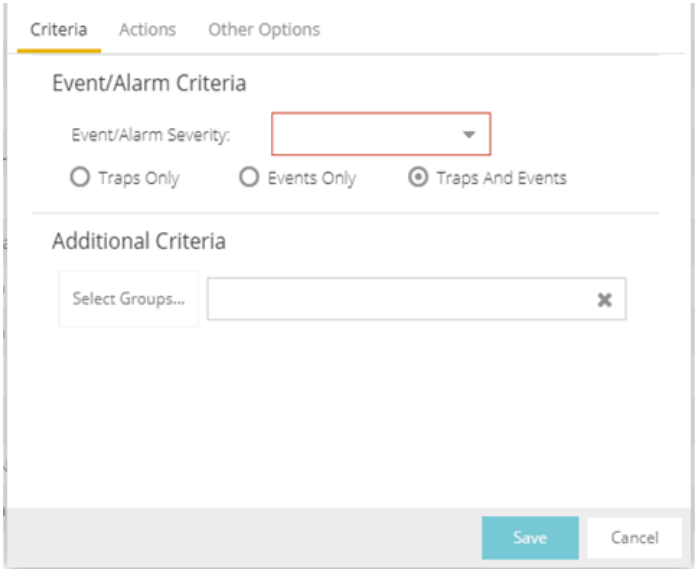
b. Select the traps that trigger the alarm.

c. Select **Save**.

d. Select **Select Groups** if the alarm only applies to a specific group of devices. Select the groups of devices in the Alarm Group Selection window and select **OK**. Not selecting any device groups means the alarm applies to all devices.

e. Select the **Actions** tab to configure the actions performed when the alarm is triggered.

Severity Alarm



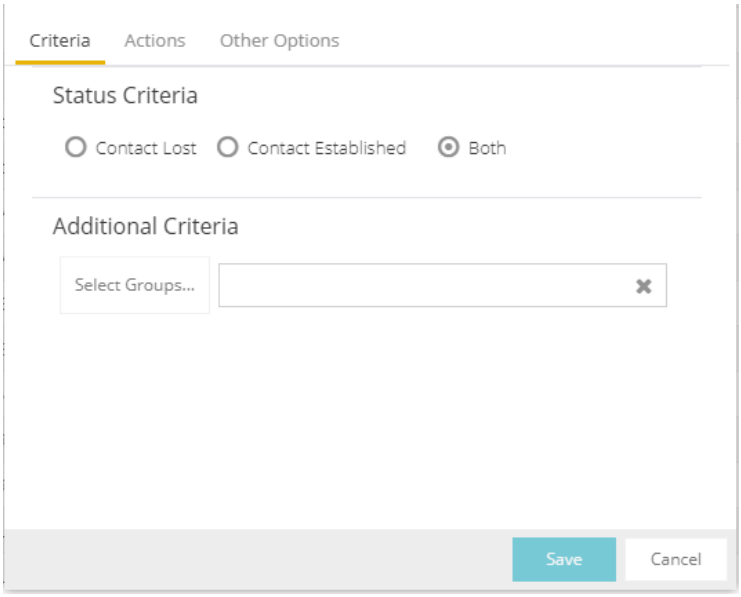
a. Select the severity of the event or trap required to generate the alarm from the drop-down list (Emergency, Alert, Critical, Error, Warning, Notice, or Info). Traps or Events that occur and match the severity in this drop-down list trigger the alarm. For example, you can create a severity alarm with a **Severity** of **Error** that is triggered when a trap or event occurs with an **Event/Alarm Severity** of **Alert**.

b. Select whether the alarm is triggered by traps, or events, or both.

c. Select **Select Groups** if the alarm only applies to a specific group of devices. Select the groups of devices in the Alarm Group Selection window and select **OK**. Not selecting any device groups means the alarm applies to all devices.

d. Select the **Actions** tab to configure the actions performed when the alarm is triggered.

Status Change Alarm

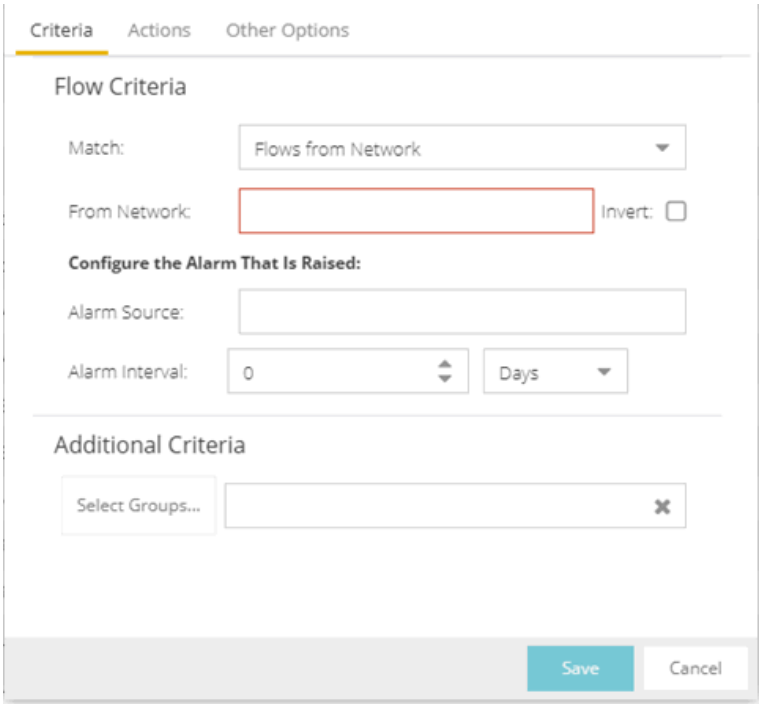


a. Select whether the alarm triggers when contact with a device is lost (Contact Lost), restored (**Contact Established**), or when contact is lost and when contact is regained (**Both**).

b. Select **Select Groups** if the alarm only applies to a specific group of devices. Select the groups of devices in the Alarm Group Selection window and select **OK**. Not selecting any device groups means the alarm applies to all devices.

c. Select the **Actions** tab to configure the actions performed when the alarm is triggered.

Flow Alarm



a. Select how the flow is matched to trigger a flow alarm in the **Match** drop-down list. Flow alarms are used for reporting network traffic flow anomalies detected by the NetFlow flow collector. NetFlow is a flow-based data collection protocol that provides information about the packet flows being sent over a network. K-Series, S-Series, and N-Series devices support NetFlow flow collection.

   Flows from Network — Match a flow's source IP address to the specified network.

   Flows to Network — Match a flow's destination IP address to the specified network.

   Flows from Network from Port — Match a flow's source IP address and port number to the specified network and port.

   Flows from Port to Network — Match a flow's source port number and destination IP address to the specified port and network.

   Flows from Network with low TTL — Match a flow's source IP address and TTL value to the specified network and the TTL at or below value.

b. Enter the **Network** or **Port** monitored by the flow alarm

   From/To Network — A network is identified as a set of IP masks. The mask is used as a filter to define a range of IP addresses. Masks can be entered in CIDR or dotted-decimal format.

      CIDR — CIDR format uses a slash followed by a number between 8 and 32, to define the number of contiguous, left-most "one" bits that define the network mask. For

example, */16* indicates a 16-bit mask. Here is an example of a From/To Network value using the CIDR format:
10.20.0.0/16,10.20.0.0/24

Dotted-Decimal — Dotted decimal format represents network masks as four octets separated by periods. For example, a 16-bit mask in dotted decimal notation is *255.255.0.0*. Here is an example of a From/To Network value using the dotted-decimal format:
10.20.0.0/255.255.0.0,10.20.88.0/255.255.255.0

For example, if you entered either 10.20.0.0/16 (CIDR) or 10.20.0.0/255.255.0.0 (Dotted-Decimal) in the From/To Network field, then all incoming packets in the range 10.20.00.00 through 10.20.255.255 would result in an address match.

From Port — Enter the port number to be matched.

TTL at or below — Enter a value that triggers an alarm when the TTL value in the packet's TTL field is equal to or less than the value entered.

Select the Invert checkbox if you want the flow criteria to trigger the alarm when it does not match the specified values.

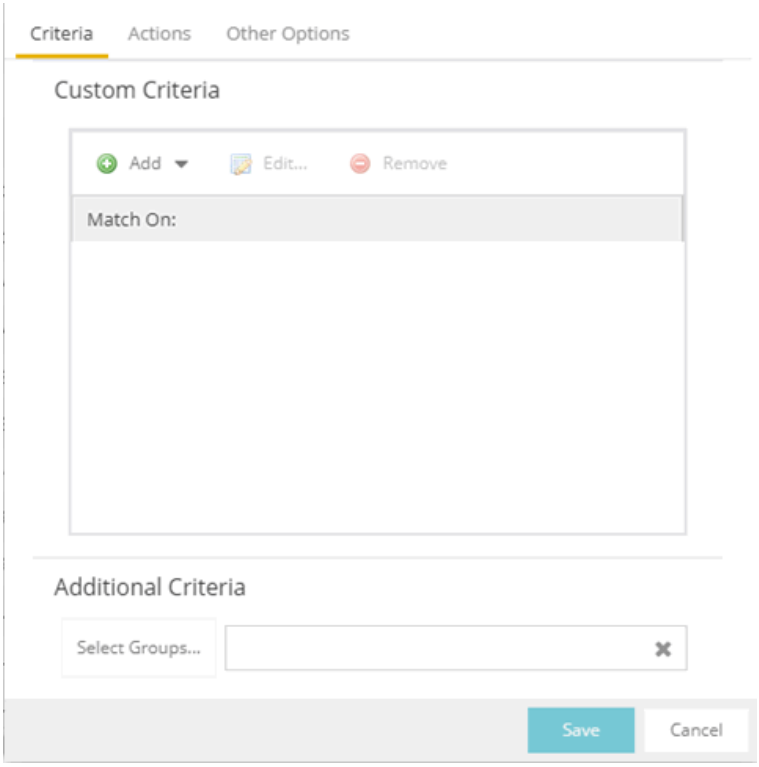
c. Enter a phrase in the **Alarm Source** field used as the source of the alarm.

d. Enter the amount of time, in minutes, hours, or days that must pass until the alarm can trigger again in the **Time until alarm can be raised again** field. This prevents a large number of alarms being triggered, if many flows match the alarm criteria. If you select **Never**, the alarm only triggers one time. After you manually clear the alarm, it can be triggered again.

e. Select **Select Groups** if the alarm only applies to a specific group of devices. Select the groups of devices in the Alarm Group Selection window and select **OK**. Not selecting any device groups means the alarm applies to all devices.

f. Select the **Actions** tab to configure the actions performed when the alarm is triggered.

Custom Criteria Alarm



a. Select the **Add** drop-down list and select the criteria by which the alarm triggers.

Severity Criteria — Select one or more severity levels against which to match.

Match Selected — The reported Severity is matched against any of the Severity levels selected in the list.

Exclude Selected — The reported Severity matches if it is not one of the Severity levels selected in the list.

Category Criteria — Select one or more event categories to match against the Category column of the event. An event category is a way to group related events. For example, all events related to device discovery would be in the "Discover" category.

Match Selected — The reported Category is matched against any of the categories selected in the list.

Exclude Selected — The reported Category matches if it is not one of the categories selected in the list.

Type Criteria — Select one or more message types (Event, Inform, Trap) to match against the Type column of the event.

Match Selected — The reported Type is matched against any of the types selected in the list.

Exclude Selected — The reported Type matches if it is not one of the message types selected in the list.

Event Criteria — Select one or more event types to match against the Event column of the event.

Match Selected — The reported Event is matched against any of the event types selected in the list.

Exclude Selected — The reported Event matches if it is not one of the event types selected in the list.

Host or IP Criteria — Select one or more host names or IP/Subnet addresses to match against the value of the address appearing in the Source column of the event. The list of host names and IP/ Subnet addresses can be edited by selecting the **Edit List** button.

Match Selected — The reported host name or IP/Subnet address is matched against any of the host or IP/Subnets selected in the list.

Exclude Selected — The reported host name or IP/Subnet address matches if it is not one of the host or IP/Subnets selected in the list.

Log Criteria — Select one or more Event Logs against which to match.

Match Selected — The log where the event was received is matched against any of the logs selected in the list.

Exclude Selected — The log where the event was received matches if it is not one of the logs selected in the list.

Information Criteria — Select one or more text strings (phrases) to match against text in the Information column of the event or trap. The list of text phrases can be edited by selecting the **Edit List** button.

Match Selected — The information text string is matched against one or more phrase selected from the list.

Exclude Selected — The information text string matches if it is not one of the phrases selected from the list.

NOTE:

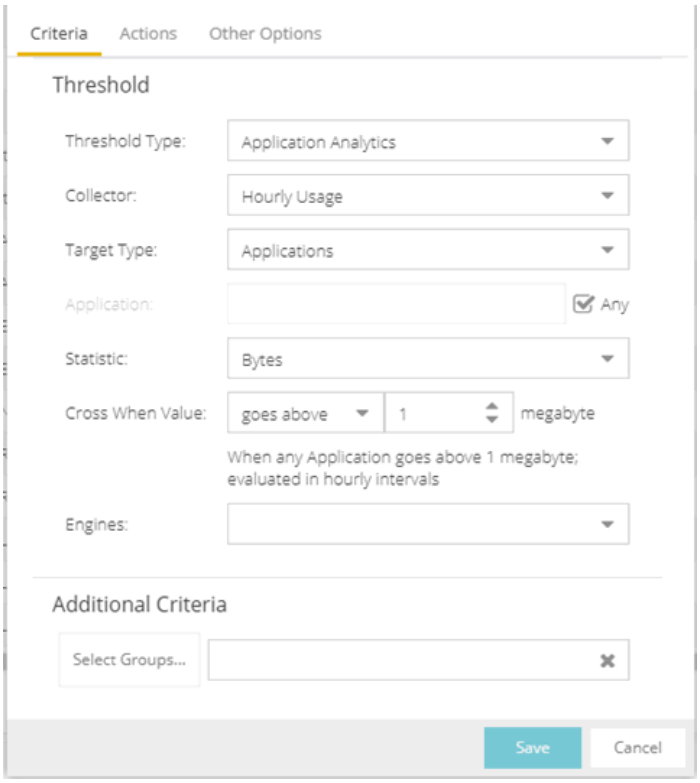
Each information phrase is interpreted as a regular expression compatible with TCL 8.1. Non-alphanumeric symbols such as the plus sign (+), the comma (,), the asterisk (*), the caret (^), and the dollar sign ($) are interpreted with their TCL regular expression meaning.

If you are configuring an alarm to catch messages that contain symbols used in regular expressions, you must escape the symbols with a backslash when adding a text phrase entry in ExtremeCloud IQ Site Engine. For example:
\+
\,
*
\^
\$

b. Select **Select Groups** if the alarm only applies to a specific group of devices. Select the groups of devices in the Alarm Group Selection window and select **OK**. Not selecting any device groups means the alarm applies to all devices.

c. Select the **Actions** tab to configure the actions performed when the alarm is triggered.

6. **Threshold Alarm**



a. Select a **Threshold Type**.

   OneView — The ExtremeCloud IQ Site Engine (formerly OneView) Collector gathers historical reporting data over time, which is then used in ExtremeCloud IQ Site Engine reports. Threshold alarms are raised when the reporting data matches a threshold alarm criteria.

   ExtremeAnalytics — The ExtremeAnalytics engine generates ExtremeAnalytics threshold alarms as part of the application usage collection process. Threshold alarms are raised when hourly or high-rate usage data matches a threshold alarm criteria. Each target record produced on the ExtremeAnalytics engine is evaluated at the end of each collection interval to see if it matches alarm criteria. If a statistic has crossed a configured threshold, an alarm in raised. Alarms can track single target types as well as target combinations. They can reference specific targets, for example a specific application such as Facebook, or they can reference all the targets in a target type, for example all applications. Only the target types and target combinations that are collected by ExtremeAnalytics can be used in alarms.

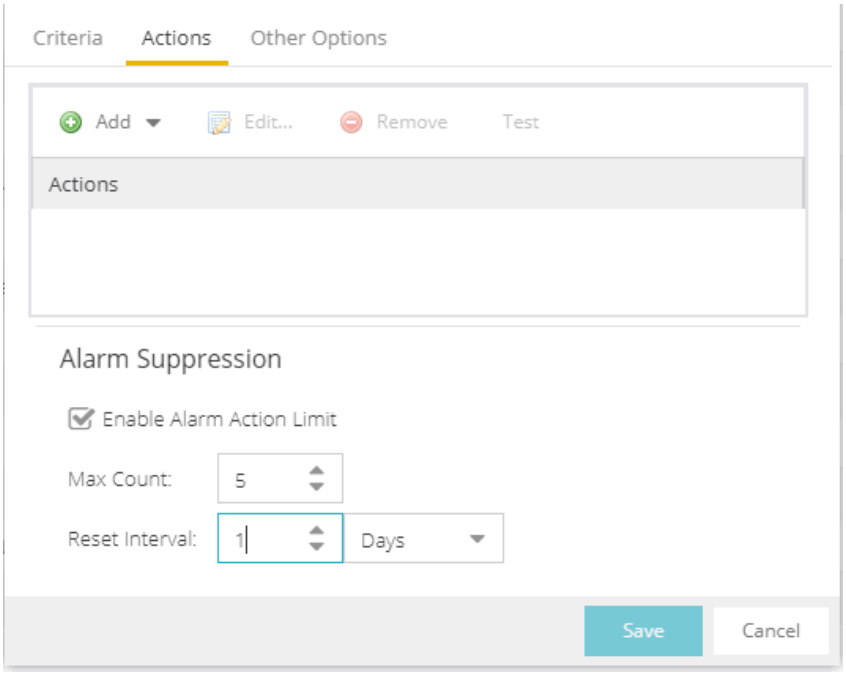
b. Select the criteria against which the threshold is compared.

c. Enter the threshold value. When the value crosses the established threshold for the criteria you select, the alarm triggers.

d. Select **Select Groups** if the alarm only applies to a specific group of devices. Select the groups of devices in the Alarm Group Selection window and select **OK**. Not selecting any device groups means the alarm applies to all devices.

e. Select the **Actions** tab to configure the actions performed when the alarm is triggered.

7. Select the **Add** drop-down list to select the actions performed when the alarm is triggered.



Add Email Action — Sends an email when the alarm is triggered. Use the **Destination** drop-down list to select one of your pre-defined email lists. ExtremeCloud IQ Site Engine comes preloaded with a default email list called Helpdesk. You can rename this list, but it cannot be deleted. Select the **Edit Email Lists** button to define a new list. Use semicolons or commas to separate individual email addresses, but do not include spaces. (You must have your SMTP E-Mail Server options configured.) There are default formats for the subject and body of the email you can override by selecting the **Override Content** checkbox. You can view a list of alarm keywords by selecting **Show Keywords**. Select the **Save** button to save the email action to the list of actions for the alarm definition.

Add Syslog Action — Creates a syslog message when the alarm is triggered. Enter the IP address or hostname that identifies the syslog server where the message is sent. There is a default format for the syslog message sent to the server you can override by selecting the **Override Content** checkbox. You can view a list of alarm keywords by selecting **Show Keywords**. Select the **Save** button to save the syslog action to the list of actions for the alarm definition.

Add Trap Action — Sends an SNMP trap when the alarm is triggered. Enter the IP address for a trap receiver where the trap is sent in the **Trap Server** field. Valid trap receivers are systems running an SNMP Trap Service. From the **Credential** drop-down list, select the appropriate SNMP credential to use when sending the trap to the trap receiver. Credentials are defined in the **Profiles/Credentials** tab in the Authorization/Device Access window (Tools > Authorization/Device Access). There is a default format for the trap message you can

override by selecting the **Override Content** checkbox. You can view a list of alarm keywords by selecting **Show Keywords**. Select the **Save** button to save the trap action to the list of actions for the alarm definition.

Add Custom Action — Runs a custom program or script on the ExtremeCloud IQ Site Engine Server when the alarm is triggered. In the **Program** field, enter the name of the program. In the **Working Directory** field, enter the path to the directory from which the program is executed. Any path references within your program that are not absolute paths, are relative to the working directory. There is a default set of arguments passed to the program you can override by selecting the **Override Content** checkbox. You can view a list of alarm keywords by selecting **Show Keywords**. Keywords are used to override content, or a custom action. Select the **Save** button to save the email action to the list of actions for the alarm definition.

Add Task Action — Select to configure a workflow task to run when the event triggers the alarm. From the **Tasks** drop-down menu, choose from the list of workflows which have been configured to be available as Alarm Actions.

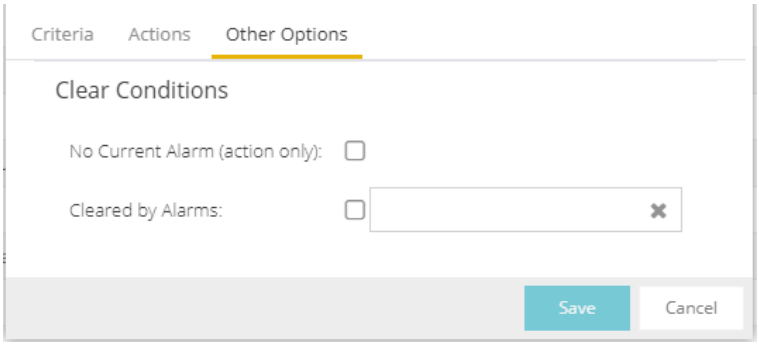
External Workflow Action — Runs a workflow action configured via a third-party application, such as StackStorm, when the alarm is triggered. Select **External Workflow Action** and then select a third-party application workflow.

If you want to set a limit on the number of times the system performs the alarm action for this alarm, check **Enable Alarm Action Limit** and type a number into the **Max Count** field. When the limit is reached, the alarm is still recorded, but no further actions are performed. If you have configured multiple action types, the limit is for the number of times the set of configured actions is performed, not for each individual action. Each alarm source has its own action count for an alarm, so when the **Max Count** limit is reached for one alarm source, actions can still occur for other alarms from that alarm source as well as for other alarm sources. If **Save** is not checked, there is no limit placed on the number of times the action is performed.

You can specify a **Reset Interval**, which automatically resets the action count after the time limit specified, allowing actions to resume for that alarm source. If the reset interval is set to **None**, then when the alarm limit is reached, the alarm does not reset unless manually reset.

You can test an alarm action by selecting the **Test** button. (You must save an alarm before you can test it.) You can also override the action.

8. In the **Other Options** subtab, select how you want to clear the alarm.



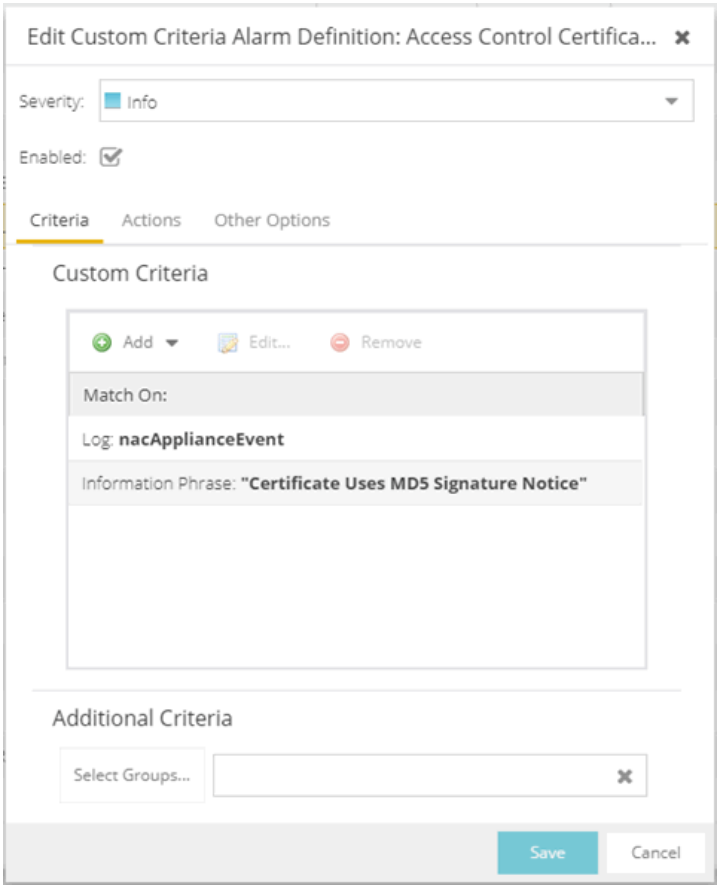
No Current Alarm (action only) — When this option is selected, the trigger event causes the system to perform the configured actions, but does not raise an alarm that becomes associated with the alarm source. The alarm status of the alarm source does not change, and no alarm is added to the system.

Cleared by Alarm — This option allows you to select the alarm(s) used to clear the alarm you are defining. You must first create the alarm definitions for the clearing alarms, which must have the alarm severity set to "Clear". The clearing alarms are triggered when the problem or condition is removed. Then, use the Select Alarms button to open a window to select one or more clearing alarms that clear the alarm you are defining.

9. Select **Save** to create the alarm and close the Alarm Configuration window.

To modify an existing alarm:

1. In the Alarm Configurations view, select the alarm definition you want to change.
2. Select the Alarm Definition. You can also select the **Edit** button or right-click the alarm definition, and select **Edit**. The Alarm Configuration window opens.



3. Edit the necessary fields. For additional information, see To create a new alarm definition.
4. Select **Save** to edit the alarm definition and close the Alarm Configuration window.

Copying an Alarm

You can also copy and modify existing alarm definitions using the **Alarm Configuration**. This provides you with a template from which to configure a new alarm.

To copy an alarm, right-click the alarm and select **Copy** to open the Copy Alarm Definition window. Enter a unique name for the new alarm and select **OK**. You can then edit the alarm to the desired configuration.

Disabling Alarms

There can be times when you want to disable an alarm definition without deleting it. For example, you might want to temporarily disable a Device Down alarm definition while you are performing maintenance on that device.

To disable an alarm, open the Alarm Configuration view, right-click the alarm you want to disable, and select **Disable**.

Deleting Alarms

To completely remove an alarm definition you no longer use, you can delete the alarm definition from ExtremeCloud IQ Site Engine.

To delete an alarm, open the Alarm Configuration view, select the alarm definition you want to delete, and select the **Delete** button.

Configuring Email Settings

From the **Alarm Configuration** tab, you can configure or edit the email address or email list to which alarm information is sent for an alarm definition when the alarm is triggered.

To configure the email address or email list to which alarm information is sent, open the **Alarm Configuration** tab, select the alarm definition for which you want to configure or change the email settings, select the **Menu** icon (☰) or right-click the alarm definition and select the **Edit** button. Email actions are configured on the **Actions** tab of the **Alarm Configuration** window.

NOTE: When creating a list of email addresses, use semicolons to separate different addresses.

Resetting Alarm Action Limits

When an action limit is reached for an alarm, the action no longer occurs when an alarm triggers. From the **Alarm Configuration** tab, you can reset the action limits for your alarms so the actions occur when an alarm is triggered.

To reset the action limits, open the **Alarm Configuration** tab, select the alarm definition for which you want to reset the action limits, select the **Menu** icon (☰) or right-click the alarm definition and select **Reset Alarm Action Limits**.

Enabling/Disabling All

From the **Alarm Configuration** tab, you can enable or disable all of your alarms at one time.

To enable or disable all of your alarms, open the **Alarm Configuration** tab, select the **Menu** icon (☰), and select **Enable All** or **Disable All**, respectively.

Restoring Default Alarms

From the **Alarm Configuration** tab, you can restore the default alarms that you delete or modify.

To restore the default alarms, open the **Alarm Configuration** tab, select the **Menu** icon (☰), and select **Restore Default Alarms**.

NOTE: The time required to restore default alarms can vary. When the process is complete, you are notified by a confirmation window.

Viewing Alarms

You can view device/alarm status in multiple places throughout ExtremeCloud IQ Site Engine.

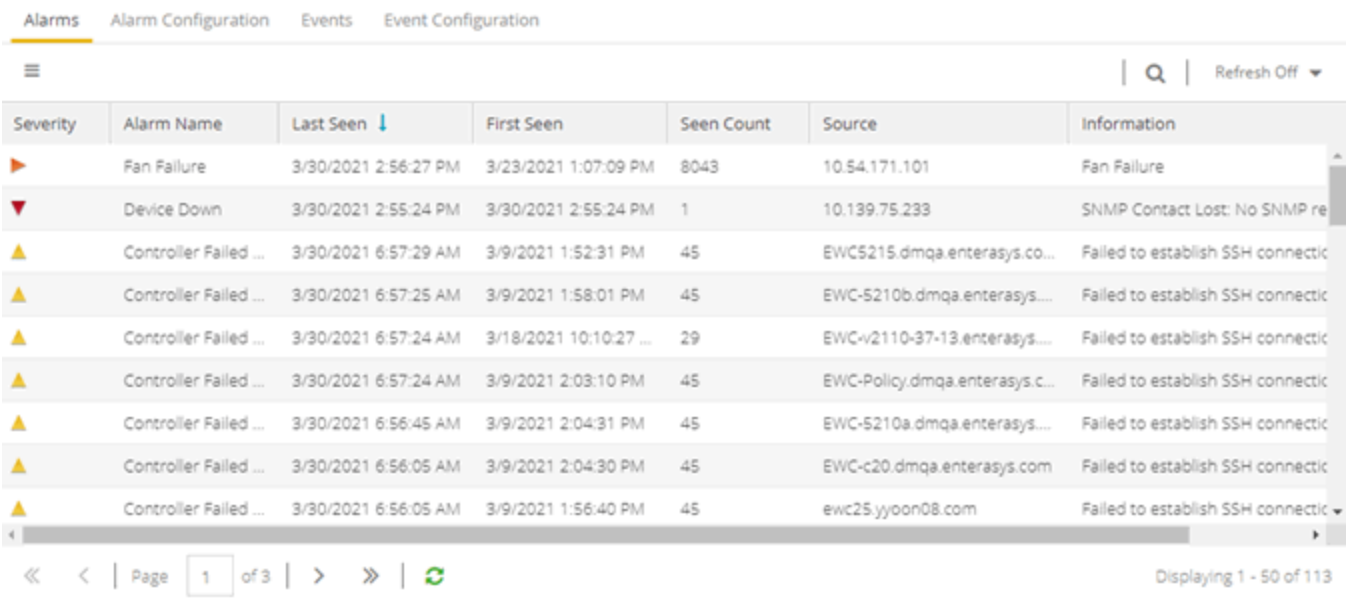
ExtremeCloud IQ Site Engine

Every ExtremeCloud IQ Site Engine page includes a system-wide Alarm Summary in the lower right corner. This indicates the number of current alarms for each severity (Critical, Error, Warning, and Info) that is present in the entire system. If there are no current alarms, the status displays all zeroes. Select an indicator to open the **Alarms** tab filtered to display the alarms of that severity.



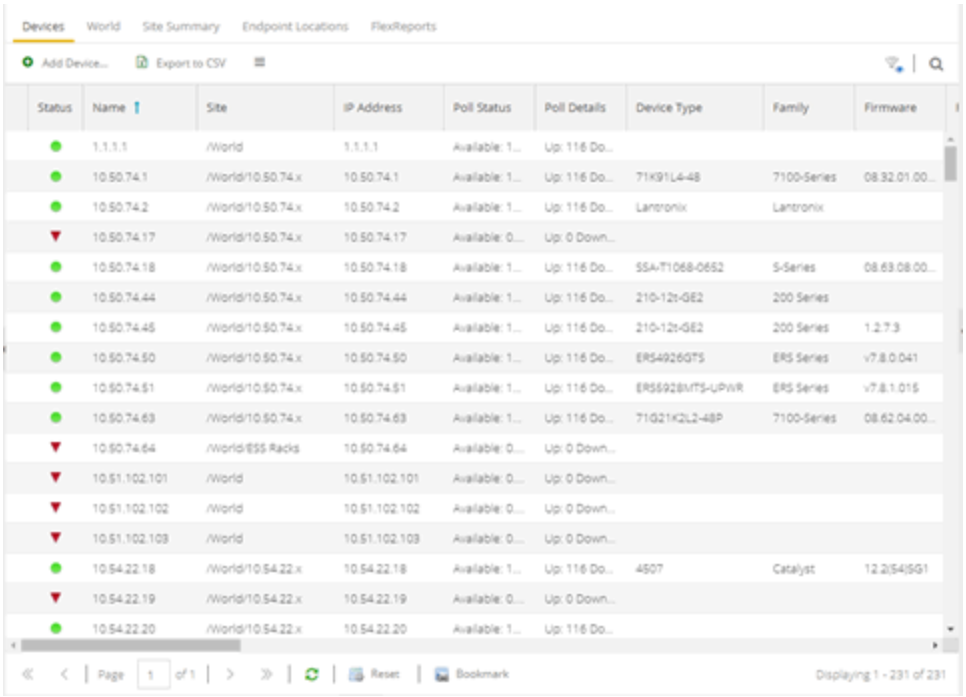
Alarms & Events Tab

View current alarm information in the **Alarms & Events** > **Alarms** tab. Use the configuration menu button or right-click on an alarm to clear the selected alarm or all alarms. If desired, you can supply a reason you cleared the alarm, which is recorded in the Alarm History.

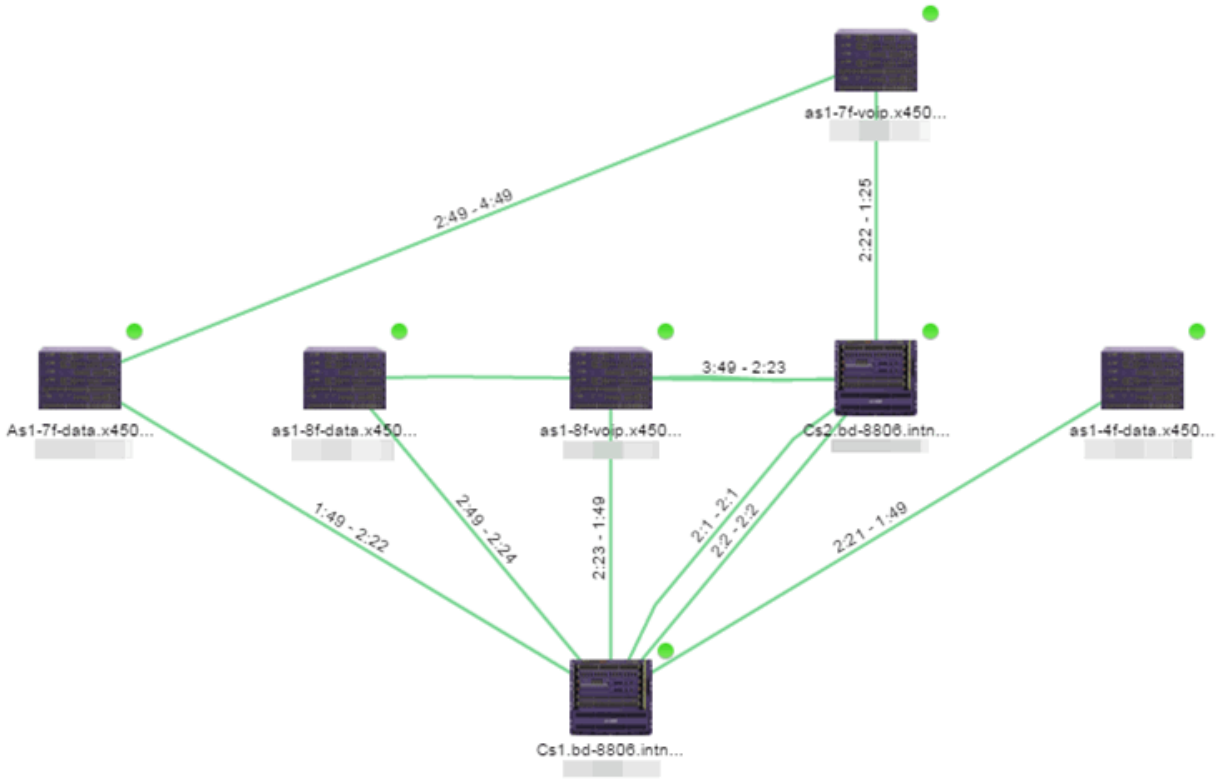


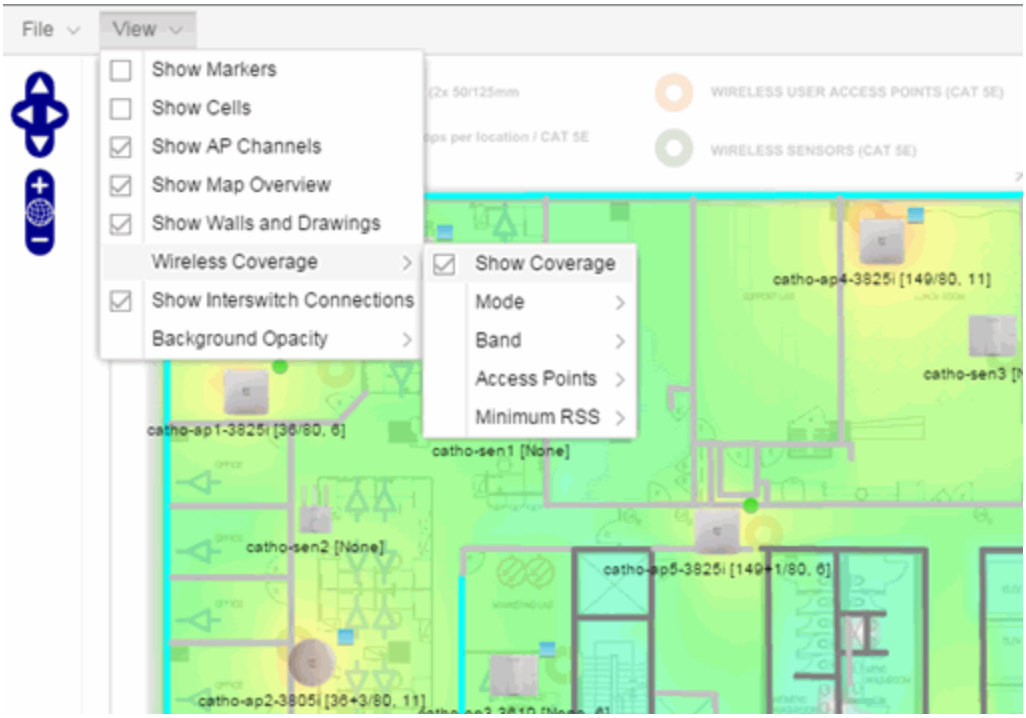
Network Tab

View the alarm status for a device in the **Status** column from within the My Network navigation tree on the **Network** tab. The colored circle indicates the severity of the most severe alarm on the device. A green icon indicates that there are no alarms and the device is up. A red icon indicates a critical alarm or the device is down. Select the **Status** icon to open a new page with detailed information about the alarms for that device. For additional information, see Network tab help topic.



View the alarm status for a device in device maps, found in the World map navigation tree. Topology and geographic maps show the status of devices in your network and floor plans show the status of wireless access points. As with devices in the My Network navigation tree, the colored circle associated with a device or access point in a map indicates the severity of the most severe alarm on the device. For additional information, see View and Search Maps.


as1-7f-voip.x450...
2:49 - 4:49
2:22 - 1:25
3:49 - 2:23
As1-7f-data.x450...
as1-8f-data.x450...
as1-8f-voip.x450...
Cs2.bd-8806.intn...
as1-4f-data.x450...
1:49 - 2:22
2:49 - 2:24
2:23 - 1:49
2:1 - 2:1
2:2 - 2:2
2:21 - 1:49
Cs1.bd-8806.intn...


File
View
Show Markers
Show Cells
Show AP Channels
Show Map Overview
Show Walls and Drawings
Wireless Coverage
Show Interswitch Connections
Background Opacity
Show Coverage
Mode
Band
Access Points
Minimum RSS
WIRELESS USER ACCESS POINTS (CAT 5E)
WIRELESS SENSORS (CAT 5E)
catho-ap4-3825i [149/80, 11]
catho-ap1-3825i [36/80, 6]
catho-sen1 [None]
catho-sen2 [None]
catho-ap5-3825i [149+1/80, 6]
catho-ap2-3805i [36+3/80, 11]

Clearing Alarms

An alarm can be cleared manually or automatically.

To clear an alarm manually:

In the **Alarms & Events** > **Alarms** tab, **Menu** icon (☰) in the upper left corner or right-click on an alarm to clear the selected alarm or all alarms. If desired, you can supply a reason that the alarm was cleared, which is recorded in the Alarm History.

To clear an alarm automatically:

An alarm is cleared automatically by another alarm called a "Clearing Alarm". For example, you can create a Device Up alarm so that when contact is established with a device, the alarm automatically clears a Device Down alarm.

Clearing Alarms are configured in the Alarm Configuration window with an **Alarm Severity** set to **Clear**. The alarm is defined so that when it is triggered, it removes an alarm rather than adds one.

Buttons, Search Field, and Paging Toolbar

Filter 

Use the filter functions to view, modify, apply, or remove filters from a table column. You can filter multiple columns in a table.

Search 

The search tool enables you to search for full or partial matches on fields in the table.

Paging Toolbar 

The paging toolbar provides four buttons that let you easily page through the table: first, previous, next, and last page.

Refresh 

Use the refresh button to update the data in the table.

Reset 

The reset button clears the search field and search results, clears all filters, and refreshes the table.

Event Configuration Tab

Use the **Event Configuration** tab to display the event types used in the **Events** tab. Additionally use the tab to add, edit, or delete those event types, which allows you to filter events in the event log based on event types you define.

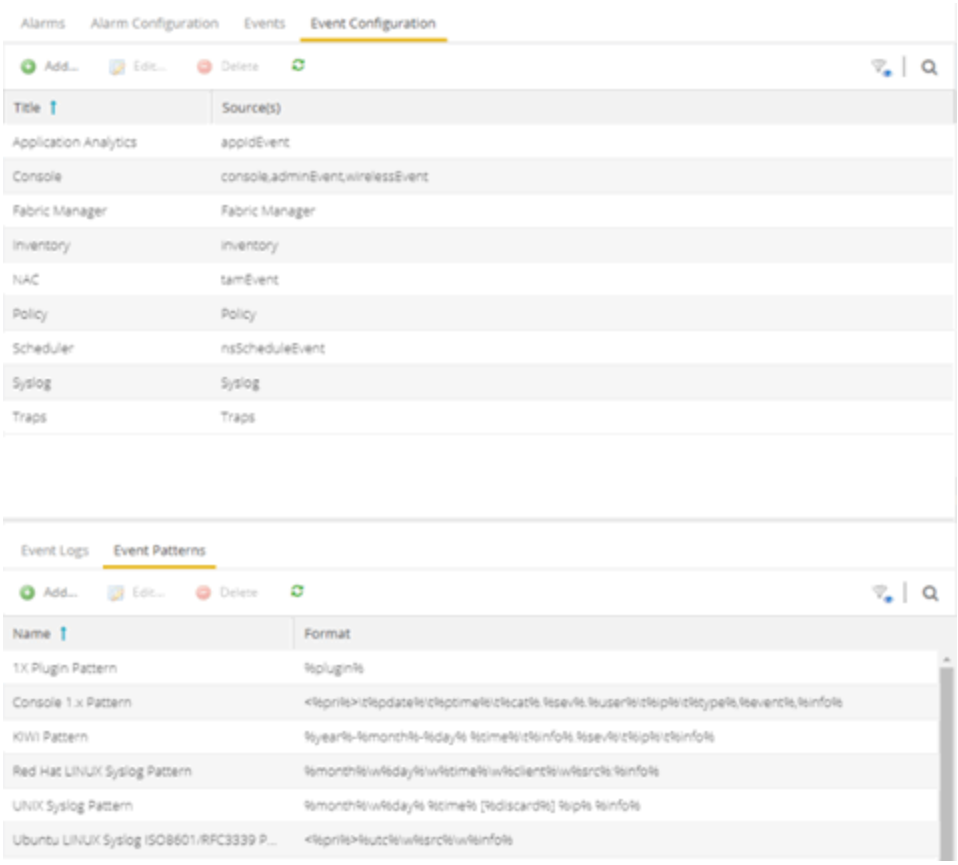
NOTE: **Access Control Audit**, **Access Control Engine**, **Admin**, **Console View**, **Compliance**, **Wireless**, and **Wireless Audit** Event Types are not configurable and not displayed on the **Event Configuration** tab.

The tab contains three sections:

- Event Type
- Event Logs
- Event Patterns

Event Type

Use the Event Type section of the tab to display a list of the event types configured in ExtremeCloud IQ Site Engine. Configure Event Types to name and sort events and traps based on the source from which they are generated. Additionally, you can use event types to combine and filter events and traps observed in ExtremeCloud IQ Site Engine on the **Events** tab.



Title

Displays the name of the event type. For system-defined event types, this is the application or area of functionality from which the event or trap is generated.

Source(s)

Displays the hostname of the source of the event or trap. To display the IP address of the host from which the event or trap is generated as the source, select the **Display Host Name in Source Column When Available** checkbox in the **Alarm/Event Logs and Tables** options.

Add

Adds a new event type to the list. The **Add Event Type** window opens, which allows you to enter a **Name** and select a **Source** from the drop-down list.

Edit

Edits the event type you select in the list. The **Edit Event Type** window opens, which allows you to modify the sources from which the events and traps are generated.

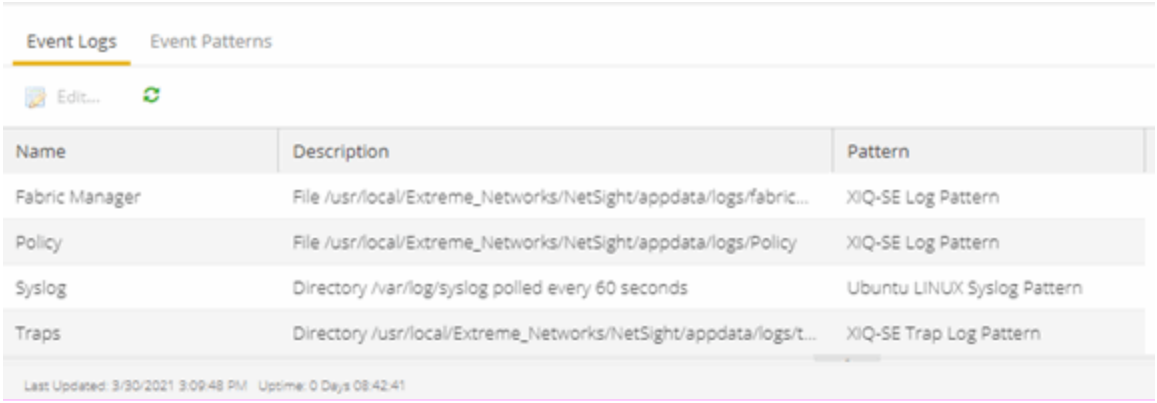
Delete

Deletes an event type you select from the list.

NOTE: You can only delete user-defined event types.

Event Logs

The **Event Logs** tab contains a list of the event and trap sources and displays the file locations in which the logs are saved. Additionally, the tab shows the log pattern, which you can configure on the Event Patterns tab.

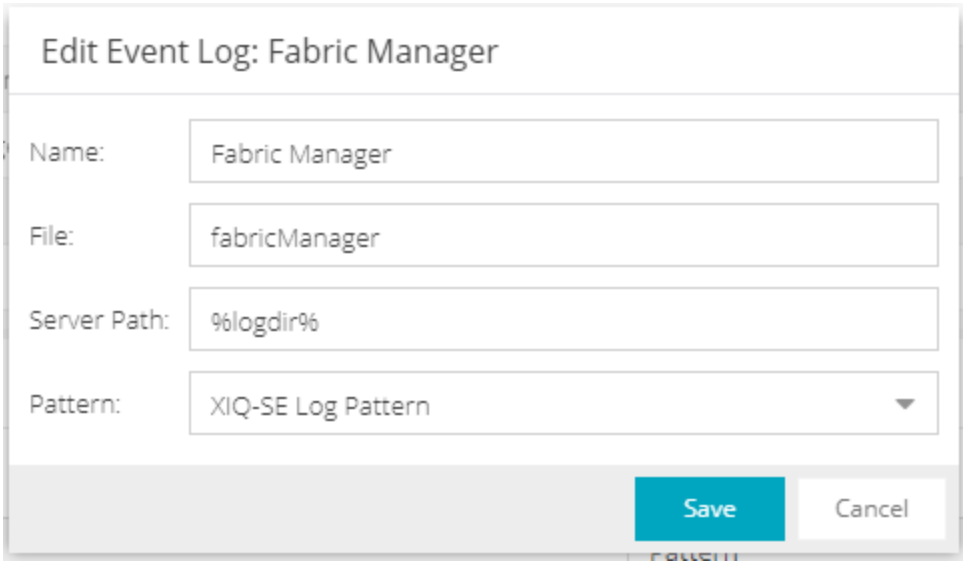


Name
: Displays the name of the Event Log. The Name Format (IP Address, System Name, Nickname) is what you selected in the **Device Tree** section of the Administration > Options tab. By default, **Names** indicate the location in ExtremeCloud IQ Site Engine from which the event is generated.

Description
: Displays the name and location of the log file.

Pattern
: Displays the pattern ExtremeCloud IQ Site Engine uses when generating the log file. This is vendor-specific depending on the type of device on which ExtremeCloud IQ Site Engine is generating the log. You can configure the pattern on the **Event Patterns** tab.

Select the **Edit** button to open the **Edit Event Log** window, where you can edit the log information.



Name
Enter the name of the event log.

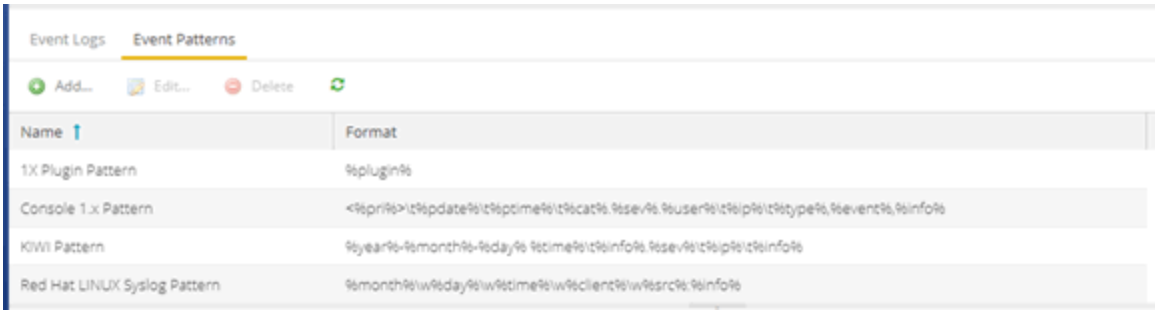
File
Enter the name of the log file.

Server Path
Enter location of the log file.

Pattern
Select the logging pattern for the log file. Configure the logging pattern on the **Event Patterns** tab.

Event Patterns

This tab lists the logging patterns used to configure the information contained in the log file.



Name
Enter the name of the event log pattern.

Format
: Displays the format of the information in the log file, which includes event fields and delimiters, to which a pattern is assigned. A field type full pattern is enclosed within angle brackets (<, >) to signify beginning and end. A newline (\n) is assumed at the end in this case, but could be made required using a delimiter character. Field types are placed within percentage symbols.

Add
: Select to open the **Add Event Pattern** window, which allows you to create a new event pattern. In the **Add Event Pattern** window, enter a **Name** and define a format

Edit
: Select to edit an existing user-defined event pattern you select in the list. The **Edit Event Pattern** window opens, which allows you to modify the **Name** and format using event fields and delimiters.

Delete
: Select to delete an existing user-defined event pattern.

Field Types

Select an Event Field in the table to add it to the Format field. The following Event Fields are available for event pattern formats:

%pri%
: Priority string

%pdate%
: Parsed Date — ExtremeCloud IQ Site Engine is capable of interpreting several date formats. Use this field with %ptime% for most standard date/time formats. If this does not present the date correctly, use the following fields to parse the individual elements in the date.

%date%
: Parses date elements and places the parsed information into the Date/Time column.

%month%, %day%, %year%
: Separately parsed date elements. The parsed results are placed in the Date/Time column.

%ptime%
: Parsed Time — ExtremeCloud IQ Site Engine is capable of interpreting several time formats. Use this field with %pdate% for most standard date/time formats. If this does not present the time correctly, use separate fields to parse the individual elements in the time.

%time%
: Parses the time elements and places the parsed information into the Date/Time column.

%hour%, %min%, %sec%, %ampm%
: Separately parsed time elements. The parsed results are placed in the Date/Time column.

%cat%
Category provides a means for sorting events (e.g., Poller, Application, Error).

%sev%
Severity

%user%
Username associated with the event.

%ip%
Host IP Address associated with the event.

%type%
Type (Event or Trap).

%event%
A more specific keyword/phrase for the event (i.e. "Contact Lost", "Contact Established").

%info%
The information string.

%discard%
Information that is not used. This is information that is skipped over to parse the next piece.

Delimiters

Select a delimiter to add it to the pattern format. The Delimiters section of the window provides a list of characters you can use to separate information types in the selected file. The list contains two types of whitespace delimiters, whitespace and tab). Use tab when a single tab separates elements in the sample line or whitespace when the separator in the sample line is a tab, a series of tabs or series of spaces.

Getting Started with ExtremeControl

ExtremeCloud IQ Site Engine's **Control** tab provides end-system and user identity reports and control capabilities, allowing better visibility and control for IT analysts, troubleshooters, and the helpdesk.

Access Requirements

To view the reports in the **Control** tab, you must be a member of an authorization group that has been assigned the appropriate capabilities:

- XIQ-SE OneView > Access OneView
- XIQ-SE OneView > ExtremeControl > Access OneView Identity and Access Reports
- XIQ-SE OneView > ExtremeControl > OneView End-Systems Read Access or Read/Write Access

NOTE: The ExtremeCloud IQ Site Engine, ExtremeControl, and ExtremeAnalytics Virtual Engine Installation Guide includes an overview of ExtremeCloud IQ Site Engine, ExtremeControl, and ExtremeAnalytics virtual engine deployment requirements and how to deploy a virtual engine on a VMware® and Hyper-V server.

Navigating the Control Tab

Selecting **Control** in the Menu Bar at the top of ExtremeCloud IQ Site Engine opens the **Control** tab. The **Control** tab provides access to four sub-tabs:

- Dashboard — Displays summary ExtremeCloud IQ Site Engine data including end-system data, system-level information, system events, ExtremeControl engine information, and network health.
- Policy — Enables you to create policy profiles, called roles, assigned to the ports in your network.
- Access Control — Allows you to configure how end-users connect to your network.
- End-Systems — Displays information about end-users connected to your network.
- Reports — Provides a variety of system reports that give information about your devices, ports, and network traffic.

Additionally, the **Menu** icon (☰) at the top of the screen provides links to additional information about your version of ExtremeCloud IQ Site Engine.

Dashboard

Select the **Dashboard** tab to view information about engines and end-systems.

Overview
Provides an overview of end-system connection information. For a description of each report, select the **Info** button in the upper right corner of the view. Enable and disable data display in each chart by selecting the data set in the chart legend. For example, if one segment represents a disproportionately large percentage of the total, mouse over the segment legend to the right of the chart and select it to remove it from the pie chart.

System
Provides system-level information for engines and end-systems. For a description of each report, select the **Info** button in the upper right corner of the view.

Health
Provides reports on end-system assessment and state information. For a description of each report, select the **Info** button in the upper right corner of the view.

Policy

Selecting the **Policy** tab lets you create policies for your network. It allows you to create policies for users and ports, enabling network engineers, information technology administrators, and business managers to work together to create the appropriate network experience for each user in their organization.

Access Control

The **Access Control** tab lets you manage the end user connection experience and control network access based on a variety of criteria including authentication, user name, MAC address, time of day, and location. The **Access Control** tab comes with a default Access Control Configuration which is automatically assigned to your Access Control engine. You can use this default configuration as is, or make changes to the default configuration, if desired.

End-Systems

Selecting the **End-Systems** tab displays end-system connection information, and lets you monitor end-system events and view the health results from an end-system's assessment. Double-click on any row in the table to open a browser window that displays End-System Details.

Reports

The **Reports** tab allows you to view information about the end-systems connecting to your network, ExtremeControl authentication information, and the top services and roles based on policy rules.

Available reports are accessible via the **Reports** drop-down list at the top of the tab and are grouped into the following reporting areas:

- End-Systems
- Access Control
- Access Control — Health
- Policy

Policy

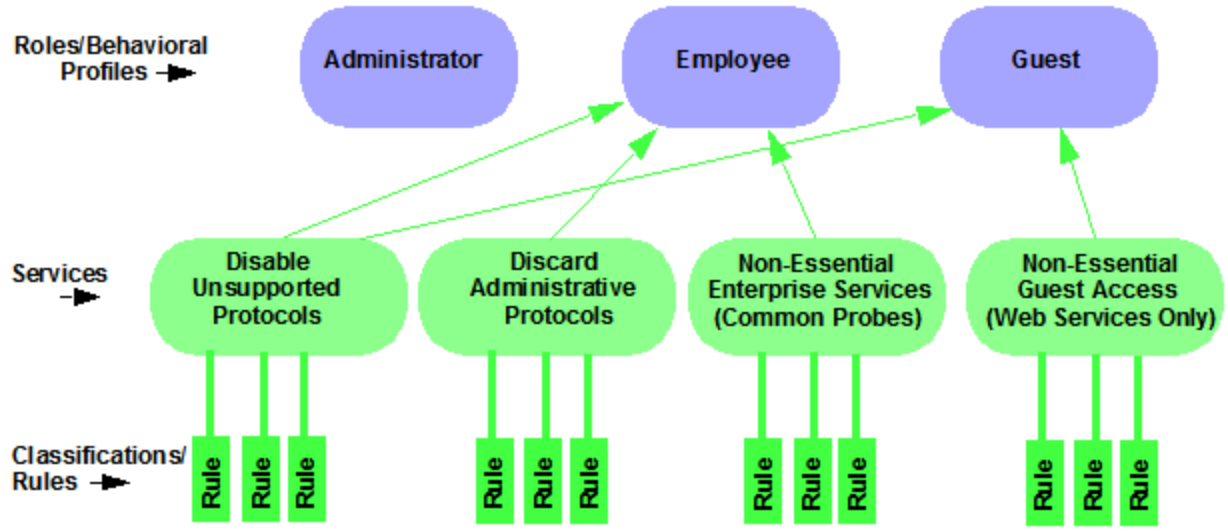
The **Policy** tab, contained in the **Control** tab of ExtremeCloud IQ Site Engine is a configuration tool that simplifies the creation and enforcement of policies on networks, enabling network engineers, information technology administrators, and business managers to work together to create the appropriate network experience for each user in their organization.

The **Policy** tab enables you to create policy profiles, called roles, which are assigned to the ports in your network. These roles are based on the existing business functions in your company and consist of services that you create, made up of traffic classification rules. Roles provide four key policy features: traffic containment, traffic filtering, traffic security, and traffic prioritization.

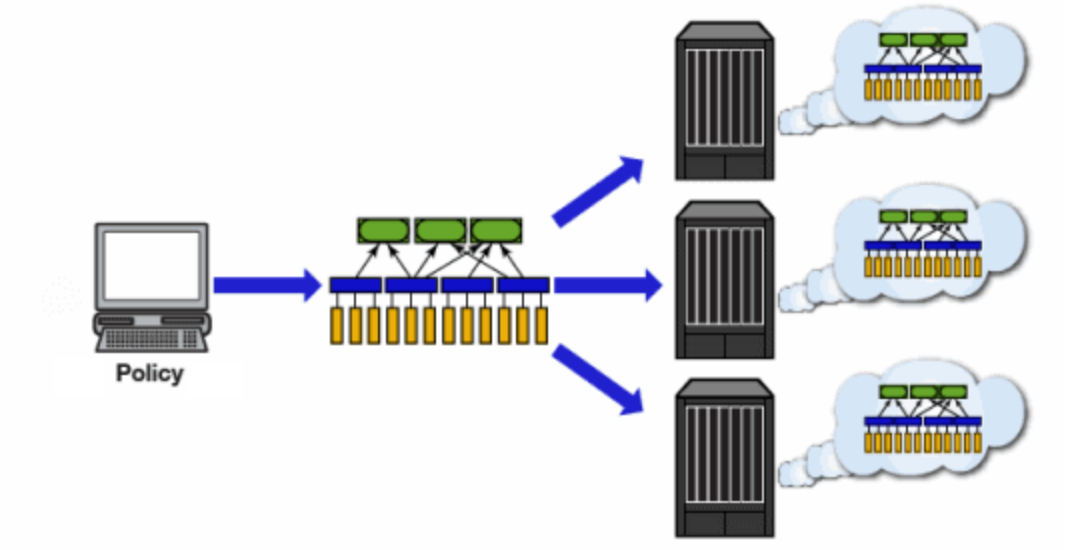
Use the following summary to guide you through the basic steps for using the **Policy** tab.

1. Create your Policy Domains (see How to Create and Use Domains.)
2. Add your devices to the ExtremeCloud IQ Site Engine Database and assign them to the appropriate domain.
3. If desired, group your ports into port groups (see How to Create a Port Group).
4. Create services (see How to Create a Service).
5. If desired, group services into service groups (see How to Create a Service Group).
6. Create roles (see How to Create a Role).
7. Write your configuration to your devices (see Enforcing).

The illustration below shows the **Policy** tab relationship hierarchy, with Rules at the base to define specific packet handling behaviors, Roles at the top to identify specific job functions in the organization, and Services in the middle, providing the interface between the two layers.



Using policy configuration tools, you can create multiple roles tailored to your specific needs and set a default policy for some or all of your network devices and ports. These policies can be deployed on multiple devices throughout your switch fabric.



The topic covers the following features:

- Understanding Policy Domains
- Understanding Roles
- Understanding Services
- Working with Service Groups
- Understanding Traffic Classification Rules

- Adding Devices
- Viewing Port Configuration Information
- Working with Port Groups
- Working with VLANs
- Viewing Classes of Service
- Saving the Domain
- Enforcing
- Verifying
- AP Aware

Understanding Policy Domains

The **Policy** tab provides the ability to create multiple policy configurations by enabling you to group your roles and devices into Policy Domains. A Policy Domain contains any number of roles and a set of devices that are uniquely assigned to that particular domain. Policy Domains are centrally managed in the database and shared between **Policy** tab clients.

The first time you launch the **Policy** tab, you are in the Default Policy Domain. You can manage your entire network in the Default Policy Domain, or you can create multiple domains each with a different policy configuration, and assign your network devices to the appropriate domain. The Default Policy Domain is pre-configured with roles and rules. The roles, services, rules, VLAN membership, and class of service in this initial configuration define a suggested implementation of how network traffic can be handled. This is a starting point for a new policy deployment and often needs customization to fully leverage the power of a policy-enabled network.

For more information about domains, see Policy Domains in the Concepts Help topic.

In the Quick Tour, we'll use the Default Policy Domain as a way to explore the basic features and functionality of the **Policy** tab. Later, the Default Policy Domain can be useful as you create your own Policy Domains.

If you have just launched the **Policy** tab for the first time, you are in the Default Policy Domain and you can proceed to the next step, Understanding Roles. If someone else has been using the **Policy** tab before you, use the following steps to create a demonstration domain you can use for the Quick Tour.

NOTE: If someone uses the **Policy** tab before you, ExtremeCloud IQ Site Engine can prompt to save the previous domain's configuration when you create the new domain. Save the previous domain's configuration if you are going to use that configuration in the future.

To create a policy domain:

1. Select Open/Manage Domains > Create Domain. Enter the domain name **`Demonstration Domain`** for the new domain and select OK. The new Demonstration Domain opens.
2. Select Open/Manage Domains > Assign Devices to Domain. Select the devices to add to the Domain and select OK. The device is added to the left-panel Devices tab.
3. Select the left-panel Roles/Services tab. Right-click Roles, Services, or Service Groups and select Create Role, Create Services, or Create Service Groups, respectively to create a role, service, or service group for the domain. For additional information on creating a role, service group, or service, see How to Create a Role, How to Create a Service, or How to Create a Service Group.
4. Select the left-panel **Class of Service** tab. Right-click Class of Service and select **Create COS** to create a class of service for the domain. For more information on creating a class of service, see How to Create a Class of Service.
5. Select the left-panel **VLANs** tab. Right-click Global VLANs and select **Create VLAN** for the domain. For more information on creating VLANs, see How to Create a VLAN.
6. Select the left-panel **Network Resources** tab. Right-click Network Resources or Global Network Resources (All Domains) and select **Create Network Resource** to create a network resource for the domain. You can also right-click Network Resource Topologies and select **Create Network Resource Topology** to create a network resource topology for the domain. For more information on creating a network resource or network resource topology, see How to Create a Network Resource.
7. Select **Open/Manage Domains > Save Domain**. The data elements are saved to the new Demonstration Domain.

For more information:

- How to Create and Use Domains

Now that you've created the demonstration domain, we can explore the Policy tab in a little more depth.

Understanding Roles

Roles are usually designed to reflect different users in your organization and to provide customized access capabilities based on the role users have in your organization. For example, accounting and engineering personnel have different network access and priority needs and therefore can have different roles.

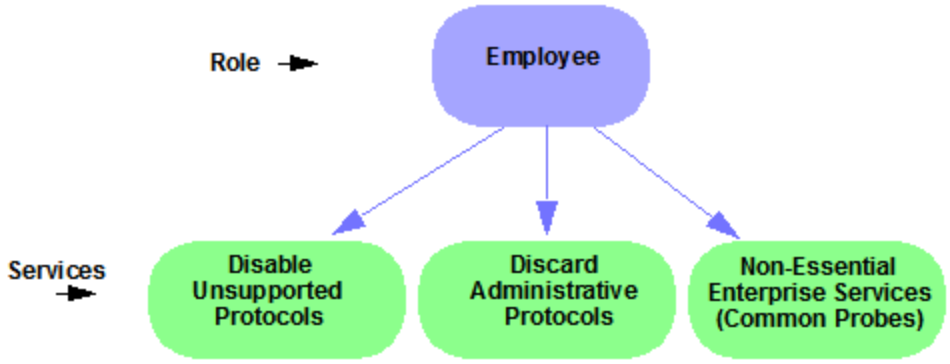
To view information about existing roles:

1. Select the left-panel Roles/Services tab in the Policy tab main window.
2. Select the left-panel Roles sub-tab in the Roles/Services tab.
3. Select a role name to see a description of the role.

4. Select the various roles listed in the left panel, and in the right panel you'll see tabs that display specific information for each role. Select the right-panel tabs to see the information they contain.

A role can be made up of one or more network access services defined in the **Policy** tab. These services determine how network traffic is handled at any network access point configured to use that role. A role can also contain default access control (VLAN) and/or class of service designations applied to traffic not handled specifically by the services contained in the role. A role can contain any number of services or service groups.

To filter through roles easily, select the Show Editable Columns drop down and select iif you wannt to hide or show editable information.



Roles are assigned to users during the authentication process. When a user successfully authenticates, the port is opened, and if a role is assigned to the user, that role is applied to the port. A role can also be directly assigned to a port as a default role for instances when authenticated users are not assigned a role. If an end user on a port is not assigned a role when logging in (authenticating), or if authentication is inactive on a port, then the port uses its default role. However, if a user is assigned a role upon login, then that role overrides any default role on the port.

To create and define a role, right-click **Roles** and select **Create Role**.

To create a role:

1. In the **Policy** tab left panel, select the **Roles/Services** tab.
2. Select the Roles sub-tab.
3. Right-click the Roles folder, and select **Create Role**.
4. Enter the role name **`Office Assistant`** in the highlighted box and press **Ok**.

For more information:

- Role
- How to Create a Role

Role Summary Column

The Summary column shows the data for the row iin a condensed form. Hovering over the cell displays the summary data in an expanded, easy too read format. This includes the rule and service usage information, traffic description, action details, automated service relevant network resources, and toplogy information.

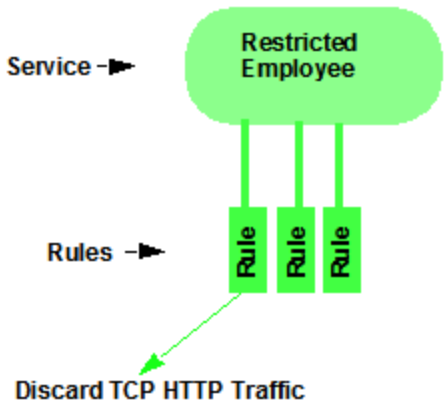
Understanding Services

Roles can be made up of one or more network access services. These services determine how network traffic is handled at any network access point configured to use that role. The **Policy** tab enables you to create Local Services (services unique to the current domain) and Global Services (services common to all domains).

Services can be one of two types:

- Manual Service — Contain customized classification rules you create.
- Automated Service — Associated with a particular set of network resources.

Manual services contain one or more traffic classification rules that define how a network access point handles traffic for a particular network service or application. For example, you might create a Manual service called "Restricted Employee" that contains a classification rule that discards TCP HTTP traffic.



We are creating a Manual service and then adding it to a role. Right now, lets take a look at the services in the domain.

To view information about existing services:

1. Select the left-panel **Roles/Services** tab in the **Policy** tab main window.
2. Expand the **Service Repository** folder and then the **Local Services** folder.

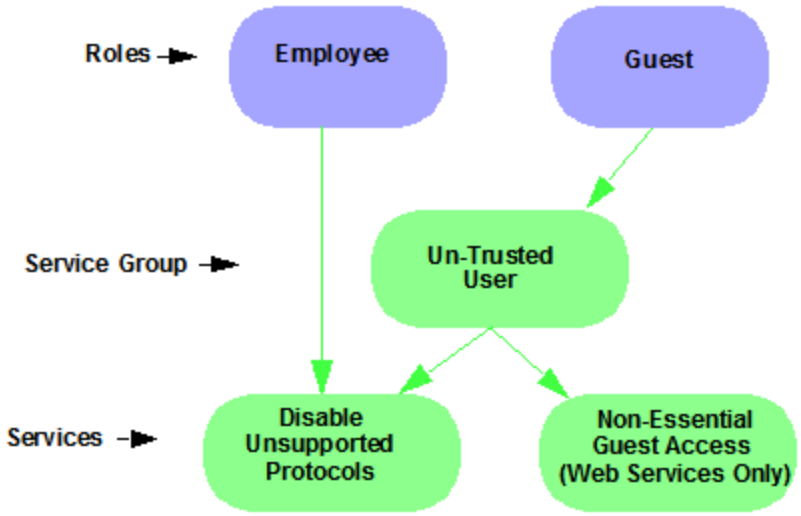
3. Expand the **Services** folder to view a list of services.
4. Expand a service or two to see the individual classification rules that make up the service.
5. Select a service or two in the left-panel to see the right-panel tabs that display specific information for each service. Select the right-panel tabs to see the information they contain.

For more information:

- Service
- How to Create a Service

Working with Service Groups

Services can be grouped together into Service Groups. This enables you to add a set of services to one or more roles.



To view information about existing service groups:

1. Select the left-panel **Service Repository** tab in the **Policy** tab main window.
2. Expand the **Service Repository** folder and then the **Local Services** folder. Expand the **Service Groups** folder.
3. Expand the **Acceptable Use Policy** service group to see its services. These services are also listed under the Services folder.

After you have defined and created your services, you can easily create a Service Group and then add your services to the group.

To create a service group:

1. Select the left-panel **Roles/Services** tab in the **Policy** tab main window.
2. Expand the **Service Repository** folder and then the **Local Services** folder.
3. Right-click the **Service Groups** folder and select **Create Service Group**.
4. Enter the service group name **`Trusted User`** in the highlighted box and press **Enter**.
5. Right-click Service Group, select **Add/Remove Services** and add one or two of the existing Acceptable Use Policy service groups into the Trusted User service group.

For more information:

- How to Create a Service Group

Understanding Traffic Classification Rules

Traffic classification rules enable you to assign access control (VLAN membership) and/or class of service to your network traffic based on the traffic's classification type. Classification types are derived from Layers 2, 3, and 4 of the OSI model and all network traffic can be classified according to specific layer 2/3/4 information contained in each frame.

A traffic classification rule has two main parts:

- Traffic Description — Identifies the traffic classification type for the rule.
- Actions — Apply access control, class of service, security, and/or accounting behavior to packets matching the rule.

To view existing rules:

1. In the left-panel, navigate to the **Service Groups** tab (Roles/Services > Service Repository > Local Services > Service Groups) and expand the **Acceptable Use Policy** service group.
2. Expand the **Deny Unsupported Protocol Access** service and select the **Discard AppleTalk** rule.
3. Use the **Edit** button to add a description to the service, for example: **AppleTalk not supported on this network**.

For more information:

- Rule
- Traffic Classification Rules
- How to Create or Modify a Rule

Adding Devices

The first step in adding network devices to **Policy** tab, is to add the devices to theExtremeCloud IQ Site Engine database. You do this initially, by using the **Discovered** tab on the **Network** tab. This section assumes you have already done this. If you need more information, refer to the **Network** tab Help page.

When you add devices to the ExtremeCloud IQ Site Engine database, you must assign the devices to a Policy Domain using the **Policy** tab. As soon as the devices are assigned to a domain, they are automatically displayed in the **Policy** tab device tree. Only devices assigned to the domain you are currently viewing are displayed.

To assign devices to a domain:

1. In the **Policy** tab main window, right-click **Devices** and select **Assign Devices to Domain**. The Assign Devices to Domain window opens.

   In the left panel, the Unassigned device tree contains all the devices in the database not assigned to a domain. The right panel displays the devices in the current domain.

2. For the Quick Tour, select a couple of devices to add to the domain and select **Add**. Select **OK** to add the devices.

   You can also use this window to remove a device from the current domain. This removes the device from the current domain and places it in the Unassigned folder. It does not delete the device from the ExtremeCloud IQ Site Engine database.

For more information:

- How to Add and Delete Devices
- How to Create and Use Domains

Viewing Port Configuration Information

After importing devices into the **Policy** tab, you can view and configure their ports by selecting a device and displaying its ports in the right-panel **Details View** tab or **Ports** tab.

To view port configuration information:

1. Select the left-panel **Devices** tab in the **Policy** tab main window.
2. Expand the **Devices** folder and select a device.
3. In the right-panel **Ports** tab, expand a **Ports** or **Slot** folder to display ports on the device.
4. Right-click a port and select **Current Domain > Show Role Details**.
5. Set Default Role, if necessary.

Working with Port Groups

The **Policy** tab enables you to group ports into User-Defined Port Groups, similar to the way you can group services into service groups. Port groups enable you to configure multiple ports on the same device or on different devices, at the same time. The **Policy** tab also provides you with Pre-Defined Port Groups. Every time one of the Pre-Defined Port Groups is accessed, the **Policy** tab goes to the devices

in the current domain and retrieves the ports which fit the pre-defined characteristics of the port group.

To view pre-defined port groups:

1. Select the left-panel **Port Groups** tab in the **Policy** tab main window.
2. Highlight a port group to display information for that port group.

For more information:

- Pre-Defined Port Groups

Working with VLANS

All traffic in a **Policy** tab network is assigned membership in a VLAN. Roles are used to assign VLAN membership to traffic either through the role's default access control or through the role's services which can include traffic classification rules that assign VLAN membership (access control).

When you open a new domain, the Global VLANs folder is prepopulated with the Default VLAN (not to be confused with a default VLAN assigned to a role, although the Default VLAN *could* be a default VLAN for a role). You can then create additional VLANs and assign them as default access control for a role and/or use them to define traffic classification rules. You can view the roles and services associated with a VLAN by selecting the VLAN in the left-panel. You can also make role and service changes from this window.

Island VLANs are used in Policy VLAN Islands, which enable you to deploy a policy across your network, while restricting user access to only selected local devices. The **Policy** tab enables you to view currently configured Island VLAN information.

To view VLANs:

1. From the **VLANs** tab, expand the **Global VLANs** folder to see individual VLANs.
2. Select the Default VLAN listed and view the VLAN information in the right panel.

For more information:

- How to Create a VLAN
- General Tab (VLAN)
- Policy VLAN Islands

Viewing Classes of Service

The **Policy** tab lets you create a class of service (CoS) that includes one or more of the following components: an 802.1p priority, an IP type of service (ToS) value, rate limits, and transmit queue configuration. You can then assign the class of service as a classification rule action, as part of the definition of an automated service, or as a role default.

To view Classes of Service:

1. From the **Policy** tab, select the **Class of Service** tab from the left-hand panel. The Class of Service section expands.

   Notice that the window is pre-populated with eight static classes of service, each associated with one of the 802.1p priorities (0-7). You can use these classes of service as is, or configure them to include ToS/DSCP, drop precedence, rate limit, and/or transmit queue values. You can also rename them, if desired. In addition, you can also create your own classes of service (user-defined CoS).

2. Select the **Class of Service** and all information related to the Class of Service selected is displayed in the right-panel.

For more information:

- Getting Started with Class of Service
- How to Define Rate Limits
- How to Configure Transmit Queues
- How to Create a Class of Service

Saving the Domain

After changing a policy domain, save the domain. This notifies all clients viewing the domain there is a change, which prevents them from saving a domain with an incorrect configuration. The system automatically updates their view with the new configuration.

To save a domain, select **Open/Manage Domains > Save Domain**.

The domain is saved and automatically updates for all clients viewing the domain. To discard unsaved changes you made to a domain, open the **Open/Manage Domains > Open Domain** menu and select the domain in which you are currently working.

For more information:

How to Create and Use Domains

Enforcing

Any time you add, make a change to, or delete a role or any part of it (any of its services and/or rules), the devices in your current domain need to be informed of the change so that your revised policy configuration can take effect. This is accomplished by enforcing — writing your policy configuration to a device or devices. Enforce operations are performed only on the current domain.

To enforce to all devices in the current domain, select **Open/Manage Domains > Enforce Domain**. To enforce to a single device, right-click the device and select **Enforce**.

Enforce Preview

The Enforce preview tool has a very similar setup to the Enforcing Domain tool. To view the enforce preview, select **Open/Manage Domains > Enforce Preview** and select the device to preview from the left dropdown.

Note: If the device has a red exclamation type next to it in the left panel, then it is incompatible with the domain configuration and should be corrected.

Enforcing preview shows you a summary of the stats and info, roles, rules, and services on device. The three preview tabs include:

Device Stats & Info: Shows information on supported role/rule counts, etc.

Roles & Rules: Shows a grid panel with roles and rules that will enforce the device. If supported, it will show a green circle. A yellow circle indicates a rule not being supported, and a red circle denotes a role not being supported. **Right-click** and select **View/Edit** which will close enforce preview and bring you to the item you wish to make changes to.

Classes of Service: Shows details of the Class of Service and the related rate limit configuration.

Rule Counts Reported by Devices

Every device has a maximum number of rules that it can follow. Going over the max number of rules on a device will create enforce failures. The max supported rules by rule type are mainly a concern for Switch Engine device, which now report the max a type supports via the value returned for etsysPolicyRuleAttributeMaxCreatable for any rule type in that group. For example, reading either instance 1 (macSource(1)) or 2 (macDestination(2)) will return the supported number of layer 2 (MAC) rules. The 4 rule “types” and the rule types () that these include are:

- MAC
    - macSource(1)
    - macDestination(2)
- IPv4
    - ip4Source(12)
    - ip4Destination(13)
    - ipFragment(14)
    - udpSourcePort(15)
    - udpDestinationPort(16)
    - tcpSourcePort(17)
    - tcpDestinationPort(18)
    - ipTtl(20)

    - ipTos(21)
    - ipType(22),
- IPv6
    - ip6Destination(10)
- L2
    - etherType(25)

The total max supported number of rules for Switch Engine devices is the sum of these 4 types, NOT the value returned by etsysPolicyRulesMaxEntries (due to that including other things by the FW).

The devices supported number of rules is only read when the device is added to the domain, the firmware is upgraded, or the device is manually refreshed.

For more information:

- Enforcing

Verifying

To determine if the roles currently in effect on your domain devices match the set of roles defined in your current Policy Domain configuration, use the Verify feature.

AP Aware

An AP is assigned "AP Aware," all traffic through this port will not need authentication. This new Role default action is configurable via a new AP Aware setting in the role configurations view. To enable AP Aware:

1. Select the left-panel **Roles/Services** tab in the Policy tab main window.
2. Select the left-panel **Roles** sub-tab in the Roles/Services tab.
3. Select a role name to see a description of the role.
4. Using the scroll bar, scroll to find the **AP Aware** column.
5. Double-click **Disabled**, and in the drop-down, select **Enabled**.

When enforce or verify occurs, the secondary logic runs which inspects all AP Aware enabled roles, and for each role finds all in-use VLANs (rule actions, role default action) and automatically adds them to that role's tagged VLAN egress list if they are not already present. This is then used for the enforce/verify logic, and returned to the client so the domain is updated accordingly.

The domain data can change from doing an enforce/verify, and needs to be saved.

For more information:

- Verifying

Policy Configuration Considerations

Review the following configuration considerations when installing and configuring ExtremeCloud IQ Site Engine's **Policy** tab.

- General Considerations
  - Authenticating without Policy
  - Terminating Role Override Sessions
  - Port-Level MAC to Role Mappings
  - Import From Device
  - Flood Control
- C1 Considerations
  - Policy Support
  - Rule Limits
- N-Series Considerations
  - Role Precedence for the N-Series Platinum
- C2 and B2 Considerations
- C3 and B3 Considerations
- Mixed-Stack C2/C3 and B2/B3 Considerations
- 7100 Considerations
- ExtremeControl Controller Configuration
- Wireless Controller Configuration

General Considerations

Authenticating without Policy

This section discusses how authentication works in a network where end users must authenticate, but there are no roles (policy) for authenticated users defined on the network devices.

The following table shows Authentication Behavior for each device type when the authenticated role is not defined on the device:

Authentication Type	K-Series, S-Series, N-Series Gold and Platinum	E6/E7	E1	RoamAbout R2 RoamAbout AP3000	C2/B2
802.1X	Successful	Successful	Successful	Successful	Successful
MAC	Successful	Successful	Successful	Successful	Successful
Web-Based	Successful	Successful on firmware version 5.06.x. Failed on older firmware versions.	Successful	Web-Based Auth Not Supported	Successful

The following table shows Authenticated Traffic Behavior for each device type when the authenticated role is not defined on the device:

Authentication Type	N-Series Gold and Platinum 4.11 and earlier	K-Series, S-Series, N-Series 5.01 and later Gold and Platinum	E6/E7	E1	RoamAbout R2 RoamAbout AP3000	C2/B2
802.1X	1	3	2	2	3	2
MAC	1	3	2	2	3	2
Web-Based	1	3	2	2	Web-Based Auth Not Supported	2

1 - Traffic is forwarded based on the 802.1Q PVID and 802.1p priority for the port, regardless of whether the port has been assigned a default role. Authenticated users display a current role of "None" in the Port Usage tab.

2 - Traffic is forwarded based on the port's default role and authenticated users will display the default role as their current role in the Port Usage tab. If no default role has been assigned to the port, the port's 802.1Q PVID and 802.1p priority are used, and the current role will be "None."

3 - Traffic is forwarded based on the Invalid Role Action configuration at the device level in the Policy tab.

Terminating Role Override Sessions

On Port Usage tabs, you cannot terminate Role Override (IP) or Role Override (MAC) sessions created through the CLI (command line interface).

Port-Level MAC to Role Mappings

Enforcing port-level MAC to Role mappings could potentially remove rules as an intrusion detection response.

Import From Device

If you perform a Verify operation following an Import Policy Configuration from Device, the Verify can fail. This is because the import operation imports only roles and rules from the device, not the complete policy configuration.

Also, if you import from more than one device and the configuration is not the same on each device, Verify fails. This is because the imported configuration will not match the configuration on any one device.

Flood Control

Individual Class of Service granularity is unsupported on fixed switches, so if any CoS is assigned a Flood Control rate, all Class of Service on these devices use that rate.

C1 Considerations

Review the following considerations prior to configuring policy on C1 devices:

Policy Support

Policy support on C1 devices utilizes both a port-level role and a device-level role. In the **Policy** tab, a role is a set of network access services made up of traffic classification rules. It can also contain default Access Control (VLAN) and/or Class of Service settings applied to traffic not handled specifically by the rules contained in the role. Although both the device-level and port-level roles can contain all of these components, only certain portions of each role are used when applied to a port on a C1 device.

On the C1, classification rules are implemented at the device level through a device-level role. The **Policy** tab enables you to set a unique device-level role for each C1 device. The device-level role is a regular role that defines how inbound traffic is handled in terms of classification rules and default Class of Service assignment. In other words, all classification rules are taken from the device-level role, and any rules defined in the port-level role are ignored when applied to a port. The Class of Service setting is also implemented through the device-level role and ignored in the port-level role. However, the default Access Control setting of the device-level role is ignored, and is defined through the port-level role.

Classification rules from the device-level role are only applied to ports which also have a port-level role applied (either statically or dynamically). This enables you to exclude the device-level role from uplink

ports and hosts ports, by not applying a port-level role to these ports and not enabling authentication on them.

When a port-level role is applied to a port, it overrides any PVID and Class of Service settings defined on the port through Console or local management. When a device-level role is applied to a port, it also overrides these PVID and Class of Service settings, and overrides any Class of Service setting defined in the port-level role. It does **not** override any default Access Control setting defined in the port-level role.

In addition, if the port-level role's default Access Control is configured to deny traffic, then **all** inbound traffic will be discarded even if it matches a (forward) classification rule.

Rule Limits

C1 devices limit the number of rules you can create for some classification types. Refer to the C1 information in the ExtremeCloud IQ Site Engine Release Notes to see which classification types limit the number of rules.

N-Series Considerations

Review the following considerations prior to configuring policy on N-Series devices:

Role Precedence for the N-Series Platinum

The following precedence determines the role (policy) that is being applied on a user/port on a N-Series Platinum device. The precedence used depends on whether the device is configured for multi-user authentication or single user authentication.

Multi-User Authentication:
Devices configured with multi-user authentication use the following precedence when applying a role on a user/port (starting with the highest precedence):

MAC override policy
Authenticated role
MAC-to-Role mapping
IP override policy
IP-to-Role mapping
VLAN-to-Role mapping
Default port role

Single User Authentication:
Devices configured with single user authentication use the following precedence when applying a role on a user/port (starting with the highest precedence):

MAC override policy
MAC-to-Role mapping
IP override policy
IP-to-Role mapping
Authenticated role
VLAN-to-Role mapping
Default port role

C2 and B2 Considerations

Review the following considerations prior to configuring policy on C2 and B2 devices.

- When TCI Overwrite is enabled on a role, C2 and B2 devices support rewriting the 802.1p bit (CoS values) but not the 802.1Q bit (VLAN ID).
- On C2 and B2 gigabit and 10/100 ports, the number of rules per port is restricted. Refer to your C2 and B2 firmware release notes for the maximum number of rules that can be utilized on a port.
- C2 and B2 10/100 ports support two priority-based rate limits (inbound only). When creating a rate limit to be used on C2 and B2 10/100 ports, create the limit with either Low priority to associate the rate limit with priorities 0-3 or High priority to associate the rate limit with priorities 4-7. You can specify both Low and High priorities if you want to associate the rate limit with priorities 0-7.
- C2 and B2 devices do not support setting a default role on a logical port.
- On C2 and B2 devices, it is strongly recommended that you do not enforce rules that assign a Class of Service (CoS) that includes Priority 7. Doing so will interfere with stack communication.
- C2 and B2 devices do not permit a mask for an IP type of service (ToS) rewrite value associated with a class of service (CoS); they will always use ff.
- C2 and B2 devices do not support VLAN ID traffic classification rules. C2 devices (firmware 3.02.xx and newer) and B2 devices (firmware 2.xx.xx) support device-level VLAN to Role mapping. However, VLAN ID traffic classification rules can be configured on C2 devices with firmware versions 3.01.xx or older, using CLI.
- B2 only. Each port on a policy-enabled B2 switch can support up to 100 rules and up to 10 masks. The maximum number of unique rules in a single switch or B2 stack is 100, while the maximum number of unique masks is 18. These unique rules and masks can be shared across any and all ports in a stack or switch.

C3 and B3 Considerations

Review the following considerations prior to configuring policy on C3 and B3 devices.

- B3/C3 devices do not support TCI Overwrite. The B3/C3 does not overwrite 802.1Q VLAN bits, but overwrites the 802.1p Priority bits.
- B3/C3 devices do not support Layer 3 ICMP rules.
- B3/C3 devices support role-based rate limiting. However, on the B3/C3, class of service inbound rate limiting works only on policy roles, not on policy rules.
- C3G and B3 devices have the following additional limitations:
    - Maximum 100 rules per policy role.
    - A system limitation of 768 unique rules.

    - Maximum of 15 roles.
- C3 and B3 devices do not support setting a default role on a logical port.

Mixed-Stack C2/C3 and B2/B3 Considerations

Review the following considerations prior to configuring policy on mixed stacks of C2/C3 and B2/B3 devices.

NOTE: While you can create mixed stacks of C2/C3 devices and mixed stacks of B2/B3 devices, you should not create mixed stacks of C and B devices (e.g. mixed stacks of C2/B2 or C3/B3 devices).

- It is strongly recommended that a C3 device be configured as the controller in a mixed C2/C3 stack.
- It is strongly recommended that a B3 device be configured as the controller in a mixed B2/B3 stack.
- When you have a mixed stack, all devices in the stack have the rule type and Class of Service limitations of a C3 or B3 device, despite the fact that the stack can report itself as a C2 or a B2. The device type that the stack reports is based on what switch is set as the controller.
- Mixed stacks with a B3/C3 controller support role-based rate limiting, however, class of service inbound rate limiting works only on policy roles, not on policy rules.
- A mixed stack containing a C2H or a B2 has the following limitations:
    - A single role limitation of 100 rules and 10 masks.
    - A system limitation of 100 unique rules and 18 unique masks.
    - No support for Layer 2 rules or Layer 3 ICMP type rules.
    - Maximum of 15 roles.
    - No support for rate limiting.
- A mixed stack containing a C2G has the following limitations:
    - A single role limitation of 100 rules and 10 masks.
    - A system limitation of 768 unique rules.
    - No support for Layer 2 rules.
    - Maximum of 15 roles.
    - No support for rate limiting.
- When adding a new device to a mixed stack, the ports should not go active unless the stack supports the policy configuration. When a device has joined the stack, no roles should be enforced that are not supported on all devices. For example:
  A C2K is added to an existing C3 stack.

- If the number of masks in the C3 stack's current configuration exceed those permitted by the C2K, its ports cannot go active.
- When the C2K joins the stack, no roles can be enforced that exceed the limitations of any device.

7100 Considerations

- 7100 devices only support fixed IRL index reference mappings for the static CoS. The IRL Index for the CoS needs to match the priority. This is the default configuration for domains, but if it is changed for a static CoS, enforce will fail.
- 7100 devices only support fixed TXQ index reference mappings for the static CoS. The TXQ Index for the CoS needs to match the priority. This is the default configuration for domains, but if it is changed for a static CoS, enforce will fail.
- 7100 devices only support fixed COS - transmit queue mappings. The transmit queue specified for a Class of Service must match the 802.1p priority, or enforce will fail.
- TCI Overwrite configuration is not supported on the 7100. It is always enabled, and cannot be turned on or off using the Policy tab.

ExtremeControl Controller Configuration

Review the following considerations prior to configuring policy on ExtremeControl Controller devices.

ExtremeControl Controllers Require Separate Domains

Access Control Controllers must by assigned to their own unique policy domain and cannot be combined with other switch types in a domain.

Modifying ExtremeControl Controllers Preconfigured Policy

Access Control Controllers are shipped with a default policy configuration already configured on the device. To modify this default policy configuration, you must create a domain for the Access Control Controller, assign the Access Control Controller to the domain, then import the policy configuration from the device into the Policy tab (File > Import > Policy Configuration from Device). You can then alter the policy configuration to define the authorization levels for the ExtremeControl process, as appropriate for your environment. If assessment will be enabled in the Extreme Networks Access Control solution, you must add classifications rules to the Quarantine and Assessing policies to permit traffic to be forwarded to the assessment servers deployed on the network. When you have finished modifying the policy configuration, you must enforce it back to the Access Control Controller.

NOTE: If you are using assisted remediation and quarantined end-users will be required to download remediation files via FTP, you will also need to add a rule to the Quarantine policy configuration that opens up ports 49152-65535. If you are concerned with security, you can configure your FTP server to use a smaller range of ports.

Modifying the Downstream Default Policy

Depending on the network configuration or circumstances, it's possible that traffic from the upstream side could be rerouted to the Access Control Controller where it would be authenticated using the upstream source IP address. To avoid this problem, add a Layer 3 IP Address Source rule to the downstream default policy configured on the Access Control Controller, using the upstream IP subnets (or critical servers located in the upstream) and containing the traffic to a VLAN.

Configuring LAG on ExtremeControl Controllers

This section provides instructions for configuring LAG (link aggregation) on your Access Control Controller appliance. The instructions vary depending on whether you are configuring LAG on a Layer 2 or Layer 3 Access Control Controller.

Configuring LAG on Layer 3 ExtremeControl Controllers – Upstream Ports

1. Configure LAG on the Access Control Controller PEP (Policy Enforcement Point) using the CLI (Command Line Interface).
2. Use the **Policy** tab to assign the appropriate upstream role as the default role on the port. For instructions, see Assigning Default Roles to Ports.

Configuring LAG on Layer 3 ExtremeControl Controllers – Downstream Ports

1. Configure LAG on the Access Control Controller PEP (Policy Enforcement Point) using the CLI (Command Line Interface).
2. In the **Policy** tab options (Tools > Options), display the Ports panel and uncheck the Hide Logical Ports option.
3. Use the **Policy** tab to assign the appropriate downstream role as the default role on the port. For instructions, see Assigning Default Roles to Ports.

Configuring LAG on Layer 2 ExtremeControl Controllers – Upstream Ports

1. Configure LAG on the Access Control Controller PEP (Policy Enforcement Point) using the CLI (Command Line Interface).
2. In the **Policy** tab options (Tools > Options), display the Ports panel and uncheck the Hide Logical Ports option.
3. Use the **Policy** tab to assign the appropriate upstream role as the default role on the port. For instructions, see Assigning Default Roles to Ports.

Configuring LAG on Layer 2 ExtremeControl Controllers – Downstream Ports

1. Configure LAG on the Access Control Controller PEP (Policy Enforcement Point) using the CLI (Command Line Interface).

2. In the **Policy** tab options (Tools > Options), display the Ports panel and uncheck the Hide Logical Ports option.
3. Use the **Policy** tab to assign the appropriate downstream role as the default role on the port. For instructions, see Assigning Default Roles to Ports.
4. Use the CLI to set the following command: nodealias maxentries 4096 <lag port>.

ExtremeWireless Controller Configuration

The following sections present information regarding support for the ExtremeWireless Controller in the **Policy** tab. Review the following considerations prior to configuring policy on wireless controller devices.

Version Supported

The Policy tab only supports Wireless Controller version 8.01.03 and higher.

Policy Rules

This section describes wireless controller support for policy rules.

Supported Rule Types

The Wireless Controller supports the following traffic classification rule types:

- Ethertype
- MAC Address Source/Destination/Bilateral
- Priority
- IP Type of Service
- IP Protocol Type[1]
- ICMP
- IP Address Source/Destination/Bilateral
- IP Socket Source/Destination/Bilateral
- IP UDP Port Source/Destination/Bilateral
- IP UDP Port Source/Destination/Bilateral Range
- IP TCP Port Source/Destination/Bilateral
- IP TCP Port Source/Destination/Bilateral Range

[1]Not all IP Protocols are supported for the wireless controller. Supported IP Protocols for this rule type are: ICMP, TCP, UDP, GRE, ESP, AH.

"No Change" Filter Sets

The wireless controller enables administrators to define policies that do not have any filters of their own, but which instead use the set of filters already assigned to a station by a previously applied policy. This type of policy is said to have a "No Change" set of policy rules. The **Policy** tab does not support policies that have "No change" policy rule sets. Using the ExtremeWireless Assistant, you need to remove any policies containing "No Change" rule sets before the wireless controller can be managed by the **Policy** tab.

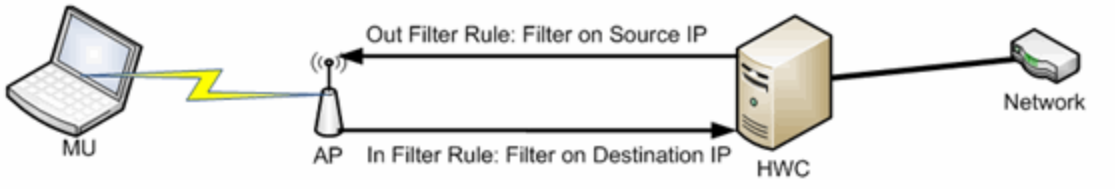
Rule Actions

The following list defines the wireless controller support for rule actions:

- Access Control: Permit, Deny, and Contain to VLAN actions are supported.
- Class of Service is supported.
- TCI Overwrite is not supported.
- System Log, Audit Trap, Disable Port, and Traffic Mirror actions are not supported.

Rule Directions

The **Policy** tab rules are applied to incoming data packets based on the source or destination address, whereas the wireless controller applies rules to packets based on In/Out direction. On the wireless controller, "In" means coming from the station into the network and "Out" means going from the network out to the station. The wireless controller applies rules to the destination address of inbound packets and to the source address of outbound packets, as shown in the illustration below.



When you create a rule in the Policy tab that permits traffic to a specific destination, that same rule permits data flow from the destination back to the traffic source. This means that Destination rules in the **Policy** tab map to In/Out rules on the wireless controller. Certain **Policy** tab rule types do not have a Source or Destination designation (such as ICMP); however, these rules still map to In/Out rules on the wireless controller to indicate the filters are applied to traffic in both directions. Unchecking the In or Out flag for non-directional rules via the ExtremeWireless Assistant does not affect the way it is reported to the **Policy** tab. As long as the rule still exists, verify succeeds.

All rules enforced from the **Policy** tab are created as "In" rules, and "Out" rules created on the controller are not reported to the **Policy** tab.

When the egress policy feature is enabled for a VNS, egressing traffic is applied to the defined "In" filters as a "reflected" Out rule (with the source and destination fields reversed) and any explicitly

defined "Out" filters created on the controller are ignored. Egress policy can be enabled per VNS by selecting Port Properties for that VNS.

The wireless controller reports to the **Policy** tab any rules created directly on the controller that contain an "In" component. "Out" rules are not reported to the Policy tab. This enables administrators to define and use "Out" rules on the wireless controller in special cases where additional restrictions need to be imposed.

Rule Limits

The wireless controller has a limit of 64 rules per policy role if the policy is enforced at the controller (bridged @ wireless controller or routed topology), and 32 rules per policy role if the policy is enforced at the AP (bridged @ AP).

Role Default Actions

The following list defines the wireless controller support for role default actions:

- Access Control: Permit, Deny, and Contain to VLAN are supported.
- Class of Service: Inbound and outbound rate limits are supported. 802.1p Priority, and ToS/DSCP Marking are supported.
- TCI Overwrite is not supported.
- System Log, Audit Trap, Disable Port, and Traffic Mirror actions are not supported.
- The wireless controller will reject policy configurations that specify a VLAN that does not have an egress port already specified.

Class of Service

The following list defines the wireless controller support for Class of Service (CoS) configuration via the **Policy** tab:

- Inbound and outbound rate limits are supported at the role-level as Class of Service default actions.
- User-based inbound/outbound rate limits are supported for the Default port group for wireless controllers only.
- 802.1p Priority configuration is supported.
- ToS/DSCP Marking is supported.
- TCI Overwrite is not supported.
- Transmit Queue Rate Shaping is not supported.

Rate Limits

The wireless controller supports inbound and outbound rate limits at the role-level as Class of Service (CoS) default actions. There are three states supported for a rate limit:

- Rate limit traffic at the specified rate.
- No Change (the CoS does not specify a rate, and the rate limit is "inherited" from the port's default role or from the global default policy, if one is defined.)

To explicitly prevent traffic from being rate limited for a role, you can map a rate limit with a value of 0 to a CoS, and set that as the default CoS for the role.

Internal VLAN

The wireless controller uses an *internal VLAN* for processing traffic. For controllers with firmware version 8.01.xx, the internal VLAN is set by default to use VID 1 and the static name of "DEFAULT VLAN." For controllers with firmware version 8.11.xx and later, the internal VLAN uses the VID 4094 and the static name of "INTERNAL VLAN."

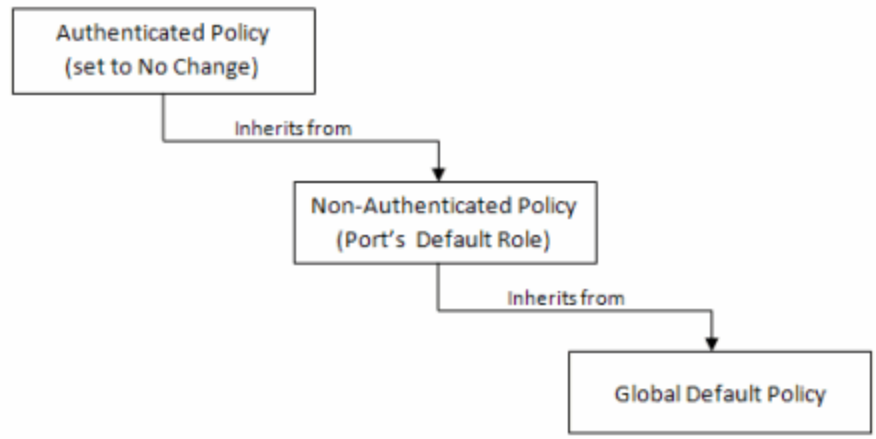
This internal VLAN cannot be used in your **Policy** tab domain configuration to tag traffic. If the VID for the internal VLAN is used in your domain configuration, the **Policy** tab enforce fails with an error message in the Event Log indicating the internal VID cannot be used.

You can use the Web UI (https:\\<controller IP>:5825 > VNS Config > Topologies > Internal VLAN) to change the internal VLAN to a different value, but your policy domain must not use that new value or the **Policy** tab enforce fails.

NOTE: For controllers with firmware version 8.01.xx. Since using a Default VLAN with a VID of 1 is valid on wired devices, the controller's internal VLAN must be changed to another value to prevent issues with the Policy tab enforcing a configuration that uses this VLAN.

Policy Inheritance

The wireless controller uses the concept of policy inheritance, which specifies that if the authenticated policy's access control (VLAN) or class of service (CoS) is set to "No Change," then the policy inheritance hierarchy is used to determine the VLAN and/or CoS. The policy inheritance hierarchy is as follows:



If the authenticated policy's VLAN and CoS are set to "No Change," then the VLAN and CoS settings for the port's default role is used. If the port's default role does not specify the VLAN and CoS, then the global default policy (specified via the ExtremeWireless Assistant) is used. (In wireless controller terminology, a VNS port's default role is the VNS's default policy.)

It is important to note that the **Policy** tab does not support "No Change" rules (filter set). If any policy's rules (filter set) are set to "No Change," then the **Policy** tab is not able to manage the device until the policy containing the "No Change" configuration is removed.

Configuring RADIUS Servers

When configuring RADIUS authentication and accounting servers, keep in mind the following differences:

- The "Number of Retries" and "Timeout Duration" settings for RADIUS authentication servers are configured on a per-server basis for wireless controller devices. For all other devices, these settings are global to all RADIUS servers, and are specified per device as client defaults.
- The "Update Interval" setting for RADIUS accounting servers is configured on a per-server basis for wireless controller devices. For all other devices, this setting is global to all RADIUS servers, and is specified per device as client defaults.
- For wireless controller devices, the Client Status (Enabled or Disabled) is automatically set to Enabled when a RADIUS server exists and Disabled when it does not. For all other devices, Client Status is configured for each device, enabling you to enable and disable communication between the device and the RADIUS servers.
- If Strict Mode is enabled, up to three RADIUS servers are automatically associated to each WLAN service. If Strict Mode is disabled, RADIUS servers must be manually added to a WLAN service via the ExtremeWireless Assistant.

Other Considerations

- The wireless controller does not support authentication configuration.
- The wireless controller does not support viewing user sessions in the Port Usage tabs.
- The wireless controller must have any VLANs used in a Role's default action already defined on the device and configured with an egress port. If the **Policy** tab enforces a domain configuration to the wireless controller using a VLAN that does not have an egress port specified, enforce fails.

ExtremeCloud IQ Site Engine Policy

ExtremeCloud IQ Site Engine **Policy** enables the creation and deployment of role-based policies that dynamically control user access, network security, application prioritization and other parameters. Policy management and role-based administration are keys to effectively enforcing business and IT rules in the network infrastructure.

Contact your sales representative for information on obtaining an ExtremeCloud IQ Site Engine software license.

Policy Tab Overview

The **Policy** tab simplifies the configuration of policies on networks, and deploys the policies on multiple devices throughout the switch fabric.

With the **Policy** tab, you can create policy profiles, called roles, assigned to the ports in your network. These roles provide four key policy features: traffic containment, traffic filtering, traffic security, and traffic prioritization. When authentication is enabled, users identify themselves to the network and are given customized access capabilities based on the role they serve in the organization.

Using the **Policy** tab configuration tools, you can create multiple roles tailored to your specific needs, and set a default role for all or some of your network devices and ports. Basic **Policy** tab operations include creating, editing, and deleting roles. You can also view role configuration on a per device and per port basis. In addition, the **Policy** tab allows you to verify the roles enforced on your network device match the roles currently configured in the application. The **Policy** tab supports a maximum of 1,000 devices (25,000 ports) and 50 roles per policy domain, and can process a maximum of 250 classification rules with a maximum of 50 classification rules per role.

Details View

Some Details View tabs display a simple list of items for the current selection in the left panel. However, other Details View tabs present more complex tables of information. To access Help topics on those tabs, expand the Details View Tabs folder in the Policy tab Help Table of Contents. The Help topics are named to reflect the item selected in the left-panel tree. For example, the Help topic for the Details View tab with a device selected in the left panel is named Details View Tab (Device).

Most Details View tabs provide the following features:

- **Right-click Menus -** Right-click an item for a menu of options.
- **Column and Table Functions** - Details View tab tables include several features and functions that enable you to customize the table data.

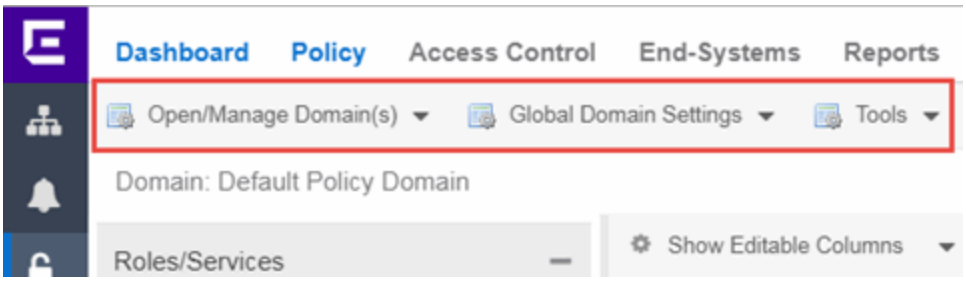
General

A **General** tab is available in the right panel of the **Policy** tab main window for many items selected in the left-panel tab. It provides general properties information about the selected item.

Help topics for the right-panel **General** tabs are named to reflect the item selected in the left-panel tree. For example, the Help topic for the **General** tab with a device selected in the left panel is named General Tab (Device). For more complete information on the different **General** tabs, expand the General Tabs section and select the desired tab.

Policy Menus

The drop-down menus on the **Policy** tab provide access to Policy tab functions. The **Open/Manage Domains** menu provides options for the domain currently accessed. The **Global Domain Settings** drop-down list enables you to configure global **Policy** tab settings. Use the **Tools** menu to configure authentication settings and review Policy events.



Open/Manage Domains Menu

The Open/Manage Domains provides the following options for the **Policy** tab:

Open Domain
: Provides a list of the available Policy Domains. Selecting a domain opens that domain, allowing you to make changes.

Lock Domain
: Lets you lock the current Policy Domain for editing purposes. The **Policy** tab automatically locks the domain when you begin to edit the domain configuration. Other **Policy** tab users are notified that the domain is locked and they are not able to save their own domain changes until the lock is released. For more information, see Controlling Client Interactions with Locks.

Save Domain
: Lets you save any changes you made to the current Policy Domain. Only users with the capability to Enforce are able to save the domain.

Enforce Domain

Writes the role and/or any changes you have made to it (rules, services) to all the devices in your current domain. See Enforcing for more information.

Verify Domain

Compares the roles in your current domain to the roles currently enforced on all the devices in the current domain. This is useful for ensuring the roles in your domain are enforced, or, if you use more than one domain, ensuring that the roles in the domain you are currently using matches what is on the devices. See Verifying for more information.

Assign Devices to Domain

Opens the Assign Devices to Domain window where you can assign devices that are in the ExtremeCloud IQ Site Engine database to the current Policy Domain.

Create Domain

Lets you create and name a new (blank) Policy Domain.

Delete Domain(s)

Opens a window where you can select one or more Policy Domains to delete.

Rename Domain

Lets you rename the current Policy Domain.

Import/Export > Import From Domain

Opens the Import from Domain window where you can import policy configuration data from one Policy Domain into another domain. (This menu option is not available if only one domain exists, as there are no other domains from which to import data.)

Import/Export > Import From File

Opens the Import from File window, which enables you to import policy data from a .pmd file into the current Policy Domain. Be aware that the import overwrites any existing data in the Policy Domain. Any devices in the .pmd file must already exist in the Console database or they won't be imported.

Import/Export > Export to File

Lets you save policy data from the current Policy Domain to a .pmd file or .xml file with the file name and location of your choosing. This file stores all information about roles, services, and rules configured in the current Policy Domain. This allows you to save a Domain configuration prior to making changes so that you can restore the original Domain configuration if required (via Import/Export > Import From File).

Global Domain Settings Menu

The Global Domain Settings Menu provides the following options:

GVRP > Ignore GVRP

To ignore GVRP status on the devices in the current domain, select this menu option and enforce. This means that the **Policy** tab ignores the GVRP configuration on a device during an Enforce operation, allowing you to configure some network devices with GVRP enabled and

others with GVRP disabled (using MIB Tools or local management), according to their configuration requirements. Be aware that for devices with GVRP set to disabled, ignoring GVRP configuration during an Enforce may affect connectivity on ports with VLANs that rely on Dynamic Egress.

GVRP > Enable GVRP
To enable GVRP on the devices in the current domain, select this menu option and enforce. If the current domain configuration contains rules that use VLAN containment, Dynamic Egress and GVRP must be enabled on the devices in the domain, or the VLANs must be properly pre-configured on the devices outside of the **Policy** tab.

GVRP > Disable GVRP
If you do not want GVRP enabled on the devices in the current domain, select this menu option and enforce. Be aware that disabling GVRP may affect connectivity through ports with VLANs that rely on Dynamic Egress.

Port Level Role Mappings Enabled
Check this box to enable any port-level Tagged Packet VLAN to role mappings or port-level MAC to role mappings that have been configured and enforced for the current domain. If the box is not checked, all port-level mappings are ignored.

Do Not Use Global Services
Check this box to hide the display of Global Services in the left-panel **Services** tab for this domain. If you use Global Services in some domains but not in others, this option allows you to hide global services in the domains where they are not used so that they won't be inadvertently used or modified.

Role ACL Mode
Select to use ACLs in place of traditional rules on Summit devices. Enabling this feature also facilitates user-specified ordering and support for creating ACL entries that support multi-traffic descriptor matching.

NOTE: Summit devices must have firmware V30.5 or later.

Tools Menu

Authentication Configuration
Opens the Authentication Configuration wizard, where you can configure authentication settings on a device.

RADIUS Configuration
Opens the RADIUS Configuration wizard, where you can configure RADIUS authentication and accounting settings on a device.

Policy Event Log
Opens the **Events** tab filtered to display only Policy events.

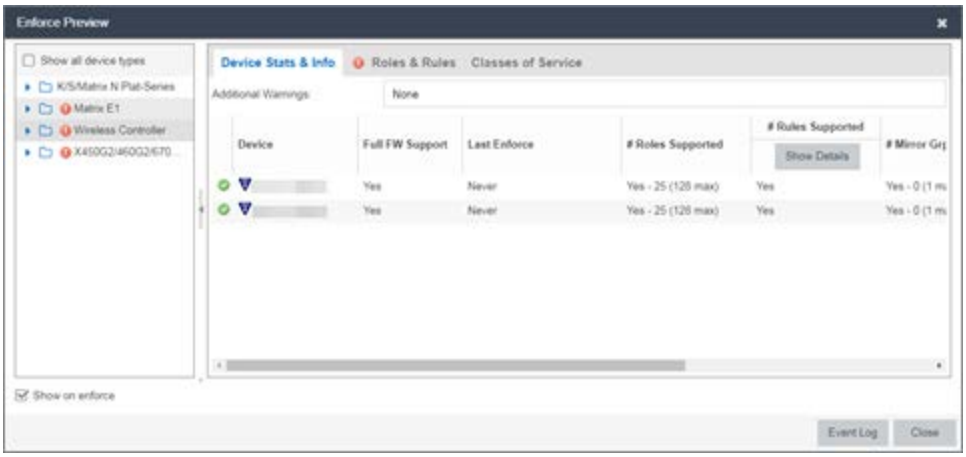
Policy Enforce Preview

Use the **Enforce Preview** window in the **Policy** tab to view the information you are writing to your devices, before you actually enforce. Use this window when enforcing to devices that only support certain aspects of policy management. For example, some devices support only the policy features of policy management; some devices support the policy features and classification rules, but do not support VLAN forwarding for certain classification rules; and some devices fully support all policy management features, including policy, classification rules, and VLAN forwarding for all classification rules.

The **Enforce Preview** window appears in the **Policy** tab by selecting **Open/Manage Domain(s) > Enforce Preview**, or selecting the enforce icon in the left panel and selecting Enforce Preview. You can control whether this view automatically appears when you select **Enforce** with the **Show on Enforce** checkbox.

What you see in the window depends on whether you are enforcing to all devices or to a subset of devices. The title bar indicates the devices to which the enforce applies. After viewing the information in this window, you can either select **Close** to back out and make changes, or **Enforce** to go ahead with the enforce.

You can view device support for specific roles, services, and rules on the **Roles & Rules** tab. Refer to the ExtremeCloud IQ Site Engine Firmware Support matrix for complete information on device support for Policy features, and VLAN and Priority classification rules.



Show on Enforce

When this checkbox is checked, the **Enforce Preview** window appears any time you enforce, before the actual enforcement takes place.

Left Panel

The left panel of the **Enforce Preview** window displays folders for different device types. Expand the folders to see your network devices and device groups organized according to device type. The

warning icon () alerts you that ExtremeCloud IQ Site Engine is not writing a staged change to this device type (e.g. rules not supported on a device).

Show all device types
Select the checkbox in the left panel to display all device types in the left panel. When the checkbox is not selected, only the devices you are changing by enforcing are displayed.

Select a specific device type to display the information ExtremeCloud IQ Site Engine is writing to those devices when you enforce in the right panel.

Right Panel

The right panel provides information about whether certain policy management features are supported and/or enabled for the device type selected in the left panel.

- Additional Warnings - If there are additional problems detected with the enforce, you will be directed to see the Event Log for details.
- GVRP - Shows whether GVRP is Enabled, Disabled, or Ignored. You can change GVRP status for the domain via the Edit menu.
- Dynamic Egress - Shows whether Dynamic Egress is Supported or Not Supported.

Device Stats & Info Tab
Displays the devices for the device type selected in the left panel and provides information about each device. If the number of roles in the domain exceeds the supported number of roles on a device, the enforce fails.

- # of Roles Supported - The maximum number of roles supported by the device.

NOTE: OnExtremeXOS/Switch Engine devices, the maximum number of rules supported is the sum of the maximum L2, MAC and IPv4 rule types reported by the device. In ACL Rule mode, the maximum number of rules supported is reported by the device. Each type (L2, MAC and IPv4) is allocated from the same shared pool of slices for ACLs.

- Domain Role Count Supported - This column says "No" if the number of roles in the domain exceeds the supported number of roles on the device. A "Yes" in this column indicates that the number of roles on the device is equal to or less than the maximum number of supported roles.

Role Statistics - Lists information about each role:

- Number of Rules - The number of traffic classification rules the role includes.
- Number of Unique Masks - The number of masks defined for the rules included in the role.

There are six tabs that provide specific information about the Roles, Classification Rules, VLANs, Classes of Service, and Mappings that will be enforced. The information displayed depends on the

device type you've selected in the left panel, and whether you have the Show All or the Show Errors and Warnings Only radio button selected. In addition, select a role in the Roles tab to filter the information for just that role.

Roles Tab

Incomplete - Lists any roles with unsupported classification rules. These roles will be written to the devices, but without the unsupported rules.
Complete - Lists any roles which do *not* include unsupported classification rules. These roles will be written to the devices as defined.

NOTE: Select a Role to display only those classification rules and VLANs associated with the selected role.

Classification Rules Tab

Excluded - Lists any unsupported classification rules that have been applied to a role. These rules will not be included when the associated roles are written to the devices.
Included - Lists any supported classification rules that have been applied to a role. These rules will be included when the associated roles are written to the devices.

NOTE: On N-Series Platinum devices, range classification rules are achieved through applying subnet masks to values. As such, in order to achieve a user-specified range, the device may need multiple rules with subnets applied to encompass that range. So, although the user created only one rule with a range, this list may show multiple instances of that rule with the name of the rule followed by the portion of the over-all range it applies to.

VLAN Tab

Excluded - Lists any VLANs associated with unsupported classification rules, or VLANs that are not supported by the device. These VLANs will not be written to the devices.
Included - Lists any VLANs associated with supported classification rules and VLANs associated with roles. These will be written to the devices.

Classes of Service Tab

Class of Service Mode - Lists the Class of Service mode that will be written to the devices.
Classes of Service Subtab - Lists the classes of service that will be written to the devices:

- Class of Service - The name of the class of service.
- 802.1p Priority - The priority associated with the class of service.
- ToS Value - The IP Type of Service value associated with this class of service, if any.
- Drop Prec - The drop precedence associated with this class of service, if any.
- TxQueue Index - The transmit queue index associated with the class of service.
- IRL Index - The role-based inbound rate limit index associated with the class of service.

- ORL Index - The role-based outbound rate limit index associated with the class of service.

For more information, see Getting Started with Class of Service and How to Create a Class of Service.

Inbound/Outbound Role-Based Rate Limit Mappings Subtabs - Lists the rate limit mappings that will be written to the devices:

- Device - The device where the rate limit mapping will be in effect.
- IRL/ORL Port Grp - The name of the port group that contains the rate limit mapping.
- IRL/ORL Index - The logical inbound rate limit (IRL) or outbound rate limit (ORL) index number. This index number is specified in a class of service and dictates the rate limiting behavior for incoming packets.
- Rate Limit - The actual rate limit that the IRL/ORL index is mapped to.
- IRL/ORL Port Type - The type of ports included in the port group. Port type is based on the number of rate limits the ports support (for example, 8-rate limit ports and 32-rate limit ports).
- Information - Information about mapping support.

Transmit Queue/Rate Shaper Mappings Subtab - Lists the transmit queue rate shaper mappings that will be written to the devices:

- Device - The device where the transmit queue rate shaper mapping will be in effect.
- TxQ Port Grp - The name of the port group that contains the transmit queue rate shaper mapping.
- TxQ Index - The logical transmit queue rate shaper index number. This index number is specified in a class of service and dictates the transmit queue and rate shaper behavior for incoming packets.
- Physical Transmit Queue / Rate Shaper - The actual transmit queue rate shaper that the index is mapped to.
- TxQ Port Type - The type of ports included in the port group. Port type is based on the number of transmit queues the ports support (for example, 4-transmit queue ports and 16-transmit queue ports).
- Information - Information about mapping support.

Mappings Tab

WARNING: Enforcing port-level MAC to Role mappings could potentially remove rules created as an intrusion detection response.

MAC to Role Mapping - Lists the device-level and port-level mappings that will be written to

the devices:

- Device/Port Level - indicates whether the mapping is a device-level mapping (all devices) or a port-level mapping (IP address and port description). Port-level mappings on frozen ports will be enforced.
- MAC Address - the MAC address mapped to the role. Masking a MAC address is only supported on N-Series Platinum devices.
- Mask - the mask associated with the MAC address.
- Role - the role mapped to the MAC address.

IP to Role Mapping - Lists the device-level mappings that will be written to the devices:

- IP Address - the IP address mapped to the role.
- Mask - the mask associated with each IP address. Masking an IP address is only supported on N-Series Gold and Platinum devices.
- Role - the role mapped to the IP address.

Tagged Packet VLAN to Role Mapping - Lists the device-level and port-level mappings that will be written to the devices:

- Device/Port Level - indicates whether the mapping is a device-level mapping (all devices) or a port-level mapping (IP address and port description). Port-level mappings on frozen ports will be enforced.
- VLAN - the VLAN mapped to the role.
- Role - the role mapped to the VLAN.

Authentication Based VLAN (RFC 3580) to Role Mapping - Lists the mappings that will be written to the devices:

- VLAN - the VLAN mapped to the role.
- Role - the role mapped to the VLAN.

Event Log Button

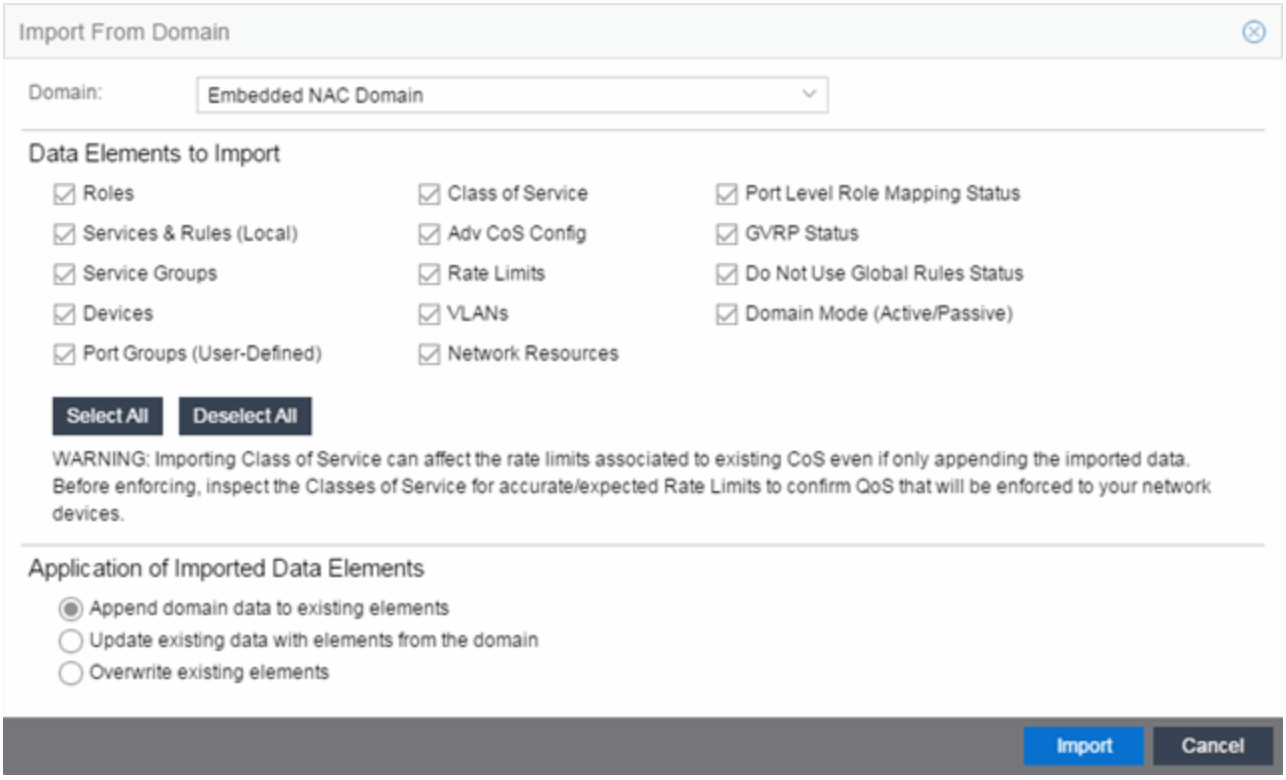
Opens the **Events** tab filtered to display events with an **Event Type** of **Policy**.

Enforce Button

Enforces the roles, classification rules and VLANs in the current data file to the devices, based on the level of support available on the devices as indicated in the **Enforce Preview** window.

Import from Domain

This window lets you import policy configuration data from one Policy Domain into another domain. To access the Import from Domain window, select Open/Manage Domain > Import/Export > Import From Domain. (This menu option is not available if only one domain exists, as there are no other domains from which to import data.)



Domain

Use the drop-down list to select the domain whose data you want to import.

Data Elements to Import

In this section, you can choose the specific data elements you want to import. Select **Select All** to select all the data import options.

Roles

Select this option to import roles, including the role's name, description, default VLAN (access control), and default class of service. If a role's services already exist in the current domain, or if you are importing them at the same time as the role, the services are associated with the role. Otherwise, the services are not imported.

Services & Rules (Local)

Select this option to import Local services (services that are unique to a specific domain) and their associated classification rules. When you import rules from another domain, the Policy tab checks for rule conflicts (see Conflict Checking for more information).

Service Groups

Select this option to import service group names. If a service group's services already exist in the current domain, or if you are importing them at the same time as the service group, the services will be associated with the group. Otherwise, the services will not be imported.

Devices

Select this option to import devices. Any devices in the .pmd file must already exist in the ExtremeCloud IQ Site Engine database or they won't be imported. (See How to Add and Delete Devices for more information on using Console to add devices to the ExtremeCloud IQ Site Engine database.) Devices that are imported are automatically assigned to the current domain and are displayed in the Policy tab Network Elements tree. If the devices being imported were already assigned to another domain, then those devices are reassigned to the current domain. Any devices that are not imported are listed in an Event Log message along with their device type and firmware version.

Port Groups (User-Defined)

Select this option to import user-defined port groups. If you are importing a port group's ports at the same time as the port group, the ports will be associated with the port group. Otherwise, the ports are not imported.

Class of Service

Select this option to import classes of service, role-based rate limit port groups, and transmit queue port groups. For the purposes of importing, a class of service is defined as the class of service name, i.e., priority is not a factor in determining uniqueness. After a class of service is imported, its associated roles, services, and rules are updated. When you import class of service data, the relationship between a class of service and its priority is retained; however, rate limiting characteristics of the priorities are not imported. If you also elect to import rate limits, the rate limits are imported first, then the classes of service are imported. You can then redefine the class of service priorities with some or all of the imported rate limits, if desired. Although ToS characteristics are not used to determine the uniqueness of a class of service for importing, if ToS is a part of a class of service, it is imported as an attribute of the class of service. See append, update and overwrite for information on how those specific actions affect the import of classes of service.

Adv CoS Config

Select this option to import the class of service configuration (basic or advanced) for the domain (whether the Advanced Class of Service Configuration option is selected).

Rate Limits

Select this option to import rate limits. For the purposes of importing, a rate limit is defined as [rate + direction] when determining uniqueness. Any other duplicates on the list are not changed. Because rate limits cannot include conflicting priority values, if a priority is already being utilized by an existing rate limit, it will not be imported. If you also elect to import classes of service, the rate limits are imported first, then the classes of service are imported. See append and update for information on how those specific actions affect the import of rate limits.

NOTE: ZTP+ functionality requires an ExtremeXOS/Switch Engine device on which version 21.1 is installed.

NOTE: Only those network elements that are recognized by the existing domain can be imported as exclusions. Others are ignored.

VLANs

Select this option to import VLANs.

Policy VLAN Islands

If applicable, Policy VLAN Islands and Island VLANs are imported via the Devices and VLANs options.

- If the Devices option is selected and the Policy VLAN Islands feature is enabled in the current domain as well as the imported domain, the Policy VLAN Islands will be imported. The Policy VLAN Island Base ID and Offset settings from the imported data will be used and those in the current domain will be lost.
- If the VLANs option is selected and the Policy VLAN Islands feature is enabled in the current domain as well as the imported domain, the Island VLANs are imported and are added to any existing Policy VLAN Islands.

Whenever Policy VLAN Islands are imported, all the island VLANs are recalculated and the island ranges may change. It is possible to import more islands and VLANs than can be configured. If this is the case, an error appears in the Event Log, asking that the Base ID and Offset settings be changed.

Network Resources

Select this option to import network resource groups. After a Network Resource is imported, the associated services are updated. If a network resource group no longer exists after an import, the service with which it was associated is changed to a manual service on the Automated Service tab for the service.

Port-Level Role Mapping Status

Select this option to import the Port-Level Role Mappings Enabled status for the domain, as specified in the Edit menu.

GVRP Status

Select this option to import the GVRP status for the domain (as specified in the Edit menu).

Do Not Use Global Services Status

Select this option to import the Do Not Use Global Services status for the domain, as specified in the Edit menu.

Domain Mode

Select this option to import the domain mode (active or passive) as specified in the Edit menu.

Application of Imported Data Elements

In this section, you can choose how you want the data elements selected above to update your current domain.

Append domain data to existing elements

Select this option to import only new data elements into your current domain. If any of the selected data elements already exist in your current domain, they will not be changed.

Rate Limits: A rate limit will not be appended if: 1) The Rate, Direction, and 802.1P Priority are already defined. 2) The Priority list is empty.

CoS: A class of service will not be appended if: 1) The name is the same as an existing class of service. 2) The class of service names are different but the rate limits for the imported class of service do not match the existing rate limit settings.

Update existing data with elements from domain

Select this option to 1) replace the selected data elements that exist in your current domain with the imported data elements, and 2) import the selected data elements that don't exist in your current domain.

Rate Limits: A rate limit will not be updated if the rate limit and direction do not match.

CoS: A class of service will not be updated if: 1) The name does not match an existing class of service. 2) The class of service name matches but the rate limits for the imported class of service do not match the existing rate limit settings.

Overwrite existing elements

Select this option to replace the selected data elements that exist in your current domain with the imported data elements.

CoS: A class of service will not be overwritten if the rate limits for the imported class of service do not match the existing rate limit settings.

NOTE: If you decide that you want to return to the previous configuration (that the import updated), you can perform a File > Read Policy Domain operation to restore the configuration, as long as you have not saved the data you imported.

Select All Button

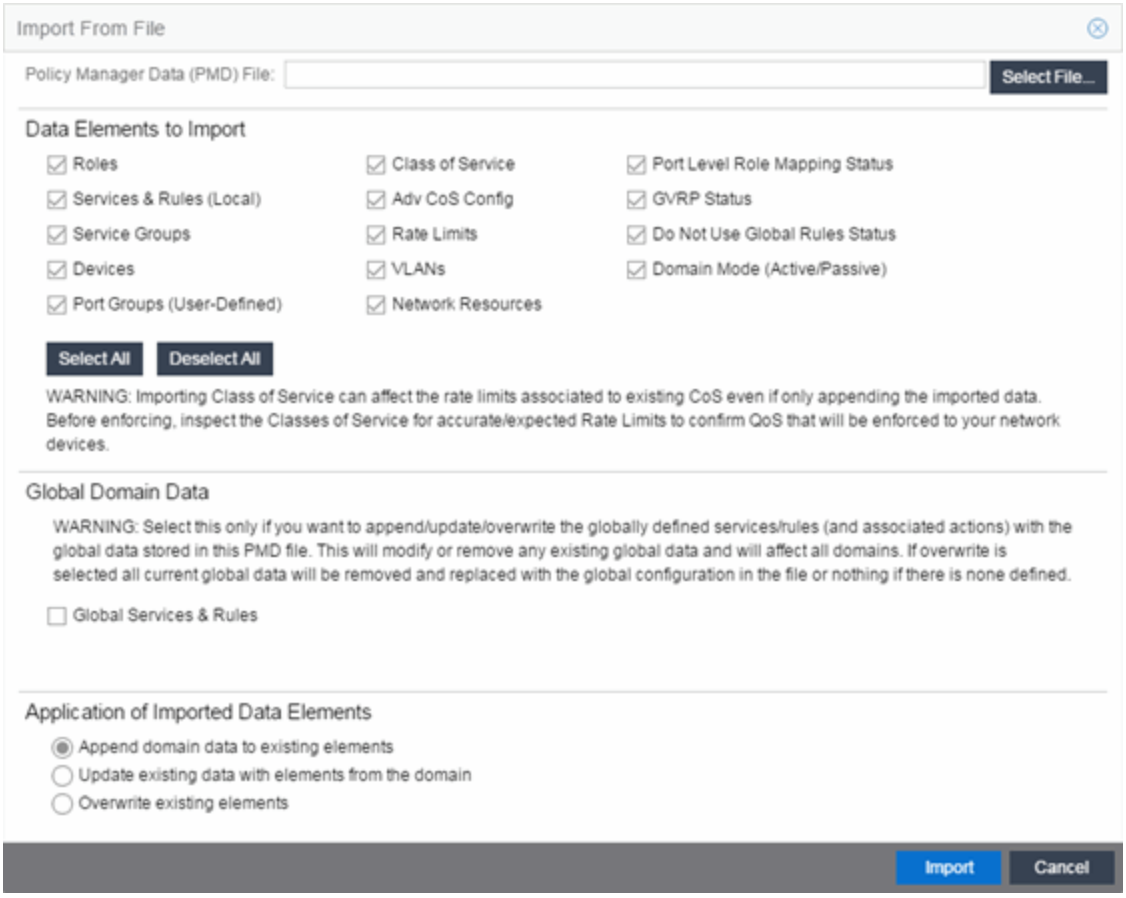
Selects all of the data elements.

Import Button

Imports the selected data and closes the window.

Import from File

This window lets you import policy data from a .pmd file into a Policy Domain. To access the window, select Open/Manage Domains > Import/Export > Import From File.



Policy Manager Data (PMD) File

Enter the name and path for the data file (.pmd) you want to import, or navigate to the file by selecting the **Select File** button.

Data Elements to Import

In this section, you can choose the specific data elements you want to import. Select **Select All** to select all the data import options.

Roles

Select this option to import roles, including the role's name, description, default VLAN (access control), and default class of service. If a role's services already exist in the current domain, or if you are importing them at the same time as the role, the services will be associated with the role. Otherwise, the services are not imported.

Services & Rules (Local)

Select this option to import Local services (services that are unique to a specific domain) and their associated classification rules. When you import rules from another domain, the **Policy** tab checks for rule conflicts (see Conflict Checking for more information).

Service Groups

Select this option to import service group names. If a service group's services already exist in the current domain, or if you are importing them at the same time as the service group, the services are associated with the group. Otherwise, the services are not imported.

Devices

Select this option to import devices. Any devices in the .pmd file must already exist in the ExtremeCloud IQ Site Engine database or they won't be imported. (See How to Add and Delete Devices for more information on using Console to add devices to the ExtremeCloud IQ Site Engine database.) Devices that are imported are automatically assigned to the current domain and are displayed in the Policy tab Network Elements tree. If the devices being imported were already assigned to another domain, then those devices are reassigned to the current domain. Any devices that are not imported are listed in an Event Log message along with their device type and firmware version.

Port Groups (User-Defined)

Select this option to import user-defined port groups. If you are importing a port group's ports at the same time as the port group, the ports are associated with the port group. Otherwise, the ports are not imported.

Class of Service

Select this option to import classes of service, role-based rate limit port groups, and transmit queue port groups. For the purposes of importing, a class of service is defined as the class of service name, i.e., priority is not a factor in determining uniqueness. After a class of service is imported, its associated roles, services, and rules are updated. When you import class of service data, the relationship between a class of service and its priority is retained; however, rate limiting characteristics of the priorities are not imported. If you also elect to import rate limits, the rate limits are imported first, then the classes of service are imported. You can then redefine the class of service priorities with some or all of the imported rate limits, if desired. Although ToS characteristics are not used to determine the uniqueness of a class of service for importing, if ToS is a part of a class of service, it is imported as an attribute of the class of service. See append, update and overwrite for information on how those specific actions affect the import of classes of service.

Adv CoS Config

Select this option to import the class of service configuration (basic or advanced) for the domain (whether the Advanced Class of Service Configuration option is selected).

Rate Limits

Select this option to import rate limits. For the purposes of importing, a rate limit is defined as [rate + direction] when determining uniqueness. Any other duplicates on the list are not changed. Because rate limits cannot include conflicting priority values, if a priority is already being utilized by an existing rate limit, it will not be imported. If you also elect to import classes of service, the rate limits are imported first, then the classes of service are imported. See append and update for information on how those specific actions affect the import of rate limits.

Note: Only those network elements that are recognized by the existing domain can be imported as exclusions. Others will be ignored.

VLANs

Select this option to import VLANs.

Policy VLAN Islands

If applicable, Policy VLAN Islands and Island VLANs are imported via the Devices and VLANs options.

- If the Devices option is selected and the Policy VLAN Islands feature is enabled in the current domain as well as the imported domain, the Policy VLAN Islands will be imported. The Policy VLAN Island Base ID and Offset settings from the imported data will be used and those in the current domain will be lost.
- If the VLANs option is selected and the Policy VLAN Islands feature is enabled in the current domain as well as the imported domain, the Island VLANs are imported and are added to any existing Policy VLAN Islands.

Whenever Policy VLAN Islands are imported, all the island VLANs are recalculated and the island ranges may change. It is possible to import more islands and VLANs than can be configured. If this is the case, an error appears in the Event Log, asking that the Base ID and Offset settings be changed.

Network Resources

Select this option to import network resource groups. After a Network Resource is imported, the associated services are updated. If a network resource group no longer exists after an import, the service with which it was associated is changed to a manual service on the Automated Service tab for the service.

Port-Level Role Mapping Status

Select this option to import the Port-Level Role Mappings Enabled status for the domain.

GVRP Status

Select this option to import the GVRP status for the domain.

Do Not Use Global Services Status

Select this option to import the Do Not Use Global Services status for the domain.

Domain Mode

Select this option to import the domain mode (active or passive) as specified in the Edit menu.

Global Domain Data

Use this option only if you want to append, update, or overwrite the globally defined services and rules in your current domain with the global domain data stored in the .pmd file you are importing. This option will modify or remove any existing global data and will affect all domains. If overwrite is selected, all current global data will be removed and replaced with the global configuration in the file, or nothing if there is no configuration defined.

Global Services & Rules

Select this option to import Global services (services that are common to all domains) and their associated classification rules. When you import rules from another domain, the Policy tab checks for rule conflicts (see Conflict Checking for more information).

Application of Imported Data Elements

In this section, you can choose how you want the data elements selected above to update your current domain.

Append domain data to existing elements

Select this option to import only new data elements into your current domain. If any of the selected data elements already exist in your current domain, they will not be changed.

Rate Limits: A rate limit will not be appended if: 1) The Rate, Direction, and 802.1P Priority are already defined. 2) The Priority list is empty.

CoS: A class of service will not be appended if: 1) The name is the same as an existing class of service. 2) The class of service names are different but the rate limits for the imported class of service do not match the existing rate limit settings.

Update existing data with elements from domain

Select this option to 1) replace the selected data elements that exist in your current domain with the imported data elements, and 2) import the selected data elements that don't exist in your current domain.

Rate Limits: A rate limit will not be updated if the rate limit and direction do not match.

CoS: A class of service will not be updated if: 1) The name does not match an existing class of service. 2) The class of service name matches but the rate limits for the imported class of service do not match the existing rate limit settings.

Overwrite existing elements

Select this option to replace the selected data elements that exist in your current domain with the imported data elements.

CoS: A class of service will not be overwritten if the rate limits for the imported class of service do not match the existing rate limit settings.

NOTE: If you decide that you want to return to the previous configuration (that the import updated), you can perform a File > Read Policy Domain operation to restore the configuration, as long as you have not saved the data you imported.

Select All Button

Selects all of the data elements.

Import Button

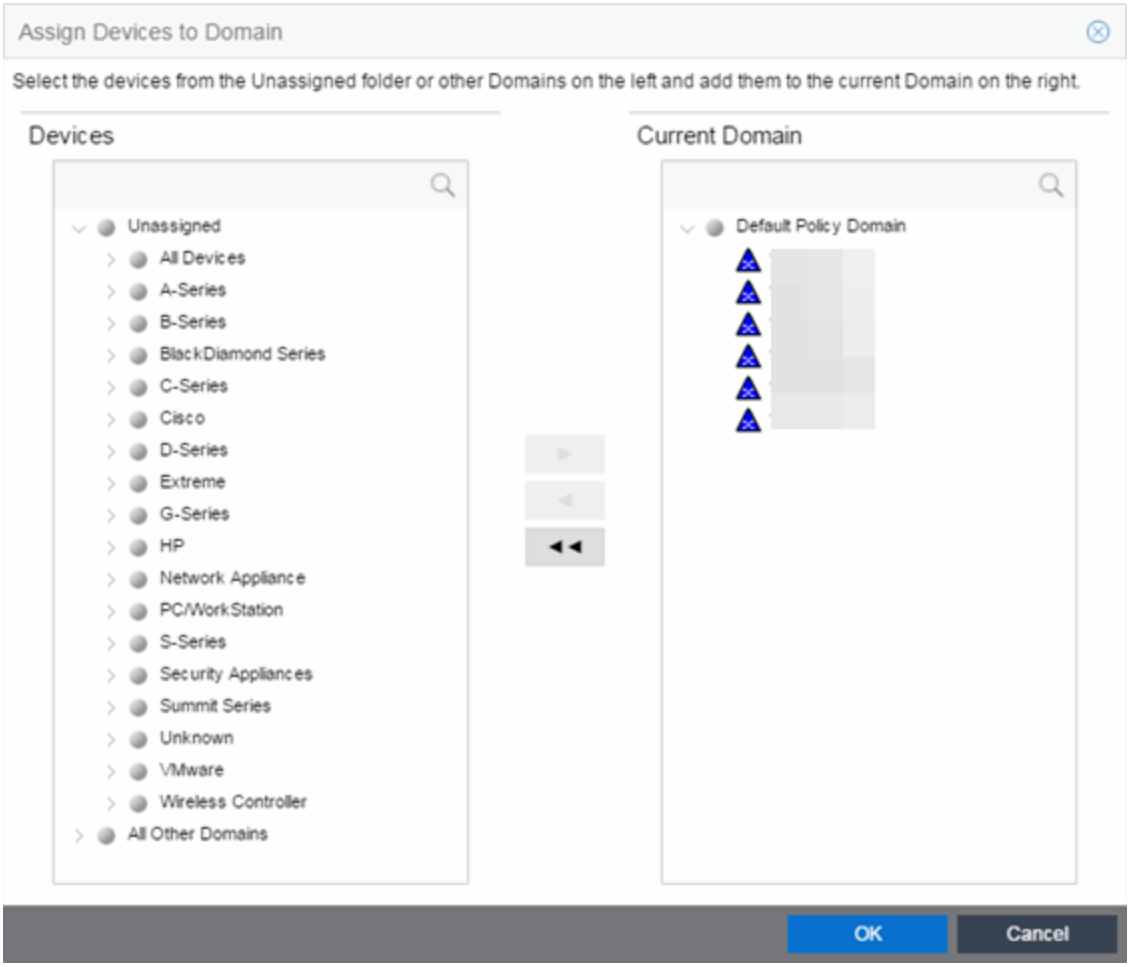
Imports the selected data and closes the window.

Assign Devices to Domain

This window lets you assign devices in the ExtremeCloud IQ Site Engine database to a Policy Domain or move devices from one domain to another. A Policy Domain contains any number of roles and a set of devices uniquely assigned to that particular domain. A device can exist in only one Policy Domain. For more information on domains, see How to Create and Use Domains.

Initially, you must add your devices to the ExtremeCloud IQ Site Engine database. When your devices are in the database, use this window to assign the devices to a Policy Domain. As soon as the devices are assigned to a domain, they display automatically in the **Policy** tab **Devices** tab. Only devices that support policy are displayed in the **Devices** tab.

To access this window, open the domain to which you want to assign devices, and select **Open/Manage Domains > Assign Devices to Domain**.



Devices

The Devices list displays all the unassigned devices in the database (including devices that do not support policy) but are not assigned to a domain. The panel also displays any other domains and the devices assigned to that domain. Use the navigation trees to select a single domain or All Other Domains.

Current Domain

The Current Domain list displays the current domain and the devices assigned to that domain. To add a device to the current domain, select the device in the left panel and select the right arrow. You can also select and add multiple devices. To remove a device from the current domain, select the device and select the left arrow. This removes the device from the current domain and places it back in the device tree as either unassigned or as a member of the domain it came from. To remove all devices, select the double left arrow.

Device Domain Membership

This section is only displayed when more than one domain exists. It lists the domain assignment for whatever device or device group you have selected in the Devices panel. This is particularly useful when you have selected All Other Domains from the drop-down list in the Devices panel, as it allows you to quickly see the domain assignment for each device.

Right Arrow Button

Adds the devices selected in the Devices list to the Current Domain list.

Remove Button

Removes the devices selected in the Current Domain list from the current domain and places it back in the Devices list as either unassigned or as a member of the domain from which it came.

NOTE: Removing a device from a domain does not delete the device from the ExtremeCloud IQ Site Engine database. To delete a device from the database, right-click on the device in the **Network** tab, and select **Device > Delete Device** from the menu. When a device is deleted from the database, it is automatically removed from the **Network** and **Policy** tabs.

Double Left Arrow Button

Removes all the devices from the current domain.

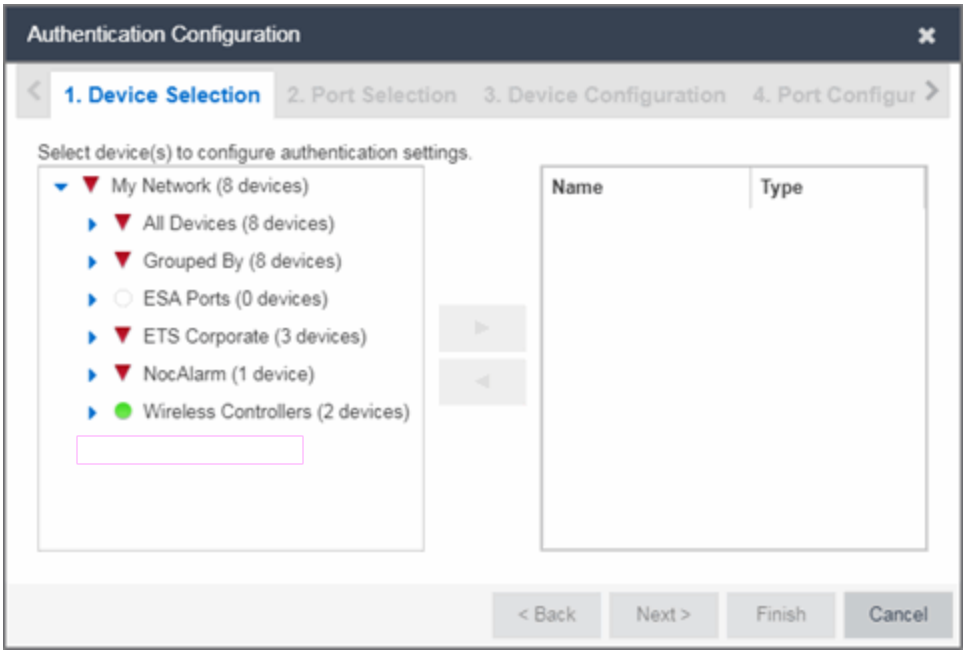
OK Button

Assigns the selected devices to the current domain and displays the devices in the **Policy** tab's **Devices** tab. Only devices that support policy are assigned to the domain and displayed in the **Devices** tab.

Authentication Configuration

The **Authentication Configuration** wizard enables you to configure and change the authentication settings on your devices. Authentication must be configured and enabled on a device in order for individual port authentication settings to take effect (see How to Configure Ports).

To access this tab, select **Authentication Configuration** from the **Tools** drop-down list.



Device Selection

Use the **Device Selection** tab to select the devices on which you are configuring authentication settings.

Select a device from the available devices list in the left of the tab and select the right arrow icon to move the device to the selected devices list. Select **Next>** to proceed to the next tab.

Port Selection

Use the **Port Selection** tab to select the ports on which you are configuring authentication settings.

Select a port from the Available Ports list at the top of the tab and select **Add Ports** to move the port to the Selected Devices list. Select **Next>** to proceed to the next tab.

Device Configuration

The **Device Configuration** tab allows you to configure authentication for a device. Use the **Port Configuration** tab to configure authentication settings for individual ports on the device. You can also use the drop-down list at the top of the tab to load device and port configuration settings from a template or import a template from the ExtremeCloud IQ Site Engine server into ExtremeCloud IQ Site Engine.

Import Template
Select to open a window from which you can select a device and port configuration template saved on the ExtremeCloud IQ Site Engine server.

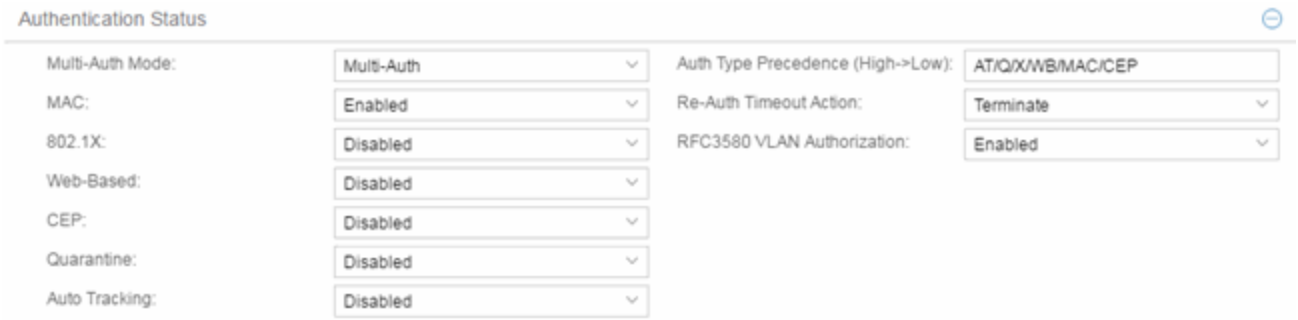
Rename/Delete Template
Select rename or delete a device and port configuration template saved on the ExtremeCloud IQ Site Engine server.

Save Device & Port Config Settings To Template
Select to save the settings you define on the **Device Configuration** and **Port Configuration** tabs to a template you can load for other devices.

Load Device & Port Config Settings From Template
Select to load a previously saved template of settings you previously defined on the **Device Configuration** and **Port Configuration** tabs.

Authentication Status

Use this section to select the authentication mode and types used on the device.



Use the fields on the left side of this section to select the appropriate single- or multi-user authentication types. Only options supported by the selected device are available for selection. Some devices support multiple authentication types and multiple users (Multi-User Authentication) per port, while others are restricted to only one or two authentication types and single users per port. Refer to the Firmware Support matrix for information on the authentication types supported by each device type.

WARNING: Switching Authentication Types, or changing the Authentication Status from Enabled to Disabled, logs off any currently authenticated users.

Auth Type Precedence (High->Low)

This displays the order in which the authentication types are attempted on the device, with the authentication type on the left having the highest precedence (attempted first). You can edit the precedence order by selecting the field. In the Edit Precedence window, select the authentication type you want to position, and use the **Up** and **Down** buttons to arrange the types in the desired order of precedence.

WARNING: Leave the default precedence, if possible. Changing the Quarantine precedence to be lower than any other type or changing the Auto Track precedence to be higher than any other type may cause problems.

Re-Auth Timeout Action

This setting defines the action for sessions that need to be re-authenticated if the RADIUS server re-authentication request times out. Select the **Terminate** option to terminate the session or the **None** option to allow the current session to continue without disruption.

Maximum Number of Users

This setting applies to devices with Multi-User as their configured authentication type. The maximum number of users that can be actively authenticated or have authentications in progress at one time on this device. You can specify the maximum number of users per port on the port's Port Properties Authentication Configuration tab.

RFC3580 VLAN Authorization

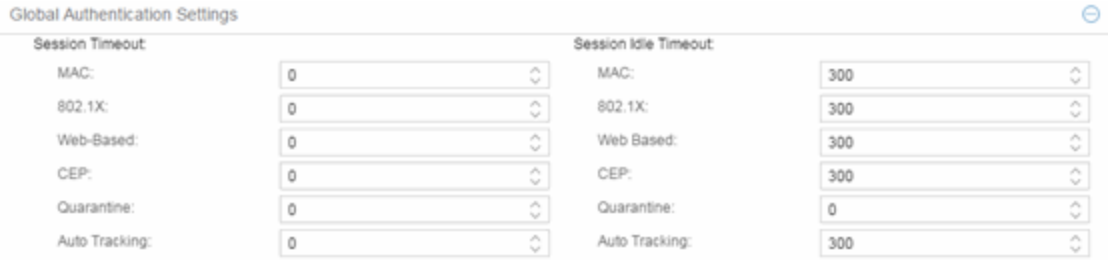
This allows you to enable and disable RFC 3580 VLAN Authorization for the selected device. RFC 3580 VLAN Authorization must be enabled on devices in networks where the RADIUS server is configured to return a VLAN ID when a user authenticates.

When RFC 3580 VLAN Authorization is enabled:

- devices that do **not** support policy tag packets with the VLAN ID.
- devices that support both policy and Authentication-Based VLAN to Role Mapping classify packets according to the role to which the VLAN ID maps.

Global Authentication Settings

This section lets you set session timeout and session idle timeout values for each authentication type.



Session Timeout

This setting represents the maximum number of seconds an authenticated session may last before automatic termination of the session. A value of zero indicates that no session timeout applies. This value may be superseded by a session timeout value provided by the authenticating server. For example, if a session is authenticated by a RADIUS server, that server may send a session timeout value in its authentication response.

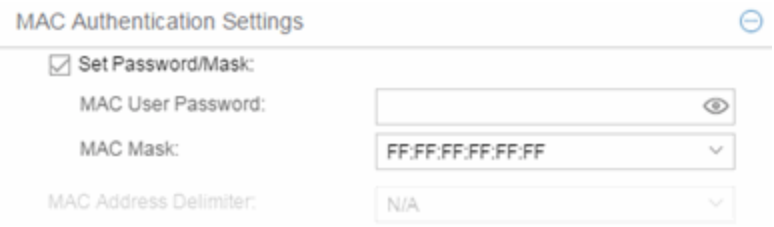
NOTE: Non-zero values are rounded to the nearest non-zero multiple of 10 by the device.

Session Idle Timeout

This displays the maximum number of consecutive seconds an authenticated session may be idle before ExtremeCloud IQ Site Engine automatically terminates the session. A value of zero indicates that no idle timeout applies. This value may be superseded by an idle timeout value provided by the authenticating server. For example, if a session is authenticated by a RADIUS server, that server may send an idle timeout value in its authentication response.

MAC Authentication Settings

This section enables you to set up the MAC password for MAC authentication. In order for MAC authentication to work, you must also configure the RADIUS server with the MAC password as well as the MAC addresses which are allowed to authenticate.



Set Password/Mask

Select this checkbox to set a password and mask for MAC authentication.

MAC User Password

The password passed to the RADIUS server for MAC authentication.

MAC Mask

You can select a mask to provide a way to authenticate end-systems based on a portion of their MAC address. For example, you could specify a mask that would base authentication on the manufacturers ID portion of the MAC address. The MAC Mask is passed to the RADIUS server for authentication after the primary attempt to authenticate using the full MAC address fails.

MAC Address Delimiter

The character used between octets in a MAC address:

- **None** — No delimiter is used in the MAC address (e.g. xxxxxxxxxxxx).
- **Hyphen** — A hyphen is used as a delimiter in the MAC address (e.g. xx-xx-xx-xx-xx-xx).

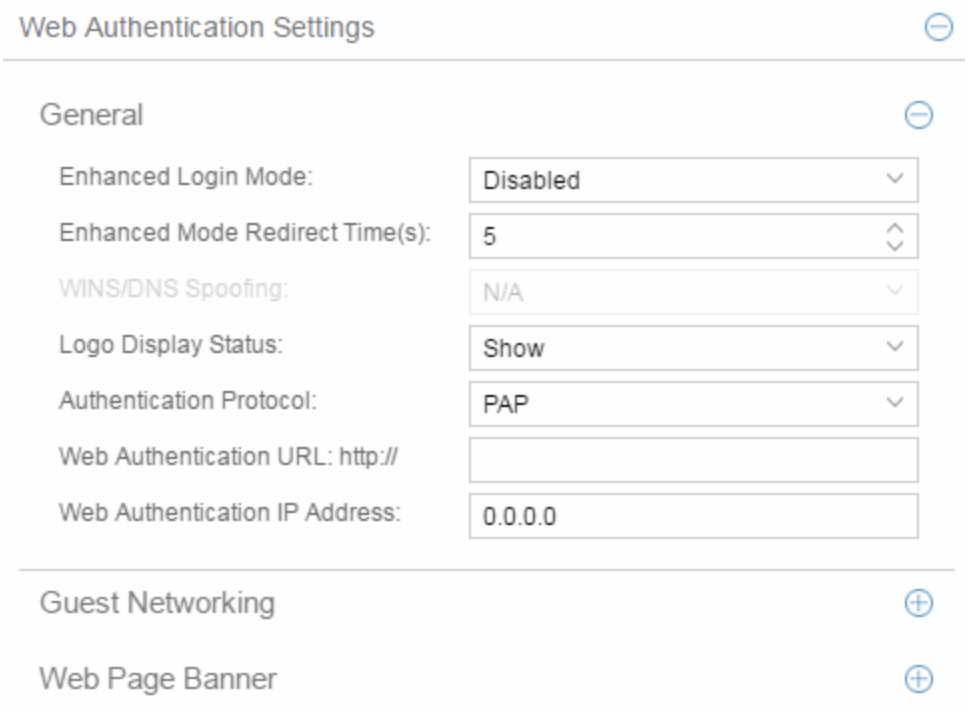
Web Authentication Settings

For users of web-based authentication, this tab lets you specify web authentication parameters using three sections:

- General
- Guest Networking
- Web Login

General

The General section lets you specify the URL of the authentication web page and the IP address of the system where it resides. It also lets you enable certain web authentication features, such as Enhanced Login Mode, on devices that support those features.



Enhanced Login Mode

Enabling the Enhanced Login Mode causes the authentication web page to be displayed regardless of whether the URL or IP address entered into the browser by the end user is the designated Web Authentication URL or IP address. This option is grayed out if the device does not support the mode.

Enhanced Mode Redirect Time(s)

This setting applies for devices with Enhanced Login Mode enabled. It specifies the amount of time (in seconds) before the end-user is redirected from the authentication web page to their requested URL.

An end-system using DHCP requires time to transition from the temporary IP address issued by the authentication process to the official IP address issued by the network. **Enhanced Mode Redirect Time** specifies the amount of time allowed for the end-system to complete this process and begin using its official IP address.

For example, if an end-user (in **Enhanced Login Mode** and a **Redirect Time** of **30 seconds**) enters the URL of "http://ExtremeNetworks.com", the user is presented the authentication web page. When the user successfully authenticates into the network, the user sees a login success page that displays "Welcome to the Network. Completing network connections. You will be redirected to http://ExtremeNetworks.com in approximately 30 seconds."

WINS/DNS Spoofing

This setting allows you to enable and disable WINS/DNS spoofing for the selected device. Spoofing allows the end-user to resolve the Web Authentication URL name to the IP address

using WINS/DNS. The default is Disabled. This option is grayed out if not supported by the device.

Logo Display Status
Specifies whether the Extreme Networks logo is displayed or hidden on the authentication web page window. This option is grayed out if not supported by the device.

Authentication Protocol
This setting is the authentication protocol being used (PAP or CHAP). PAP (Password Authentication Protocol) provides an automated way for a PPP (Point-to Point Protocol) server to request the identity of user, and confirm it via a password. CHAP (Challenge Handshake Authentication Protocol), the more secure of the two protocols, provides a similar function, except that the confirmation is accomplished using a challenge and response authentication dialog.

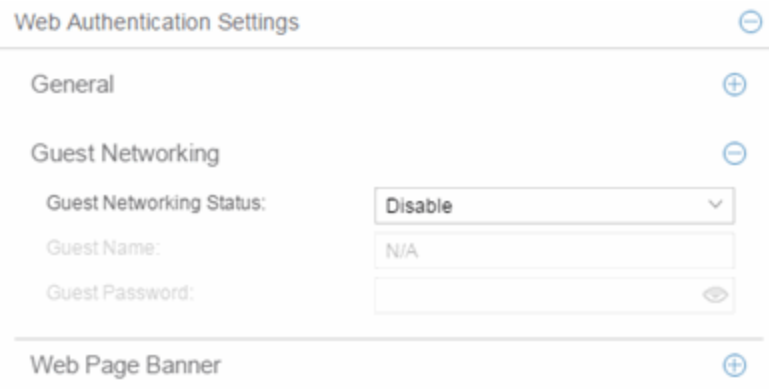
Web Authentication URL
This is the URL for your authentication web page. Users wishing to receive network services access the web page from a browser using this URL. The **http://** is supplied. Alphabetical characters, numerical characters and dashes are allowed as part of the URL, but dots are not. The URL needs to be mapped to the Web Authentication IP address in DNS or in the hosts file of each client. It must be resolvable via DNS/WINS, either on the device or at corporate, assuming the Web Authentication mapping has been set up on the corporate DNS/WINS service. This option is grayed out if not supported by the device.

Web Authentication IP Address
This is the IP address of your authentication web page server. If you have specified a Web Authentication URL, the IP address needs to be mapped to the URL in DNS or in the host file of each client.

Guest Networking

The **Guest Networking** section lets you configure guest networking, a feature that allows any user to access the network and obtain a guest policy without having to know a username or password. The user accesses the authentication web page, where the username and password fields are automatically filled in, allowing them to log access as a guest. If the user does not want to log in as a guest, they can type in their valid username and password to log in.

NOTE: Guest networking is designed for networks using web-based authentication, with port mode set to Active/Discard.



Guest Networking Status

Use the drop-down list to specify guest networking status:

- **Disable** — Guest networking is unavailable.
- **Local Auth** — Guest Networking is enabled. The user accesses the authentication web page where the username field is automatically filled in with the specified Guest Name. When the user submits the web page using this guest name, the default policy of that port becomes the active policy. The port mode must be set to Active/Discard mode.
- **RADIUS Auth** — Guest Networking is enabled. The user accesses the authentication web page, where the username field is automatically filled in with the specified Guest Name, and the password field is masked out with asterisks. When the user submits the web page using these credentials, the value of the Guest Password is used for authentication. Following successful authentication from the RADIUS server, the port applies the policy (role) returned from the RADIUS server. The port mode must be set to Active/Discard mode.

Guest Name

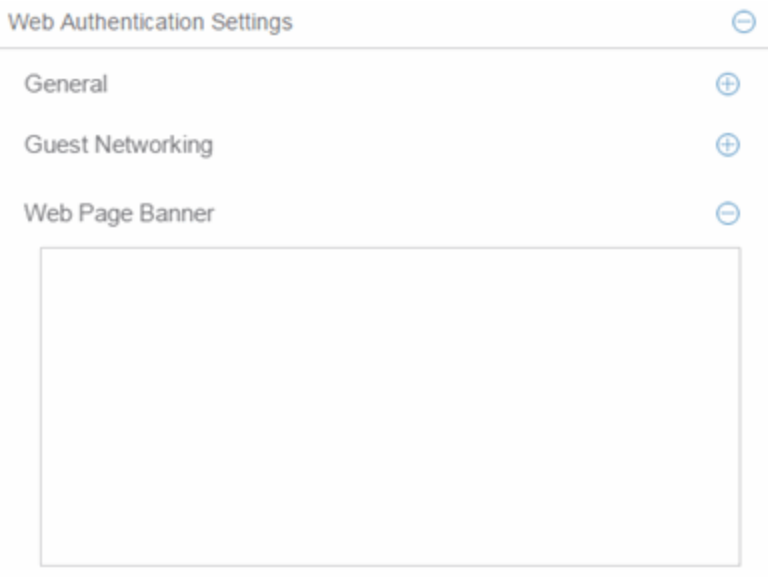
The username that Guest Networking uses to authenticate users. The guest name is displayed automatically on the authentication web page. If the user does not want to log in as a guest, they can type in their valid username to override the guest username.

Guest Password

The password that Guest Networking uses to authenticate users when RADIUS Auth is selected.

Web Page Banner

The Web Page Banner section allows you to customize the banner end users see at the top of the authentication web page and set a Redirect Time, if applicable.



Web Page Banner

Use this area to create a banner end users see at the top of the authentication web page. For example, you might include your company name and information on what to do if the user has questions or problems. Because this banner also appears in messages that occur during successful login and failed authentication, as well as on the "Radius Busy" screen, it is not appropriate to include "Welcome to [Your Company]" in the banner.

The **Default** button allows you to reset the banner to default text provided in a text file (pwa_banner.txt). Initially, the default banner text is the Extreme Networks contact information. However, you can customize the text for your network by editing the pwa_banner.txt file, located in the top level of the Policy Manager install directory. Then, when you select the Default button, the new text will be displayed in the Web Page Banner area.

Convergence End-Point Settings

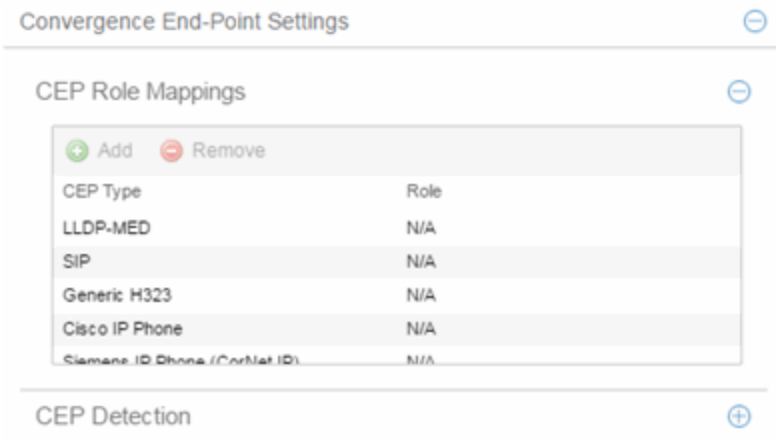
This section provides a way to identify Convergence End-Points (IP phones) connecting to the device, and apply a role to the end-point based on the type of end-point detected. The CEP Detection section lets you create detection rules for identifying the end-points, and the CEP Role Mappings section lets you map a role to each CEP product type.

In addition to configuring CEP on the device, you must also enable CEP protocols on each port using the CEP Access section in the Port Authentication Tab. After you have configured CEP on the device and each port, you can monitor CEP usage on the Port Usage Tab (Port) or Port Usage Tab (Device).

CEP Role Mappings

This section lets you select the CEP product types supported on the device, and map a role for each type. Then, when a convergence end-point (such as an IP phone) connects to the network, the device

identifies the type of end-point (using CEP detection rules) and applies the assigned role.



CEP Type
Lists the CEP types supported by the device.

Role
Lists the role mapped to each **CEP Type**.

Add
Select a CEP Type and select the **Add** button to open the Add Role Mapping window, where you can select a role for the selected **CEP Type**. Your selections are added to the CEP Role Mappings list.

Remove
Select the **CEP Type** and select **Remove** to remove the **CEP Type** in the CEP Role Mappings list.

CEP Detection Tab

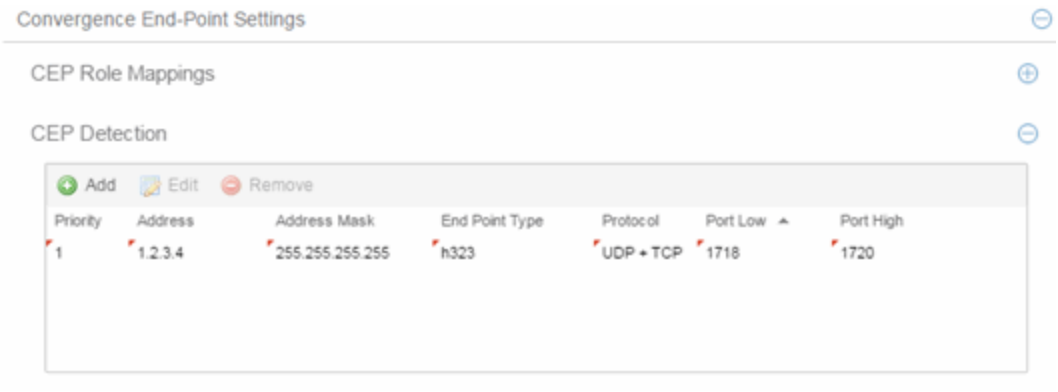
Use this section to create CEP detection rules used to determine if a connecting end-system is a CEP device and the type of CEP device. This allows ExtremeCloud IQ Site Engine to assign the appropriate role to the port based on the type of CEP device detected.

NOTE: CEP detection rules apply only to Siemens, H.323, and SIP (Session Initiation Protocol) phone detection. Cisco detection uses CiscoDP as its detection method.

CEP detection rules are based on two detection methods:

- TCP/UDP Port Number detection — Many CEP vendors use specific TCP/UDP port numbers for call setup on their IP phones. You can create detection rules that identify CEP devices based on specific TCP/UDP port numbers. By default, Siemens Hi-Path phones are detected on TCP/UDP port 4060.
- IP Address detection — H.323 phones use a reserved IP multicast address and UDP port number for call setup. You can create detection rules to detect an IP phone based on its IP

address in combination with an IP address mask. By default, H.323 phones are detected using the multicast address 224.0.1.41 and the TCP/UDP ports 1718, 1719, and 1720. SIP phones are detected using the multicast address 224.0.1.75 and the TCP/UDP port 5060. H.323 and SIP phones are also detected using only their respective multicast addresses without the TCP/UDP ports.



Priority

The rule priority with one (1) being the highest priority. The rule with the highest priority is used first, so it is recommended the highest priority be given to the predominate protocol in the network to provide for greater efficiency.

Address

If the rule is based on IP address detection, this field displays the IP address that incoming packets matched against. By default, H.323 uses 224.0.1.41 as its IP address, SIP uses 224.0.1.75 as its IP address, and Siemens has no IP address configured.

Address Mask

If the rule is based on IP address detection, this field displays the IP address mask against which incoming packets are matched.

End Point Type

Specifies the end-point type assigned (H.323, Siemens, or SIP) if incoming packets match this rule.

Protocol

If the rule is based on TCP/UDP port detection, this field displays the protocol type used for matching, using a port range defined with the Port Low and Port High values:

- UDP + TCP — Match the port number for both UDP and TCP frames.
- TCP — Match the port number only for TCP frames.
- UDP — Match the port number only for UDP frames.

Port Low

The low end of the port range defined for detection on UDP and/or TCP ports.

Port High
The high end of the port range defined for detection on UDP and/or TCP ports.

Add
Opens the Add/Edit CEP Detection Rule window where you can create CEP detection rules.

Remove
To remove a CEP detection rule, select the entry and select **Remove**.

Edit
To edit a CEP detection rule, select the rule and select **Edit**. The Add/Edit CEP Detection Rule window opens where you edit the rule's parameters. You can also double-click an entry in the table to open the edit window.

Port Configuration

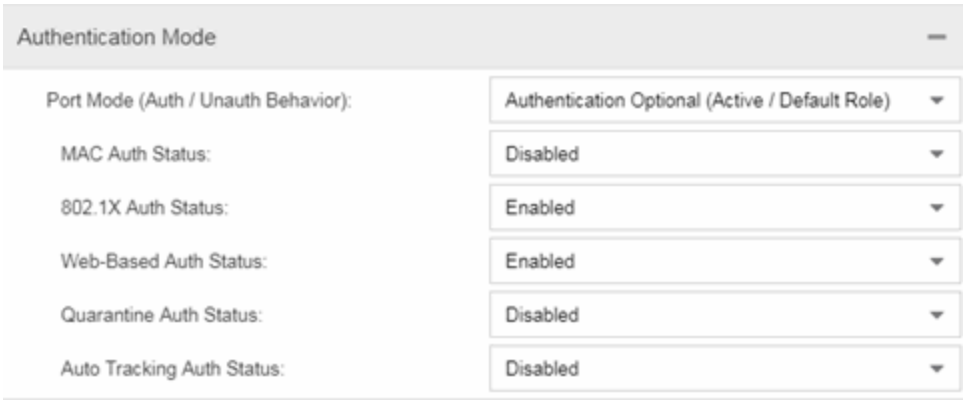
The **Port Configuration** tab allows you to configure authentication for the ports of a device.

The **Authentication Configuration** tab has six sections:

- Authentication Mode
- RFC3580 VLAN Authorization
- Login Settings
- Automatic Re-Authentication
- Authenticated User Counts
- CEP Access

Authentication Mode

This section displays general authentication and port mode information about the port.



Port Mode

Port mode defines whether or not a user is required to authenticate on a port, and how unauthenticated traffic will be handled. It is a combination of Authentication Behavior (whether or not authentication is enabled on the port), and Unauthenticated Behavior (whether unauthenticated traffic will be assigned to the port's default role or discarded).

- **Authentication Behavior** -- Defines whether or not end users are required to authenticate on the port (device).
    - **Active** -- Normal authentication procedures are implemented. End users are required to authenticate.
    - **Inactive** -- Authentication of end users is not required.
- **Unauthenticated Behavior** -- Defines how the traffic of unauthenticated end users will be handled on the port.
    - **Default Role** -- If the end user is unauthenticated, the port will implement its default role. If there is no default role, there will be no role on the port.
    - **Discard** -- If the end user is unauthenticated, no traffic is allowed on the port.

These two settings can be combined to create four possible port modes.

- **Inactive/Discard Mode**: In this mode, authentication is inactive for the port. All traffic from users connected to the port is discarded. This effectively turns the port off. This port mode is not available for Single User MAC Authentication.

- **Inactive/Default Role Mode**: In this mode, authentication is inactive for the port. All users connecting to this port will use the default role, if one has been assigned to the port, in combination with any existing static classifications. If there is no default role assigned to the port, the port uses only the static classification rules which exist. If there are no static rules, the port uses the PVID and default class of service for the port. This is the default port mode for ports.

- **Active/Discard Mode**: In this mode, authentication is active for the port and end users are required to authenticate. All traffic from unauthenticated users connected to the port is discarded. The Unauthenticated Behavior varies depending on the type of authentication configured on the device.

  Single User Web-based Authentication: If authentication is successful, the port is assigned the end user's role as its current role. If unsuccessful, all traffic is discarded. A default role has no meaning on this Active/Discard port, since all unauthenticated traffic is discarded.

  Single User 802.1X and 802.1X+MAC Authentication: If authentication is successful, the port is assigned the end user's role as its current role. If unsuccessful, all traffic is discarded. This

mode requires that there be **no** default role assigned to the port.

Single User MAC Authentication: This port mode is not available for Single User MAC Authentication.

Multi-User 802.1X and MAC Authentication: If authentication is successful, the port is assigned the end user's role as its current role. If unsuccessful, all traffic is discarded. A default role has no meaning on this Active/Discard port, since all unauthenticated traffic is discarded.

Multi-User Web-based Authentication: This port mode is not available for Multi-User Web-based Authentication.

Advantages of Active/Discard mode: This mode is highly secure, since the end user receives no network services at all until authentication is successful.

Disadvantages of Active/Discard mode: The unauthenticated end user is unable to connect to any network services, such as the Domain Controller (if using a Microsoft operating system), DHCP services, DNS services, or the Web proxy. In single user web-based authentication, the device spoofs WINS/DNS services (if the functionality is enabled) in order to allow the user to communicate with it for authentication.

- **Active/Default Role Mode** - In this mode, authentication is active for the port and end users are required to authenticate. If authentication is successful, the port is assigned the end user's role as its current role. All unauthenticated users connected to the port will use the default role, if one has been assigned to the port, in combination with any existing static classifications. If there is no default role assigned to the port, the port uses only the static classification rules which exist. If there are no static rules, the port uses the PVID and default class of service for the port. For Single User 802.1X and 802.1X+MAC Authentication, this mode **requires** that a default role be assigned to the port.

  Advantages of Active/Default Role mode: In this mode, a default role is applied to the port to allow unauthenticated end users access to basic services such as the DHCP Server, Domain Services, WINS, and the Web proxy. When the end user is authenticated, that user's role is applied to the port, providing a customized set of services allowed by his or her role. Active/Default Role mode is an alternative to Active/Discard mode, which is limiting in that there are no network services available at all until the end user is authenticated.

  Disadvantages of Active/Default Role mode: This mode is less secure than Active/Discard, in that the user receives some network access prior to authentication.

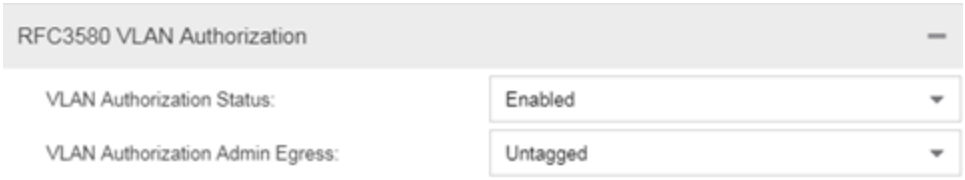
RFC3580 VLAN Authorization Tab

This tab lets you enable or disable RFC 3580 VLAN Authorization on the port and specify an egress state. RFC 3580 VLAN Authorization must be enabled in networks where the RADIUS server has been configured to return a VLAN ID when a user authenticates.

When RFC 3580 VLAN Authorization is enabled:

- ports on devices that do **not** support policy tag packets with the VLAN ID.
- ports on devices that do support policy and also support Authentication-Based VLAN to Role Mapping classify packets according to the role to which the VLAN ID maps.

You can also enable and disable VLAN Authorization at the device level using the device **Authentication** tab. If the device does not support RFC 3580, this tab is grayed out.



VLAN Authorization Status

Allows you to enable and disable RFC 3580 VLAN Authorization for the selected port. This option is grayed out if not supported by the device.

VLAN Authorization Admin Egress

Allows you to modify the VLAN egress list for the VLAN ID returned by the RADIUS server when a user authenticates on the port:

- None - No modification to the VLAN egress list will be made.
- Tagged - The port will be added to the list with the egress state set to Tagged (frames will be forwarded as tagged).
- Untagged - The port will be added to the list with the egress state set to Untagged (frames will be forwarded as untagged).
- Dynamic - The port will use information returned in the RADIUS response to modify the VLAN egress list. This value is supported only if the device supports a mechanism through which the egress state may be returned in the RADIUS response.

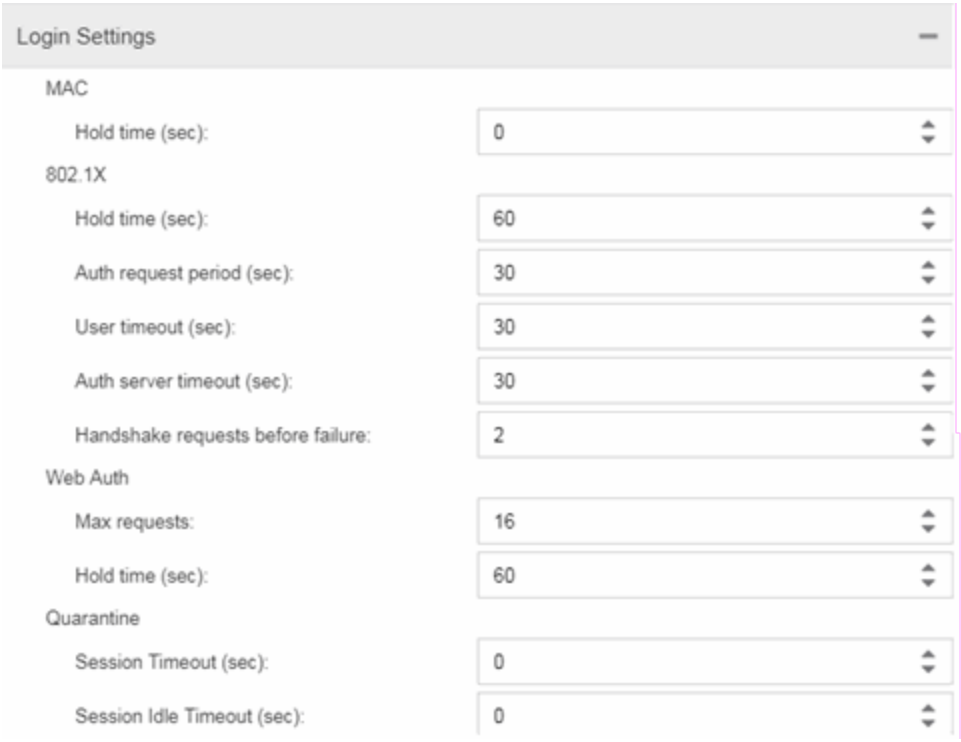
The current egress settings for the port are displayed in the VLAN Oper Egress column in the **User Sessions** tab. These options are grayed out if not supported by the device.

Apply Button

Saves any change you made to the VLAN Authorization settings.

Login Settings

This tab displays the current login settings for the port and allows you to change the settings if desired. The options available depend on what type(s) of authentication are enabled on the device.



Number of Attempts Before Timeout

Number of times a user can attempt to log in before authentication fails and login attempts are not allowed. For web-based authentication, valid values are 1-2147483647, zero is not allowed, and the default is 2. For 802.1X and MAC authentication, this value is permanently set to 1.

Hold Time (seconds)

Amount of time (in seconds) authentication will remain timed out after the specified Number of Attempts Before Timeout has been reached. Valid values are 0-65535. The default is 60. (Hold Time is also known as Quiet Period in web-based and MAC authentication.)

Authentication Request Period

For 802.1X authentication, how often (in seconds) the device queries the port to see if there is a new user on it. If a user is found, the device then attempts to authenticate the user. Valid values are 1-65535. The default is 30.

User Timeout

For 802.1X authentication, the amount of time (in seconds) the device waits for an answer when querying the port for the existence of a user. Valid values are 1-300. The default is 30.

Authentication Server Timeout
For 802.1X authentication, if a user is found on the port, the amount of time (in seconds) the device waits for a response from the authentication server before timing out. Valid values are 1-300. The default is 30.

Port Handshake Requests Before Failure
For 802.1X authentication, the number of times the device tries to finalize the authentication process with the user before the authentication request is considered invalid and authentication fails. Valid values are 1-10. The default is 2.

Quarantine Session Timeout (sec)
For Quarantine authentication, the maximum number of seconds an authenticated session may last before automatic termination of the session. A value of zero indicates that no session timeout will be applied.

Quarantine Session Idle Timeout (sec)
For Quarantine authentication, the maximum number of consecutive seconds an authenticated session may be idle before automatic termination of the session. A value of zero indicates that the device level setting is used.

Auto Tracking Session Timeout (sec)
For Auto Tracking sessions, the maximum number of seconds a session may last before automatic termination of the session. A value of zero indicates that the device level setting is used.

Auto Tracking Session Idle Timeout (sec)
For Auto Tracking sessions, the maximum number of consecutive seconds a session may be idle before automatic termination of the session. A value of zero indicates that the device level setting is used.

Apply Button
Applies the Login Settings changes to the port.

Automatic Re-Authentication

This tab is grayed out if only web-based authentication is enabled on the device. For 802.1X and MAC authentication, the Automatic Re-Authentication tab lets you set up the periodic automatic re-authentication of logged-in users on this port. Without disrupting the user's session, the device repeats the authentication process using the most recently obtained user login information to see if the same user is still logged in. Authenticated logged-in users are not required to log in again for re-authentication, as this occurs "behind the scenes."



802.1X Re-auth Status

If **Active** is selected, the re-authentication feature is enabled for 802.1X authentication. If **Inactive** is selected, the re-authentication feature is disabled.

802.1X Re-auth Frequency (sec)

How often (in seconds) the device checks the port to re-authenticate the logged-in user via 802.1X authentication. Valid values are 1-2147483647. The default is 3600.

MAC Re-auth Status

If **Active** is selected, the re-authentication feature is enabled for MAC authentication. If **Inactive** is selected, the re-authentication feature is disabled.

MAC Re-auth Frequency (sec)

How often (in seconds) the device checks the port to re-authenticate the logged in user via MAC authentication. Valid values are 1-2147483647. The default is 3600.

Authenticated User Counts

This tab provides authenticated user-count information for devices with Multi-User as their configured authentication type. See the device Authentication tab for information on setting the device authentication type.



Current Number of Users

The current number of users actively authenticated or have authentications in progress on this interface. If **Multi-User** authentication is disabled, this number is **0**. Any unauthenticated traffic on the port is not included in this count.

Number of Users Allowed (up to 2048)

The number of users that can be actively authenticated or have authentications in progress at one time on this interface. If you set this value below the current number of users, end-user sessions exceeding that number are terminated.

NOTE: B2/C2 Devices. If you are configuring a single user and an IP phone per port, set this value to **2**.

Number of MAC Users Allowed (up to 2048)

The number of users that can be actively authenticated via MAC authentication, or have MAC authentications in progress at one time on this interface. The number of MAC users allowed cannot exceed the number of users allowed. If you set this value below the current number of users, end user sessions exceeding that number are terminated. If MAC is not selected as a **Multi-User** authentication type on the device Authentication tab, this field will be grayed out.

Number of Quarantine Users Allowed (up to 2048)

The number of users that can be actively authenticated via Quarantine authentication, or have Quarantine authentications in progress at one time on this interface. The number of Quarantine users allowed cannot exceed the number of users allowed. If you set this value below the current number of users, end user sessions exceeding that number are terminated. If Quarantine Auth is not enabled on the device Authentication tab, this field will be grayed out.

Number of Auto Tracking Users Allowed (up to 2048)

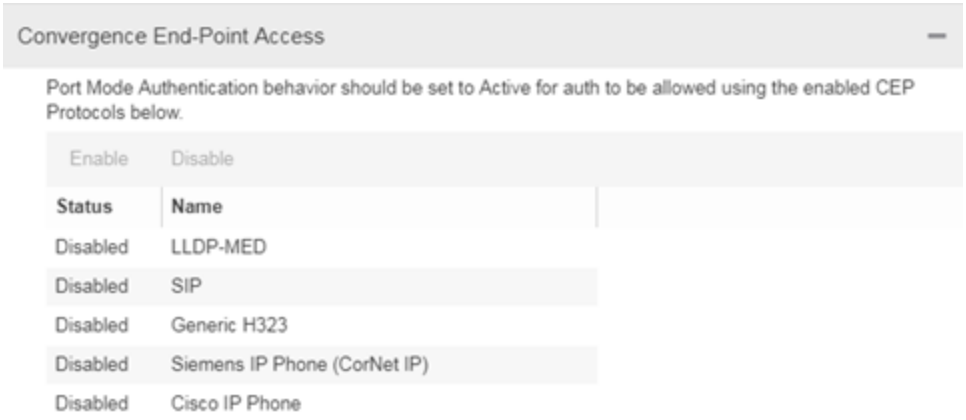
The number of Auto Tracking users that can be actively authenticated or have authentications in progress at one time on this interface. The number of Auto Tracking users allowed cannot exceed the number of users allowed. If you set this value below the current number of users, end user sessions exceeding that number will be terminated. If Auto Tracking is not enabled on the device Authentication tab, this field is grayed out.

Convergence End-Point Access

This tab lists all the CEP (Convergence End-Point) protocols supported by the device on which the port resides, and lets you enable or disable them for that port. For devices that do not support CEP, the tab is blank.

NOTE: Port Mode Authentication Behavior must be set to **Active** (on the General sub-tab) for authentication to be allowed using these CEP Protocols.

Enable CEP protocols for multiple ports using the Port Configuration Wizard. In addition to enabling protocols on the port, you must also configure CEP for the device on which the port resides. Configure CEP for a single device using the device Authentication tab (CEP sub-tab) or for multiple devices using the Device Configuration Wizard.



CEP Access

Lists all the CEP protocols supported by the device on which the port resides. Use the checkboxes to enable or disable CEP protocols on this port. If the device does not support the CEP feature, this area is blank.

Enable All Button

Selects all the checkboxes and enables all the CEP protocols for this port.

Disable All Button

Deselects all the checkboxes and disables all the CEP protocols for this port.

Apply Button

Applies CEP access changes to the port.

Policy Main Window

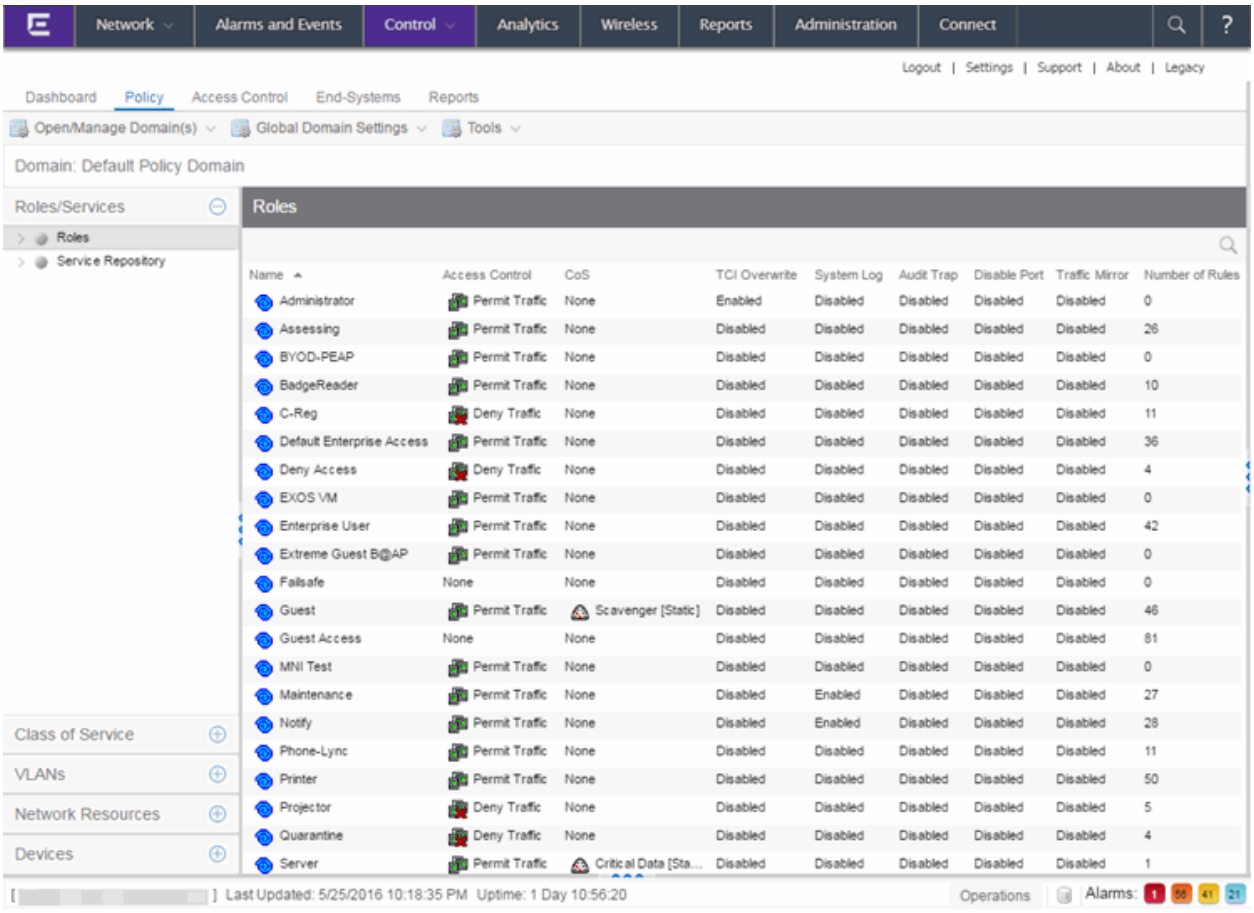
The **Control** > **Policy** tab main window is the central point for all **Policy** tab tasks. It is divided into a left panel and a right panel. The tabs in the left panel display hierarchical trees that represent the roles, services, network elements, devices and port groups involved in managing policies for your network. There are five left-panel tabs: Roles/Services, Class of Service, VLANs, Network Resources, and Devices. The tabbed pages in the right panel display detailed information about the item selected in the left panel.

Menu Tabs

The Menu tabs on the **Policy** tab provide access to Policy tab functions. The **Open/Manage Domains** menu provides options for the domain currently accessed. The **Global Domain Settings** drop-down list enables you to configure global **Policy** tab settings. Use the **Tools** menu to configure authentication settings and review Policy events.

Information on Policy tab features:

- Dialog Boxes (Messages)
- Icons
- Left Panel



Dialog Boxes (Messages)

In the course of using the **Policy** tab, message dialog boxes appear confirming certain tasks are complete, or warning of the consequences of performing a certain action.

Icons

The icons used in the **Policy** tab and their meanings are as follows:

Icon	Definition	Icon	Definition
	Pre-Defined Groups		User-Defined Groups
	Device/Wireless Device		Port Group
	Port		Frozen Port
	Role		Quarantine Role

Icon	Definition	Icon	Definition
	Rule		Disabled Rule
	Device-specific Rule		Service Group
	Automated Service		Manual Service
	Network Resource Group		Slot/Logical Ports/Ports
	Contain VLAN		Deny VLAN
	VLAN or Network Resource Island		Island VLAN
	Warning		CoS (Class of Service)
	802.1p Priority		IP Type of Service Value
	CoS Port Group		Rate Limit
	Transmit Queue		Network Resource Topology

Open/Manage Domain Menu Icons

The following icons appear in the **Open/Manage Domains** drop-down list:

 **Lock**

Reminds you the current Policy Domain is locked for editing purposes. You can lock and unlock the domain from the Lock tool bar button.

 **Save**

Reminds you that you've made changes, and you need to save the data to the Policy Domain. Selecting this icon initiates the save operation. Only users with the capability to Enforce are able to save the domain.

 **Enforce**

Reminds you that you've made changes to roles that you need to enforce. Selecting this icon initiates the enforce operation.

Policy Windows

The **Windows** Help section contains Help topics describing **Policy** tab windows and their field definitions.

Policy Concepts

This topic explains concepts used in the **Policy** tab.

Information on:

- Policy
- Role
    - What is a Role
    - Default Role
- Policy Domains
- Service
- Rule
    - What is a Rule
    - Disabling Rules
    - Conflict Checking
- Packet Tagging
- VLAN to Role Mapping
- Dynamic Egress
    - Setting Domain GVRP Status
- Policy VLAN Islands
- Traffic Mirroring
- Port Groups
- Network Resource Groups
    - Network Resource Topologies
- Verifying
- Enforcing
- Controlling Client Interactions with Locks

Policy

In the **Policy** tab, network access policies are called Roles. See Role, below, for a description.

Role

What is a Role

A role is a set of network access services that can be applied at various access points in a policy-enabled network. A port takes on a user's role when the user authenticates. Roles are usually named for a type of user such as Student or Engineering. Often, role names match the naming conventions that already exist in the organization. A role can contain any number of services in the **Policy** tab.

A role can also contain default access control (VLAN) and/or class of service (priority) characteristics that will be applied to traffic not identified specifically by the set of access services contained in the role. The set of services included in a role, along with any access control or class of service defaults, determine how all network traffic will be handled at any network access point configured to use that role.

Default Role

After you have created a role, assign it as the default role for a port (see Assigning Default Roles to Ports).

Policy Domains

The **Policy** tab provides the ability to create multiple policy configurations by allowing you to group your roles and devices into Policy Domains. A Policy Domain contains any number of roles and a set of devices that are uniquely assigned to that particular domain. Policy Domains are centrally managed in the database and shared between the **Policy** tab clients.

In the **Policy** tab, you work in one current domain at a time. Each domain is identified by a unique name. The Domain menu lets you easily switch from one domain to another. There is no limit to the number of domains you can create, however, a device can exist in only one Policy Domain.

The first time you launch the **Policy** tab, you are in the Default Policy Domain. You can manage your entire network in the Default Policy Domain, or you can create multiple domains each with a different policy configuration, and assign your network devices to the appropriate domain. The roles, services, rules, VLAN membership, and class of service in this initial configuration define a suggested implementation of how network traffic can be handled. This is a starting point for a new policy deployment and often needs customization to fully leverage the power of a policy-enabled network.

The **Policy** tab ships with a set of domain configurations that provide ready-made workflows for common policy scenarios. Each domain configuration contains all the elements (roles, services, rules, VLAN membership, class of service) that define how network traffic is handled for each scenario. These domains are listed in the Open/Manage Domain menu.

You can import the data elements from one domain into another domain. You can also import a domain saved as a policy Database file (.pmd file) or data from a Database file into a domain, and you can export a domain or data from a domain to a .pmd file, (one file per domain) for backup and troubleshooting purposes. Verify and Enforce operations are performed only on the current domain.

In order for your network devices to be displayed on the left-panel **Devices** tab, they must be assigned to a Policy Domain. Initially, you must add your devices to the ExtremeCloud IQ Site Engine database. After devices have been added to the ExtremeCloud IQ Site Engine database, you can assign the devices to a Policy Domain using the **Policy** tab. As soon as a device is assigned to a domain, it is automatically displayed on the left-panel **Devices** tab. Only devices that support policy are displayed in the **Policy** tab.

The **Policy** tab automatically locks the current Policy Domain when you begin to edit the domain configuration. Other users are notified that the domain is locked and they are not be able to save their own domain changes until the lock is released. For more information, see Controlling Client Interactions with Locks. After a Policy Domain has been changed, you must save the domain to notify all clients viewing that domain of the change and automatically update their view with the new configuration.

Service

Services are sets of rules that define how network traffic for a particular network service or application should be handled by a network access device. A service might consist of only one rule governing, for example, email priority, or it might consist of a complex set of rules combining class of service, filtering, rate limiting, and access control (VLAN) assignment. The **Policy** tab allows you to create Local Services (services that are unique to the current domain) and Global Services (services that are common to all domains). Global Services let you easily create and manage services shared between all your domains. A service can be included in any number of roles.

As an example, you might create a service called `High Priority Internet Web Access` that contains priority classification rules for traffic directed toward each of your organization's Internet proxy servers. This service would likely contain one traffic classification rule for each of your Internet proxy servers.

Services can be one of two types: Manual Service or Automated Service.

- **Manual Service** – This service consists of one or more traffic classification rules you create based on your requirements. Manual services are good for applying customized sets of rules to roles.
- **Automated Service** – This service automatically creates a rule with a specified action (class of service and/or access control), for each device in a particular network resource group. You create a network resource group using a list of IP addresses or an IP subnet, and then associate the group with the Automated service (see How to Create a Network Resource Group for more information). Automated rule types include Layer 3 IP Address and IP Socket rules, and Layer 4 IP UDP Port and IP TCP Port rules.

Services provide a common language that network engineers, information technology administrators, and business managers understand. See How to Create a Service for more information.

Rule

What is a Rule

Policy rules define one element of how traffic for a particular network service or application is handled by a network access device. For example, you might create a rule that assigns a certain priority to all email traffic, by adding an 802.1p, ToS, or DiffServ value to all SMTP traffic. A policy rule can be included in any number of services and you can select the types of devices to which the rule applies. You create rules by right-clicking a Service in the **Service Repository** tab and selecting **Create Rule**
.

See Traffic Classification Rules for a detailed explanation of rules.

Disabling Rules

You can elect to disable a rule during or after its creation. If you disable a rule, it is temporarily unavailable for use by the current service, but it can still be copied to other services and enabled, or re-enabled at another time for the current service. Disabling a rule is a way to temporarily remove a rule from your service without having to delete and recreate it. You disable rules by right-clicking a Service in the **Service Repository** tab and selecting **Disable Rule**.

Conflict Checking

As you create your Policy view services and rules, you can define conflicting rules. A conflict exists when two rules in the same service or role define different actions for the same traffic description. For example, two rules might have the same traffic description, but forward traffic to different VLANs, or have different priorities. ExtremeCloud IQ Site Engine ensures that conflicting rules do not coexist in the same role or service by checking rule traffic descriptions and action values, providing a message if conflicts are found, and writing the conflict information to the Event Log. If a rule is disabled, conflicts between that rule and others are ignored.

The one exception to this conflict checking behavior, is when the conflicting rules coexist in the same role, but one rule exists in a Local service and the other exists in a Global service. In this case, the rule defined in the Local service takes precedence over the rule defined in the Global service because the Local service is specific to the current domain. Consider the following example:

In the North Campus domain you have a Local service "A" that assigns an Ethertype IP rule to the Red VLAN. The "A" service is assigned to the Student Role. In addition, a Global service "B" exists that assigns Ethertype IP rules to the Blue VLAN. The "B" service is also assigned to the Student Role. In this case, the Local service takes precedence over the Global service in the North Campus domain. Note that the precedence pertains to the rule's actions: class of service (priority) and access control (VLAN). For example, if a rule in a Local service and a rule in a Global service both have the same traffic description, and the Local rule's actions apply CoS Priority 1 and no access control (no VLAN), while the Global rule's actions apply CoS Priority 2 and VLAN Blue(2), then the rule will be enforced using CoS Priority 1 and VLAN Blue(2). In addition, if *either* the Local or Global service has the Accounting or Security actions enabled, then they will be enforced to the devices.

Packet Tagging

Packet tagging in a Policy view environment occurs as follows:

Tagged packets and ingress filtering are processed first. Then, VLAN ID and priority are determined.

- *VLAN ID*: If the packet matches an active VLAN classification rule on the ingress port, the VID (VLAN ID) specified in the matching VLAN classification rule is assigned. Otherwise, if there is an active role on the ingress port and it specifies a default VLAN, the default VID from the active role on the ingress port is assigned. If there is no active role and no classification rule

matches, the 802.1Q PVID for the ingress port is assigned.

- *Priority*: If the packet matches an active priority classification rule on the ingress port, the priority specified in the matching priority classification rule is assigned. Otherwise, if there is an active role on the ingress port and it specifies a default priority, the default priority from the active role on the ingress port is assigned. If there is no active role and no classification rule matches, the 802.1Q_PPRI for the ingress port is assigned.

The set of classification rules active on a port includes statically created rules that specify the ingress port on their port list, as well as any rules established as a result of a role being applied on that port. If the port has no active role and thus no default access control (VLAN) or class of service (priority), untagged packets that do not match any classification rules are assigned a VLAN and priority from the 802.1Q and 802.1p defaults for the ingress port.

For a graphical illustration of the packet tagging process in a Policy view scenario, see the Packet Flow Diagram. The packet passes through the decision-making process illustrated in the graphic twice — one time for VLAN tagging and one time for priority tagging.

VLAN to Role Mapping

VLAN to Role mapping lets you assign a role to an end user based on a VLAN ID. There are two kinds of VLAN to Role Mapping: Authentication-Based and Tagged Packet.

- **Authentication-Based VLAN to Role Mapping** (RFC 3580) — Provides a way to assign a role to a user during the authentication process, based on a VLAN Attribute. An end user connects to a policy-enabled device that supports 802.1X authentication using a RADIUS Server. During the authentication process, the RADIUS server returns a VLAN ID in its RADIUS VLAN Tunnel Attribute. The device uses the Authentication-Based VLAN to Role mapping list to determine what role to assign to the end user, based on the VLAN Tunnel Attribute. Authentication-Based VLAN to Role mappings are only configured at the device level (for all devices).

  NOTE: When configuring Authentication-Based VLAN to role mapping, you must enable RFC3580 VLAN Authorization on the device via the device Authentication tab. In addition, VLAN IDs must be configured on the RADIUS server for each user authorized to access the network. If a user does not have a configured VLAN ID, the default role (if there is one) or the 802.1Q PVID for the ingress port is assigned. For more information on configuring VLAN ID attributes on the RADIUS server, refer to your device firmware documentation, RFC 3580, and your RADIUS server documentation.

- **Tagged Packet VLAN to Role Mapping** - Provides a way to let policy-enabled devices assign a role to network traffic, based on a VLAN ID. When a device receives network traffic that has been tagged with a VLAN ID (tagged packet) it uses the Tagged Packet VLAN to Role mapping list to determine what role to assign the traffic based on the VLAN ID. Tagged Packet VLAN to Role mapping can be configured at the device level (all devices) and at the port level (for an individual port on a device). A VLAN can only be mapped to one role at the device level, but the

same VLAN can be mapped to a different role at the port level. A mapping does not have to exist at the device level to be created at the port level, and port-level mappings will override any device-level mappings.

NOTE: **TCI Overwrite Requirement**
-- Tagged Packet VLAN to Role Mapping will apply the Role definition to incoming packets using a mapped VLAN. This definition will apply a COS and determine if the packet is discarded or permitted, and if TCI Overwrite is enabled will re-specify the VLAN ID defined by the Rule / Role Default. If TCI Overwrite is disabled, the packet will egress (if permitted by the Rule Hit) with the original VLAN ID it ingressed with.
-- If supported by the device, you can enable TCI Overwrite for an individual role in the role's **General** tab. The stackable devices support rewriting the CoS values but not the VLAN ID.

To configure VLAN to Role Mapping in the Policy view, use the role's **Mappings** tab and/or the VLAN's **General** tab.

Dynamic Egress

In the **VLANs** tab, you can enable Dynamic Egress for a VLAN by selecting the **Dynamic Egress** checkbox when you select a VLAN.

When Dynamic Egress is enabled for a VLAN, any time a device tags a packet with that VLAN ID, the ingress port is automatically added to the VLAN's egress list, enabling the reply packet to be forwarded back to the source. This means you do not need to add the ingress port to the VLAN's egress list manually. (See Example 1, below.)

Dynamic Egress affects only the egress lists for the source and destination ingress ports. However, GVRP (GARP VLAN Registration Protocol) automatically adds the interswitch ingress ports to the egress lists of VLANs. (See Example 2, below.) You can enable GVRP for the domain by selecting the **Global Domain Settings > GVRP > Enable** menu option.

NOTE: If you do not want GVRP enabled on your network, you can disable it by selecting the **Global Domain Settings > GVRP > Disable** menu option. If necessary, you can then manually configure the interswitch ports to do what GVRP does automatically, using local management to set up your interswitch links as Q trunks. The trunk ports will be automatically added to the egress lists of all the VLANs at the time of trunk configuration. For more information on using GVRP in the Policy view, see the section on Setting Domain GVRP Status below.

When you disable Dynamic Egress for a VLAN, the VLAN effectively becomes a discard VLAN. Since the destination port is not added to the egress list of the VLAN, the device discards the traffic. If you want a VLAN to act as a discard VLAN, disable Dynamic Egress for that VLAN. (See Example 3, below.)

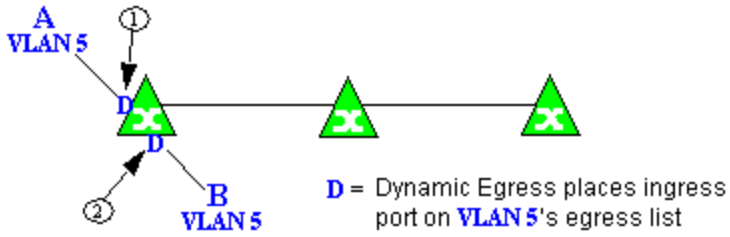
If an endstation is talking to a "silent" endstation which does not send responses, like a printer, you need to add the silent endstation's ingress port to the VLAN's egress list manually using local management.

Dynamic Egress and GVRP take care of adding the other ingress ports to the VLAN's egress list. (See Example 4, below.)

CAUTION: If no packets are tagged with the applicable VLAN on a port within five minutes, Dynamic Egress list entries time out. The result is that ExtremeCloud IQ Site Engine indicates that the endstation is "silent" if the VLAN has not been used within that time period. For example, if there is a "telnet" rule and two users (A and B) are on ports whose role includes a service containing the "telnet" rule, if User B has not utilized the "telnet" rule within the five minute time frame, User A is not able to telnet to User B. For this reason, the best application of Dynamic Egress is for containing undirected traffic on "chatty" clients which utilize, for example, IPX, NetBIOS, AppleTalk, and/or broadcast/multicast protocols such as routing protocols.

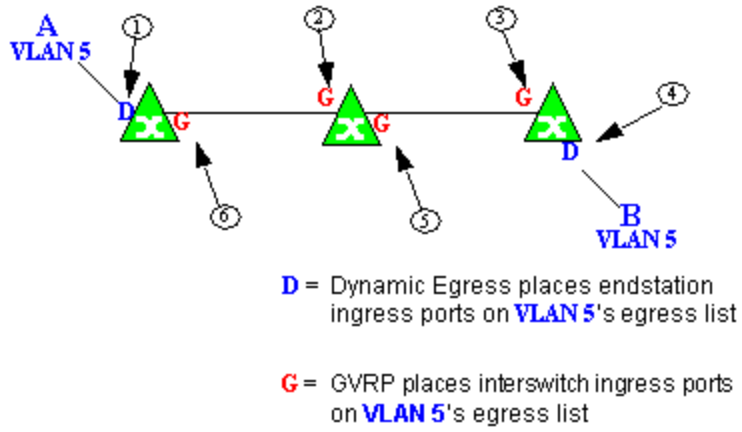
Example 1: Dynamic Egress Enabled

In this example, Dynamic Egress is enabled for VLAN 5. When source endstation A is tagged with VLAN 5, Dynamic Egress places A's ingress port (1) on VLAN 5's egress list. When destination endstation B's traffic is tagged with VLAN 5, Dynamic Egress places B's ingress port (2) on VLAN 5's egress list. The device can then forward traffic to both endstations.



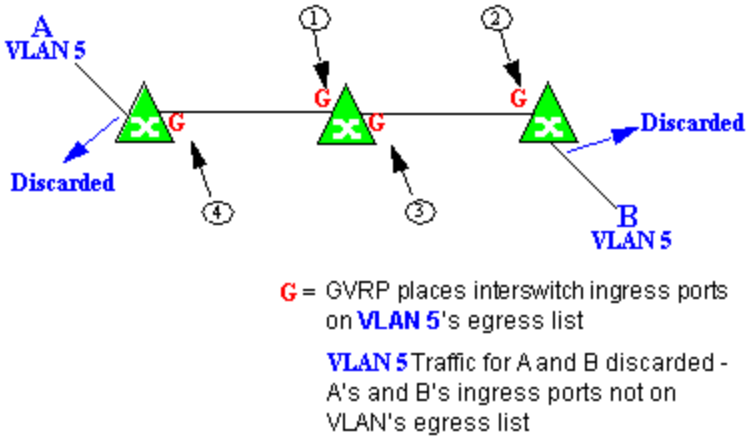
Example 2: Dynamic Egress + GVRP

In this example, Dynamic Egress is enabled for VLAN 5, and the destination endstation, B, is on a different device from the source endstation, A. When A is tagged with VLAN 5, Dynamic Egress places A's ingress port (1) on VLAN 5's egress list. GVRP then places interswitch ingress ports (2) and (3) on VLAN 5's egress list. When B's traffic is tagged with VLAN 5, Dynamic Egress places B's ingress port (4) on VLAN 5's egress list. GVRP then places interswitch ingress ports (5) and (6) on VLAN 5's egress list. The devices can then forward traffic to both endstations.



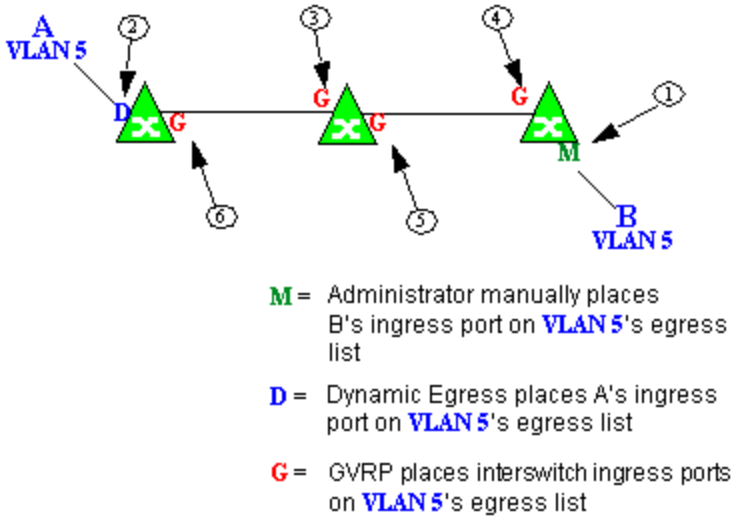
Example 3: Dynamic Egress Disabled

In this example, Dynamic Egress is disabled. When source endstation A is tagged with VLAN 5, A's ingress port is not placed on VLAN 5's egress list. GVRP places interswitch ingress ports (1) and (2) on VLAN 5's egress list. When B's traffic is tagged with VLAN 5, B's ingress port is not placed on VLAN5's egress list. GVRP places interswitch ingress ports (3) and (4) on VLAN 5's egress list. But VLAN 5 traffic for both A and B is discarded, because VLAN 5 is not aware of the ingress ports for A and B.



Example 4: Silent Endstation

In this example, Dynamic Egress is enabled for VLAN 5, but the destination endstation, B, is a "silent" endpoint, like a printer. Endstation B does not send responses, so the Administrator must place B's ingress port on VLAN 5's egress list manually (1). When A is tagged with VLAN 5, Dynamic Egress places A's ingress port (2) on VLAN 5's egress list. GVRP then places interswitch ingress ports (3) and (4), then (5) and (6) on VLAN 5's egress list. Endstation A is then able to communicate with the printer.



Setting Domain GVRP Status

The Policy view allows you to set the domain GVRP (GARP VLAN Registration Protocol) status via the Edit menu. There are three GVRP status options. To set the GVRP status for all the devices in the current domain, select a status and then enforce.

- **Ignore** — When this option is selected, ExtremeCloud IQ Site Engine ignores the GVRP configuration on a device during an Enforce operation. This allows you to configure some network switches with GVRP enabled and others with GVRP disabled, according to their configuration requirements.
- **Enable** — When this option is selected, GVRP is enabled for the devices in the current domain.
- **Disable** — Select this option if you do not want GVRP enabled on the devices in the current domain. Disabling GVRP can affect connectivity through ports with VLANs that rely on Dynamic Egress. If GVRP is disabled, rules using VLAN containment do not work properly unless the VLANs have been pre-configured on the devices outside of ExtremeCloud IQ Site Engine.

The following table shows how domain GVRP status affects device-level and port-level GVRP status when an Enforce operation is performed.

Domain GVRP Status	Device Set on Enforce
Domain GVRP status is set to **Ignore**.	No GVRP status is written to devices on Enforce.
Domain GVRP status is set to **Enable** and the device-level GVRP is enabled.	No GVRP status is written to the device on Enforce.
Domain GVRP status is set to **Enable** and the device-level GVRP is disabled.	Device-level GVRP status and port-level GVRP status is set to enabled on Enforce.

Domain GVRP Status	Device Set on Enforce
Domain GVRP status is set to **Disable** and the device-level GVRP is disabled.	No GVRP status is written to the device on Enforce.
Domain GVRP status is set to **Disable** and the device-level GVRP is enabled.	Device level GVRP status is set to disabled and no change is made to the port-level GVRP status on Enforce.

Policy VLAN Islands

The Policy view offers you the ability to set up Policy VLAN Islands which enable you to deploy a policy across your network, while restricting user access to only selected local devices. For example, if you want to have a guest VLAN but you do not want the guests in one facility to be able to communicate with guests in another facility, you can set up a VLAN island containing only selected devices in each facility, with access controlled by island VLANs.

- **Global VLAN** — Global VLANs are written to all selected devices with the same VID. They are referenced in the format <VID[name]>.
- **Island VLAN** — An Island VLAN is a conceptual VLAN and does not have an actual VID. The VID is assigned automatically based on the island it belongs to.

NOTE: The Policy view provides management of Global VLAN settings, but does not provide management of Island VLANs beyond setting the appropriate VIDs in the Role defaults and Rule access control actions. Also, you must manage separately other related settings in the qBridgeMib such as name, and dynamic egress values.

See How to Create a Policy VLAN Island for more information.

Traffic Mirroring

The Policy view provides policy-based traffic mirroring functionality that allows network administrators to monitor traffic received at a particular port on the network, by defining a class of traffic that will be duplicated (mirrored) to another port on that same device where the traffic can then be analyzed. Traffic mirroring can be configured for a rule (based on a traffic classification) or as a role default action. Only incoming traffic can be mirrored using policy-based traffic mirroring, and the traffic mirroring configuration takes precedence over regular port-based mirroring.

Traffic mirroring uses existing the Policy view port groups (created using the Port Groups tab) to specify the ports where the mirrored traffic will be sent for monitoring and analysis. When an end user connects to the device where the specified ports exist, and is assigned the role that has traffic mirroring configured, then there is a traffic mirror set up for the port the end user connected to. However, if the end user is assigned a role that does not have traffic mirroring configured, or if the end user connects to a device that doesn't have any ports in the specified port groups, then no traffic mirror will exist.

Examples of how traffic mirroring might be used include:

- Mirroring the traffic from suspicious users based on their MAC or IP address.
- Monitoring VoIP calls by IP address or port range.
- Mirroring traffic to optimized IDS systems, for example one system for all HTTP traffic (to look for suspicious websites) or one system for all emails (to look for spam).
- Mirroring traffic to ExtremeAnalytics appliances for use in ExtremeCloud IQ Site Engine application identification reports and analysis.

For information on configuring traffic mirroring, see the **Role** tab and the **Rule General** tab.

Port Groups

ExtremeCloud IQ Site Engine allows ports to be combined into groups, similar to the way services can be combined into service groups. Port groups enable you to configure multiple ports on the same device or on different devices simultaneously, or to retrieve port information from them. You can view port groups on the left-panel **Port Groups** tab.

The Policy view provides you with several commonly used port groups for your convenience, called Pre-Defined Port Groups. You can also create your own port groups, called User-Defined Port Groups.

User-Defined Port Groups

The Policy view also enables you to create your own port groups and select individual ports to add to the group.

Network Resource Groups

Network Resource Groups provide a quick and easy way to define traffic classification rules for groups of network resources such as routers, VoIP (Voice over IP) gateways, and servers. The default Policy domain configuration contains examples of network resource groups that you might want to create, such as Internet Proxy Servers and SAP Servers. Use the Network Resource Configuration window to view and define your network resource groups. See How to Create a Network Resource for more information.

After a network resource group has been defined, you can associate it with an Automated service (see How to Create a Service for more information). The Automated service automatically creates a rule with a specified action (class of service and/or access control), for each resource in the network resource group. Automated rule types include Layer 2 MAC Address rules, Layer 3 IP Address and IP Socket rules, and Layer 4 IP UDP Port and IP TCP Port rules.

Network Resource Topologies

Network Resource Topologies are used to divide the devices in a domain into groups called islands. Each network resource group specifies a topology and can then define a unique resource list for each island within that topology, allowing user access to resources on the network based on the physical location at which they authenticate.

For example, you could create a topology called "Campus Printers" that could be used to restrict printer access to only the printers in the building where the end user is physically located. This topology might define islands such as "Library," "Admissions Office," or "Science Building." Each island would include the network devices for that location. Then, in the Network Resource Group that specifies this topology, there would be resource lists that define the printers for each of those islands.

In addition to defining topologies based on physical location (such as geographic region, corporate offices, or campus buildings) a topology could also be used to define resources based on the departments within a company (such as Sales, IT, or Human Resources).

When you create a topology, it contains a Default Island that includes all the devices in your domain. You can then create additional islands and distribute your devices between the different islands according to your needs. Each device in a domain must belong to one island in each topology. You can set any island as the Default island for new devices that are added to the domain.

Verifying

The Verify feature lets you verify that the roles in your current domain have been enforced. Verify operations are performed only on the current domain. The Verify operation compares the roles currently in effect (enforced) on your domain devices with the roles defined in the current Policy Domain.

NOTE: If you perform a Verify operation following an Import Policy Configuration from Device, the Verify can fail. This is because the import operation imports only roles and rules from the device, not the complete policy configuration. Also, when you import device-specific rules, these rules are converted to a Rule Type of "All Devices," and this will cause Verify to fail. If you want the rules to be device-specific, you will have to change their Rule Type via the Rule General tab after the import and prior to Enforce.

You can verify using the Open/Manage Domain > Verify Domain menu option, both of which verify the information on all the devices in the current domain. You can also selectively verify on individual devices or device groups in the domain by right-clicking the device or group in the left panel or in the right-panel Details View tab for the Devices folder or Device Group folder, and choosing **Verify** from the menu.

After verifying, you see a window that reports any discrepancies. The title bar of the window lets you know if the verify was done on all devices in the domain, or a subset of devices. From this window, you can select **Enforce Domain** to open the Enforce Preview window, where you can view the effects enforcing the current role set would have, prior to actually enforcing. You can also view the full results of the Verify operation in the event log, which displays any discrepancies and statistics of the operation itself.

Enforcing

In the **Policy** tab, enforcing means writing role information to a device or devices. Enforce operations are performed only on the current domain. Any time you add, make a change to, or delete a role or any

part of it (any of its services and/or rules), the devices in your current domain need to be informed of the change, otherwise the role will not take effect. To determine if the roles currently in effect on your domain devices match the set of roles you have defined in your current Policy Domain configuration, use the Verify feature.

NOTE: **Setting up Profiles and Credentials for Enforce.** All SNMP operations that are performed from the Policy view client use the SNMP credentials of the logged-in user. For example, when devices are identified, the credentials associated with the user's group are used to communicate with the devices. However, the Enforce operation occurs on the server and uses the Netsight Administrator profile to communicate with devices. Because of this, the Netsight Administrator profile must have write privileges on the devices that users can enforce.

When an Enforce is initiated, the Policy Domain is locked to prevent other clients from enforcing at the same time. Different Policy Domains can be enforced at the same time, but if another user attempts to enforce the same domain at the same time, that user will be notified that the domain is already locked.

To enforce, select the **Open/Manage Domains** > **Enforce Domain** menu option. You can also selectively enforce on individual devices by right-clicking the device in the **Devices** tab left panel or in the right-panel **Devices** tab and choosing **Enforce** from the menu. Only users that have been assigned the Enforce capability are allowed to perform an Enforce.

Controlling Client Interactions with Locks

Because the Policy view uses a Client/Server architecture, it is important to maintain a proper sequence of client interactions to ensure a consistent view of Policy Domains among all clients. To do this, the Policy view uses Server Locks to manage user interactions. When a user begins editing a Policy Domain (for example by assigning devices or adding a role), a lock is acquired for that domain at the server. That lock is not released until the same user saves the domain data. This guarantees a consistent view of that domain for all clients. Users are given the option of revoking locks held by other users. This protects against the possibility that users forget they have locked a domain and keep that lock for an extended period of time.

A domain is locked automatically when a user begins to edit the domain data or a user can lock/unlock a domain by selecting the Lock toolbar button. When a domain is locked, the title bar states that the policy data is being edited and specifies the user who has locked the domain. Other Policy view clients are notified that the domain is locked and they will not be able to save their own domain changes until the lock is released.

Here are some important things to remember about locks:

- Locks operate on individual Policy Domains. When a user edits a domain, a lock is acquired for that domain and it remains locked until the same user saves the domain data or the lock is revoked by another user. You cannot save a domain that is locked by another user.

- During Enforce, a lock is acquired on the domain which is being enforced. This ensures a consistent view of the domain while it is being used by the server.
- When devices are being assigned to a Policy Domain, multiple domains can be locked concurrently. This will happen if devices from one domain are being reassigned to another domain. In this case, locks for both domains are acquired.
- When a lock is revoked, the last domain save "wins." While consistency is always maintained by the server, the order of domain saves cannot be guaranteed when locks are revoked, and consequently work done by one user can be lost.

You can view server locks for all clients via the Options > **Server Information** tab.



Policy Tab Right-Panel

The **Policy** tab main window is divided into two panels: a left panel and a right panel. The Right-Panel Tabs Help section contains Help topics describing the tabs and their field definitions.

The right panel displays different tabs and information depending on the item selected in the left-panel tree. Help topics for right-panel tabs are named in a manner to reflect this. For example, the help topic named Details View Tab (Device Group), provides information on the right-panel **Details View** tab when a device group is selected in the left-panel tree.

Policy Left Panel

The left panel of the **Policy** tab contains tabs that display hierarchical trees representing the roles, services, classes of service, VLANs, network resources, devices, and port groups involved in managing policies for your network. What you select in the left panel determines what is displayed in the right panel. When you first open the Policy tab, the Roles tab is displayed in the left panel, by default.

Features of the left panel include:

- *Expanding and collapsing items in the hierarchy:* Double-click the item or its icon, or select the turner to the left of the icon.
- *Right-click menus:* Right-click a folder or other item in the left panel, and a menu of the options you can perform on your selection appears.

Information on the left-panel tabs:

- Roles/Services Tab
- Class of Service Tab
- VLAN Tab

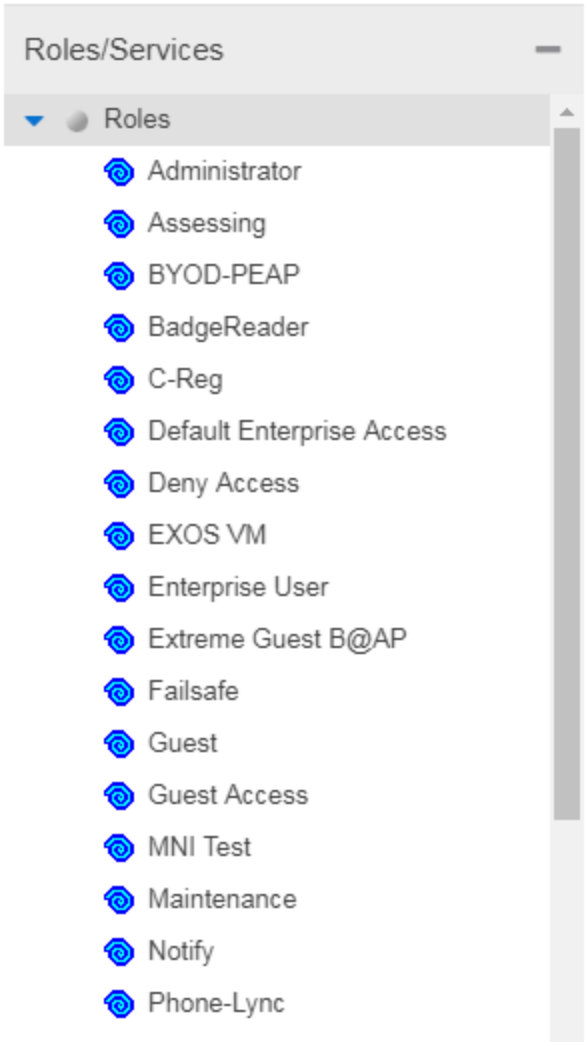
- Network Resources Configuration
- Devices/Port Groups Tab

Roles/Services Tab

This tab displays the Roles and Service Repository trees.

Roles Tree

The Roles tree lists the roles defined for the current domain. A role is a set of network access services that can be applied at various access points in a policy-enabled network.



Roles Folder

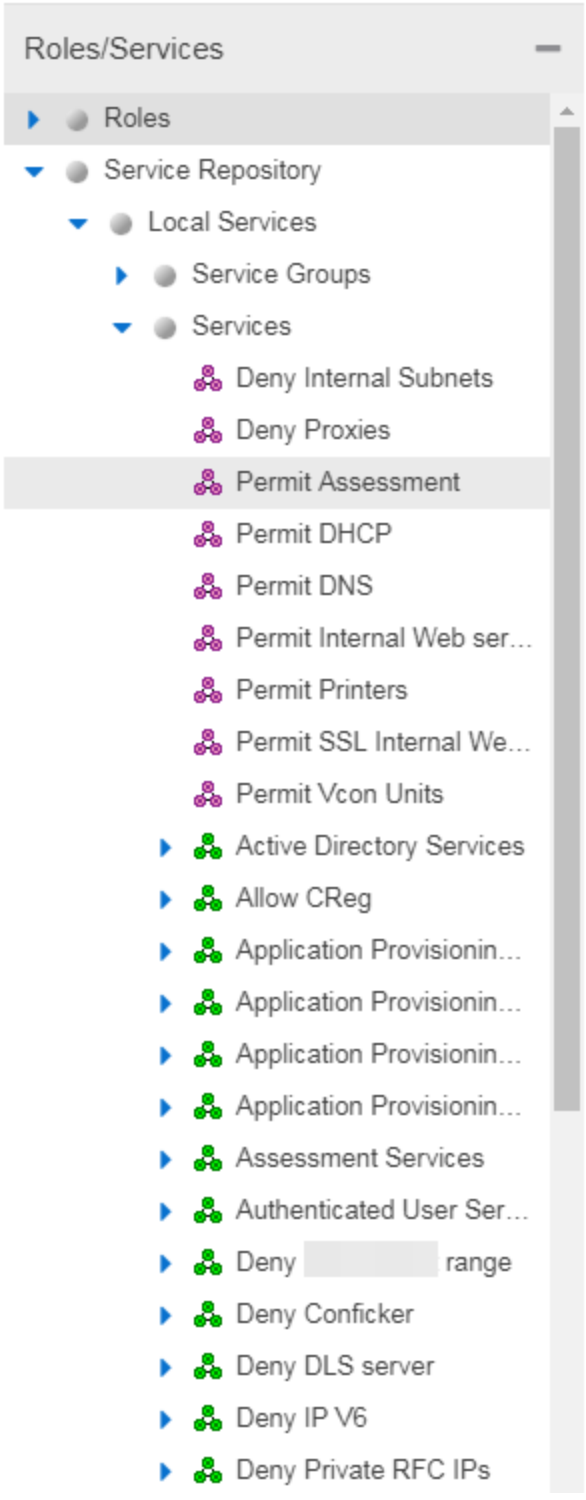
This folder contains the roles defined for the current domain. See How to Create a Role for more information.

Role

Individual roles are listed by name. Select a role in the left panel, and view information about that role in the right-panel tabs. Only Quarantine roles are displayed with a red icon .

Service Repository Tree

The Service Repository tree displays your Local and Global services and service groups. Services are sets of rules that define how network traffic for a particular network service or application is handled by a network access device. Local Services are services unique to the current domain. Global Services are services common to all domains. The tab also displays your network resource groups.


Roles/Services
Roles
Service Repository
Local Services
Service Groups
Services
Deny Internal Subnets
Deny Proxies
Permit Assessment
Permit DHCP
Permit DNS
Permit Internal Web ser...
Permit Printers
Permit SSL Internal We...
Permit Vcon Units
Active Directory Services
Allow CReg
Application Provisionin...
Application Provisionin...
Application Provisionin...
Application Provisionin...
Assessment Services
Authenticated User Ser...
Deny range
Deny Conficker
Deny DLS server
Deny IP V6
Deny Private RFC IPs

Local Services Folder

Local Services are services unique to the current domain. This folder contains the local service groups and services defined for the current domain. For more information, see How to Create a Service Group.

Global Services Folder

Global Services are services that are common across all domains. This folder contains the global service groups and services shared by all domains. For more information, see How to Create a Service Group.

Service Groups Folder

The **Policy** tab lets you create categories (service groups) into which you can group services. This folder contains the defined service groups. For more information, see How to Create a Service Group.

Service Group 

Individual service groups are listed by name. Expand the service group to see the services and service groups included in that group.

Services Folder

This folder contains the automated and manual services that have been defined. For more information, see How to Create a Service.

Automated Service 

Individual Automated services are listed under the Services Folder or within a service group in the Service Groups folder.

Manual Service 

Individual Manual services are listed under the Services Folder. Expand the service to see the rules associated with it.

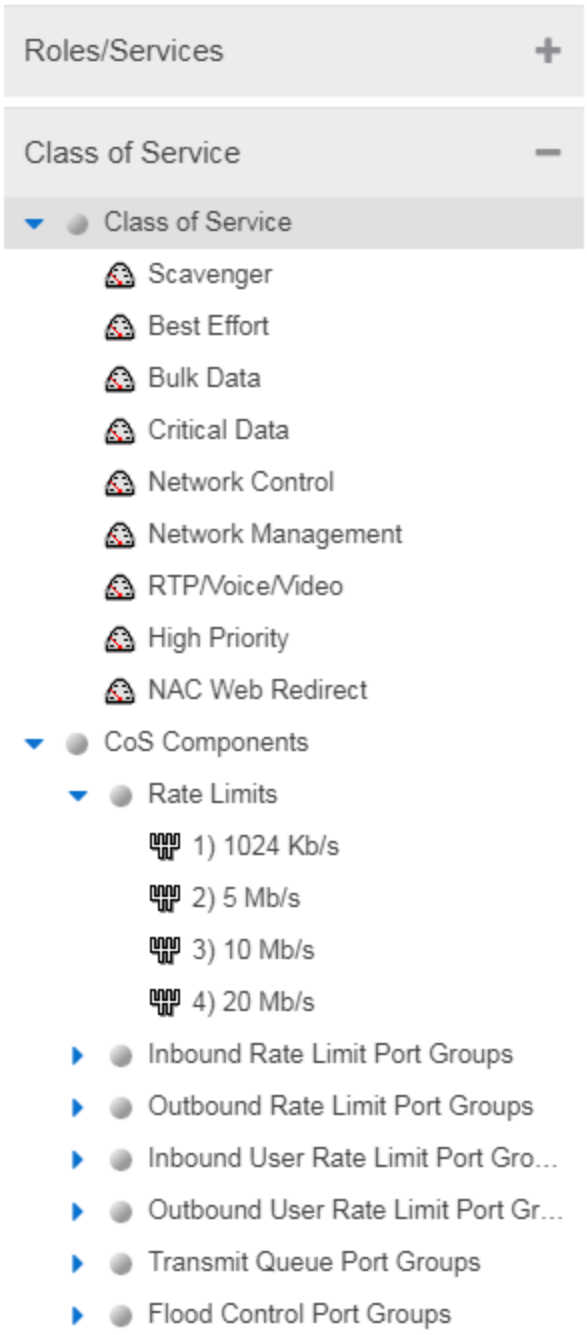
Rule 

Individual rules are listed by name. If the rule is disabled, the rule icon displays a red X . If the rule is device-specific, the rule icon displays a small switch .

Class of Service Tab

The left panel Class of Service tab displays your Classes of Service defined for the current domain.

Classes of Service prioritize traffic with an 802.1p priority, and optionally an IP type of service (ToS/DSCP) value, rate limits, and transmit queue configuration. You can then assign the class of service as a classification rule action, as part of the definition of an Automated service, or as a role default. For more information, see Getting Started with Class of Service.



Classes of Service Folder

When you first access the **Policy** tab, the left-panel Classes of Service tab is pre-populated with eight classes of service, each associated with one of the 802.1p priorities (0-7). These are static classes of service and cannot be deleted. You can use these classes of service as is, or configure them to include ToS/DSCP, rate limit, and/or transmit queue values. You can also rename them, if desired. In addition, you can also create your own classes of service. After you have created and defined your classes of service, they are then available when you make a

class of service selection for a rule action (Rule tab), a role default (General tab), or an automated service (General tab).

Class of Service

Select a Class of Service in the left panel, and view information about that service in the right-panel tabs. For more information, see How to Create a Class of Service.

CoS Components Folder

This folder contains subfolders of the possible components of a class of service (Rate Limits, Inbound Rate Limit Port Groups, Outbound Rate Limit Port Groups, and Transmit Queue Port Groups).

Rate Limits Folder

This folder contains the currently defined rate limits, listed in the order of precedence. For more information, see How to Define Rate Limits.

Inbound Rate Limit Port Groups

This folders contains the currently defined inbound rate limit port groups. Select a port group in the left panel and view information about that group in the right-panel tabs. For more information, see Creating Class of Service Port Groups.

Outbound Rate Limit Port Groups

These folders contain the currently defined outbound rate limit port groups. Select a port group in the left panel and view information about that group in the right-panel tabs. For more information, see Creating Class of Service Port Groups.

Transmit Queue Port Groups Folder

This folder contains the currently defined transmit queue port groups and the transmit queues defined for each group. For more information, see How to Configure Transmit Queues.

VLAN Tab

The left panel VLAN tab displays the Global VLANs for the current domain. If you have enabled Policy VLAN Islands, it also displays your Island VLANs and Policy VLAN Islands.



Global VLANs Folder
This folder contains your currently defined global VLANs for this domain.

VLAN 
The VLAN icon indicates the access control for the VLAN-- if it is a Discard VLAN, the icon displays a red X . Otherwise, it is a Contain VLAN.

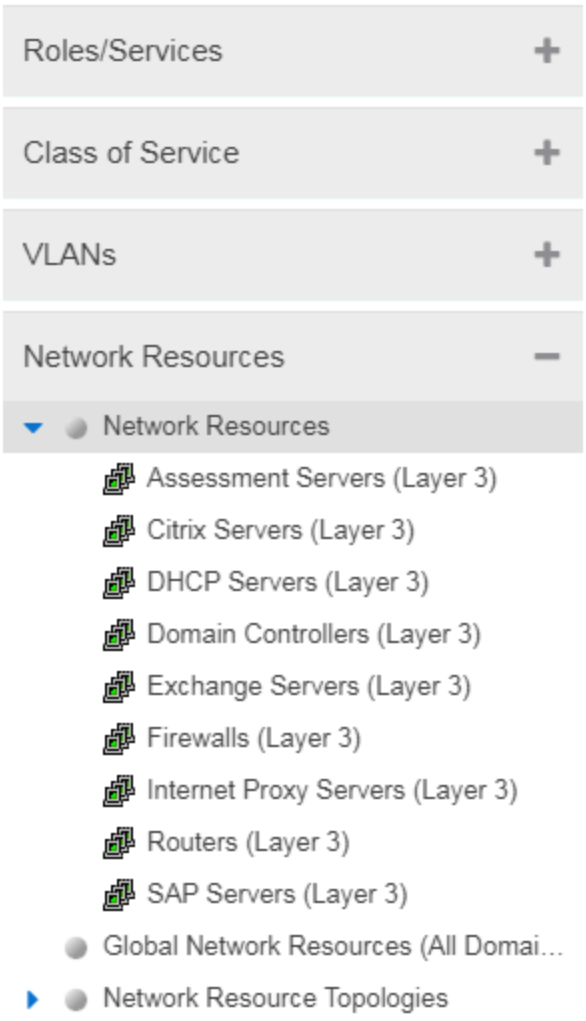
Island VLANs Folder
This folder appears only when the Policy VLAN Islands feature is enabled, and contains your currently defined Island VLANs for this domain.

Policy VLAN Islands Folder
This folder appears only when the Policy VLAN Islands feature is enabled, and contains your currently defined VLAN islands and the devices that belong to them. When you enable Policy VLAN Islands, this folder is pre-populated with a Default Island containing all the devices in the domain.

VLAN Island 
Select a VLAN island to see the devices associated with it listed in the right-panel Details View tab. The Default Island is created by the Policy tab when you enable Policy VLAN Islands, and it cannot be deleted.

Network Resources Configuration

The **Network Resources** left-panel tab displays the network resources and network resource topologies for the current domain.



Network Resources Folder

This folder contains any network resource groups you have created. For more information, see How to Create a Network Resource.

Network Resource

Individual network resource groups are listed by name. Select a resource in the left panel, and view information about that resource in the right-panel tabs.

Global Network Resources Folder

Global Network Resources are network resources that are common across all domains. For more information, see How to Create a Network Resource.

Network Resource Topologies Folder

This folder contains the network resource topologies currently defined for this domain.

Network Resource Topology 

A network resource topology can be used to divide the devices in a domain into groups called islands. You can then define a unique network resource list for each island within that topology, allowing user access to resources on the network based on the physical location at which they authenticate. If you are not using custom topologies to group your devices, you will use the Domain Wide topology, which contains just one island for all your domain devices.

Topology Island 

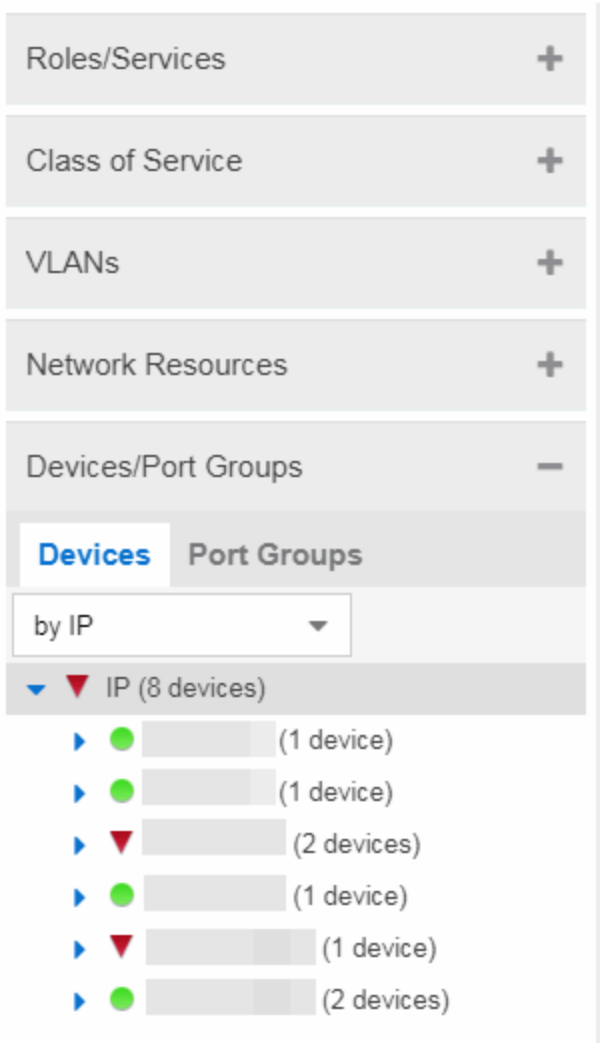
A topology island is a group of devices that have a unique network resource list, allowing you to set up network resource access based on the location where end users authenticate.

Devices/Port Groups Tab

This tab displays the Devices and Port Groups trees.

Devices Tree

The Devices tree displays the devices assigned to the current domain, organized into groups.



Devices

This tab contains all the devices assigned to the current domain. For information on adding devices to the domain, see How to Add and Delete Devices.

ExtremeControl > Policy supports Per-User ACLs (PU-ACL) from third-party vendors passed via RADIUS authentication requests. During a policy enforce, the roles and associated rules are translated into ACLs and pushes them to the appropriate Access Control Engines. You can manage ACL rules onExtremeXOS/Switch Engine devices on which version 30.5 or later is installed. By using ACLs, the access control entries (ACEs) can be ordered by the administrator, allowing for more flexibility in the configuration and better utilization of hardware resources on the device.

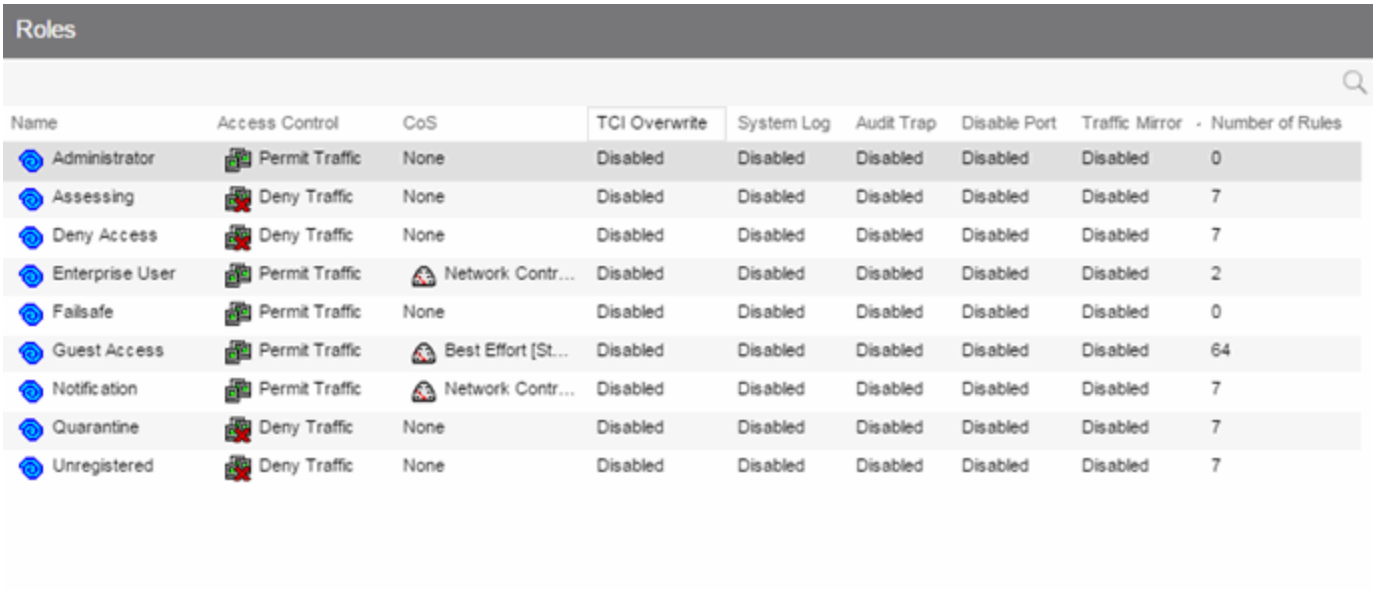
The **Control > Policy > Devices/Port Groups > Devices** tab includes ACL Rule Usage and Rule Hit Count details.

Port Groups

This tab contains the Pre-Defined and User-Defined Port Groups for the current domain. The **Policy** tab allows ports to be combined into groups, similar to the way devices are combined into device groups. Port groups enable you to configure multiple ports on the same device or on different devices simultaneously, or to retrieve port information from them. For more information, see How to Create a Port Group.

Summary (Roles)

This tab provides a summary view of the domain's roles. To access this tab, select the **Roles** left-panel tab in the Roles/Services tab. Right-click a role to add/remove services, rename the role, or delete the role.

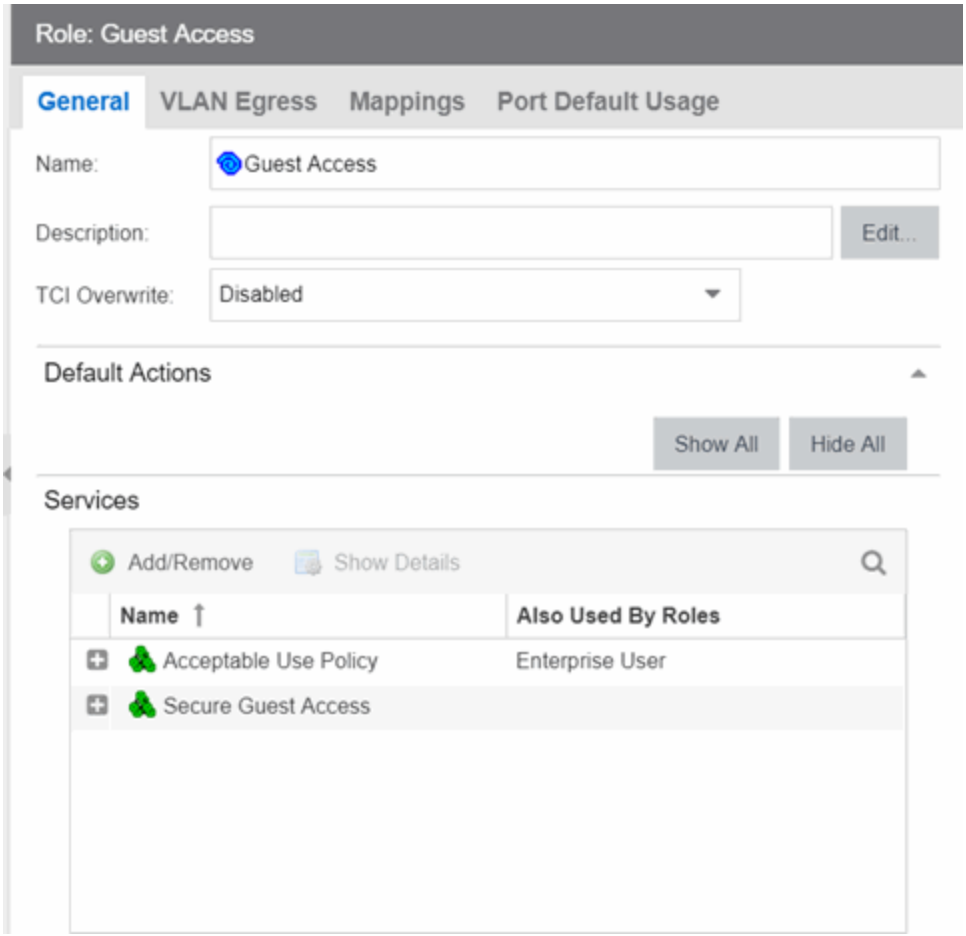


General (Role)

The role **General** tab lets you assign default actions for a role applied to traffic not identified specifically by the set of access services contained in the role. You can also use this tab to enable TCI Overwrite functionality for the role, and enter or edit the description of the role.

The Services section displays a list of the services and service groups associated with the selected role, and provides buttons for adding and removing services, creating a new service, viewing and editing a service or service group, and showing conflicting rules.

To access this tab, select a role in the left panel's **Roles** tab, then select the **General** tab in the right panel. Any additions or changes you make to this tab must be enforced in order to take effect.



Name

Name of the selected role.

Description

Use the **Edit** button to open a window where you can enter or modify a description of the role.

TCI Overwrite

Enable or disable TCI Overwrite functionality for the role. Enabling TCI Overwrite enables the VLAN (access control) and class of service characteristics defined in this role or any of its rules to overwrite the VLAN or class of service (CoS) tag in a received packet if that packet has already been tagged with VLAN or CoS information. If TCI Overwrite is not enabled, tagged packets will egress using the TCI data they already contain. You can also enable TCI Overwrite on a per-rule basis in the Rule Tab.

Default Actions

Default actions for a role are applied to traffic not identified specifically by the set of access services contained in the role.

Access Control

Use the drop-down list to choose a default access control (VLAN) for the role. You can select:

- None - No default access control specified.
- Permit Traffic - Enables traffic to be forwarded with the port's assigned VID.
- Deny Traffic - Traffic will be automatically discarded.
- Contain To VLAN - This option contains traffic to the VLAN specified. Use the drop-down list to the right to select the desired VLAN. You can also define the Service ID to extend the VLAN address space. The Service ID is the implementation of ExtremeCloud IQ Site Engine for the I-SID (also called Network Service Identifier = NSI), which increases the number of available VLANs.

Class of Service

Use the drop-down list to choose a default class of service (priority) for the role, create a new class of service, or select None if no class of service is desired. The drop-down list displays all of the classes of service for the current domain and also enables you to edit a class of service using the Edit button .

System Log

When this option is enabled, a syslog message is generated as long as no matching rules specify that sending a syslog message is prohibited (that is, the rule's system log action is set to "Prohibited" on the Rule Tab). When the option is disabled, the system log setting is ignored.

Audit Trap

When this option is enabled, an audit trap is generated as long no matching rules specify that sending an audit trap is prohibited (that is, the rule's audit trap action is set to "Prohibited" on the Rule Tab). When the option is disabled, the audit trap setting is ignored.

Disable Port

When this option is enabled, the port is disabled as long no matching rules specify that disabling the port is prohibited (that is, the rule's disable port action is set to "Prohibited" on the Rule Tab). Ports that have been disabled due to this option are displayed in the device Role/Rule tab. When the option is disabled, the disable port setting is ignored.

Traffic Mirror

Use the drop-down list to specify port groups where mirrored traffic is sent for monitoring and analysis. Select View/Modify Port Groups to open the Port Groups tab where you can define user-defined port groups for selection.

To the right of the drop-down list is an option to mirror only the first (N) packets of a flow. This option is intended for use when mirroring traffic to an ExtremeAnalytics engine. The

ExtremeAnalytics engine only needs the initial packets of a flow to properly identify the traffic, and setting this option will reduce network traffic overhead for the switch and engine. By default this number is set to 10, but can be changed by selecting the Edit button . Note that the value you set is used by all mirror actions in use in the current domain.

Services

Name

Lists the names of the services and service groups (local and global) associated with the selected role.

Also Used By Roles

List the other roles using this service. If the service is a global service, the domain name is also displayed if the role is in a different domain.

Add/Remove Services Button

Opens the role Add/Remove Services window, where you can add and remove services and service groups to and from any of the existing roles.

Show Details Button

Select a service or service group in the table and select this button to open the left-panel Services tab. The appropriate service or service group will be selected and you can access its right-panel tabs.

Show Conflicting Rules Button

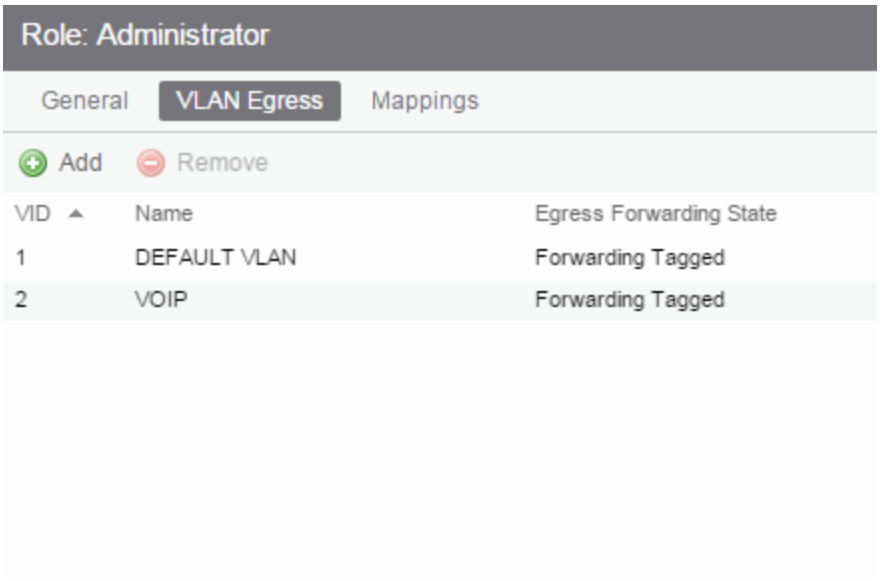
If the rules in a Global service conflict with the rules in a Local service, the Name column will display a message indicating that the global rules will be overridden by the local rules. Select the **Show Conflicting Rules** button to open a window that displays the rule conflicts and shows specifically which rules will be used and which will be overridden. For more information, see Conflict Checking.



VLAN Egress (Role)

The role VLAN Egress tab displays the list of VLANs on the selected role's egress list, and allows you to add and remove VLANs and set their Egress Forwarding State. Ports that the selected role is active on forwards traffic belonging to the listed VLANs according to the specified forwarding state. Both the role's egress list and the VLAN egress list are checked for egress information. If the lists have duplications, the Forbid Forwarding state takes precedence.

To access this tab, select a role in the left panel's **Roles/Services** tab and select the **VLAN Egress** tab in the right panel. Any changes made on this tab need to be enforced.



VID

The VLAN ID.

Name

The VLAN Name.

Egress Forwarding State

Ports on which the selected role is active forward traffic belonging to this VLAN according to the egress forwarding state: Tagged (frames are forwarded as tagged), Untagged (frames are forwarded as untagged), or Forbid Forwarding (frames are not forwarded; they are discarded).

Add

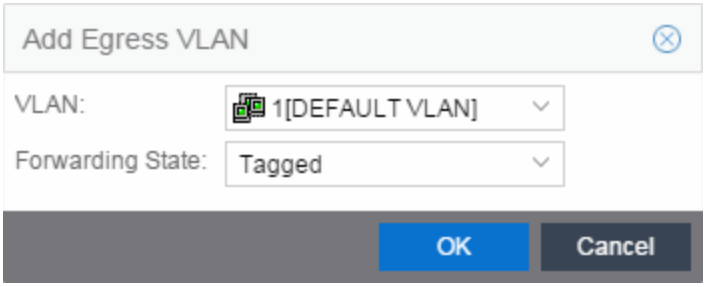
Opens the Add Egress VLAN Window, where you can choose a VLAN for the role's egress list and specify the egress forwarding state.

Remove

Select a VLAN and select **Remove** to remove the VLAN from the list.

Add Egress VLAN Window

The Add Egress VLAN window appears when you select the **Add** button in the role's VLAN Egress tab. It allows you to add a VLAN to the Role's Egress list and specify the egress forwarding state.



VLAN

This is a drop-down list of the available VLANs.

Forwarding State

Select the desired forwarding state: Tagged (frames are forwarded as tagged), Untagged (frames are forwarded as untagged), or Forbidden (frames are not forwarded; they are discarded).

Mappings (Role)

This tab lets you view and configure four different mapping lists for the selected role:

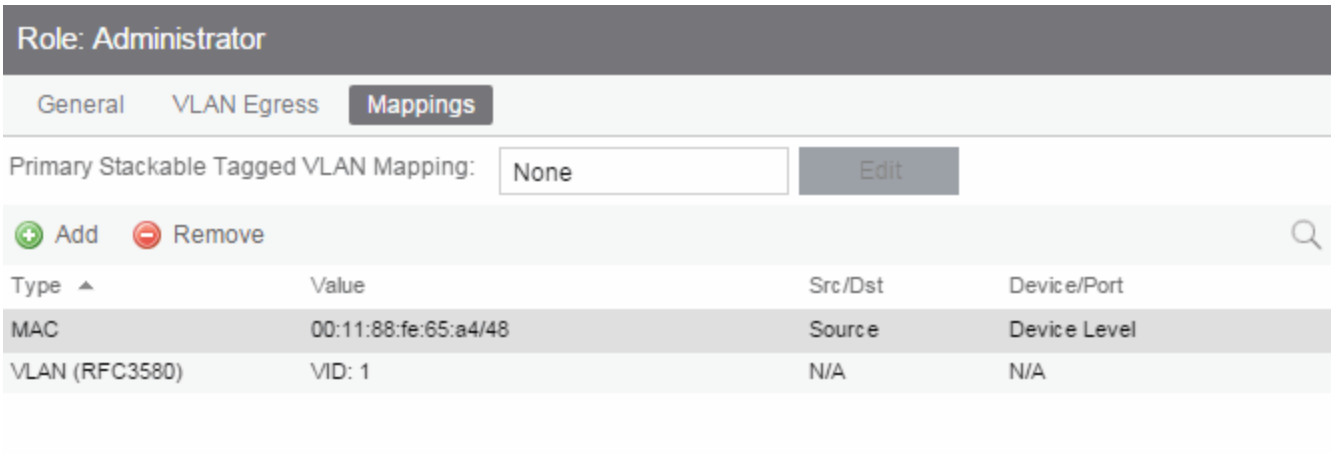
- **MAC to Role Mapping** — Lets you assign the role to an end user based on the user's MAC address.
- **IP to Role Mapping** — Lets you assign the role to an end user based on the user's IP address.
- **Tagged Packet VLAN to Role Mapping** — Lets you assign the role to network traffic based on the traffic's VLAN ID.
- **Authentication-Based VLAN to Role Mapping** — Lets you assign the role to an end user during the authentication process, based on a VLAN Attribute.

To access this tab, select a role in the left-panel **Roles** tab and select the **Mappings** tab in the right panel. Any additions or changes you make to this tab must be enforced in order to take effect.

NOTE: TCI Overwrite Requirement

-- Tagged Packet VLAN to Role Mapping applies the Role definition to incoming packets using a mapped VLAN. This definition applies a CoS and determine if the packet is discarded or permitted, and if TCI Overwrite is enabled re-specifies the VLAN ID defined by the Rule / Role Default. If TCI Overwrite is disabled, the packet egresses (if permitted by the Rule Hit) with the original VLAN ID with which it ingressed.

-- If supported by the device, you can enable TCI Overwrite for an individual role in the role's General tab. The stackable devices support rewriting the CoS values but not the VLAN ID.



Primary Stackable Tagged VLAN Mapping

Use this column to select the device-level VLAN to role mapping used for C2/C3/C5 and B2/B3/B5 devices (C2 firmware version 03.02.xx and higher/B2 firmware version 02.00.16 and higher), and D2, A4, and G3 devices (G3 firmware version 6.03.xx and higher). These devices only support one device-level VLAN to role mapping. If you do not make a selection, there will be no device-level mapping for these devices. Use the Mappings tab in the Enforce Preview window to quickly see which VLAN to role mapping is selected for these devices.

Type

This column indicates the type of mapping: MAC to Role, IP to Role, Tagged Packet VLAN to Role, and Authentication based VLAN to Role.

Value

The MAC addresses, IP addresses, or VLAN mapped to this role.

Src/Dst

Specifies whether the MAC address is a source or destination address.

Device/Port Level

This column indicates whether the mapping is a device-level mapping (all devices) or a port-level mapping (IP address and port description).

Add Button

Opens the Add Role Mapping window, where you can add a new Role mapping by entering the Mapping Type, Value, and Direction.

Remove Button

Remove the selected mapping from the list by selecting **Remove**.

MAC to Role Mapping

MAC to Role mapping provides a way to assign a role to an end station based on its MAC address. This enables you to create a specific role for a group of end stations (such as IP phones), and assign it to

them based on their MAC address. When the end stations connect to the network, the policy-enabled device identifies the source MAC address and applies the mapped role.

IP to Role Mapping

IP to Role mapping provides a way to assign a role to an end station based on its IP address. For example, in networks that haven't deployed authentication, this would enable you to map an individual IP address such as an administrator's laptop, to a specific role. When the end station connects to the network, the policy-enabled device identifies the IP address and applies the mapped role.

Tagged Packet VLAN to Role Mapping

Tagged Packet VLAN to Role mapping provides a way to let policy-enabled devices assign a role to network traffic, based on a VLAN ID. When a device receives network traffic that has been tagged with a VLAN ID (tagged packet) it uses the Tagged Packet VLAN to Role mapping list to determine what role to assign the traffic based on the VLAN ID. For more information, see VLAN to Role Mapping in the Concepts Help topic.

Authentication-Based VLAN to Role Mapping

Authentication-Based VLAN to Role mapping provides a way to assign a role to a user during the authentication process, based on a VLAN Attribute. An end user connects to a policy-enabled device that supports 802.1X authentication using a RADIUS Server. During the authentication process, the RADIUS server returns a VLAN ID in its RADIUS VLAN Tunnel Attribute. The device uses the Authentication-Based VLAN to Role mapping list to determine what role to assign to the end user, based on the VLAN Tunnel Attribute. Use this table to view and configure the VLANs that will map to the selected role. For more information, see VLAN to Role Mapping in the Concepts Help topic.



Pre-configured Domains (Legacy)

To help you quickly achieve the best policy configuration for your network, the **Policy** tab provides pre-configured domains that include roles, services, and rules designed for specific network scenarios. You can use these pre-configured domains as templates, customizing them for your own network requirements.

When you first access the **Policy** tab, it opens to the Default Domain. This domain can be deployed "as-is" for most networks, and provides a complete set of roles, services, and rules, as well as multiple switch platform support.

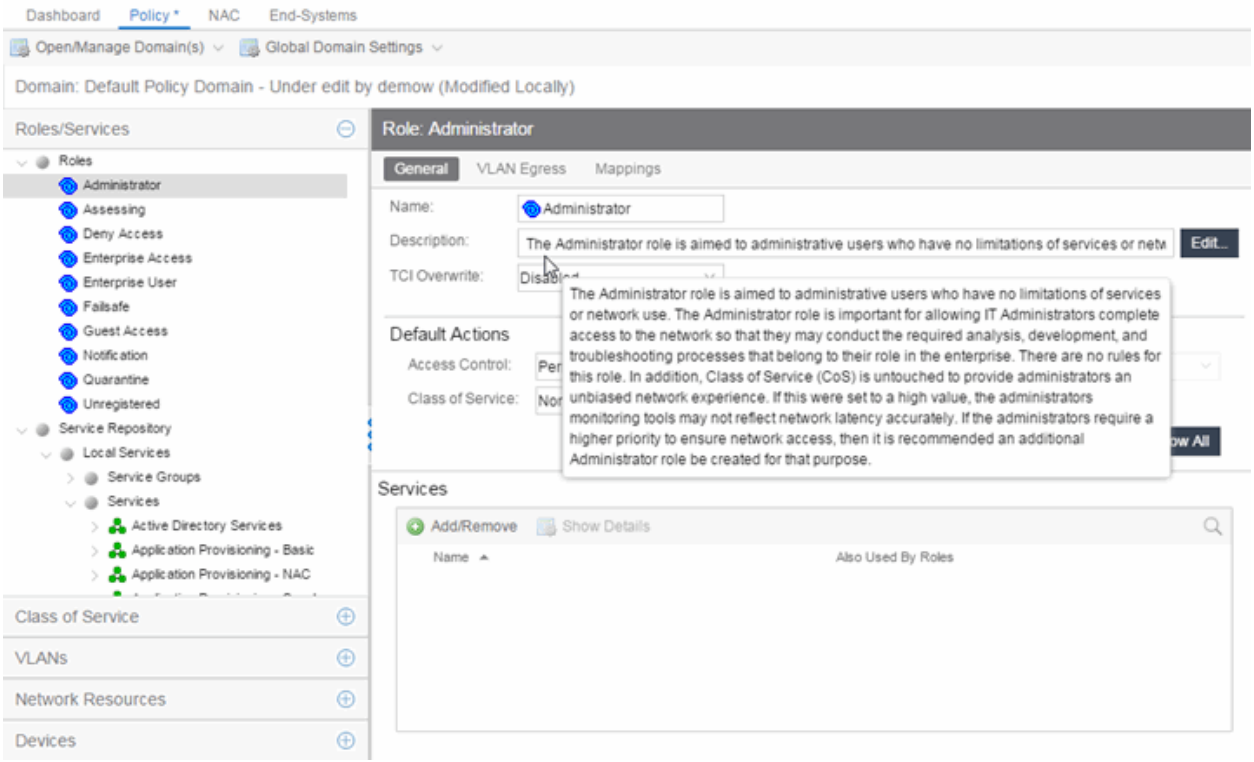
The **Policy** tab also provides additional pre-configured domains tailored to more specific network scenarios. These domains are named according to the policy configuration they provide, for example,

HealthCare Services and Secure Guest. Below is a brief description of each domain along with some suggestions on how to use the domain in your network environment.

Access Pre-Configured Domains

Access the pre-configured domains from the **Open/Manage Domain** drop-down list. At the top of the menu, the **Open Domain** menu displays all available domains from which you can select. To open a domain, select it in the menu. The domain opens in the **Policy** tab and you can look at the various roles, services, and rules that have been pre-configured in the domain.

As you look at a domain, use the extensive tool tips for the roles and services (as shown below) to view specific information on how to customize the domain to meet your requirements.



Pre-configured Domain Descriptions

The following sections describe the pre-configured domains available from the Domain menu.

Embedded NAC Domain

This domain can be used to configure the policy used by the Embedded Access Control engine. By default it will let traffic through unrestricted as you monitor your network.

Generic Services N-Series

This domain is designed to help networks that use Enterasys N-Series devices to increase security in their existing infrastructure. The roles defined in this domain leverage the capabilities supported on the N-Series. They are based on the best-practice of "least privilege" where all incoming traffic is denied access, and permit rules are used to permit only specific traffic onto the network. The rules also provide appropriate traffic classification.

Start with the roles, services, and rules defined in this domain for your N-Series devices and then expand and customize the domain to meet your own day-to-day business requirements.

Generic Services SecureStack

This domain is designed to help networks that use Enterasys SecureStack devices to increase security in their existing infrastructure. The roles defined in this domain leverage the capabilities supported on the SecureStack products, but will also work on N-Series devices. They are based on the best-practice of "least privilege" where all incoming traffic is denied access, and permit rules are used to permit only specific traffic onto the network. The rules also provide appropriate traffic classification.

Start with the roles, services, and rules defined in this domain for your Securestack devices and then expand and customize the domain to meet your own day-to-day business requirements.

HealthCare Services

The Healthcare Services domain provides a template of roles and services that can be utilized in healthcare industry networks. Roles correspond to the different business roles in health care settings, such as Physician, Nurse, Patient, IT, Hospital Administration, Management, and Guest. Services support a wide range of hospital departments, such as Cardiology, Emergency, Pediatrics, and Payroll/Benefits.

Quickstart

The Quickstart domain gets you up and running quickly with a set of roles, services, and rules that will increase security on your network. Most of the defined roles permit access to the network with certain rules designed to deny or prioritize applications, protocols, and communication traffic on the network. The services are bare minimum examples, and it is suggested that you modify or add roles, services, and rules to meet your day-to-day business requirements. HOW IS THIS DIFFERENT FROM THE DEFAULT DOMAIN?

Note: Before enforcing the policy configuration, set Class of Service mode for the device (select the device in the Policy Manager Network Elements tab, then select the General tab) to "Role-Based Rate Limits / Transmit Queue Configuration". The default Class of Service mode can be specified in the Tools->Options view, and multiple devices can have their Class of Service mode changed using the Device Configuration Wizard in the Tools menu. THIS NOTE IS IN THE TAB DESCRIPTION, IS IT NEEDED?

Secure Guest

Secure Guest is a collection of sample services that you can use to increase security on edge ports where guest users connect.

There is one Secure Guest Access role that enables the end user basic guest services based on the principle of "least privilege" and will permit end users access to HTTP, HTTPS, and PPTP services. Apply this role to an Enterasys policy capable switch port.

The services are bare minimum examples, and it is suggested that you modify or add roles, services, and rules to meet your own business requirements.

ShoreTel

The ShoreTel domain provides a template for traffic prioritization of VoIP traffic on ShoreTel IP Phones that operate with the Media Gateway Control Protocol (MGCP) protocol. Class of Service is configured to provide higher priority to VoIP data, signaling and call control protocol, while lower priority is assigned to other required ShoreTel traffic such as DHCP and TFP.

The defined ShoreTel_IP_Phone role is based on the best practices methodology of "least privilege" where all incoming traffic is denied access, and permit rules are used to permit only specific traffic onto the network. Start by using the template for your N-Series devices, then add custom roles, services, and rules to meet your own network requirements.

VPN Termination Point

VPN Termination Point is a collection of Site-to-Site and Client-to-Site Roles that you can use to enable a VPN Concentrator to initiate, respond-to, and communicate to other VPN termination end points.

Add/Remove Services (Roles)

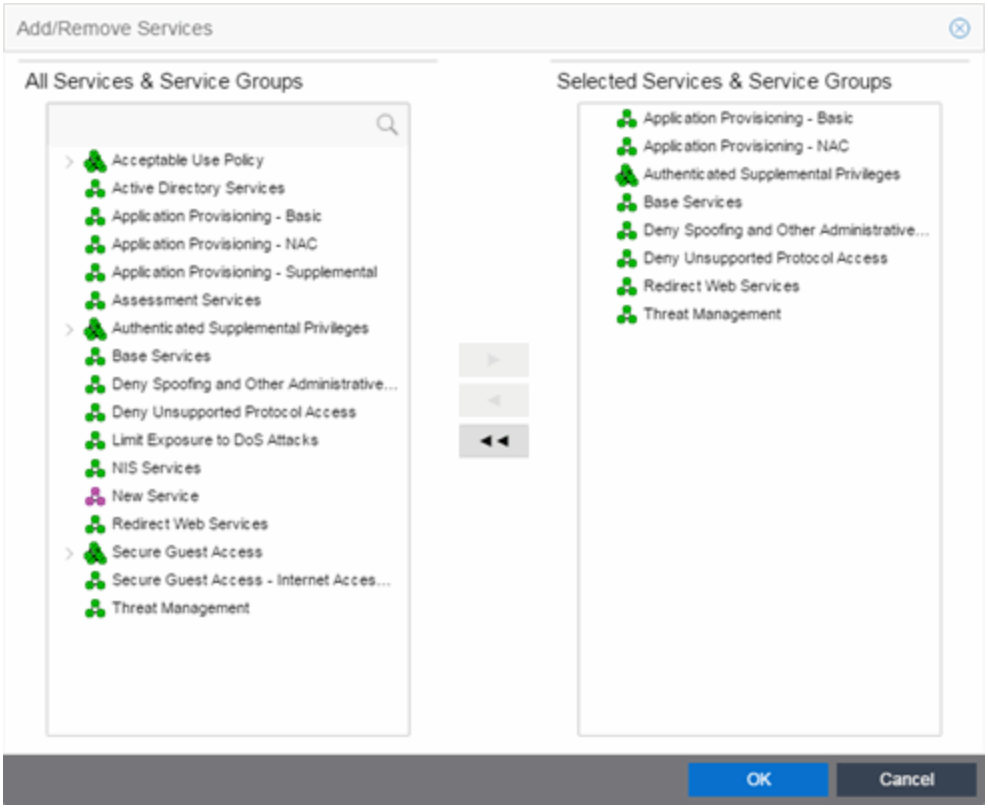
Add and remove services and service groups from roles using the Add/Remove Services window.

To access the Add/Remove Services window, you must have a role selected in the left-panel **Roles** tab. Select the **Add/Remove** button in the Services section of the Role window.

If you add a service to a role and any or all of the following conditions exist, you are in effect adding an "empty" service, and a warning message displays when you select **OK**:

- No traffic description exists for one or more of the classification rules.
- No access control or class of service has been defined for one or more of the classification rules.
- All of the classification rules are disabled.

When you add a service to a role which already has services associated with it, the **Policy** tab checks for rule conflicts. See Conflict Checking for more information.



All Services & Service Groups

This field displays all the services (local and global) and service groups in the current domain. Select the service groups or services you want to add to the role.

Selected Services & Service Groups

This field displays all the services currently defined for the selected role. Select the services you want to remove from the role.

Right Arrow

Select the **Right Arrow** to add the services or service groups selected in the All Services & Service Groups column to the Selected Services & Service Groups field.

Left Arrow

Select the **Left Arrow** to remove the services selected in the Selected Services & Service Groups field.

Double Left Arrow

Select the **Double Left Arrow** to remove all the services in the Selected Services & Service Groups field.

Details View (Service)

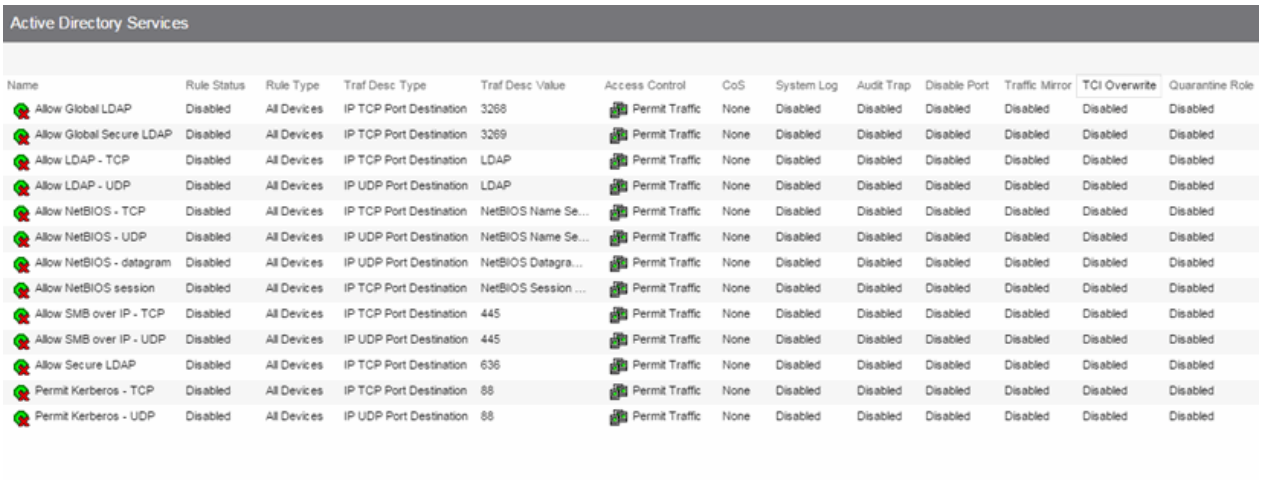
This tab displays information about the rules contained in a Manual service or an Automated service. To display this tab:

1. Select a service in the left-panel's **Roles/Services > Service Repository** tab.
2. Open either the **Local Services** tab or **Global Services** tab, depending on the type of service.
3. Select a service from within the **Services** left-panel tab.

The Details View tab opens in the right panel. Right-click a rule in the table to see a menu of available options.

NOTE: Rules included in services are read in the order in which they are listed in ExtremeCloud IQ Site Engine. To configure rules for ExtremeCloud IQ Controller (formally called XCC or XCA) devices, ensure ExtremeCloud IQ Site Engine lists the rules in the correct order or the service may not execute the correct rule. To reorder rules in the same service, use drag-and-drop capabilities to move from one group to another.

For Manual services, you can double-click on any of the table columns opens the rule's General tab.



Name

Name of the rule. For rules contained in an Automated service, this column gives detailed information about the rule including the associated Network Resource (NR), if multiple resource groups are specified. You can rename a rule by right-clicking the rule and selecting **Rename**.

Rule Status

Indicates whether the rule is currently available for use by this service (Enabled), or not (Disabled), as set in the General tab for the rule. If the rule is disabled, the rule icon displays a

red X . You can enable or disable a rule by right-clicking and selecting **Enable Rule** or **Disable Rule**, respectively.

Rule Type

Indicates the device types to which the rule applies. (See Create Classification Rule Window for more information.)

Traf Desc Type

Traffic classification type for the rule. (See Classification Types and their Parameters for more information.)

Traf Desc Value

Values associated with the traffic classification type for the rule. (See Classification Types and their Parameters for more information.) Double-clicking on this column opens the Edit Rule window, where you can edit the parameters or values for the rule's classification type.

Access Control

VLAN action associated with the rule. Double-clicking on this column allows you change the setting. You can permit traffic to be forwarded, deny traffic altogether, or select a VLAN to contain traffic. Select **None** to disable access control for this rule.

CoS

Class of service action associated with the rule. Double-clicking on this column allows you change the setting.

System Log

Displays whether the syslog functionality (a syslog message is generated when the rule is used) is enabled, disabled, or prohibited for the rule. Double-clicking on this column allows you change the setting.

- **Enabled** - If this option is enabled, a syslog message is generated when the rule is used. This option must be enabled if you are configuring Policy Rule Hit Reporting on your devices.
- **Disabled** - If this option is disabled and this rule is hit, it does not generate a Syslog message, but lower-precedence rules and the role default actions may still specify a syslog message be sent for this data packet if there is a match.
- **Prohibited** - If this rule is hit, no syslog message is generated for this data packet, even when a lower-precedence rule or the role default actions has the System Log action set to enabled.

Audit Trap

Displays whether the audit trap functionality (an audit trap is generated when the rule is used) is enabled, disabled, or prohibited for the rule. Double-clicking on this column allows you change the setting.

- **Enabled** - If this option is enabled, an audit trap is generated when the rule is used.
- **Disabled** - If this option is disabled and this rule is hit, it does not generate an audit trap, but lower-precedence rules and the role default actions may still specify generating an audit trap for this data packet if there is a match.
- **Prohibited** - If this rule is hit, no audit trap is generated for this data packet, even when a lower-precedence rule or the role default actions has the Audit Trap action set to enabled.

Disable Port

Displays whether the disable port functionality (ports reported as using this rule will be disabled) is enabled, disabled, or prohibited for the rule. Double-clicking on this column allows you change the setting.

- **Enabled** - If this option is enabled, any port reported as using this rule are disabled.
- **Disabled** - If this option is disabled and this rule is hit, it does not disable the port, but lower-precedence rules and the role default actions may still specify disabling the port for this data packet if there is a match.
- **Prohibited** - If this rule is hit, the port is not disabled, even when a lower-precedence rule or the role default actions has the Disable Port action set to enabled.

Traffic Mirror

Displays whether the traffic mirror functionality is enabled, disabled, or prohibited for the rule. Double-clicking on this column allows you change the setting.

- **Select port group(s)** - Use the drop-down list to specify the port groups where mirrored traffic will be sent for monitoring and analysis.
- **Disabled** - If this option is disabled and this rule is hit, traffic mirroring will not take place, but lower-precedence rules and the role default actions may still specify traffic mirroring for this data packet if there is a match.
- **Prohibited** - If this rule is hit, traffic mirroring is disabled, even when a lower-precedence rule or the role default actions has the Traffic Mirror action specified.

TCI Overwrite

Displays whether TCI Overwrite is enabled, disabled, or prohibited for the rule. Double-clicking on this column allows you change the setting.

- **Enabled** - Enabling TCI Overwrite allows the VLAN (access control) and class of service characteristics defined in this rule to overwrite the VLAN or class of service (CoS) tag in a received packet, if that packet has already been tagged with VLAN or CoS information.
- **Disabled** - If this option is disabled the TCI Overwrite option is ignored, but lower-precedence rules and the role default actions may still specify TCI Overwrite for the data packet if there is a match.
- **Prohibited** - Do not set TCI Overwrite for this data packet, even when a lower-precedence rule or the role default actions has the TCI Overwrite option set to enabled.

Quarantine Role

Displays whether a Quarantine role is enabled, disabled, or prohibited for the rule. Double-clicking on this column allows you change the setting.

- **Select Role** - Use the drop-down list to select the role that you want to assign as a Quarantine role.
- **Disabled** - If this option is disabled and this rule is hit, a Quarantine role will not be assigned, but lower-precedence rules may still specify a Quarantine role for this data packet if there is a match.
- **Prohibited** - If this rule is hit, a Quarantine role will not be assigned, even when a lower-precedence rule has a Quarantine role action specified.



Service Repository

Selecting Service Repository in the Roles/Services navigation panel in the left panel opens the Service Repository panel.

Double-click Local Services to display the service groups and services associated with the current domain or Global Services (All Domains) to display the service groups and services available to all domains.



Name

Displays the Local or Global service groups and services.

Local/Global Services

Selecting Local Services or Global Services (All Domains) in the Roles/Services > Service Repository navigation panel in the left panel opens the Local Services or Global Services (All Domains) panel, respectively.

Double-click Service Groups to display the services that are part of a service group or Services to view services not contained within a service group.



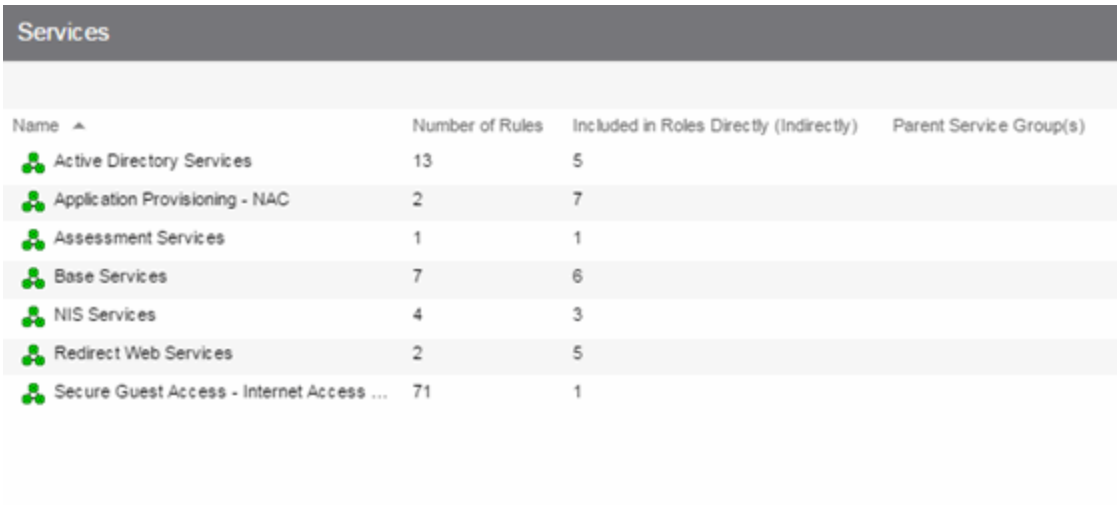
Name

Double-click one of the options to display the Service Groups or Services.

Details View (Services)

This tab lists the Automated and Manual services you create in the **Policy** tab. To display the tab, expand the **Local Services** or **Global Services** left-panel tab in the **Roles/Services > Service Repository** tab, and select the **Services** tab. To see a menu of options available for a service, right-click the service.

For information on the differences between automated or manual services, and local or global services, see the Policy tab Concepts Help topic's section on Services.



Name
Name of the service.

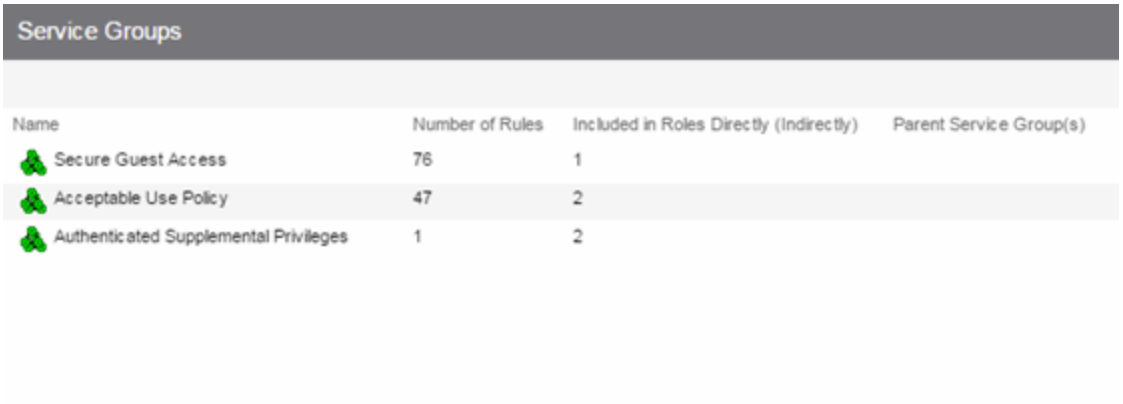
Number of Rules
Number of rules associated with the service.

Included in Roles Directly (Indirectly)
Number of roles in which the service is included.

Parent Service Group
The service group in which the service is included.

Details View (Service Group)

This tab lists information about the services or service groups contained in a **Local** or **Global** service group. To display this tab, select a service group in the left-panel **Roles/Services > Service Repository** tab.



Name
The name of the service or service group.

Number of Rules
The number of rules included in the service or service group.

Included in Roles Directly (Indirectly)
The number of roles where the service or service group exists directly in the role's Services list (as viewed on the role's **General** tab). If a service group also exists indirectly in other roles as part of another service group, that number of roles is displayed in parenthesis. In the example above, the service group called "Authenticated Supplemental Privileges" displays "1 (1)" in this column, showing that it is associated directly with one role (exists in that role's services list) and is also part of a service group associated with one other role.

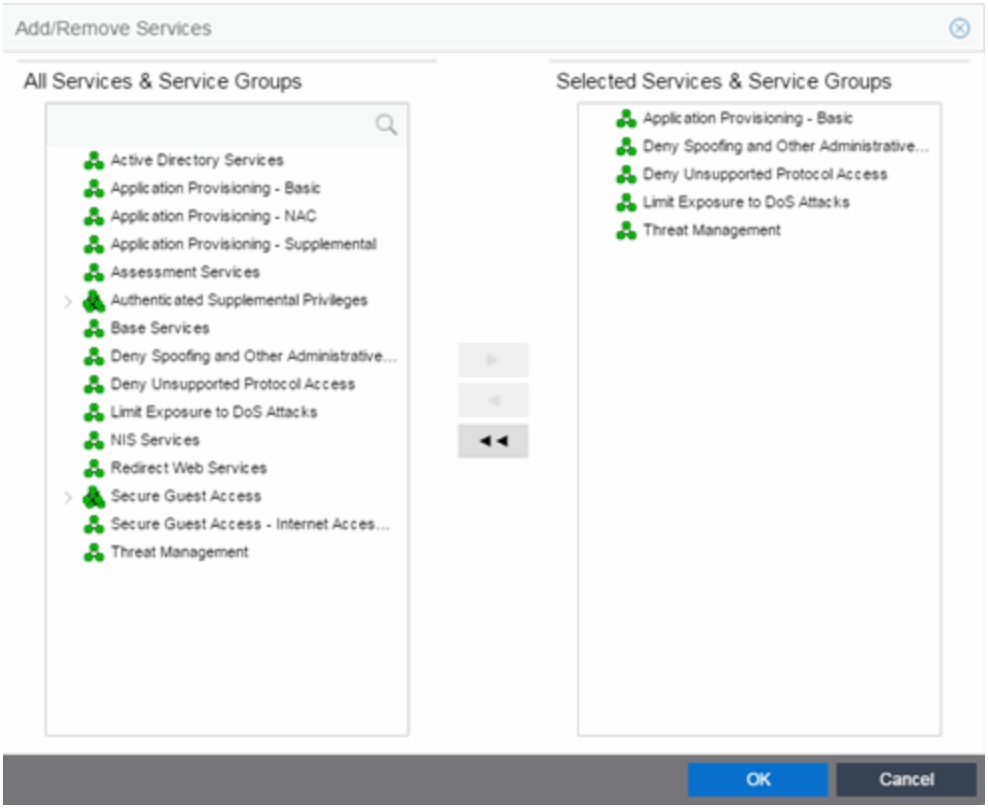
Parent Service Group(s)
Displays all the "parent" service groups to which the service or service group belongs. This gives you an idea of the service group hierarchy without having to expand the left-panel tree.

- How to Create a Service

Add/Remove Services (Service Groups)

You can add and remove services from service groups using the Add/Remove Services window.

To access the Add/Remove Services window, either select the **Service Groups** tab in the **Local Services** or **Global Services** left-panel tab, right-click on a service group in the right panel and select **Add/Remove Services**. You can also right-click on a service group in the **Service Groups** left-panel tab and select **Add/Remove Services** from the menu.



All Services & Service Groups

This list displays all the local or global services and service groups in the current domain, depending whether you launched the window with a local or global service group selected. Select the services you want to add to the service group.

Selected Services & Service Groups

This list displays all the services currently defined for the selected service group. Select the services you want to remove from the service group.

Right Arrow Button

Select the **Right Arrow** button to add the services selected in the All Services & Service Groups list to the Selected Services & Service Groups list.

Left Arrow Button

Select the **Left Arrow** button to remove the services selected in the Selected Services & Service Groups list.

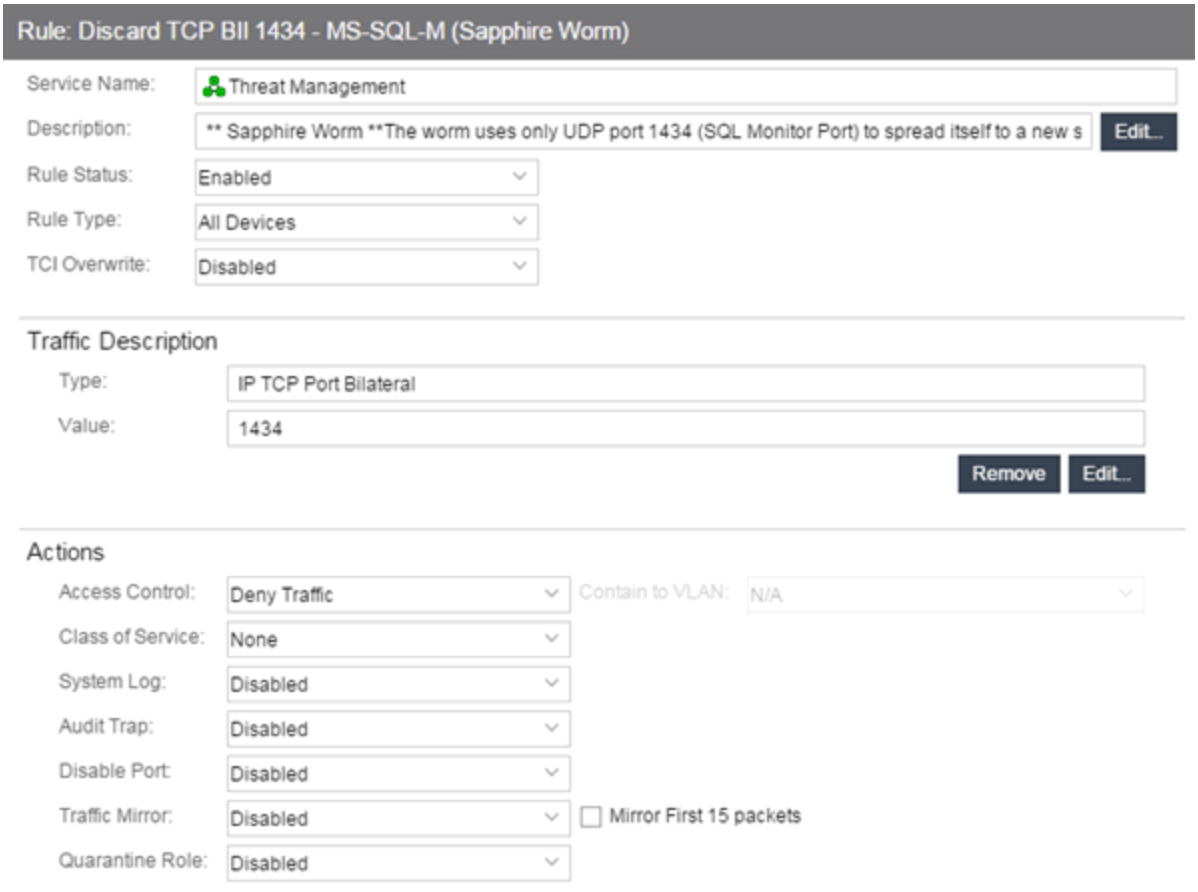
Double Left Arrow Button

Select the **Double Left Arrow** button to remove all the services from the Selected Services & Service Groups list.

Rule

The rule **General** tab displays general information about the rule selected for a Service in the left-panel **Roles/Services > Service Repository > Local or Global Services** tab and enables you to change it. In addition, you can view and change the Traffic Description and Actions associated with the rule. Traffic Description identifies the type of traffic to which the rule pertains. Actions apply class of service, access control, and/or accounting and security behavior to packets matching the rule.

Any additions or changes you make to this tab must be enforced in order to take effect. If you modify an enabled rule's actions, the Policy tab checks for conflicts with other rules in the services and roles with which the newly modified rule is associated. See Conflict Checking for more information.



General Area

Service Name

Displays the name of the rule.

Description

Use the **Edit** button to open a window where you can enter or modify a description of the rule.

Rule Status

Lets you disable the rule, or enable it if it's already disabled. If the rule is disabled, it is unavailable for use by the current service, but can still be copied to other services and enabled, or re-enabled at another time for the current service. Disabling a rule is an alternative to deleting and recreating it. The rule icon in the left panel displays a red X if the rule is disabled.

Rule Type

Use the drop-down list to select the types of devices to which you wish this rule to apply when enforced. The recommended selection is All Devices, unless there is a specific need for a device-specific rule. If this need arises, the Rule Type feature enables services to be customized to contain rules specific to a device's type when support for a traffic description and/or action is not be available on all managed devices.

For device-specific rules, only those traffic descriptions supported on the device are available when you define the rule's traffic description on this tab. For All Devices rules, all traffic descriptions are available; however, you must be aware that you cannot enforce the rule to a device on which it is not supported.

TCI Overwrite

Specify the TCI Overwrite functionality for the rule:

- **Enabled** — Enabling TCI Overwrite enables the VLAN (access control) and class of service characteristics defined in this rule to overwrite the VLAN or class of service (CoS) tag in a received packet, if that packet has already been tagged with VLAN or CoS information.
- **Disabled** — If this option is disabled the TCI Overwrite option is ignored, but lower-precedence rules and the role default actions can still specify TCI Overwrite for the data packet if there is a match.
- **Prohibited** — Do not set TCI Overwrite for this data packet, even when a lower-precedence rule or the role default actions has the TCI Overwrite option set to enabled.

Traffic Description Area

The Traffic Description area enables you to view and change the traffic description associated with a rule. The Traffic Description identifies the traffic classification type for the rule. Rules enable you to assign access control (VLAN membership) and/or class of service to network traffic depending on the traffic's classification type.

Type

Displays the Classification Type selected for the rule.

Value
Displays the values/parameters selected for the rule's Classification Type. See Classification Types and their Parameters for parameter information.

Remove Button
Removes the traffic description from the rule.

Edit Button
If a Traffic Description Type has been defined for the rule, selecting Edit opens the Edit Rule window, where you can edit the parameters or values for the rule's classification type.

Actions Area

The Actions area enables you to view and change the actions associated with a rule. Actions apply access control, class of service, security, and/or accounting behavior to packets matching the rule.

Access Control
Use this drop-down list to select the appropriate access control for the rule. You can permit traffic to be forwarded, deny traffic altogether, or contain traffic to a VLAN. Select **None** to disable access control for this rule.

- **Permit Traffic** — enables traffic to be forwarded with the port's assigned VID.
- **Deny Traffic** — traffic will be automatically discarded.
- **Contain to VLAN** — contains traffic to a specific VLAN. Use the drop-down list to select the desired VLAN.

Class of Service
Use the drop-down list to select a class of service to associate with the rule. The Policy tab lets you define classes of service that each include an 802.1p priority, and optionally an IP type of service (ToS/DSCP) value, rate limits, and transmit queue configuration. You can then assign a class of service as a classification rule action. See Getting Started with Class of Service and How to Create a Class of Service for more information. Select **None** to disable class of service for this rule.

When rule accounting is enabled on a device, each rule keeps a list of the ports on which it has been used. Use the following three options to specify certain rule usage actions to take place when a "rule hit" is reported.

System Log
Specify System Log functionality for the rule.

- **Enabled** — If this option is enabled, a syslog message is generated when the rule is used. This option must be enabled if you are configuring Policy Rule Hit Reporting on your devices.
- **Disabled** — If this option is disabled and this rule is hit, it does not generate a Syslog message, but lower-precedence rules and the role default actions can still specify a syslog message be sent for this data packet if there is a match.

- **Prohibited** — If this rule is hit, no syslog message is generated for this data packet, even when a lower-precedence rule or the role default actions has the System Log action set to enabled.

Audit Trap

Specify Audit Trap functionality for the rule:

- **Enabled** — If this option is enabled, an audit trap is generated when the rule is used.
- **Disabled** — If this option is disabled and this rule is hit, it does not generate an audit trap, but lower-precedence rules and the role default actions can still specify generating an audit trap for this data packet if there is a match.
- **Prohibited** — If this rule is hit, no audit trap is generated for this data packet, even when a lower-precedence rule or the role default actions has the Audit Trap action set to enabled.

Disable Port

Specify Disable Port functionality for the rule:

- **Enabled** — If this option is enabled, any port reported as using this rule will be disabled. Ports that have been disabled due to this option are displayed in the device Role/Rule tab.
- **Disabled** — If this option is disabled and this rule is hit, it does not disable the port, but lower-precedence rules and the role default actions can still specify disabling the port for this data packet if there is a match.
- **Prohibited** — If this rule is hit, the port is not disabled, even when a lower-precedence rule or the role default actions has the Disable Port action set to enabled.

Traffic Mirror

Specify traffic mirroring functionality for the rule:

- **Select port group(s)** — Use the drop-down list to specify the port groups where mirrored traffic will be sent for monitoring and analysis. Select View/Modify Port Groups to open the Port Groups tab where you can define user-defined port groups for selection.
  To the right of the drop-down list is an option to mirror only the first (N) packets of a flow. This option is intended for use when mirroring traffic to an ExtremeAnalytics engine. The ExtremeAnalytics engine only needs the initial packets of a flow to properly identify the traffic, and setting this option will reduce network traffic overhead for the switch and engine. By default this number is set to 10, but can be changed by selecting the Edit button . Note that the value you set is used by all mirror actions in use in the current domain.
- **Disabled** — If this option is disabled and this rule is hit, traffic mirroring will not take place, but lower-precedence rules and the role default actions can still specify traffic mirroring for this data packet if there is a match.

- **Prohibited** — If this rule is hit, traffic mirroring is disabled, even when a lower-precedence rule or the role default actions has the Traffic Mirror action specified.

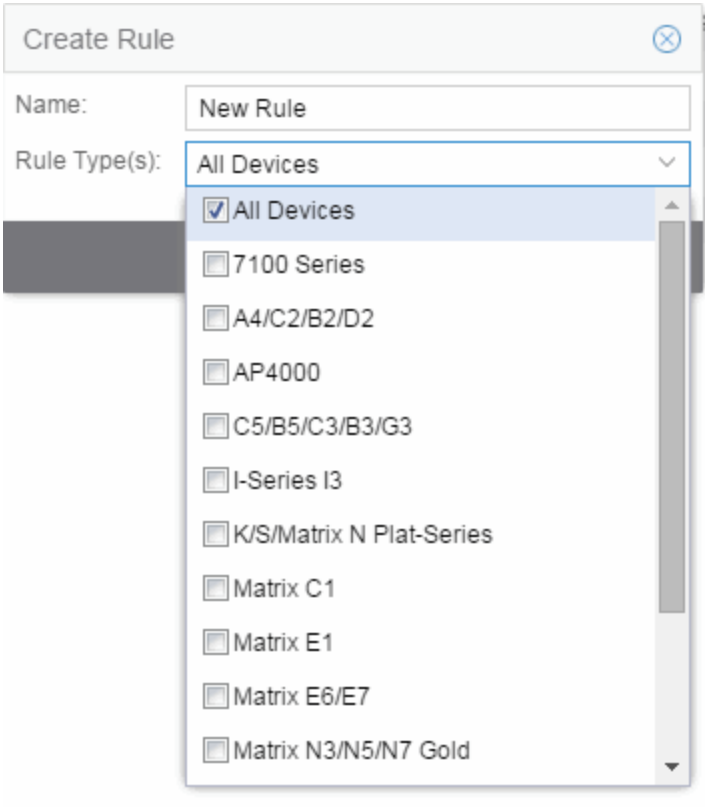
Quarantine Role

Specify the Quarantine Role functionality for the rule:

- **Select Role** — Use the drop-down list to select the role that you want to assign as a Quarantine role. Specifying a role as a Quarantine role turns the role's icon red, denoting its restrictive nature.
- **Disabled** — If this option is disabled and this rule is hit, a Quarantine role will not be assigned, but lower-precedence rules can still specify a Quarantine role for this data packet if there is a match.
- **Prohibited** — If this rule is hit, a Quarantine role will not be assigned, even when a lower-precedence rule has a Quarantine role action specified.

Create Rule

This window displays when you right-click a service group or the **Services** tab in the left-panel and select **Create Rule**. If you use this window, traffic descriptions and actions can be added to the rule afterwards (see Using the Rule Tabs). In order for a rule to be applied to devices, you must enforce.



Name
Enter a name for the rule.

Type
Select the types of devices to which you wish this rule to apply when enforced. See Rule Type for more information on the consequences of your choice.

OK
Select **OK** to create the rule and close the **Create Rule** window.

Apply
Select **Apply** to create the rule and remain in the **Create Rule** window.

Cancel
Select **Cancel** to close the **Create Rule** window without saving your changes.

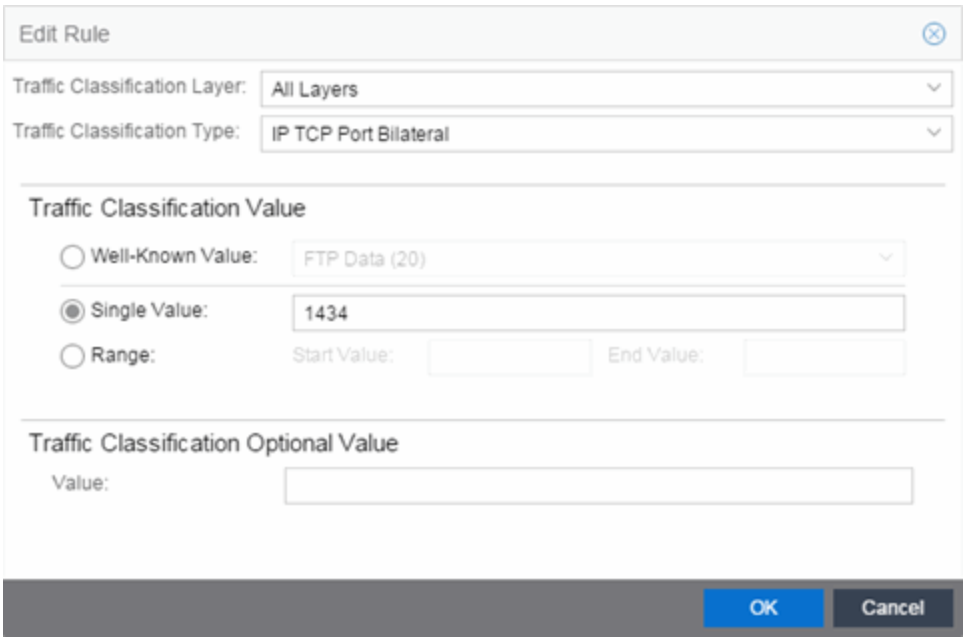
Edit Rule

The Edit Rule window allows you to change the traffic description associated with a rule. The Traffic Description, which includes the traffic classification layer, traffic classification type, and traffic value, was entered when the rule was created (see How to Create or Modify a Rule).

To display the Edit Rule window, select the rule in the left panel's **Services** tab. In the Traffic Description section, select **Edit** to bring up the Edit Rule window.

If you modify an enabled rule's traffic descriptions, the **Policy** tab checks for conflicts with other rules in the services and roles with which the newly modified rule is associated. See Conflict Checking for more information.

The contents of the Edit Rule window varies according to the selected rule and traffic description.



Layer Area

Traffic Classification Layer

The OSI model classification layer (or All Layers) currently associated with the rule. Each layer has multiple classification types from which you can select. If you change the layer, the Type and Value sections in the window change, and you must make new selections in those sections. See Classification Types and their Parameters for information.

Traffic Classification Type

The traffic classification type currently associated with the rule. Each classification type consists of certain parameters and/or values. If you change the type, the Value section of the window changes, and you must make new selections in that section. See Classification Types and their Parameters for information.

Value Area

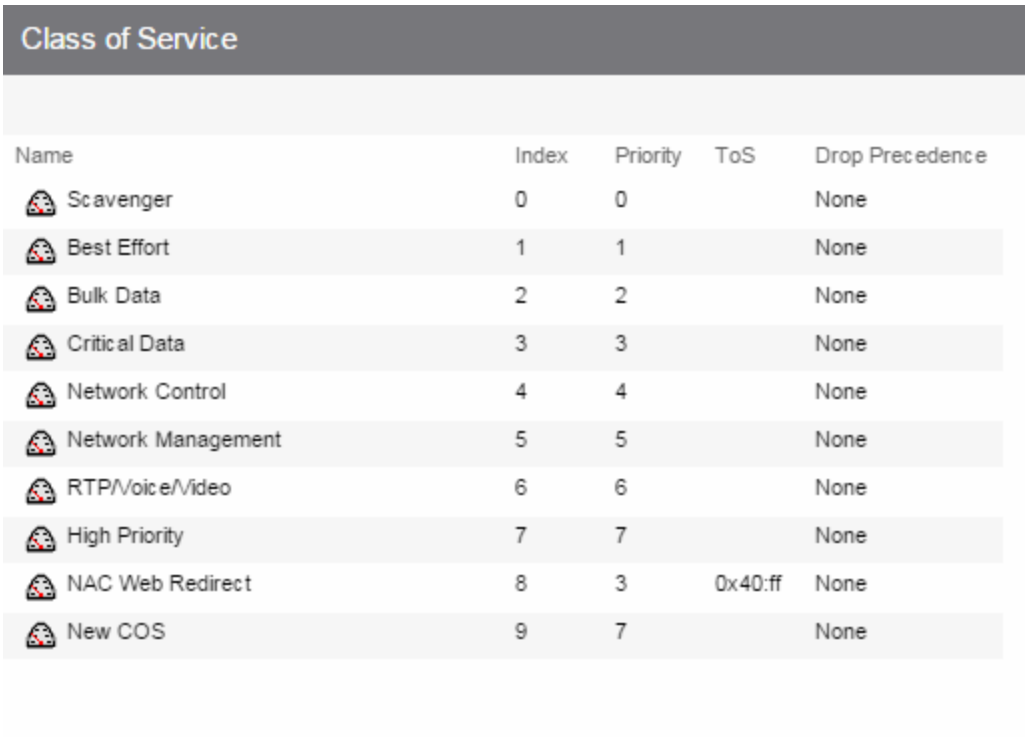
This area displays the values currently selected for the traffic classification type, and allows you to change those values. Each traffic classification type requires certain parameters and/or values. See Classification Types and their Parameters for parameter information.

Class of Service Overview

Use this tab to view the Class of Service (CoS) configuration for the current domain. To access this window, select the **Class of Service** left-panel tab from the **Policy** tab.

This window displays the eight pre-populated static classes of service, each associated with one of the 802.1p priorities (0-7). Use these predefined classes of service or create your own classes of service.

Expanding this tab in the left panel allows you to select individual classes of service in the right panel, which opens them in the Class of Service tab, where you can edit the configuration for the selected CoS.



Name
The name of the class of service.

Index
The index number automatically assigned to the class of service.

Priority
The 802.1p priority associated with the class of service. The priority for the eight static classes of service provided by the Policy tab (Priority 0-7), cannot be disabled or changed.

ToS
The IP type of service value associated with this class of service, if any. See IP Type of Service for more information.

Drop Precedence
The drop precedence associated with this class of service. Double-click in the column to select a Drop Precedence value: Low, Medium, or High.

Getting Started with Class of Service

This Help topic provides an overview of **Policy** tab's class of service (CoS) functionality, including information about defining rate limits and configuring transmit queues.

After you have read this topic, look at an example of how a network administrator might use CoS to configure VoIP traffic with appropriate priority, ToS, queue treatment, and flood control by selecting the link: Class of Service Example.

This guide includes the following information:

- Class of Service Overview
- Rate Limits
- Transmit Queues
- Flood Control

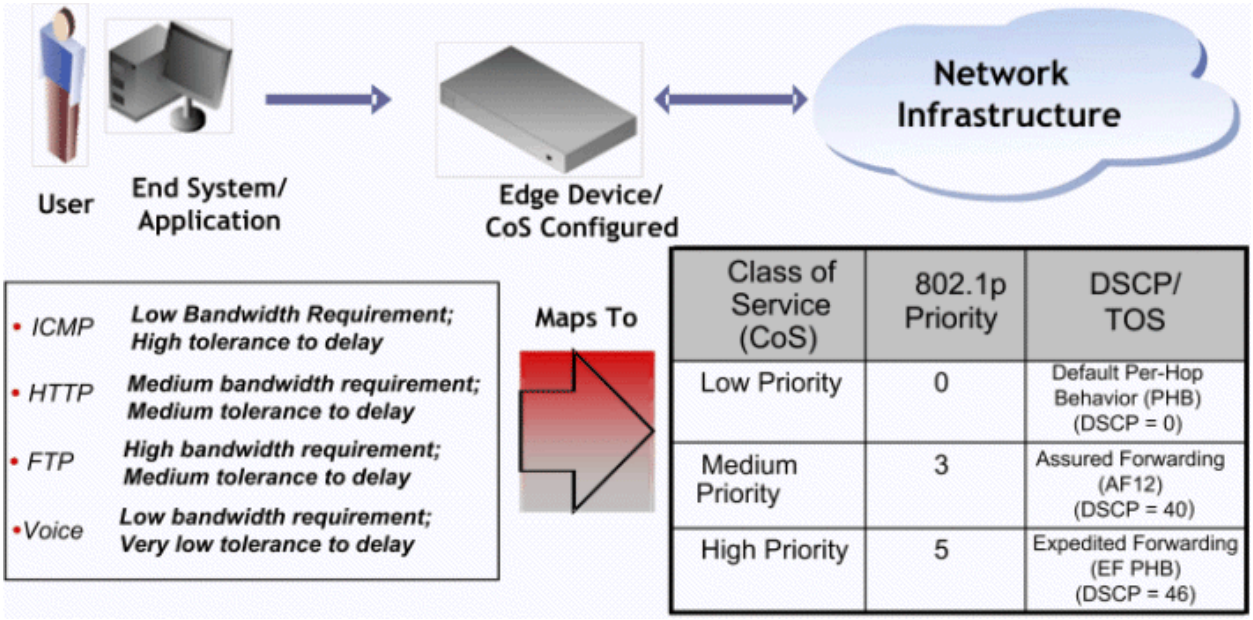
Class of Service Overview

Class of Service (CoS) provides the ability to give certain network traffic preferential treatment over other traffic. It classifies traffic into categories such as high, medium, and low, where high-priority traffic gets the best service while low-priority traffic is "drop eligible."

Class of Service helps you manage the bandwidth requirements of a given network flow with the available port resources on your network devices. (In a CoS context, a flow is a stream of packets classified with the same class of service as the packets transit the interface). Using CoS, you can:

- Assign different priority levels to different packet flows.
- Mark or re-mark the packet priority at port ingress with a Type of Service (ToS).
- Sort flows by transit queue. Higher priority queues get preferential access to bandwidth during packet forwarding.
- Limit the amount of bandwidth available to a given flow by either dropping (rate limiting) or buffering (rate shaping) packets in excess of configured limits.

The following figure shows how you can manage network bandwidth requirements by assigning different classes of service to different types of network traffic.



The ICMP protocol, used for error messaging, has a low bandwidth requirement, with a high tolerance for delay and jitter, and is appropriate for a low priority setting. HTTP and FTP protocols, used respectively for browser-generated and file transfer traffic, have a medium to high bandwidth requirement, with a medium to high tolerance for delay and jitter, and are appropriate for a medium priority level. Voice (VoIP), used for voice calls, has a low bandwidth requirement, but is very sensitive to delay and jitter and is appropriate for a high priority level.

Implementing CoS

CoS determines how a given network flow is assigned bandwidth as it transits your network devices. As a preliminary step to using CoS, it is important that you understand the characteristics of the flows on your network and associate these flows with your policy roles. In this sense, CoS is the third step in a three step process:

1. Understand your network flows using NetFlow.
2. Associate your network flows with a **Policy** tab role.
3. Configure your classes of service and associate them with the rules contained in your roles.

Configuring CoS

The **Policy** tab lets you configure multiple classes of service that include one or more of the following components:

- 802.1p priority
- IP type of service (ToS) value
- drop precedence
- inbound and outbound rate limits

- outbound rate shaper per transmit queue.
- flood control rate limits

After you have created and defined your classes of service, they are then available when you make a class of service selection for a rule action (**Rule** tab), a role default (**General** tab), or an automated service (**Automated Service** tab).

To view and configure CoS, open the **Class of Service Overview** tab from the **Policy** tab. It is pre-populated with eight static classes of service, each associated with one of the 802.1p priorities (0-7). You can use these classes of service as is, or configure them to include ToS, drop precedence, rate limit, and/or transmit queue values. In addition, you can also create your own classes of service (user-defined CoS).

Rate Limits

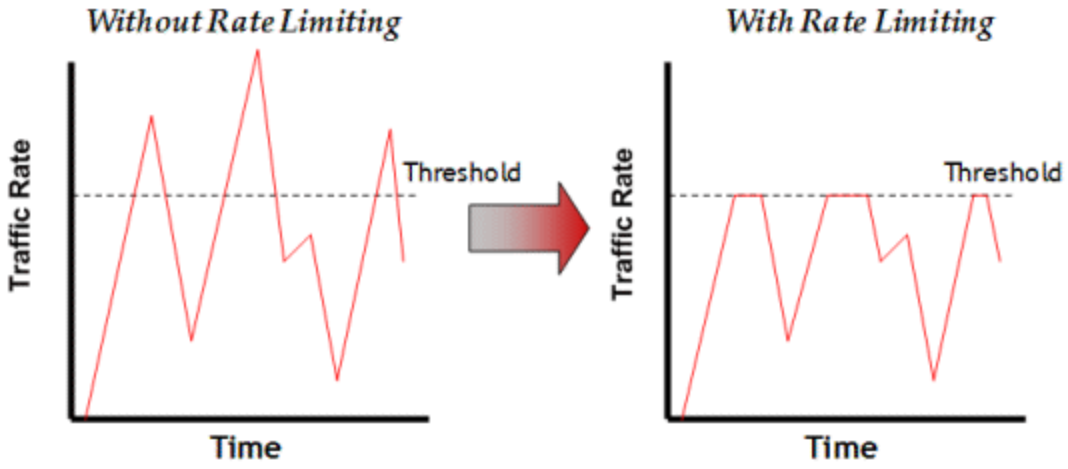
Rate limits are one component of a **Policy** tab class of service. They control the transmit rate at which traffic enters and exits ports in your network. All traffic mapped to a Class of Service on a given port share the bandwidth specified by the rate limit.

For instructions on how to configure rate limits, see How to Define Rate Limits.

Rate limits are tied directly to roles and rules, and are written to a device when the role/rule is enforced. When rate limits are implemented, all traffic on the port that matches the rule with the associated rate limit cannot exceed the configured limit. If the rate exceeds the configured limit, frames are dropped until the rate falls below the limit.

The rate limit remains on the port only as long as the role using the rate limit is active on the port either as the authenticated role or as the port's default role.

The following figure shows how bursty traffic is clipped above the assigned threshold when rate limiting is applied.



The CoS can be configured to perform one or all of the following actions when a rate limit is exceeded:

- Generate System Log on Rate Violation – a syslog message is generated when the rate limit is first exceeded.
- Generate Audit Trap on Rate Violation – an audit trap is generated when the rate limit is first exceeded.
- Disable Port on Rate Violation – the port is disabled when the rate limit is first exceeded.

The **Policy** tab class of service also provides the ability to create rate limit port groups. Port groups let you specify different rate limits within the same class of service. For example, you might create a port group for edge ports and a port group for core ports, and assign two different rate limits. For more information on rate limit port groups, see Creating Class of Service Port Groups.

Transmit Queues

Transmit queue configuration is defined within a class of service and associated with a specific role via a rule action or as a role default. It is implemented based on the role assigned to a port. All traffic received on a port and matching a rule with the associated class of service is forwarded using the defined transmit queue configuration.

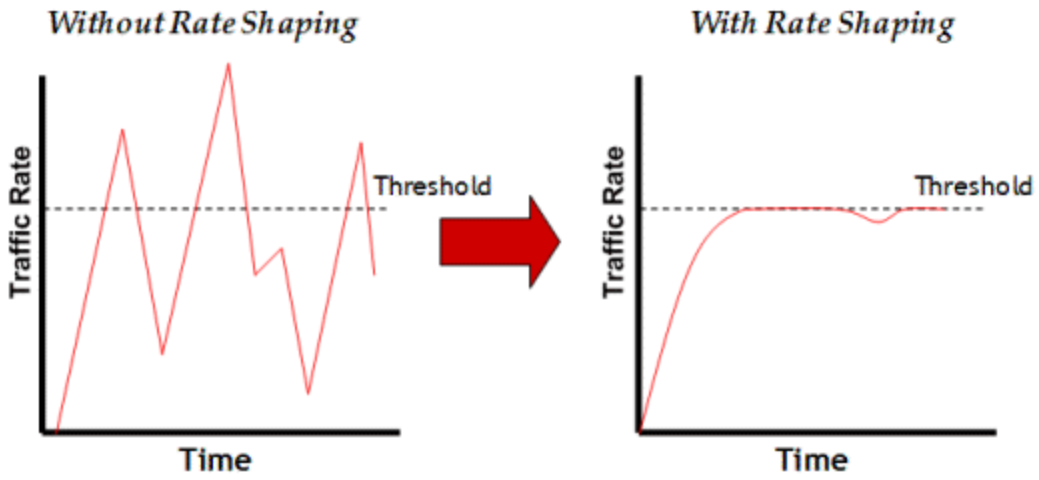
For instructions on how to configure transmit queues, see How to Configure Transmit Queues.

There are three components to transmit queue configuration:

- Transmit Queue Configuration enables you to set the transmit queue associated with the class of service.
- Transmit Queue Rate Shapers let you pace the rate at which traffic is transmitted out of that transmit queue.
- Bandwidth Configuration enables you to specify how the traffic in each transmit queue is serviced as it egresses the port.

The transmit queue configuration remains on the port only as long as the role using the configuration is active on the port either as the authenticated role or as the port's default role.

The following figure shows how bursty traffic is smoothed out when it goes above the assigned threshold when rate shaping is applied.



Rate shaping retains excess packets in a queue and then schedules these packets for later transmission over time. Therefore, the packet output rate is smoothed and bursts in transmission are not propagated as seen with rate limiting.

Rate shaping can be used for the following reasons:

- to control bandwidth
- to offer differing levels of service
- to avoid traffic congestion on other network links by removing the bursty property of traffic that can lead to discarded packets

The **Policy** tab class of service also provides the ability to create transmit queue shaper port groups that enable you to isolate certain kinds of sensitive network traffic so that you can vary the bandwidth of the shape for that single queue. For more information on transmit queue port groups, see Creating Class of Service Port Groups.

Flood Control

Flood control provides rate limiting capabilities to individual Class of Service to permit certain types of flooded traffic to be dropped. When enabled, incoming traffic is monitored over one second intervals. Traffic is identified using the following configuration types:

- unknown - unicast
- broadcast
- multicast

A traffic control rate sets the acceptable flow for each type, specified in packets per second. If, during a one second interval, the incoming traffic of a configured type reaches the traffic control rate on the port, the traffic is dropped until the interval ends. Packets are then permitted to flow again until the limit is reached.

By default, Flood Control is disabled for each CoS. Similar to CoS Port Groups, a different configuration can be assigned for each group. Since Flood Control is shared across all CoS, when Flood Control is enabled on at least one CoS, those rates apply to all ports that have Flood Control enabled.

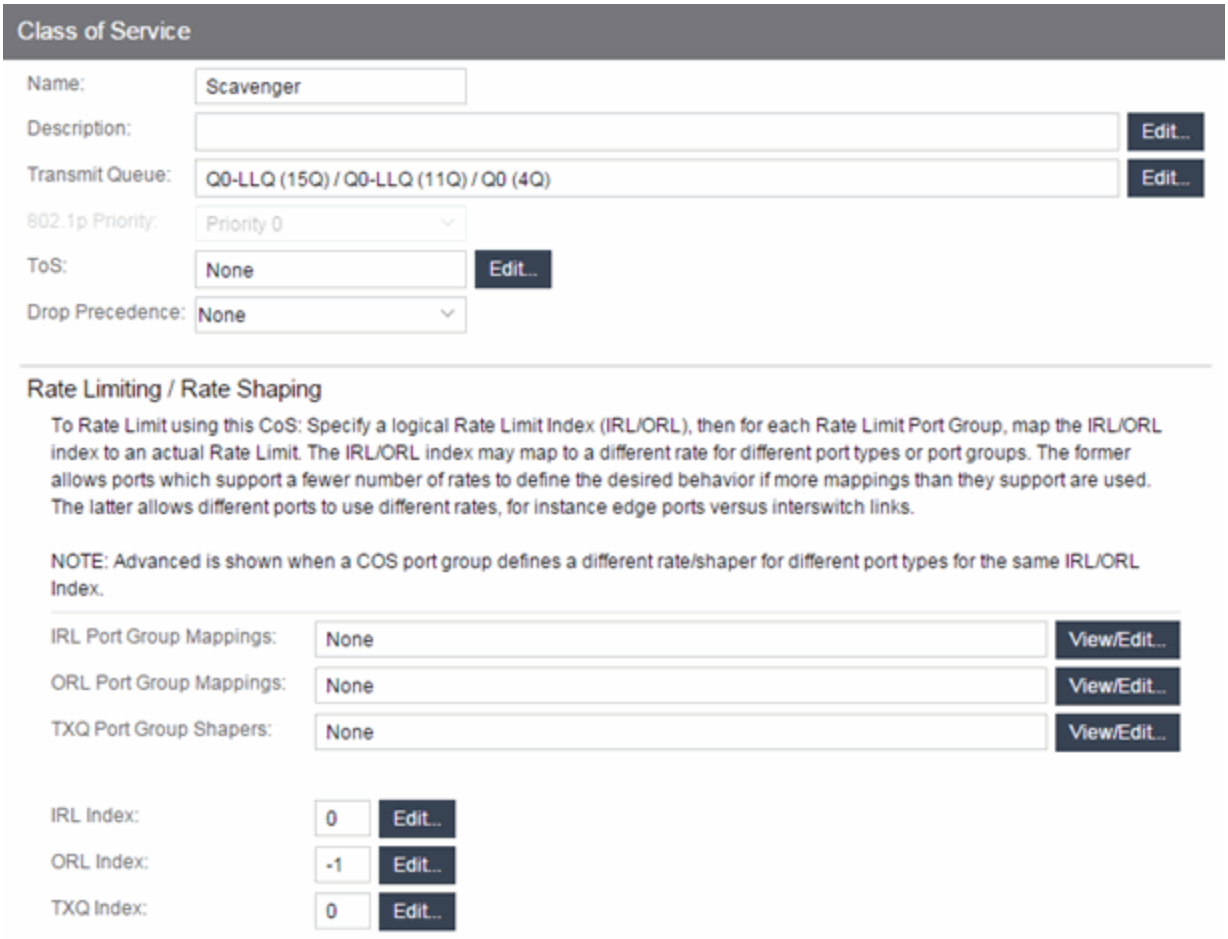
For instructions on how to configure flood controls, see How to Configure Flood Control.

Class of Service

This tab lets you view and configure the components of a class of service (CoS). See below for a description of each section. For more information, see How to Create a Class of Service.

Once you have created and defined a class of service, you can then apply it as a classification rule action, as part of the definition of an automated service, or as a role default. For more information, see Getting Started with Class of Service.

To access this tab, select the **Class of Service** left-panel tab on the **Policy** tab. Select a class of service in the tree, and the information for the selected class of service displays in the right panel.



General

Name

Name of the selected class of service.

Description

Use the **Edit** button to open a window where you can add or modify a description for the class of service.

Transmit Queue

This field displays the transmit queue associated with the class of service for each port type. Use the **Edit** button to display a menu where you can select a new transmit queue, if desired.

802.1p Priority

This drop-down list lets you select the 802.1p priority associated with the class of service, if desired. This field is grayed out for the eight static classes of service provided by the Policy tab (Priority 0-7), because the 802.1p priority cannot be disabled or changed.

ToS

Some IP rules enable a ToS value to be written to the ToS field in the IP header of incoming packets. Select the **Edit** button to open the Edit ToS window, where you can enter a ToS value. The value must be an 8-bit hexadecimal number between 0 and FF (see IP Type of Service for more information).

Drop Precedence

The Drop Precedence option is used in conjunction with the Flex-Edge feature available on K-Series and S-Series (Release 7.11 or higher) devices. Flex-Edge provides the unique capability to prioritize traffic in the MAC chip as it enters the switch. When the Class of Service is assigned to a policy role, and that role is applied to a port via a MAC source address mapping or the port default role, the drop precedence dictates the internal priority (within the MAC chip) used for packets received on the port. If congestion occurs, packets with a high drop precedence are discarded first. Therefore, if a packet is important, it should have a low drop precedence. Refer to the K-Series or S-Series Configuration Guide for more information on the Flex-Edge feature and drop precedence.

Rate Limiting/Rate Shaping

This section displays the inbound/outbound rate limits (IRL/ORL) and the outbound transmit queue (TxQ) rate shapers that are configured for the Default port groups associated with the class of service. If you have created additional port groups, the information displays for those groups as well.

With port rate limits, all traffic assigned to this class of service on a given port shares bandwidth specified by the rate limit. Rate shaping paces the rate at which traffic is transmitted out of the transmit queue. You can add or change a rate limit or a rate shaper by double-clicking on the area below a port group name.

If you have ExtremeWireless Controllers (Release 8.01.xx or higher) on your network, you also see the IRL and ORL user rate limits associated with the class of service. User rate limits specify the bandwidth given to each individual user on a port. Currently, user rate limits are only available on wireless controllers.

For more information, see Advanced Rate Limiting by Port Type and How to Configure Transmit Queues.

Index Numbers

At the bottom of the tab there is a section for configuring the rate limit and transmit queue index numbers associated with this class of service. These index numbers are used to map the class of service to the actual rate limits and transmit queue configuration on the device.

Typically, each class of service uses a different index number. The Policy tab automatically assigns these index numbers when you configure a class of services' rate limits and transmit queue shapers. An index number of "-1" indicates that no mappings are associated with the class of service.

All CoS using the same index will use the same rate limit and rate shaping assignments, and thus all traffic using those CoS will share the bandwidth.

IRL/ORL Index (Inbound/Outbound Rate Limits Index)

The inbound/outbound port rate limit index associated with the class of service. Index numbers map logical rate limit indexes to the actual physical rate limits you have created in the Policy tab. Select the button to open the Rate Limits selection view window, and select an index for the CoS. For convenience, existing index to rate limit mappings are displayed; if one of the existing indexes is selected, the displayed mappings will apply for this CoS. (Selecting an index highlights all the mappings configured for that index number within the selection view.)

TxQ Index (Transmit Queue Index)

The transmit queue index associated with the class of service. Index numbers map logical transmit queue indexes on the ports to the actual physical transmit queues you have configured in the **Policy** tab. If you have selected an 802.1p priority for this class of service, a default transmit queue index is automatically specified based on the selected priority. You can use the default index or change it according to your own transmit queue configuration. Select the button to open the Transmit Queues selection view window, which lists all the possible transmit queues, organized by index number for each existing port type and group. Selecting an index automatically includes all the transmit queues configured for that index number.

IUB/OUB Index (Inbound/Outbound User-Based Rates Index)

If you have ExtremeWireless Controllers (Release 8.01.xx or higher) on your network, you also see the inbound/outbound user rate limits associated with the class of service. User rate limits specify the bandwidth given to each individual user on a port. Currently, user rate limits are only available for these wireless controllers. Select the button to open the Rate Limits selection view window, and select an index for the CoS. For convenience, existing index to rate limit mappings are displayed; if one of the existing indexes is selected, the displayed mappings

apply for this CoS. (Selecting an index highlights all the mappings configured for that index number within the selection view.)

Flood Ctrl Port Groups

CoS-based flood control is a form of rate limiting that prevents configured ports from being disrupted by a traffic storm, by rate limiting specific types of packets through those ports. When flood control is enabled on a port, incoming traffic is monitored over one second intervals. During an interval, the incoming traffic rate for each configured traffic type (unknown-unicast, broadcast, or multicast) is compared with the configured traffic flood control rate, specified in packets per second. If, during a one second interval, the incoming traffic of a configured type reaches the traffic flood control rate configured on the port, CoS-based flood control drops the traffic until the interval ends. Packets are then permitted to flow again until the limit is again reached.

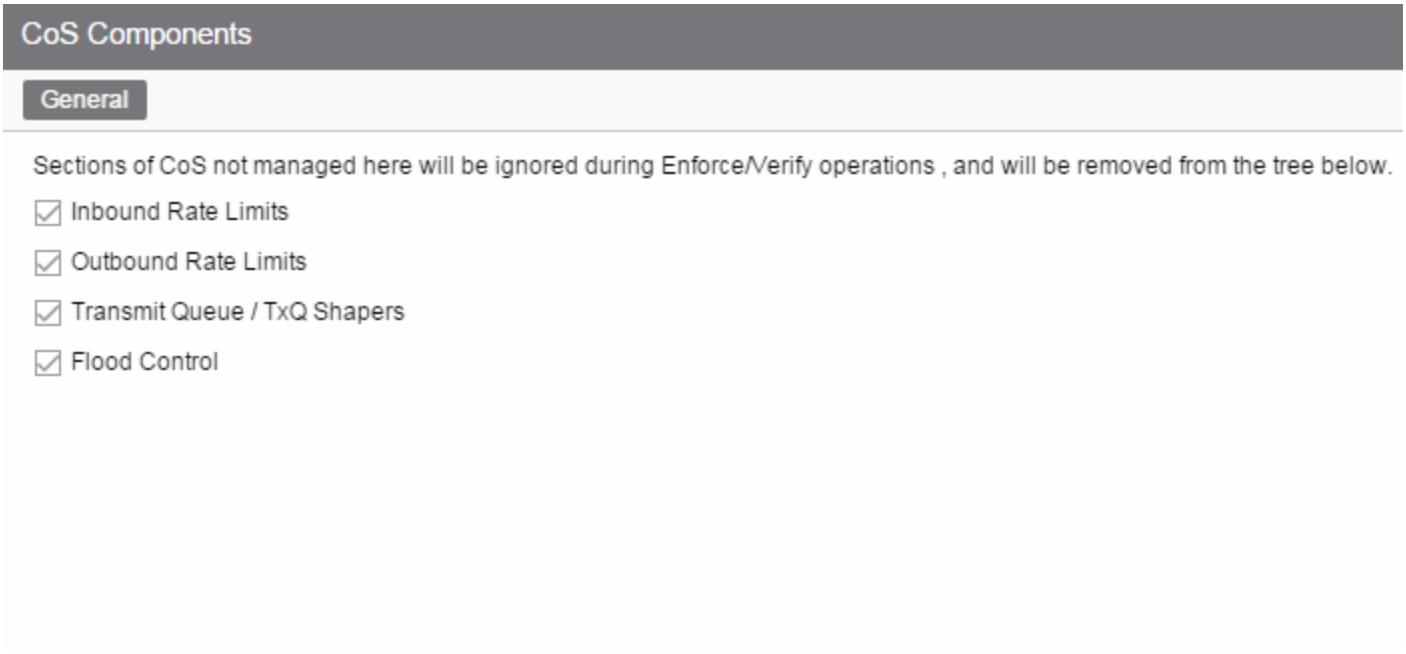
NOTE: By default, Flood Control is not managed by the **Policy** tab. To manage flood control configuration on devices in a domain, it can be enabled via the Domain Managed CoS Components drop-down list by selecting All CoS Components or by selecting Flood Control.



General (CoS Components Folder)

This tab lists the elements that comprise a class of service. It displays when you select the CoS Components tab in the Class of Service left-panel tab of the Policy tab.

See Getting Started with Class of Service for more information about these components.



Inbound Rate Limits
Select this checkbox to enable the **Inbound Rate Limit Port Groups tab** in the **CoS Components** left-panel tab.

Inbound Rate Limits
Select this checkbox to enable the **Outbound Rate Limit Port Groups tab** in the **CoS Components** left-panel tab.

Transmit Queue/TxQ Shapers
Select this checkbox to enable the **Transmit Queue Port Groups tab** in the **CoS Components** left-panel tab.

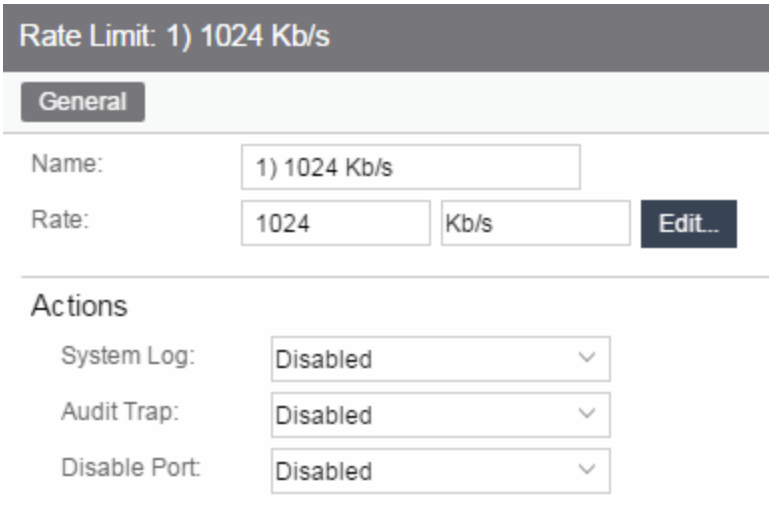
Flood Control Port Groups
Select this checkbox to enable the **Flood Control Port Groups tab** in the **CoS Components** left-panel tab.

General (Rate Limits)

This tab allows you to create and define a rate limit. Rate limits are components of a class of service and are used to control the transmit rate at which traffic enters and exits ports in your network.

To access this window, open the **Control** tab, select the **Policy** tab > **Class of Service** left-panel tab > **CoS Components** left-panel tab > **Rate Limits** tab. Select an existing rate limit to view or modify a rate limit or right-click the **Rate Limits** left-panel tab and select the **Create Rate Limit** option to create a new rate limit.

To create the rate limit, fill out the window and select **OK** (to create a single rate limit) or **Apply** (to create more rate limits). After you create the rate limit, the General tab for the new rate limit displays, where you can configure additional rate limit parameters.



Name

Specify the name of the rate limit.

Rate Limit

Select the **Edit** button to specify the highest transmission rate at which traffic can enter or exit a port before packets are rate limited:

- % - A percentage of the total bandwidth available (not available for priority-based rate limits)
- PPS - Packets per second (not available for priority-based rate limits)
- Kb/s - Kilobits per second
- Mb/s - Megabits per second
- Gb/s - Gigabits per second

Actions

Select the action(s) you would like this rate limit to use:

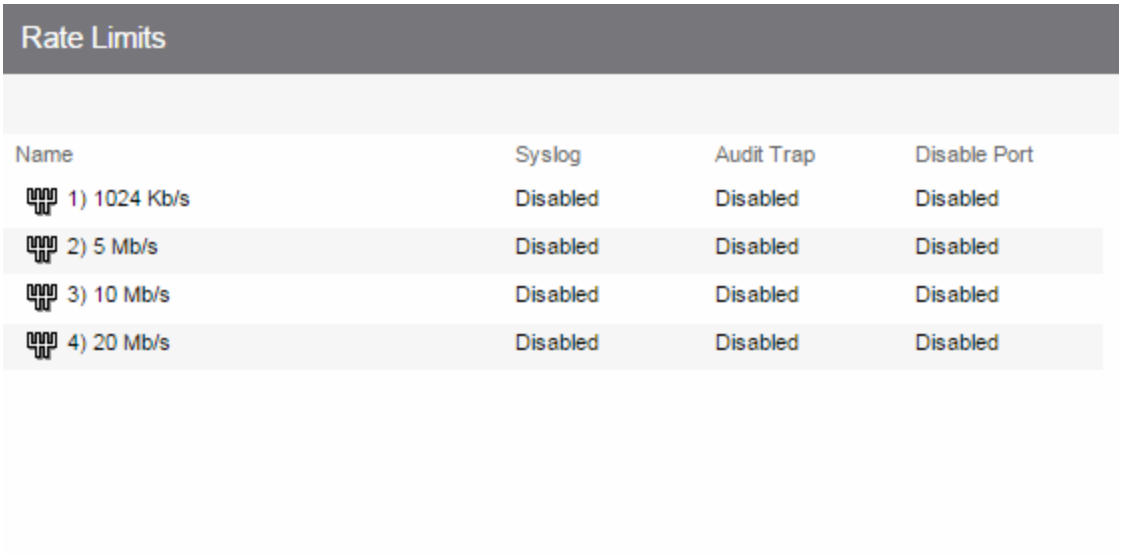
- System Log - a syslog message is generated when the rate limit is first exceeded.
- Audit Trap - an audit trap is generated when the rate limit is first exceeded.
- Disable Port - the port is disabled when the rate limit is first exceeded.

NOTE: N-Series Gold devices do not support rate limit notification.

Details View (Rate Limits Folder)

This tab lists information on any rate limits that have been defined in the **Policy** tab.

To access this tab, select the **Class of Service > CoS Components > Rate Limits** left-panel tab. See How to Define Rate Limits for more information.



Name
Name of the rate limit.

Syslog
Specifies whether a syslog message will be generated when the rate limit is first exceeded.

Audit Trap
Specifies whether an audit trap will be generated when the rate limit is first exceeded.

Disable Port
Specifies whether the port will be disabled when the rate limit is first exceeded.

Priority-Based Rate Limits

Priority-based rate limits are used primarily by legacy devices. They are rate limits that are associated with one or more of the eight 802.1p priorities (0-7). When the associated priority is selected for a class of service, the rate limit becomes part of that class of service.

These rate limits are written directly to each port (unless the port is specified in the rate limit's exclusion list), and are implemented based on the 802.1p priority assigned to a data packet appearing on that port. While priority-based rate limits are not tied directly to roles or rules, they are displayed with the associated priority when you select a class of service while creating a rule, automated service, or role.

When priority-based rate limiting is implemented, the combined rate of all traffic on the port that matches the priorities associated with the rate limit cannot exceed the configured limit. If the rate exceeds the configured limit, frames are dropped until the rate falls below the limit.

When a rate limit is associated with a priority, that priority includes rate limiting wherever and however it is used, until the rate limit is deleted from ExtremeCloud IQ Site Engine. Also, when a priority-based rate limit is applied to a port, it remains on the port even if the role that originally used the rate limit is no longer associated with the port. For example, if an untagged packet arrives on a port where there is no role or default priority, but the port's 802.1p priority includes a rate limit, that traffic is rate limited. As another example, if the priority of a tagged packet matches a priority-based rate limit on a port, the traffic is rate limited.

To configure a priority-based rate limit, you need to specify the following components:

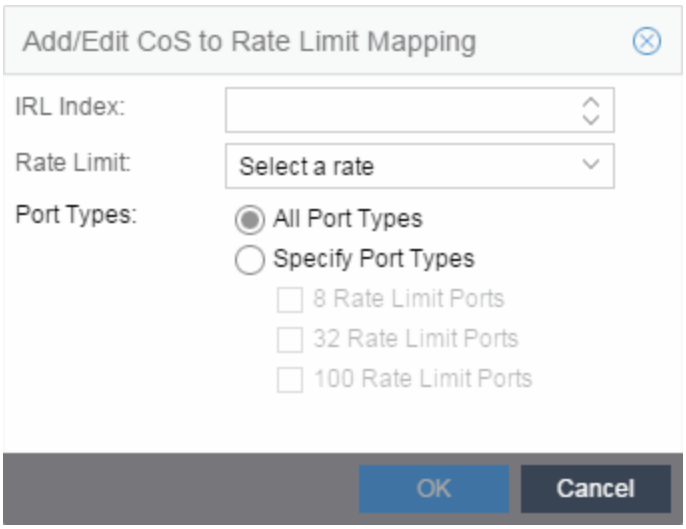
- *Rate Limit* - The highest transmission rate at which traffic can enter or exit a port.
- *Direction* - The direction to which the limit applies (inbound or outbound traffic). In order to control traffic inbound and outbound on the same port, two rate limits must be configured (one inbound and one outbound). Inbound rate limiting takes place after a frame is classified into one of the eight priorities. Outbound rate limiting takes place just before a frame is queued for transmission. A single frame can pass through inbound and outbound rate limits depending on the path it takes through the device and the rate limiting configuration on the device.
- *Priority* - The 802.1p priority or priorities with which the rate limit is associated.
- *Precedence* - The order in which the rate limit is written to supported devices. ExtremeCloud IQ Site Engine allows you to define as many rate limits as you wish; however, the number written to a device is restricted by the number of rate limits supported by the device. Each port on the device can utilize any or all of the defined rate limits up to the number of rate limits it supports.
- *Exclusion* - The devices/ports you wish to be excluded from the rate limit. For example, rate limiting is most often used for edge devices; therefore, you might want to exclude a device group or port group containing non-edge devices or ports.

Add/Edit CoS to Rate Limit Mapping

This window lets you configure the rate limit mappings for a rate limit port group. Rate limit mappings map a logical rate limit index to an actual physical rate limit you have created in ExtremeCloud IQ Site Engine.

For reference, the CoS IRL/ORL Index table (at the bottom of the window) displays classes of service that already have an IRL/ORL index specified, so that you can see which classes of service are affected by mapping an index to a rate limit.

To access this window, open the select the **Add/Edit** button on the **CoS – Rate Limit Mappings** tab (**Control** tab > **Policy** tab > **Class of Service** left-panel tab > **CoS Components** left-panel tab and select a port group in either the **Inbound Rate Limit Port Groups** or **Outbound Rate Limit Port Groups** left-panel tab, depending on the type of rate limit.



IRL/ORL Index

Specify the IRL (Inbound Rate Limit) or ORL (Outbound Rate Limit) Index you are mapping.

Rate Limit

Use the drop-down list to select a rate limit to map to the index. Rate limits are listed by the rate limit name followed by the precedence. For information on how to create a rate limit, see How to Define Rate Limits. Select **None** to remove an existing mapping for the specified port types.

Port Types

These options allow you to create a mapping for all port types, or create a mapping just for specific port types.

Advanced Rate Limiting by Port Type

The **Policy** tab class of service feature provides the ability to create rate limit port groups that let you group together ports with similar rate limiting requirements. For instructions on creating a port group, see Creating Class of Service Port Groups.

This Help topic provides information about an advanced port group feature that lets you specify different rate limits for the different port types contained in a port group: 8-rate limit, 32-rate limit, 64-rate limit, and 100-rate limit port types.

After you have created your port groups, you can use the CoS to rate limit mappings tab to configure rate limit index mappings for each group. These mappings map a logical rate limit index to an actual physical rate limit created in the Policy tab. For each class of service, you can select one mapping index that gives you the desired physical rate limit for each port group (see the Index Numbers section of the CoS General tab for more information on CoS Index Numbers).

The **Policy** tab supports a maximum of 100 logical rate limit indexes and each rate limit port group lets you map all 100 indexes. For 8-rate limit, 32-rate limit, and 64-rate limit ports, this means that the number of logical indexes might be greater than the actual number of rate limits the port supports. The port group can map 100 logical rate limit indexes, but they can only be mapped to a maximum of 8, 32, or 64 different physical rate limits on those ports.

For example, you want to have 25 rate limits for 25 different CoS. You need to define the behavior for the 8-rate port type, since when you get to the 9th rate, you would have no more resources available for the remaining rates (9-25). You would either need to share some of the same resources, or not rate limit with the remaining rates.

The maximum supported indexes for a device is based on the largest number of rates supported for that device. On devices supporting a maximum of 8 rate limits, indexes 0-7 are supported. On devices supporting a maximum of 32 rate limits, indexes 0-31 are supported. On devices supporting 64 rate limits, IRL indexes 0-63 are supported. If a rate limit port group maps indexes greater than the supported value, they are ignored during Enforce (indicated in the Class of Service > Rate Limit Mappings tables of Enforce Preview)

Instructions on:

- Configuring Rate Limit Mappings
- Associating Rate Limits with a Class of Service

Configuring Rate Limit Mappings

Use the following instructions configure rate limit mappings for a port group.

1. Open the **Class of Service > CoS Components** left-panel tab.
2. Select either the **Inbound Rate Limit Port Groups** or **Outbound Rate Limit Port Groups** left-panel tab.

3. Select the right-panel **CoS - Rate Limit Mappings** tab.
4. Select **Add/Edit** to open the Add/Edit CoS to Rate Limit Mappings window.
5. In the window, specify the IRL (Inbound Rate Limit) or ORL (Outbound Rate Limit) Index you are mapping.
6. Use the drop-down list to select a rate limit to map to the index.
7. The port type options enable you to create a mapping for all port types at one time, or create a mapping just for specific port types.
8. Select the **OK** button to map all your indexes and close the window. The Mappings tab displays your index to rate limit mapping configuration.

Associating Rate Limits with a Class of Service

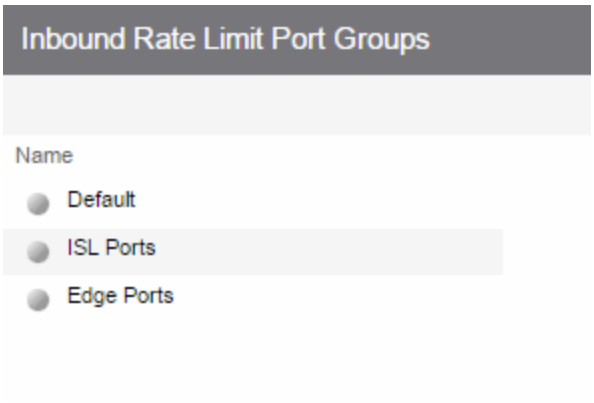
After you have configured the rate limit mappings for a port group, you can associate a rate limit mapping index with a class of service.

1. Open the **Class of Service** left-panel tab.
2. Select the CoS in the left-panel tree. (If you have not created the class of service, see How to Create a Class of Service.)
3. At the bottom of the **Class of Service** tab in the right panel, select the **Edit** button next to the IRL or ORL index that you want to configure. The Edit Index window opens.
4. This window lists all the currently mapped rate limits, organized by index number for each existing port type and group. Selecting one index number automatically includes all the rate limits configured for that index number. To configure new mappings for the CoS, you can first select an index that is not currently mapped, then create the mappings as described in Configuring Rate Limit Mappings above. Select **OK**.
5. After you have selected the mapping index, the table below displays the actual rate limits used by each rate limit port group for that class of service.
6. Select **Open/Manage Domains > Save Domain**.

Summary (Rate Limit Port Groups Folder)

This tab lists the name of all the inbound or outbound rate limit port groups (depending on the left-panel tab you select). Rate limit mappings map a logical rate limit index (IRL/ORL Index) to an actual physical rate limit. You can configure a port group's mappings on the port group **Mappings** tab.

To access this tab, open the **Class of Service > CoS Components** left-panel tab, then, select either the **Inbound Rate Limit Port Groups** left-panel tab or the **Outbound Rate Limit Port Groups** tab. The Summary tab displays in the right panel.



Name

The name of the port group.

CoS - Rate Limit Mappings (Rate Limit Port Group)

This tab lets you view and configure the rate limit mappings for a rate limit port group. Rate limit mappings map a logical rate limit index used by classes of service to an actual physical rate limit you create in ExtremeCloud IQ Site Engine.

Each port group has its own set of index mappings. ExtremeCloud IQ Site Engine automatically assigns these index numbers when you configure a class of services' rate limits and transmit queue shapers.

The rate limit mappings tab allows you to do two things:

- Map the index to a different rate for different port groups (edge ports versus inter-switch links). See Creating Class of Service Port Groups.
- Map the index to a different rate limit for each port type (8-rate limit, 32-rate limit, 64-rate limit, and 100-rate limit) in a port group. See Advanced Rate Limiting by Port Type.

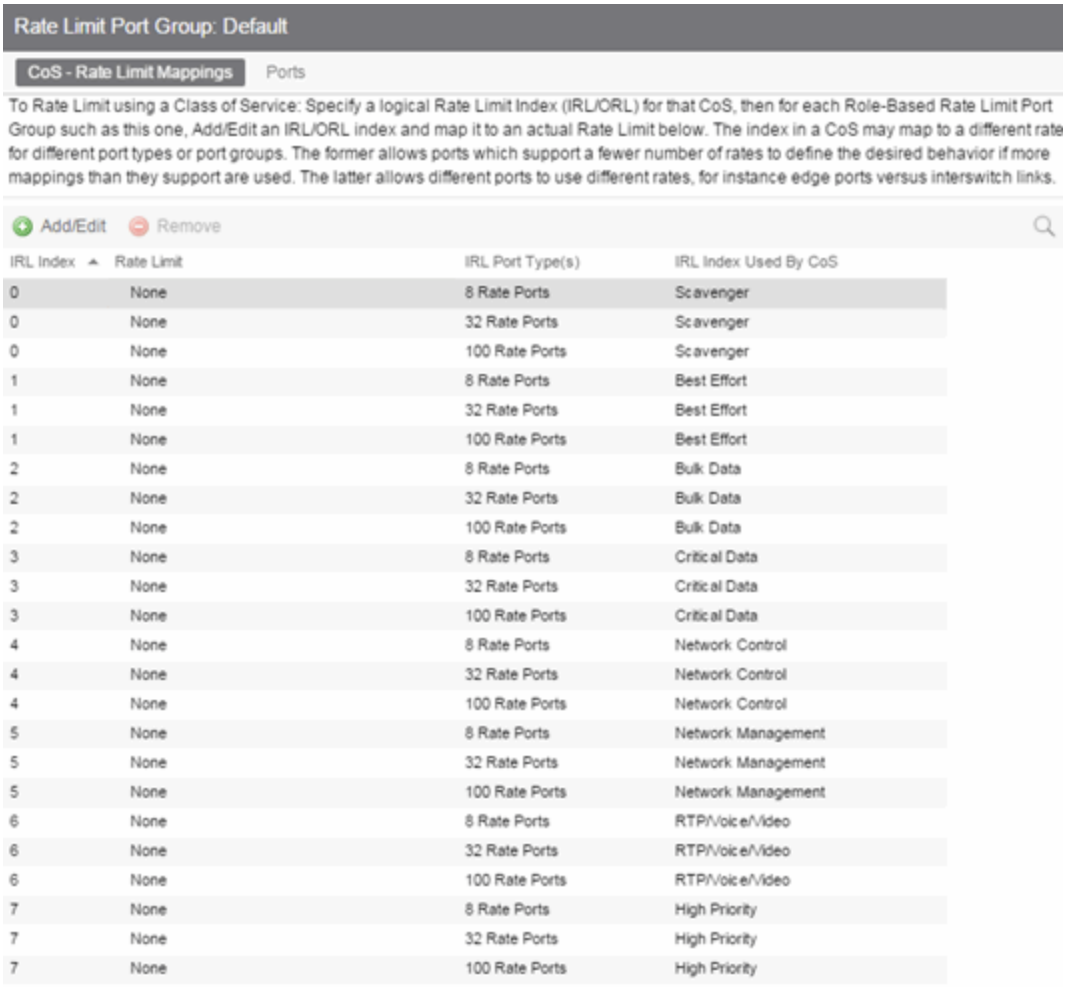
To access this tab:

1. Open the **Control** tab.
2. Open the **Policy** tab.
3. Open the **Class of Service** > **CoS Components** left-panel tab.
4. Select either the **Inbound Rate Limit Port Groups** or **Outbound Rate Limit Port Groups** left-panel tab, depending on whether the rate limit is inbound or outbound.

5. Select a existing port group in the left panel to open it in the **Rate Limit Port Group** tab.

   NOTE: Create a new port group by right-clicking the **Inbound Rate Limit Port Groups** or **Outbound Rate Limit Port Groups** left-panel tab, selecting **Create Port Group**, entering a **Name** for the port group, and selecting **OK**.

6. Select the **CoS - Rate Limit Mappings** tab in the right panel.



IRL/ORL Index

The logical inbound rate limit (IRL) or outbound rate limit (ORL) index number. This index number is specified in a class of service and dictates the rate limiting behavior for incoming or outgoing packets. For each rate limit port group, use this tab to map the index number to an actual rate limit.

Rate Limit

The actual rate limit to which the IRL/ORL index is mapped.

IRL/ORL Port Type(s)
The type of ports included in the port group. Port type is based on the number of rate limits the ports support (for example, 8-rate limit ports and 32-rate limit ports).

IRL/ORL Index Used By CoS
The classes of service using this IRL/ORL index.

Add/Edit Button
Opens the Add/Edit CoS to Rate Limit Mappings window where you can add or edit rate limit mappings for the rate limit port group

Remove Button
Removes the mapping(s) selected in the table.

Ports (Rate Limit Port Group)

The rate limit port group **Ports** tab lets you view all the ports in the selected port group, as well as add and remove ports to and from the group. It provides information about each port, and lets you view and edit port information (via the port's **General** tab).

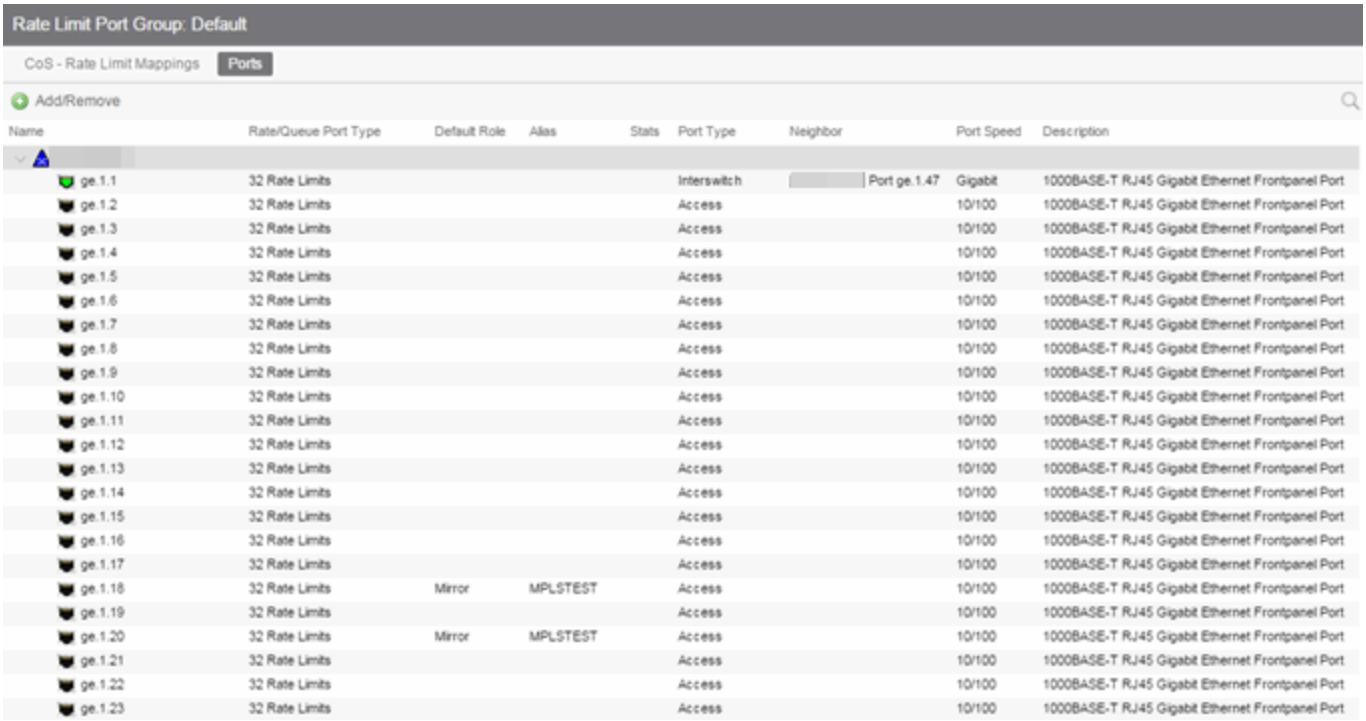
To access this tab:

1. Open the **Control** tab.
2. Open the **Policy** tab.
3. Open the **Class of Service** > **CoS Components** left-panel tab.
4. Select either the **Inbound Rate Limit Port Groups** or **Outbound Rate Limit Port Groups** left-panel tab, depending on whether the rate limit is inbound or outbound.
5. Select a existing port group in the left panel to open it in the **Rate Limit Port Group** tab.

   NOTE: Create a new port group by right-clicking the **Inbound Rate Limit Port Groups** or **Outbound Rate Limit Port Groups** left-panel tab, selecting **Create Port Group**, entering a **Name** for the port group, and selecting **OK**.

6. Select the **Ports** tab in the right panel.

Create a new port group by right-clicking the **Inbound Rate Limit Port Groups** or **Outbound Rate Limit Port Groups** left-panel tab, selecting **Create Port Group**, entering a **Name** for the port group, and selecting **OK**.



Name	Rate/Queue Port Type	Default Role	Alias	Stats	Port Type	Neighbor	Port Speed	Description
ge.1.1	32 Rate Limits				Interswitch	Port ge.1.47	Gigabit	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.2	32 Rate Limits				Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.3	32 Rate Limits				Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.4	32 Rate Limits				Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.5	32 Rate Limits				Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.6	32 Rate Limits				Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.7	32 Rate Limits				Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.8	32 Rate Limits				Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.9	32 Rate Limits				Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.10	32 Rate Limits				Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.11	32 Rate Limits				Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.12	32 Rate Limits				Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.13	32 Rate Limits				Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.14	32 Rate Limits				Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.15	32 Rate Limits				Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.16	32 Rate Limits				Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.17	32 Rate Limits				Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.18	32 Rate Limits	Mirror	MPLSTEST		Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.19	32 Rate Limits				Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.20	32 Rate Limits	Mirror	MPLSTEST		Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.21	32 Rate Limits				Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.22	32 Rate Limits				Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port
ge.1.23	32 Rate Limits				Access		10/100	1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port

Name

Name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

Rate/Queue Port Type

The number of rate limits the port supports.

Default Role

The Default Role assigned to the port.

Alias

Shows the alias (ifAlias) for the interface, if one is assigned.

Stats

Shows statistics collected for a port, enabled via the Flow Collection & Interface setting in the PortView.

Port Type

Type of port. Possible values include: Access, Interswitch Backplane, Backplane, Interswitch, and Logical.

Neighbor

The port's neighbor port.

Port Speed

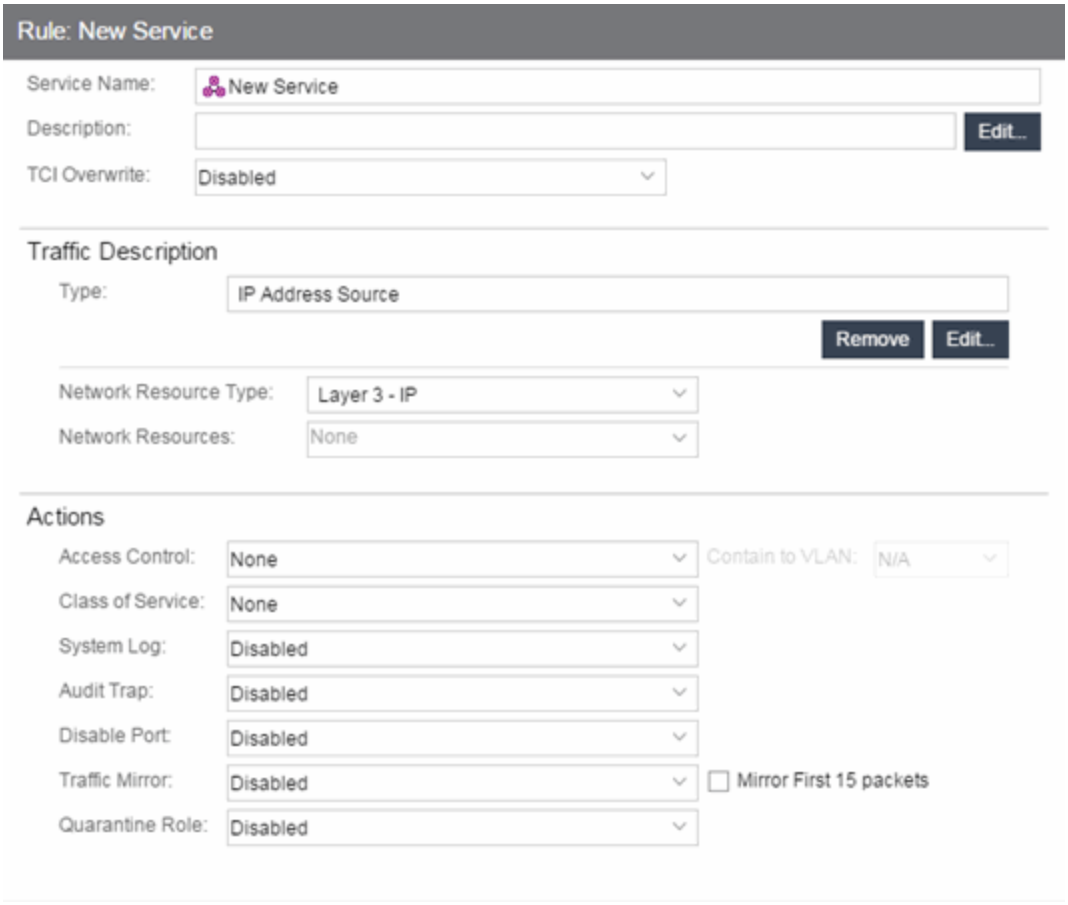
Speed of the port. Possible values include: 10/100, speed in megabits per second (for example, 800.0 Mbps), Unknown (displayed for logical ports).

Description
A description of the port.

Add/Remove Ports Button
Opens the Add/Remove Ports window, where you can add and remove ports to and from the port group. When you create new port groups, you add ports from the Default group into your newly defined port groups.

Automated Service

Selecting an Automated Service opens the **Automated Service** tab which enables you to define settings for the service. For more information on services, see How to Create a Service.



Service Name
Name of the selected service.

Description
: Use the **Edit** button to open a window where you can enter or modify a description of the service.

TCI Overwrite
: Specify the TCI Overwrite functionality for the service:

- **Enabled** - Enabling TCI Overwrite enables the VLAN (access control) and class of service characteristics defined in this service to overwrite the VLAN or class of service (CoS) tag in a received packet, if that packet has already been tagged with VLAN or CoS information.
- **Disabled** - If this option is disabled the TCI Overwrite option is ignored, but lower-precedence rules and the role default actions can still specify TCI Overwrite for the data packet if there is a match.
- **Prohibited** - Do not set TCI Overwrite for this data packet, even when a lower-precedence rule or the role default actions has the TCI Overwrite option set to enabled.

Traffic Description Area

Use this area to provide the specifications for an automated service. Specify the network resource type, the network resources for the service, and the rule type. Some rule types require that you enter certain parameters and/or values. This section is not displayed for a Manual service.

Type
: Select the **Edit** button to select the type of rule you want to create for the network resources. Some rule types require you enter certain parameters and/or values. See Classification Types and their Parameters for parameter information. Select and/or enter the required parameters.

Network Resource Type
: Select the network resource type (Layer 2 MAC or Layer 3 IP). This will determine the list of network resources available for selection for this service.

Network Resources
: Use the drop-down list to select the network resources to associate with the automated service. Use the configuration menu button to the right of the list to add a network resource or view and edit your network resources. For more information, see How to Create a Network Resource.

Actions Area

Use this area to define the access control and/or a class of service for the Automated service rule. This section is not displayed for a Manual service.

Access Control
: Use this drop-down list to select the appropriate access control for the rule. You can permit traffic to be forwarded, deny traffic altogether, or contain traffic to a VLAN. Select **None** to

disable access control for this rule.

- **Permit Traffic** - enables traffic to be forwarded with the port's assigned VID.
- **Deny Traffic** - traffic will be automatically discarded.
- **Contain to VLAN** - contains traffic to a specific VLAN. Use the drop-down list to select the desired VLAN. Use the **Contain to VLAN** drop-down list to select a VLAN.

Class of Service

Use the drop-down list to select a class of service to associate with the service. The Policy tab lets you define classes of service that each include an 802.1p priority, and optionally an IP type of service (ToS/DSCP) value, rate limits, and transmit queue configuration. You can then assign a class of service as a classification rule action. See Getting Started with Class of Service and How to Create a Class of Service for more information. Select **None** to disable class of service for this rule. Use the configuration menu button to the right of the drop-down list to add or edit a Class of Service.

When rule accounting is enabled on a device, each rule keeps a list of the ports on which it has been used. The next three options enable you to specify certain rule usage actions to take place when a "rule hit" is reported.

System Log

Specify System Log functionality for the rule:

- **Enabled** - If this option is enabled, a syslog message is generated when the rule is used. This option must be enabled if you are configuring Policy Rule Hit Reporting on your devices.
- **Disabled** - If this option is disabled and this rule is hit, it does not generate a Syslog message, but lower-precedence rules and the role default actions can still specify a syslog message be sent for this data packet if there is a match.
- **Prohibited** - If this rule is hit, no syslog message is generated for this data packet, even when a lower-precedence rule or the role default actions has the System Log action set to enabled.

Audit Trap

Specify Audit Trap functionality for the rule:

- **Enabled** - If this option is enabled, an audit trap is generated when the rule is used.
- **Disabled** - If this option is disabled and this rule is hit, it does not generate an audit trap, but lower-precedence rules and the role default actions can still specify generating an audit trap for this data packet if there is a match.
- **Prohibited** - If this rule is hit, no audit trap is generated for this data packet, even when a lower-precedence rule or the role default actions has the Audit Trap action set to enabled.

Disable Port

Specify Disable Port functionality for the rule:

- **Enabled** - If this option is enabled, any port reported as using this rule is disabled. Ports that have been disabled due to this option are displayed in the device Role/Rule tab.
- **Disabled** - If this option is disabled and this rule is hit, it does not disable the port, but lower-precedence rules and the role default actions can still specify disabling the port for this data packet if there is a match.
- **Prohibited** - If this rule is hit, the port is not disabled, even when a lower-precedence rule or the role default actions has the Disable Port action set to enabled.

Traffic Mirror

Specify traffic mirroring functionality for the rule:

- **Select port group(s)** - Use the drop-down list to select the port groups where mirrored traffic will be sent for monitoring and analysis. Use the configuration menu button to the right of the drop-down list and select View/Modify Port Groups to open the Port Groups tab where you can define user-defined port groups for selection.
- **Disabled** - If this option is disabled and this rule is hit, traffic mirroring will not take place, but lower-precedence rules and the role default actions can still specify traffic mirroring for this data packet if there is a match.
- **Prohibited** - If this rule is hit, traffic mirroring is disabled, even when a lower-precedence rule or the role default actions has the Traffic Mirror action specified.

Quarantine Role

Specify Quarantine role functionality for the rule:

- **Enabled** - If this option is enabled, any role reported as using this rule is quarantined.
- **Disabled** - If this option is disabled and this rule is hit, it does not quarantine the role, but lower-precedence rules and the role default actions can still specify quarantining the role for this data packet if there is a match.
- **Prohibited** - If this rule is hit, the role is not quarantined, even when a lower-precedence rule or the role default actions has the Quarantine Role action set to enabled.

Traffic Classification Rules

Traffic Classification rules allow you to assign VLAN membership and/or class of service to your network traffic based on the traffic's classification type. Classification types are derived from Layers 2, 3, 4, and 7 of the OSI model, and all network traffic can be classified according to specific layer 2/3/4/7 information contained in each frame. In the Policy tab, rules are used to provide four key policy features: traffic containment, traffic filtering, traffic security, and traffic prioritization. Examples of how to design rules for each of these features are given below.

A Traffic Classification rule has two main parts: Traffic Description and Actions. The Traffic Description identifies the traffic classification type for the rule. The Actions specify whether traffic matching that classification type will be assigned VLAN membership, class of service, or both. When a frame arrives on a port, the switch checks to see if the frame's classification type matches the type specified in a rule. If it does, then the actions defined in that rule will apply to the frame.

In the **Policy** tab, rules are created and then grouped together into Services, which are then used to define roles. A role is assigned to each port either through end user authentication or as the port's default role. This means that there can be multiple rules active on a port. When a frame is received on a port, if the frame's classification type matches more than one rule, classification precedence rules are used to determine which rule to use.

NOTE: Rules included in services are read in the order in which they are listed in ExtremeCloud IQ Site Engine. To configure rules for ExtremeCloud IQ Controller (formally called XCC or XCA) devices, ensure ExtremeCloud IQ Site Engine lists the rules in the correct order or the service may not execute the correct rule. To reorder rules in the same service, use drag-and-drop capabilities to move from one group to another.

The following information is discussed in this file:

- Traffic Descriptions
- Actions
  - VLAN Membership
  - Priority (Class of Service)
- Classification Types and their Parameters
  - Layer 2 Data Link Classification Types
  - Layer 3 Network Classification Types
  - Layer 4 Application Transport Classification Types
  - Layer 7 Application Classification Type
- Examples of How Rules are Used
  - Traffic Containment
  - Traffic Filtering
  - Traffic Security
  - Traffic Prioritization

Traffic Descriptions

When you create a Traffic Classification rule in the **Policy** tab, you must define the rule's traffic description. The traffic description identifies the traffic classification type for that rule. You must select

a classification type, and then select or enter certain parameters or values for each type.

Classification types are grouped according to Layers 2, 3, 4, and 7 of the OSI model and there are multiple classification types for each layer.

OSI Model
Layer 7 - Application
Layer 6 - Presentation
Layer 5 - Session
Layer 4 - Transport
Layer 3 - Network
Layer 2 - Data Link
Layer 1 - Physical

Specific Layer 2/3/4/7 information contained in each frame is used to identify the frame's classification type. Each layer uses different information to classify frames.

- **Layer 2 Data Link** -- classifies frames based on an exact match of the MAC address or specific protocol type of each frame.
- **Layer 3 Network** -- classifies IP or IPX frames based on specific information contained within the Layer 3 header.
- **Layer 4 Transport** -- classifies IP frames based on specific Layer 4 TCP or UDP port numbers contained in the header.
- **Layer 7 Application** -- classifies frames based on specific Layer 7 application types.

For a complete description of Layer 2, 3, 4, and 7 classifications, refer to Classification Types and Their Parameters.

Actions

When you create a Traffic Classification rule in the **Policy** tab, you must define the actions the rule performs. When a frame arrives on a port, the switch checks to see if the frame's classification type matches the type specified in a rule. If it does, then the actions defined in that rule will apply to the frame. Actions specify whether the frame will be assigned VLAN membership (access control) and/or priority (class of service).

VLAN Membership (Access Control)

In your network domains, you can create VLANs (Virtual Local Area Networks) that allow end-systems connected to separate ports to send and receive traffic as though they were all connected to the same network segment. Using traffic classification rules, you can classify a frame based on the frame's

classification type to have membership in a specific VLAN, providing important traffic containment, filtering, and security for your network.

For example, a network administrator could use rules to separate end user traffic into VLANs according to protocol, subnet, or application. Rules could also be used to group geographically separate end-systems into job-specific workgroups.

Priority (Class of Service)

Traffic Classification rules allow you to assign a transmission priority to frames received on a port based on the frame's classification type. For example, a network administrator could use rules to assign priority to one network application over another.

Priority is a value between 0 and 7 assigned to each frame as it is received on a port, with 7 being the highest priority. Frames assigned a higher priority will be transmitted before frames with a lower priority. Each of the priorities is mapped into a specific transmit queue by the switch or router. The insertion of the priority value (0-7) allows all 802.1Q devices in the network to make intelligent forwarding decisions based on its own level of support for prioritization.

The **Policy** tab enables you to utilize priority by creating classes of service that each include an 802.1p priority, and optionally an IP type of service (ToS/DSCP) value, rate limits, and transmit queue configuration. You can then assign the class of service as a classification rule action, as part of the definition of an automated service, or as a role default. See Getting Started with Class of Service for more information.

Classification Types and their Parameters

When you define a rule's traffic description, you select a classification type, and then select or enter certain parameters or values for each type. Classification types are grouped according to Layers 2, 3, 4, or 7 of the OSI model.

Layer 2 -- Data Link Classification Types

Layer 2 classification types allow you to define classification rules based on an exact match of the MAC address or specific protocol type of each frame.

MAC Address Source, MAC Address Destination, MAC Address Bilateral

These classification types are based on an exact match of the source, destination, or bilateral (either source or destination) MAC address contained in an Ethernet frame. Enter a valid MAC address or select Select to open a window where you can select a MAC address read from your network devices. You can specify a mask, however masking a MAC address is not supported on legacy devices.

Ethertype

This classification type is based on the specific protocol type of each frame defined in the two-byte Ethertype field. Select an Ethertype from the list of well-known values, or select

Other and manually enter a single value in hexadecimal form. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

Well-known Ethertypes	Values
IP	0x0800
ARP	0x0806
Reverse ARP	0x8035
Novell IPX 1	0x8137
Novell IPX 2	0x8138
Banyan	0x0bad
AppleTalk	0x809b
AppleTalk ARP	0x80f3
IPv6	0x86dd
Decnet Phase 4	0x6003

DSAP/SSAP

This classification type is based on the specific protocol type of each frame defined in the DSAP and SSAP fields. Select a protocol from the list of well-known values, or select **Other** and manually enter a custom two-byte value in hexadecimal format (0xFFFF). The LSB of the DSAP address specifies Individual(0) or Group(1), while the LSB of the SSAP address specifies Command(0) or Response(1). For the SNAP frame type, you may enter Advanced DSAP/SSAP configurations. The advanced fields are not supported on legacy devices and are ignored.

Well-known DSAP/SSAP Types	Values
IP	0x0606
IPX	0xe0e0
NetBIOS	0xf0f0
Banyan Vines	0xbcbc
SNA	0x0404
SNAP	0xAAAA
Other	a two-byte value

VLAN ID

This classification type is based on an exact match of the VLAN tag contained within a frame. Select a VLAN ID (VID) from the list of VLANs defined in the Policy tab. If you select **Other**, you must enter a single VID or specify a range of VIDs in decimal form. Range rules are not supported on legacy devices.

Priority

This classification type is based on an exact match of the Priority tag contained within a frame. Select a Priority value 0 - 7 from the list of well-known values, or select **Other** and enter a value in decimal form.

Layer 3 -- Network Classification Types

Layer 3 Network classification types allow you to define classification rules based on specific information contained within the Layer 3 header of an IP or IPX frame.

IP Time to Live (TTL)

This classification type is based on an exact match of the TTL field contained in the IP header of a frame. The TTL field indicates the maximum number of router hops the packet can make before being discarded. The TTL field is set by the packet sender and reduced by every router on the route to its destination. If the TTL field reaches zero before the packet arrives at its destination, then the packet is discarded. IP Time to Live rules are only supported on K-Series and S-Series devices.

IPX Network Source, IPX Network Destination, IPX Network Bilateral

These classification types are based on specific information contained within the Layer 3 header of an IPX frame. It is a four-byte user-defined value that represents the IPX source, destination, or bilateral (either source or destination) network number. This value must be a valid IPX network address in hexadecimal form. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

IPX Socket Source, IPX Socket Destination, IPX Socket Bilateral

These classification types are based on specific information contained within the Layer 3 header of an IPX frame. It is a two-byte, user-defined value that represents the IPX source, destination, or bilateral (either source or destination) socket numbers. This value is used by higher layer protocols to target specific applications running among hosts. Select an IPX Socket type from the list of well-known values, or select **Other** and manually enter the value in decimal form. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

Well-known IPX Socket Types	Values
NCP	1105
SAP	1106
RIP	1107
NetBIOS	1109
Diagnostics	1110
NSLP	36865
IPX Wan	56868
Other	0-65535

IPX Class of Service

This classification type is based on specific information contained within the Layer 3 header of an IPX frame. This is a one-byte field used for transmission control (hop count) by IPX routers. Enter a valid IPX Class of Service in decimal form, 0-255. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

IPX Packet Type

This classification type is based on specific information contained within the Layer 3 header of an IPX frame. Select an IPX Packet type from the list of well-known values or select **Other** and manually enter the value in decimal form. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

Well-known IPX Packet Types	Values
Hello/SAP	0
RIP	1
Echo Packet	2
Error Packet	3
NetWare 386	4
SeqPackProt	5
NetWare 286	17
Other	0-31

IPv6 Address Source, IPv6 Address Destination, IPv6 Address Bilateral

These classification types are based on an exact match of the source, destination, or bilateral (either source or destination) IPv6 address information contained within the IPv6 header of each frame. Enter a valid IPv6 address and optional mask ("/n") in the Value field.

IPv6 Socket Source, IPv6 Socket Destination, IPv6 Socket Bilateral

These classification types are based on an exact match of a specific source, destination, or bilateral (either source or destination) IPv6 address and a UDP/TCP port number (type) contained within the IPv6 header of each frame. Enter an IPv6 address in the Value field. Then, select a UDP/TCP type from the list of well-known values, or select **Other** and manually enter the value in
form. (UDP/TCP port numbers are defined in RFC 1700.) If you select **Other**, you can enter a range of values.

Well-known UDP/TCP Types	Values
FTP Data	20
FTP	21

Well-known UDP/TCP Types	Values
SSH	22
Telnet	23
SMTP	25
TACACS	49
DNS	53
BootP Server	67
BootP Client	68
TFTP	69
Finger	79
HTTP	80
POP3	110
Portmapper	111
NNTP	119
NTP	123
NetBIOS Name Service	137
NetBIOS Datagram Service	138
NetBIOS Session Service	139
IMAP2/IMAP4	143
SNMP	161
IMAP3	220
LDAP	389
HTTPS	443
R-Exec	512
R-Login	513
R-Shell	514
LPR	515
RIP	520
SOCKS	1080
Citrix ICA	1494
RADIUS	1812
RADIUS Accounting	1813

Well-known UDP/TCP Types	Values
NFS	2049
X11 (Range Start)	6000
X11 (Range End)	6063
Other	0-65535

IPv6 Flow Label

These classification types are based on the exact match of the value in the 20-bit Flow Label field in the IPv6 header. This field is used to identify packets belonging to particular traffic flow that needs special traffic handling. Enter a flow label value and sigbits mask.

IP Address Source, IP Address Destination, IP Address Bilateral

These classification types are based on an exact match of the source, destination, or bilateral (either source or destination) IP address information contained within the IP header of each frame. Enter a valid IP address and optional mask ("/n") in the Value field.

IP Socket Source, IP Socket Destination, IP Socket Bilateral

These classification types are based on an exact match of a specific source, destination, or bilateral (either source or destination) IP address and a UDP/TCP port number (type) contained within the IP header of each frame. Enter an IP address in the Value field. Then, select a UDP/TCP type from the list of well-known values, or select **Other** and manually enter the value in decimal form. (UDP/TCP port numbers are defined in RFC 1700.) If you select **Other**, you can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

Well-known UDP/TCP Types	Values
FTP Data	20
FTP	21
SSH	22
Telnet	23
SMTP	25
TACACS	49
DNS	53
BootP Server	67
BootP Client	68
TFTP	69
Finger	79

Well-known UDP/TCP Types	Values
HTTP	80
POP3	110
Portmapper	111
NNTP	119
NTP	123
NetBIOS Name Service	137
NetBIOS Datagram Service	138
NetBIOS Session Service	139
IMAP2/IMAP4	143
SNMP	161
IMAP3	220
LDAP	389
HTTPS	443
R-Exec	512
R-Login	513
R-Shell	514
LPR	515
RIP	520
SOCKS	1080
Citrix ICA	1494
RADIUS	1812
RADIUS Accounting	1813
NFS	2049
X11 (Range Start)	6000
X11 (Range End)	6063
Other	0-65535

IP Fragment

This classification type is based on Layer 4 information in fragmented frames. IP supports frame fragmentation, where large frames are divided into smaller fragments and sent wrapped in the original Layer 3 (IP) header. When a frame is fragmented, information that is Layer 4 and above is only present in the first fragment. For example, the first fragment may be classified to Layer 4, while subsequent fragments will be classified only to Layer 3. The product line does not support Layer 4 classification for IP frames that have been fragmented, as the Layer 4

information is not present in these frames. Using the IP Fragment classification rule, any frame which is a fragment of a larger frame, is classified according to the information in the original frame. If the first fragment is classified to Layer 4, subsequent fragments will also be classified to Layer 4.

ICMP and ICMPv6

These classification types are based on an exact match of the ICMP (Internet Control Message Protocol) message contained in the ICMP tag within a frame. Select an ICMP well-known value type from the list of well-known values (some well-known value types also let you select a code), or select **Other** and manually enter the value in hexadecimal form. The format of the value is 0xXXYY, where "XX" is the ICMP type, and "YY" is the associated code, if applicable. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

IP Type of Service

This classification type is based on an exact match of the one-byte ToS/DSCP field contained in the IP header of a frame. The ToS (Type of Service) or DSCP (Diffserve Codepoint) value is defined by an 8-bit hexadecimal number between 0 and FF. Enter a value or select Select to open a window where you can generate a hex value.

Type of Service can be used by applications to indicate priority and Quality of Service for each frame. The level of service is determined by a set of service parameters which provide a three way trade-off between low-delay, high-reliability, and high-throughput. The use of service parameters may increase the cost of service. In many networks, better performance for one of these parameters is coupled with worse performance on another. Except for very unusual cases, at most, two of the parameters should be set.

For a ToS value, the 8-bit hexadecimal number breaks down as follows:

Bits 0-2: Precedence
Bit 3: 0=Normal Delay, 1=Low Delay
Bit 4: 0=Normal Throughput, 1=High Throughput
Bit 5: 0=Normal Reliability, 1=High Reliability
Bits 6-7: Explicit Congestion Notification

The precedence bits (bits 0-2) break down as follows:

111 - Network Control
110 - Internetwork Control
101 - CRITIC/ECP
100 - Flash Override
011 - Flash
010 - Immediate
001 - Priority
000 - Routine

The Network Control precedence designation is intended to be used within a network only. The actual use and control of that designation is up to each network. The Internetwork Control designation is intended for use by gateway originators only.

For a DSCP value, the value represents codepoints for two Differentiated Services (DS) Per-Hop-Behavior (PHB) groups called Expedited Forwarding (EF) and Assured Forwarding (AF). For more information on these PHB groups, refer to RFC 2597 and RFC 2598.

IP Protocol Type

This classification type is based on the specific protocol type defined in a field contained in the IP header of each frame. Select a protocol from the list of well-known values, or select **Other** and manually enter the value in decimal form. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

Well-known IP Protocol Types	Values
ICMP	1
IGMP	2
TCP	6
EGP	8
UDP	17
IPv6 (encapsulated in IPv4 packets)	41
RSVP	46
GRE	47
ESP	50
AH	51
ICMPv6	58
EIGRP	88
OSPF	89
PIM	103
VRRP	112
L2TP	115
Other	0-255

Layer 4 -- Application Transport Classification Types

Layer 4 IP classification types allow you to define classification rules based on specific Layer 4 TCP or UDP port numbers contained in the header of an IP frame. You can specify a specific port number, a range of port numbers, or a range of port numbers.

Note: Certain devices do not support Layer 4 classification for IP frames that have been fragmented, as the Layer 4 information is not present in these frames. If a device has an FDDI HSIM installed, Layer 4 classification will not be supported for any frames larger than 1500 bytes. Frames larger than 1500 bytes are fragmented internally in the switch. When creating classification rules based on specific Layer 4 information, using the IP Fragment classification rule will allow fragmented frames to be classified according to the Layer 4 information contained in the original frame.

IP UDP Port Source, IP UDP Port Destination, IP UDP Port Bilateral

These classification types are based on specific Layer 4 UDP port numbers contained within the header of an IP frame. Select a UDP type from the list of well-known values, or select **Other** and manually enter the value in decimal form. (UDP port numbers are defined in RFC 1700.) You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold. Enter a valid IPv4 or IPv6 address and optional mask ("/n"), if desired. The IP address is an optional field and does not have to be specified. It is only valid for non-range port values.

Well-known UDP Types	Values
FTP Data	20
FTP	21
SSH	22
Telnet	23
SMTP	25
TACACS	49
DNS	53
BootP Server	67
BootP Client	68
TFTP	69
Finger	79
HTTP	80
POP3	110
Portmapper	111
NNTP	119
NTP	123
NetBIOS Name Service	137
NetBIOS Datagram Service	138
NetBIOS Session Service	139

Well-known UDP Types	Values
IMAP2/IMAP4	143
SNMP	161
IMAP3	220
LDAP	389
HTTPS	443
R-Exec	512
R-Login	513
R-Shell	514
LPR	515
RIP	520
SOCKS	1080
Citrix ICA	1494
RADIUS	1812
RADIUS Accounting	1813
NFS	2049
X11 (Range Start)	6000
X11 (Range End)	6063
Other	0-65535

IP TCP Port Source, IP TCP Port Destination, IP TCP Port Bilateral

These classification types are based on specific Layer 4 TCP port numbers contained within the header of an IP frame. Select a TCP type from the list of well-known values, or select **Other** and manually enter the value in decimal form. (TCP port numbers are defined in RFC 1700.) You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold. Enter a valid IPv4 or IPv6 address and optional mask ("/n"), if desired. The IP address is an optional field and does not have to be specified. It is only valid for non-range port values.

Well-known TCP Types	Values
FTP Data	20
FTP	21
SSH	22
Telnet	23

Well-known TCP Types	Values
SMTP	25
TACACS	49
DNS	53
BootP Server	67
BootP Client	68
TFTP	69
Finger	79
HTTP	80
POP3	110
Portmapper	111
NNTP	119
NTP	123
NetBIOS Name Service	137
NetBIOS Datagram Service	138
NetBIOS Session Service	139
IMAP2/IMAP4	143
SNMP	161
IMAP3	220
LDAP	389
HTTPS	443
R-Exec	512
R-Login	513
R-Shell	514
LPR	515
RIP	520
SOCKS	1080
Citrix ICA	1494
RADIUS	1812
RADIUS Accounting	1813
NFS	2049
X11 (Range Start)	6000

Well-known TCP Types	Values
X11 (Range End)	6063
Other	0-65535

IP UDP Port Source Range, IP UDP Port Destination Range, IP UDP Port Bilateral Range

These classification types are based on Layer 4 UDP port numbers contained within the header of an IP frame. When you select this type, you enter a range of UDP port numbers that the port number in the header will be matched against. Enter the start and end range values in decimal form. UDP port numbers are defined in RFC 1700.

IP TCP Port Source Range, IP TCP Port Destination Range, IP TCP Port Bilateral Range

These classification types are based on Layer 4 TCP port numbers contained within the header of an IP frame. When you select this type, you enter a range of TCP port numbers that the port number in the header will be matched against. Enter the start and end range values in decimal form. TCP port numbers are defined in RFC 1700.

IP UDP Port Source List, IP UDP Port Destination List

These classification types are based on Layer 4 UDP port numbers contained within the header of an IP frame. When you select this type, you enter a list of UDP port numbers that the port number in the header will be matched against. Enter the port numbers in decimal form, separated by commas (for example, 67, 68, 123). UDP port numbers are defined in RFC 1700. These classification types are available for Fabric Engine (VOSS) devices running VOSS 8.9 or later. When enforced, ExtremeControl generates a single compressed ACE entry containing all specified ports. List classification types are available when creating rules in both Per-User ACL mode and Role ACL mode.

IP TCP Port Source List, IP TCP Port Destination List

These classification types are based on Layer 4 TCP port numbers contained within the header of an IP frame. When you select this type, you enter a list of TCP port numbers that the port number in the header will be matched against. Enter the port numbers in decimal form, separated by commas (for example, 37, 38, 1427). TCP port numbers are defined in RFC 1700. These classification types are available for Fabric Engine (VOSS) devices running VOSS 8.9 or later. When enforced, ExtremeControl generates a single compressed ACE entry containing all specified ports. List classification types are available when creating rules in both Per-User ACL mode and Role ACL mode.

NOTE: Port values in Range and List fields must be valid numeric values between 0 and 65535. Entering invalid characters can result in unexpected values being saved.

Layer 7 -- Application Classification Types

Layer 7 IP classification types allow you to define classification rules based on specific Layer 7 application types.

Application

This rule type allows management of traffic for a specific application type, for example Apple traffic (Bonjour) using mDNS-SD. The following application types are supported:

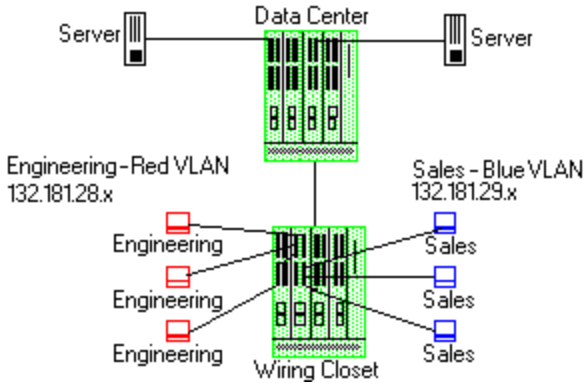
- LLMNR - (Link Local Multicast Name Resolution) Query/Response
  This protocol is based on the Domain Name System (DNS) packet format. It allows hosts to perform name resolution for hosts on the same local link.
- SSDP - (Simple Service Discovery Protocol) Query/Response
  SSDP is a Universal Plug-and-Play (UPnP) based protocol. SSDP uses the NOTIFY and MSEARCH HTTP methods to discover and advertise services on the network.
- mDNS-SD - (Multicast Domain Name System – Service Discovery) Query/Response
  DNS-SD is a service discovery protocol that utilizes the Domain Name System. Multicast DNS is a protocol that is mostly compatible with normal DNS but uses link local multicast addressing, allowing for zero configuration networking (zeroconf) functionality.

Examples of How Rules are Used

Traffic Classification rules are used to provide four key policy features: Traffic Containment, Traffic Filtering, Traffic Security, and Traffic Priority.

Traffic Containment

Using classification rules, network administrators can group together users of a given protocol, subnet, or application, and control where their traffic can logically go on the network.



The figure above shows a configuration where the network administrator wants to separate end-user traffic into VLANs based on the assigned IP subnet of each department. This can easily be accomplished by creating two Layer 3 classification rules based on the IP subnet range of the respective departments.

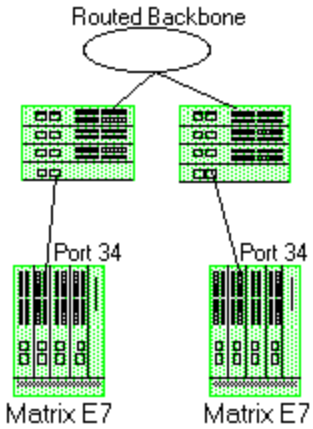
Rule 1 - Engineering, which uses the 132.181.28.x subnet, will be assigned to the Red VLAN.

Rule 2 - Sales, which uses the 132.181.29.x subnet, will be assigned to the Blue VLAN.

Based on these two Layer 3 classification rules, the traffic from the Engineering VLAN will be isolated from the Sales VLAN. Since these rules are based on Layer 3 information, an Engineering user could enter the network from a connection in the Sales department, and that user would still be contained in the Engineering VLAN.

Traffic Filtering

Classification rules can also be used to filter out (discard) specific unwanted traffic. Filter criteria can include things such as broadcast routing protocols, specific IP addresses, or even applications such as HTTP or SMTP.



The figure above shows a common configuration in which a routed backbone is using both RIP and OSPF for its routing protocols. The network administrator does not want the multicast OSPF and broadcast RIP frames propagated to the end stations. The network is designed so that only end users are attached to the E7 devices.

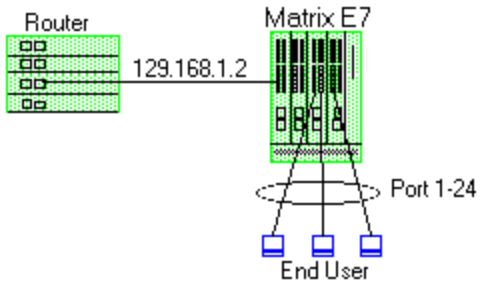
To implement filtering in this scenario, a Layer 3 rule and a Layer 4 rule will be created.

> Rule 1 (Layer 3) - Any frame received with an IP Protocol Type of 89 (OSPF) will be discarded.
>
> Rule 2 (Layer 4) - Any frame received with a Bilateral UDP port number of 520 (RIP) will be discarded.

Based on this configuration, all RIP and OSPF frames will be filtered from the end users.

Traffic Security

Traffic Security uses the same concepts as Traffic Filtering. Imagine a scenario where network access is provided to a group of unknown users. There have been problems with these unknown users "hacking" into the router and altering the configuration. A simple classification rule can be put in place that will prevent these types of occurrences.



In the figure above, the network components include a router and an E7 device. In this configuration end-users connect to the ports of the E7 device.

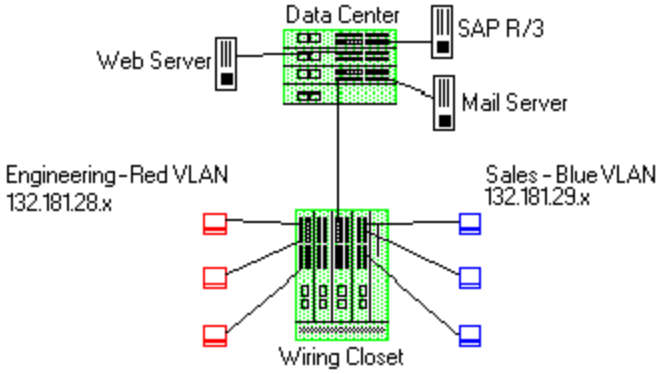
Since the end-users would never need to communicate directly to the router using the router's IP address, a Layer 3 IP classification rule will be used.

> Rule - Any frames received by the switch with a destination IP address of the router (129.168.1.2) will be discarded.

The end result is that any frames from a user trying to "hack" into the router will be discarded before ever reaching the router.

Traffic Prioritization

Classification rules can be used to specify that certain network applications receive the highest transmission priority. For example, a network administrator wants to assign priority to three network applications, SAP R/3, web traffic, and email, in that order.



To accomplish the prioritization goals in this example, there are two main steps required: creating the classification rules, and then configuring the priority-to-transmit queue mapping for the switch, if needed.

First, create one Layer 3 and two Layer 4 classification rules.

> Rule 1, Layer 3 (SAP R/3) - All frames to or from the IP address of the SAP R/3 server will be tagged with a priority indicator of 7 (highest).

Rule 2, Layer 4 (Web) - All frames with a TCP port number of 80 (HTTP) will be tagged with a priority indicator of 5.

Rule 3, Layer 4 (email) - All frames with a TCP port number of 25 (SMTP) will be tagged with a priority indicator of 3.

Note: An IP address classification was selected for Rule 1 because it has been observed that SAP R/3 dynamically negotiates the TCP/UDP port used, so the port number selections vary from session to session. If this was not the case, a Layer 4 UDP classification could be used.

Then, configure the priority-to-transmit queue mappings. Each switch has default priority-to-transmit queue mappings. You can use these defaults or change the mappings using local management. In addition, the Policy tab provides the ability to configure transmit queues as part of the Role-Based Rate Limits and Transmit Queue Configuration class of service mode. This functionality is available only on certain devices such as the S-Series and N-Series Gold and Platinum devices (refer to the ExtremeCloud IQ Site Engine Firmware Support matrix for specific device/firmware rate limit support).

Based on the default priority-to-traffic queue mapping for an E7 device, the priorities assigned above will work out so that each frame classification type will be mapped to the desired traffic queue. This means that no user configuration of the priority-to-transmit queue mapping would be required.

With the classification rules described above, the network traffic would be prioritized as shown in the table below:

Application	Classification Type	Desired Priority	Priority Value	E7 Traffic Queue
SAP R/3	Bilateral IP	High	7	3
Web	TCP Port Number	Medium	5	2
Email	TCP Port Number	Low	3	1

Ports (Transmit Queue Port Group)

The Ports tab lets you view all the ports in the selected transmit queue port group, as well as add and remove ports to and from the group. It provides information about each port, and lets you view and edit port information.

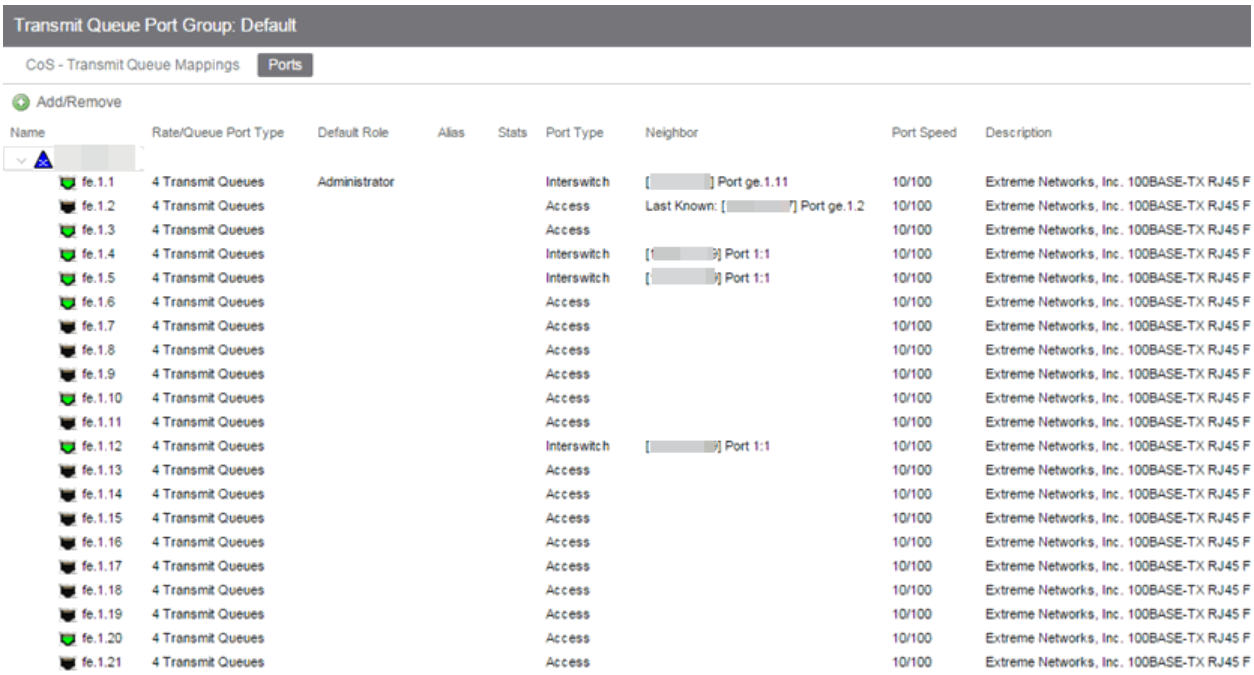
To access this tab:

1. Open the **Control** tab.
2. Open the **Policy** tab.
3. Open the **Class of Service** > **CoS Components** left-panel tab.
4. Select either the **Transmit Queue Port Groups** left-panel tab.

5. Select a existing port group in the left panel to open it in the **Transmit Queue Port Group** tab.

   NOTE: Create a new port group by right-clicking the **Transmit Queue Port Groups** left-panel tab, selecting **Create Port Group**, entering a **Name** for the port group, and selecting **OK**.

6. Select the **Ports** tab in the right panel.



Name

Name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

Rate/Queue Port Type

The number of rate limits the port supports.

Default Role

The Default Role assigned to the port.

Alias

Shows the alias (ifAlias) for the interface, if one is assigned.

Stats

Shows statistics collected for a port, enabled via the Flow Collection & Interface setting in the PortView.

Port Type

Type of port. Possible values include: Access, Interswitch Backplane, Backplane, Interswitch, and Logical.

Neighbor
The port's neighbor port.

Port Speed
Speed of the port. Possible values include: 10/100, speed in megabits per second (for example, 800.0 Mbps), Unknown (displayed for logical ports).

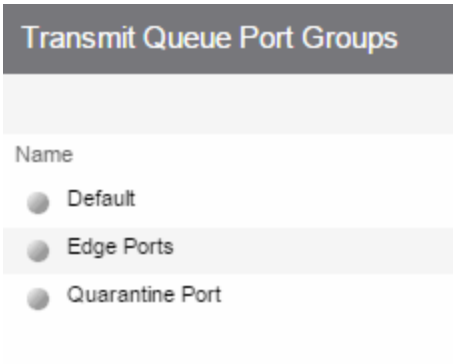
Description
A description of the port.

Add/Remove Ports Button
Opens the Add/Remove Ports window, where you can add and remove ports to and from the port group. When you create new port groups, you add ports from the Default group into your newly defined port groups.

Summary (Transmit Queue Port Groups)

This tab displays the transmit queue port groups. Transmit queue mapping maps a logical transmit queue index (used by a class of service) to an actual physical transmit queue you have configured in the **Policy** tab. You can configure transmit queue mappings for a port group using the CoS - Transmit Queue Mappings tab.

To access this tab, open the **Class of Service > CoS Components** tab. Then, select the select the **Transmit Queue Port Groups** tab in the left panel. The Summary tab displays in the right panel.



Name
The name of the transmit queue port group.

CoS - Transmit Queue Mappings (Transmit Queue Port Group)

This tab lets you view and configure the transmit queue mappings for a port group. Transmit queue mappings map a logical rate limit index used by classes of service to an actual physical rate limit you have created in ExtremeCloud IQ Site Engine.

Each port group has its own set of index mappings. ExtremeCloud IQ Site Engine automatically assigns these index numbers when you configure a class of services' rate limits and transmit queue shapers.

The Transmit Queue Mappings tab allows you to do two things:

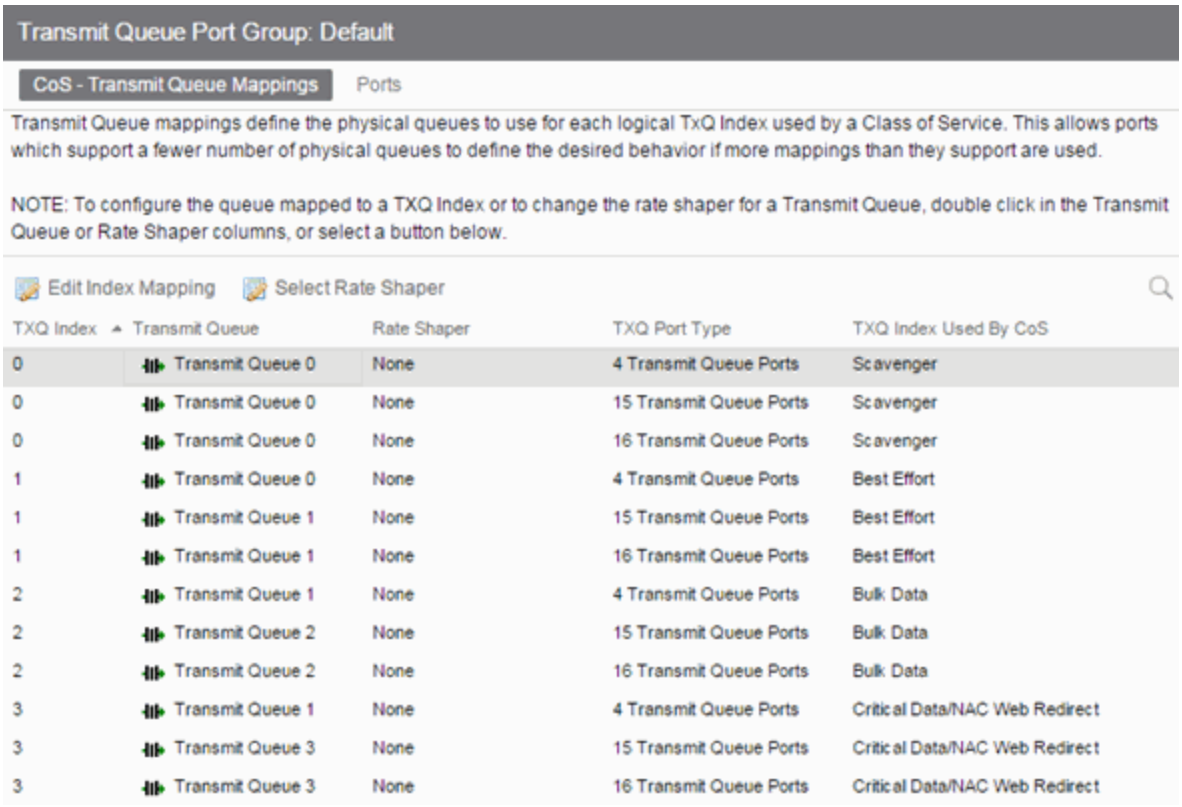
- Map the index to a different rate for different port groups (edge ports versus inter-switch links). See Creating Class of Service Port Groups
- Map the index to a different rate limit for each port type (8-rate limit, 32-rate limit, 64-rate limit, and 100-rate limit) in a port group. See Advanced Rate Limiting by Port Type.

To access this tab:

1. Open the **Control** tab.
2. Open the **Policy** tab.
3. Open the **Class of Service** > **CoS Components** left-panel tab.
4. Select either the **Transmit Queue Port Groups** left-panel tab.
5. Select a existing port group in the left panel to open it in the **Transmit Queue Port Group** tab.

   NOTE: Create a new port group by right-clicking the **Transmit Queue Port Groups** left-panel tab, selecting **Create Port Group**, entering a **Name** for the port group, and selecting **OK**.

6. Select the **CoS - Transmit Queue Mappings** tab in the right panel.



TXQ Index

The logical transmit queue index. This index number is specified in a class of service and dictates the queue and shaping behavior for incoming packets.

Transmit Queue

Displays the physical transmit queue used to map to each transmit queue index. To change this value, select the **Edit Index Mapping** button to open the Edit Transmit Queue Mapping window and select a value in the **Transmit Queue** drop-down list.

Rate Shaper

The transmit queue's associated rate shaper. To change this value, select the **Select Rate Shaper** button to open the Select Transmit Queue Rate Shaper window and select a value in the **Rate Limit** field.

TXQ Port Type

The Port Type is based on the number of transmit queues the port supports: 4 transmit queues or 16 transmit queues.

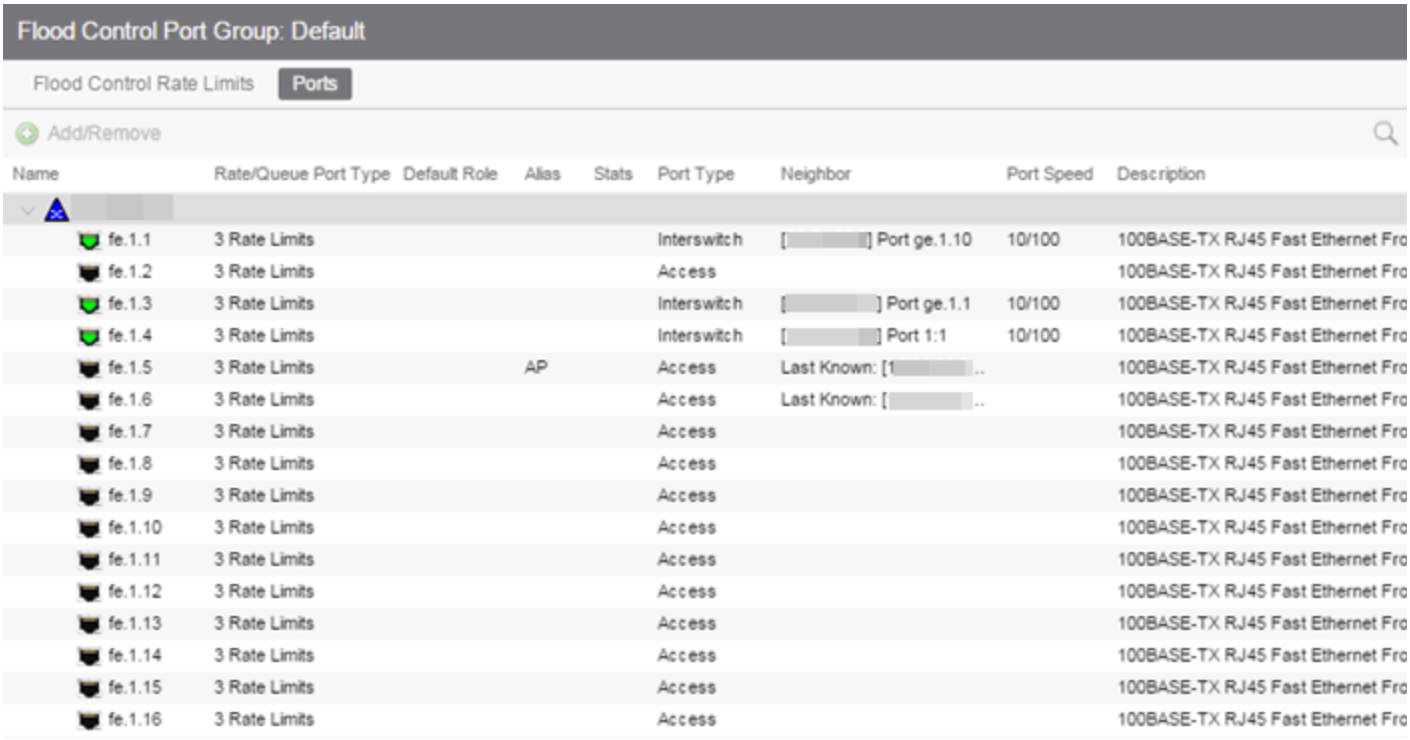
TXQ Index Used By CoS

The Class of Service using this TXQ index.

Ports (Flood Control Port Groups)

The **Flood Control Port Group Ports** tab provides a table of information about the ports in the selected port group. It also includes buttons that enable you to retrieve the latest information about the ports and to add and remove ports. To access this tab, select a port group in the left-panel **Flood Control Port Groups** tab, then select the **Ports** tab in the right panel.

NOTE: The **Ports** tab is only available when a Flood Control port group is selected, and when advanced mode is enabled on the CoS Components tab.



Name

Name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

Rate/Queue Port Type

Shows the selected port type rate/queue.

Default Role

Shows the default role for the port. See Default Role in the Concepts topic for information on default roles. For additional information, see Port Mode.

Alias

Shows the alias (ifAlias) for the interface, if one is assigned.

Stats
Shows that statistics are being collected for a port, enabled via the PortView.

Port Type
Type of port. Possible values include: Access, Interswitch Backplane, Backplane, Interswitch, and Logical.

Neighbor
Port to which the port is connected.

Port Speed
Speed of the port. Possible values include: 10/100, speed in megabits per second (for example, 800.0 Mbps), Unknown (displayed for logical ports).

Description
A description of the port.

Add/Remove Button
Selecting a port in the table and selecting this button opens the Add/Remove Ports window, which enables you to add and remove ports to and from the port group. This option is available for user-defined port groups only.

Flood Control Port Groups

This panel lists port groups on which you can configure flood control. Each port group supports rate limits for three separate configured traffic types (Unicast, Multicast, and Broadcast).

To access this tab, open Class of Service > CoS Components left panel of the Policy tab and select Flood Control Port Groups.



Name
The name of the port group.

Flood Control Rate Limits (Flood Control Port Groups)

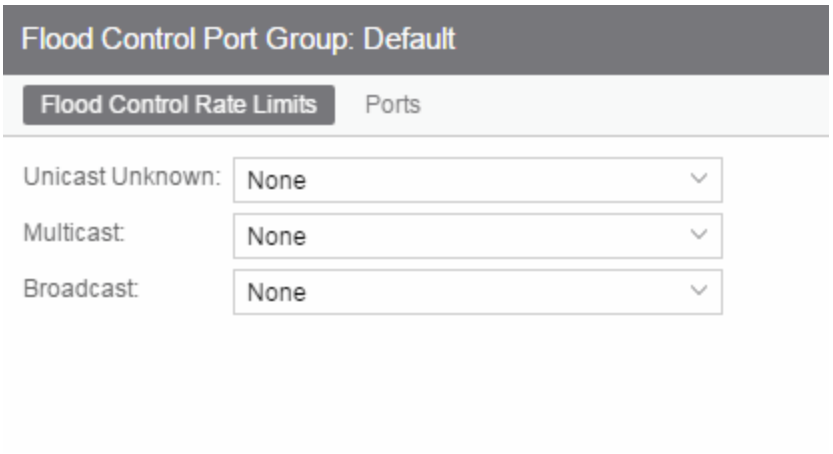
This tab allows you to set individual flood control rates for each traffic type (Unicast, Multicast, and Broadcast).

Choices include:

- None
- Rate limits created in the **Rate Limit** tab. For additional information, see Create Rate Limit/Shaper.

As flood control is enabled/disabled for a Class of Service, when enabled, each column displays a rate limit, or **None**, if no rate has been defined for that portion of flood control.

To access this tab, open the **Class of Service** > **CoS Components** left-panel tab. Then, select the **Flood Control** checkbox from the **General** tab in the left-panel to display the **Flood Control Port Groups** tab in the left panel. Expand the **Flood Control Port Groups** tab, and select a flood control port group in the tree. The **Flood Control Port Groups** tab is displayed in the right panel.



Unicast Unknown

Select a rate, create a new rate, or edit an existing flood control rate limit for Unicast traffic.

Multicast

Select a rate, create a new rate, or edit an existing flood control rate limit for Multicast traffic.

Broadcast

Select a rate, create a new rate, or edit an existing flood control rate limit for Broadcast traffic.

Class of Service Example

This Help topic provides an example of how class of service (CoS) can be configured on a network to manage bandwidth requirements of network traffic. Before you look at this example, read Getting Started with Class of Service.

In this example, an organization's network administrator needs to assure that VoIP traffic, both originating in and transiting a network of edge switches and a core router, is configured with appropriate priority, ToS, and queue treatment. We also rate limit the VoIP traffic at the edge to 1 Mb/s to guard against DOS attacks, VoIP traffic into the core at 25 Mb/s, and H.323 call setup at 5 PPS. Data traffic retains the default configuration.

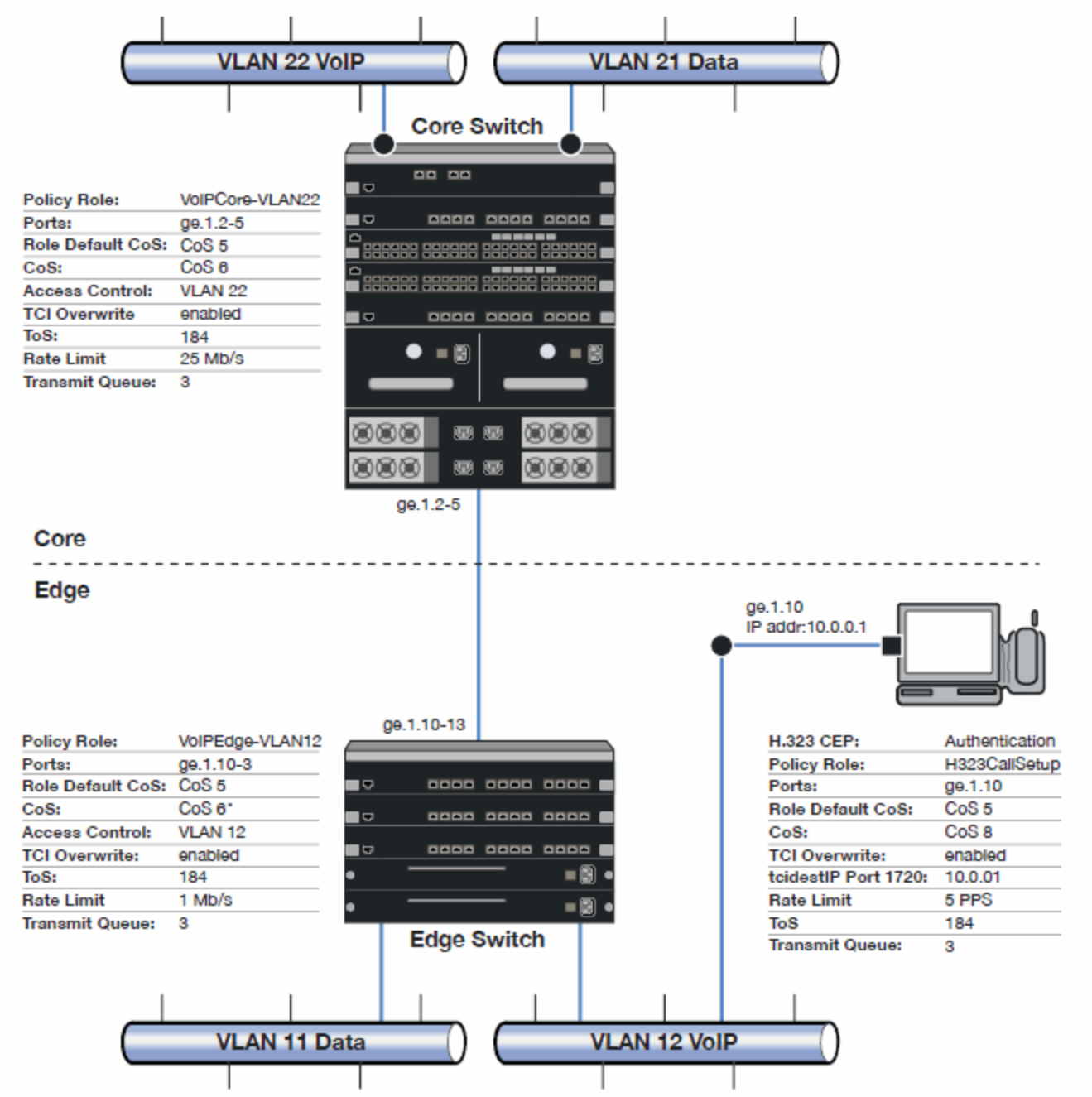
This example assumes CEP authentication using H.323 for VoIP. For networks that do not authenticate VoIP end point with CEP H.323 authentication, the VoIP policy needs to be adjusted accordingly. For instance, SIP uses UDP port 5060, not the TCP port 1720.

To simplify the discussion of the configuration process, this example is limited to the VoIP configuration context. The following table provides a set of sample values for priority, inbound rate limit (IRL), and transmit queue across a number of real world traffic types. This table can be used as an aid in thinking about how you might want to apply CoS across your network. Note that Scavenger class is traffic that should be treated as less than best effort: external web traffic, for instance.

CoS Name	CoS Index	Priority	IRL		Transmit Queue					
					Queue #		Shaping		Bandwidth	
			Edge	Core	Edge	Core	Edge	Core	Edge	Core
Scavenger (Static)	0	0	15 Mb/s		0	0	10%		5%	5%
Best Effort (Static)	1	1			1	1	80%		45%	45%
Bulk Data (Static)	2	2								
Critical Data (Static)	3	3								
Network Control (Static)	4	4	40 PPS	1 Mb/s	2	2	1 Mb/s		25%	25%
Network Mgmt (Static)	5	5	2 Mb/s							
RTP/Voice/Video (Static)	6	6	1 Mb/s	25 Mb/s	3	3			25%	25%
High Priority (Static)	7	7								
VoIP Call Setup	8	7	5 PPS		3	3			25%	25%

The following figure displays the network setup for this example configuration, with the desired Profile/CoS summary for each network device. Each device is configured with VoIP and Data VLANs. Each VoIP VLAN contains four 1-gigabit interfaces for each device.

CoS VoIP Configuration Example



Edge and Core port groups in the RTP/Voice/Video (Static) CoS provide for the difference in rate limiting needs between the end user and aggregation devices. A VoIP Call Setup CoS provides rate limiting for the setup aspect of the VoIP call.

The Edge, Core, and H.323 Call Setup roles are configured with TCI Overwrite, default CoS 5 (best default priority for voice and video), and default access control that contains traffic to the appropriate VLAN.

Use the Policy tab to configure the policy roles and related services using the following instructions. For more information, see How to Create a Class of Service and How to Define Rate Limits.

Configure the Classes of Service

Use the Class of Service tab to configure the static RTP/Voice/Video CoS with the appropriate edge and core rate limits, and create a new CoS for the call setup rate limits.

1. For the static RTP/Voice/Video CoS (CoS Index 6):
    a. Set the ToS to B8.
    b. Create two new Inbound RL port groups called Edge and Core.
    c. Set the Edge port group rate limit to 1 Mb/s and the Core port group rate limit to 25 Mb/s. (You can create these rate limits first.)
    d. Add the appropriate ports to each port group.
2. Create a new class of service and name it VoIP Call Setup (CoS Index 8).
    a. Set the rate limit to 5 PPS for all port groups. (You can create this rate limit first.)
    b. Set the ToS to B8.

Create the VoIP Core Role

For the core router, create a policy role for VoIP Core. VoIP Core policy deals with packets transiting the core network using VoIP VLAN 22.

1. Name the role VoIPCore-VLAN22.
2. Enable TCI overwrite so that ToS is rewritten for this role.
3. Set the default access control action to Contain to VLAN 22.
4. Set default Class of Service to CoS Index 5.

Create a VoIP Core Service

1. Name the service VoIPCore.
2. Add the service to the VoIPCore-VLAN22 role.

Create a Rule

1. Create a Layer 2 traffic classification rule for VLAN ID 22 within the VoIPCore service.
2. Assign the static RTP/Voice/Video CoS (CoS Index 6) as the Class of Service action for the rule.

Creating the VoIP Edge Role

For the edge switches, create a policy role for VoIP Edge. VoIP Edge policy deals with packets transiting the edge network using VoIP VLAN 12.

1. Name the role VoIPEdge-VLAN12.
2. Enable TCI overwrite so that ToS is rewritten for this role.
3. Set the default access control action to Contain to VLAN 12.
4. Set default Class of Service to CoS Index 5.

Create a VoIP Edge Service

1. Name the service VoIPEdge.
2. Add the service to the VoIPEdge-VLAN12 role.

Create a Rule

1. Create a Layer 2 traffic classification rule for VLAN ID 12 within the VoIPEdge service.
2. Assign the static RTP/Voice/Video CoS (CoS Index 6) as the Class of Service action for the rule.

Creating the H.323 Call Setup Role

The H.323 Call Setup role deals with the call setup traffic for VoIP H.323 authenticated users directly attached to the switch using link ge.1.10.

1. Name the role H323CallSetup.
2. Enable TCI overwrite so that ToS is rewritten for this policy.
3. Set default Class of Service to CoS Index 5.

Create a H.323 Call Setup Service

1. Name the service H323CallSetup.
2. Add the service to the H323CallSetup role.

Create a Rule

Create a Layer 4 traffic classification rule as follows:

1. Traffic Classification Type: IP TCP Port Destination
2. Enter in Single Value field: 1720 (TCP Port ID).
3. For IP TCP Port Destination value: 10.0.0.1 with a mask of 255.255.255.255.
4. Assign the new VoIP Call Setup CoS (CoS Index 8) as the Class of Service action for the rule.

Apply the Roles to Network Devices

After you have created your roles, you must apply them to the network devices as follows:

Core Router

Apply the VoIPCore-VLAN22 role to ports ge.1.2-5.

Edge Switch

Apply the VoIPEdge-VLAN12 role to ports ge.1.10-13.

Apply the H323CallSetup role to port ge.1.10

ToS/DSCP Value Definition Chart

Use this chart to compare ToS and DSCP values.

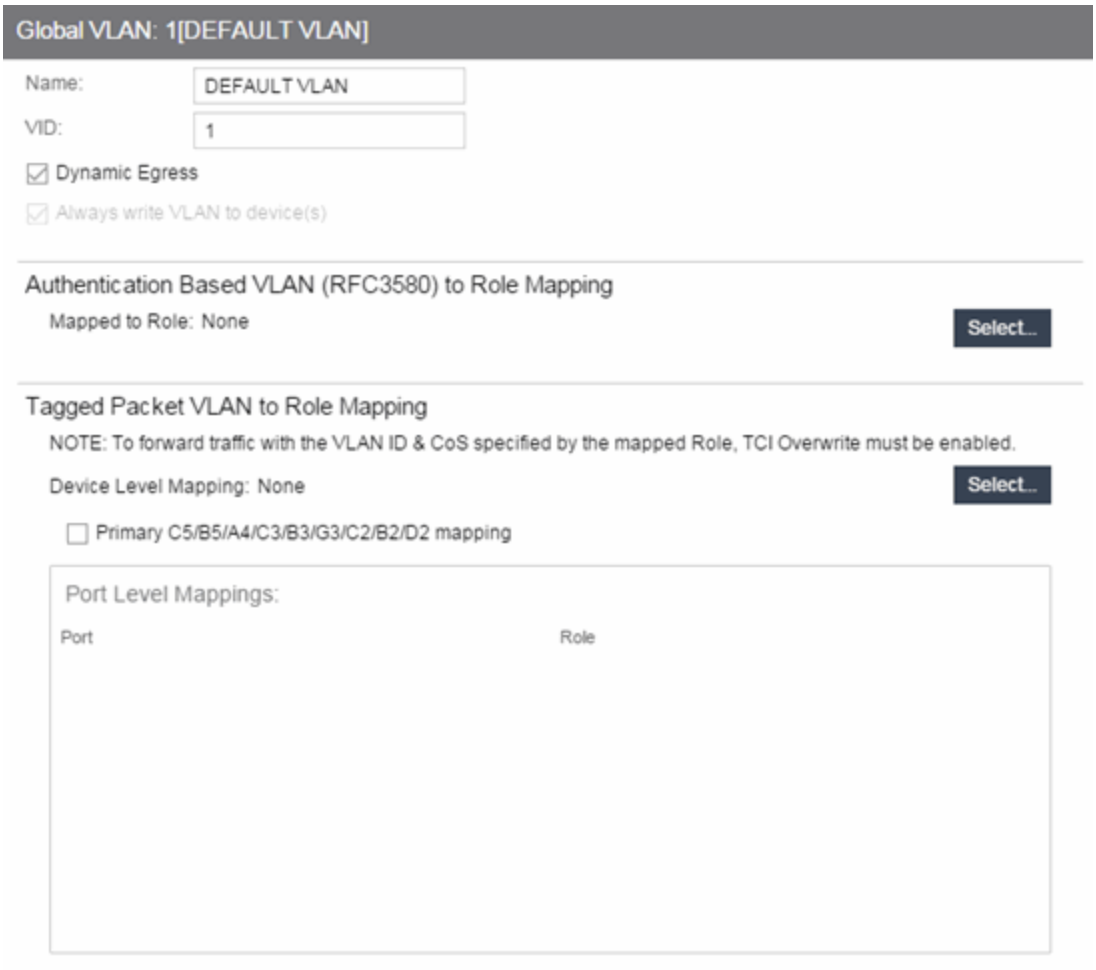
ToS (Dec)	ToS (Hex)	ToS (Binary)	ToS Precedence (Binary)	ToS Precedence (Decimal)	ToS Precedence Name	ToS Delay Flag	ToS Throughput Flag	ToS Reliability Flag	DSCP (Binary)	DSCP (Hex)	DSCP (Decimal)	DSCP Class
0	0x00	00000000	000	0	Routine	0	0	0	000000	0x00	0	none
32	0x20	00100000	001	1	Priority	0	0	0	001000	0x08	8	cs1
40	0x28	00101000	001	1	Priority	0	1	0	001010	0x0A	10	af11
48	0x30	00110000	001	1	Priority	1	0	0	001100	0x0C	12	af12
56	0x38	00111000	001	1	Priority	1	1	0	001110	0x0E	14	af13
64	0x40	01000000	010	2	Immediate	0	0	0	010000	0x10	16	cs2
72	0x48	01001000	010	2	Immediate	0	1	0	010010	0x12	18	af21
80	0x50	01010000	010	2	Immediate	1	0	0	010100	0x14	20	af22
88	0x58	01011000	010	2	Immediate	1	1	0	010110	0x16	22	af23
96	0x60	01100000	011	3	Flash	0	0	0	011000	0x18	24	cs3
104	0x68	01101000	011	3	Flash	0	1	0	011010	0x1A	26	af31
112	0x70	01110000	011	3	Flash	1	0	0	011100	0x1C	28	af32
120	0x78	01111000	011	3	Flash	1	1	0	011110	0x1E	30	af33
128	0x80	10000000	100	4	FlashOverride	0	0	0	100000	0x20	32	cs4
136	0x88	10001000	100	4	FlashOverride	0	1	0	100010	0x22	34	af41
144	0x90	10010000	100	4	FlashOverride	1	0	0	100100	0x24	36	af42
152	0x98	10011000	100	4	FlashOverride	1	1	0	100110	0x26	38	af43
160	0xA0	10100000	101	5	Critical	0	0	0	101000	0x28	40	cs5

ToS (Dec)	ToS (Hex)	ToS (Binary)	ToS Precedence (Binary)	ToS Precedence (Decimal)	ToS Precedence Name	ToS Delay Flag	ToS Throughput Flag	ToS Reliability Flag	DSCP (Binary)	DSCP (Hex)	DSCP (Decimal)	DSCP Class
184	0xB8	10111000	101	5	Critical	1	1	0	101110	0x2E	46	ef
192	0xC0	11000000	110	6	InterNetwork Control	0	0	0	110000	0x30	48	cs6
224	0xE0	11100000	111	7	Network Control	0	0	0	111000	0x38	56	cs7

Policy VLAN Tab Overview

The **VLAN** tab displays information about the VLAN selected in the left panel and lets you configure certain VLAN parameters. If you are using VLAN to Role mapping in your network, you can also use this tab to map the VLAN to a specific role. If you make a change on this tab, you need to enforce it.

To view this tab, select **Control > Policy > VLANs** and select a VLAN from the drop down.



General

This area provides general information about the VLAN and enables you to configure the VLAN.

Name

Name of the VLAN selected in the left panel.

VID

Unique number assigned to the VLAN, also called VID (for VLAN ID). This ID was either assigned by an administrator or assigned automatically by the system when the VLAN was created. The value can be anywhere between 1 and 4094, with VID 1 being reserved for the DEFAULT VLAN (a name for a particular VLAN, not to be confused with a role's assigned default VLAN).

Dynamic Egress

Dynamically add all ports which use this VLAN to this VLAN's egress list. Dynamic Egress is enabled by default in Policy Manager. Leave disabled for discard VLANs. See Dynamic Egress for more information.

Always write VLAN to device(s)

If the box is checked, the VLAN is written to the device whether the VLAN is being used in a rule or role, or not. If it is not checked, the VLAN is not written to the device even though it is being used in a rule or role. Enabling this option is a way of ensuring that the device is aware of a VLAN that is being used for something other than policy configuration, and it enables you to configure that VLAN for Dynamic Egress. If the Default VLAN (VID=1) is selected in the left panel, this option is checked and cannot be edited, as the default VLAN is always on the device.

NOTE: On wireless devices (for example, ExtremeWireless and ExtremeCloud Appliance), the VLAN is always written to the device if it is being used in a rule or role, regardless whether this checkbox is checked or not.

Authentication-Based VLAN to Role Mapping

Authentication-Based VLAN to Role Mapping provides a way to assign a role to a user during the authentication process, based on a VLAN Attribute. (For more information, see VLAN to Role Mapping in the Concepts help topic.) This area displays what role (if any) the VLAN is mapped to (at the device-level) and lets you configure a mapping, if desired.

Mapped to Role

The role to which the VLAN is mapped. To select a role, select **Select**, select the **Assign RFC3580 VLAN -> Role Mapping** radio button, choose a role in the drop-down list, and select **OK**.

Select

Opens the role Selection View, where you can choose a role to associate with the VLAN.

Tagged Packet VLAN to Role Mapping

Tagged Packet VLAN to Role Mapping provides a way to let policy-enabled devices assign a role to network traffic, based on a VLAN ID. (For more information, see VLAN to Role Mapping in the Concepts help topic.) This area displays what role (if any) the VLAN is mapped to at both the device-level and port-level, and lets you configure mappings, if desired.

NOTE: TCI Overwrite Requirement

Tagged Packet VLAN to Role Mapping will apply the Role definition to incoming packets using a mapped VLAN. This definition will apply a CoS and determine if the packet is discarded or permitted, and if TCI Overwrite is enabled will re-specify the VLAN ID defined by the Rule / Role Default. If TCI Overwrite is disabled, the packet will egress (if permitted by the Rule Hit) with the original VLAN ID it ingressed with.

If supported by the device, you can enable TCI Overwrite for an individual role in the role's General tab. The stackable devices support rewriting the CoS values but not the VLAN ID.

Device Level Mapping

The role the VLAN is mapped to at the device level (all devices). To select a role, select **Select**, choose a role, and select **OK**.

Select

Opens the role Selection View, where you can choose a role to associate with the VLAN at the device level.

Primary C2/B2/D2/C3/B3/G3/C5/B5/A4 mapping

Use this checkbox to specify that this VLAN to role mapping will be the primary mapping for C2/C3/C5 and B2/B3/B5 devices (C2 firmware version 03.02.xx and higher/B2 firmware version 02.00.16 and higher), and D2, A4, and G3 devices (G3 firmware version 6.03.xx and higher). These devices only support one device-level VLAN to role mapping. If you do not make this selection, there will be no device-level mapping for these devices.

Port Level Mappings

This table lists any port-level Tagged Packet VLAN to Role Mappings configured for this VLAN. Port-level mappings override any device-level mapping.

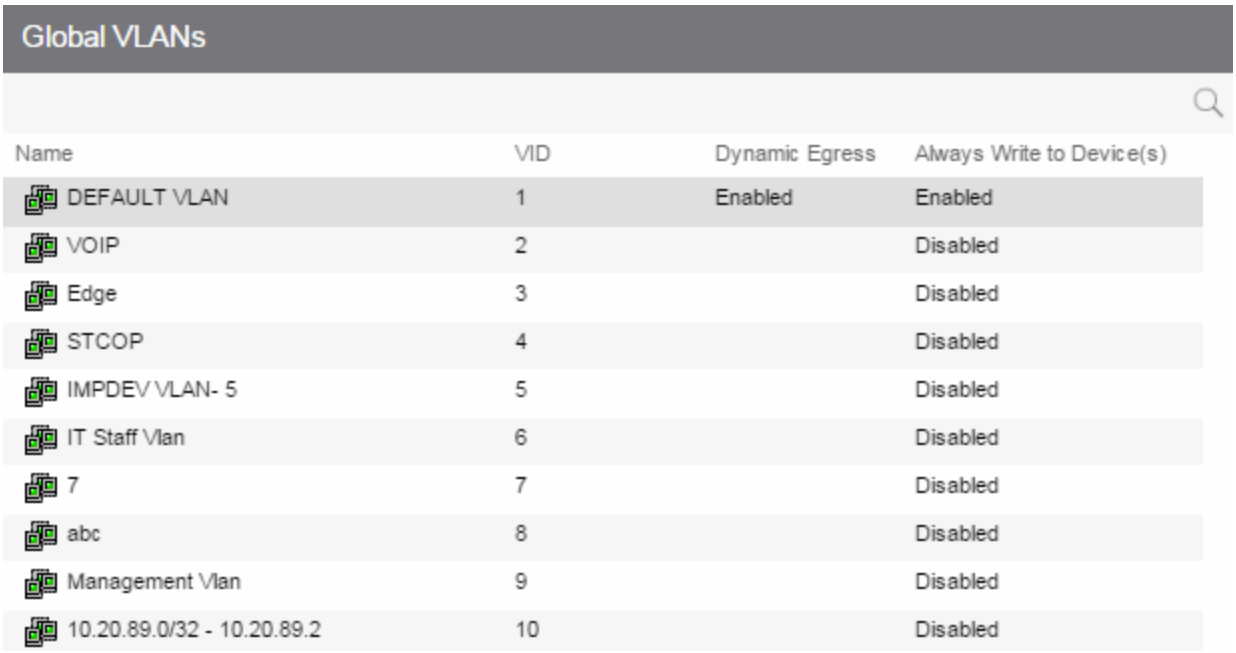
NOTE: This functionality is not yet enabled.

Global VLANs

This tab displays when you select the **Global VLANs** tab in the **VLANs** left-panel tab. It displays a table of information about the existing VLANs.

Right-clicking the **Global VLANs** tab allows you to create a new VLAN by selecting the **Create VLAN** option, while selecting **Reload VLANs** updates the list of VLANs with the latest information.

If you right-click a VLAN in the left-panel tab or in the right-panel table, you have the option to rename and delete the selected VLAN.



Name

Name of the VLAN.

VID

Unique number assigned to the VLAN, also called VID (for VLAN ID). For Global VLANs, this ID was either assigned by an administrator or assigned automatically by the system when the VLAN is created. The value can be anywhere between 1 and 4094, with VID 1 being reserved for the DEFAULT VLAN (a name for a particular VLAN, not to be confused with a role's assigned default VLAN).

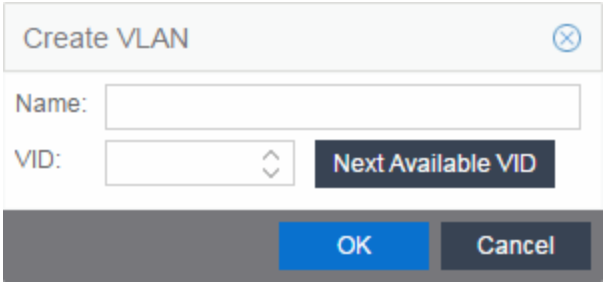
Dynamic Egress

Indicates whether the Dynamic Egress feature is on (**Enabled**) or off (**Disabled**) for the VLAN. The default is **Enabled**; therefore, this column displays **Enabled** unless a user has turned it off for a particular VLAN.

Always Write to Device(s)
If enabled, the VLAN is written to the device whether or not it is being used in a rule or role.

Create VLAN

This window displays when you right-click the **Global VLANs** left-panel tab and select **Create VLAN**. See How to Create a VLAN, How to Create a Policy VLAN Island, and Roles for additional information.



Name
The name for the VLAN you want to create. VLAN names can be up to 32 characters in length, including spaces. Do not create a VLAN name that uses any letters with diacritical marks. Diacritical marked letters are not supported by SNMP. VLAN names are case sensitive. For example, "Sales" and "sales" would be considered two different VLAN names. You can have multiple VLANs with the same name but with different VLAN IDs in the Policy tab.

VID
Unique numerical identifier for the VLAN, also known as VLAN ID. Can be a value between 1 and 4094, with VID1 being reserved for the DEFAULT VLAN (a name for a particular VLAN, not to be confused with a default VLAN you assign to a role). To select the next VID in sequence, select **Next Available VID**.

Next Available VID Button
Enters the next unassigned VID in the **VLAN ID** field.

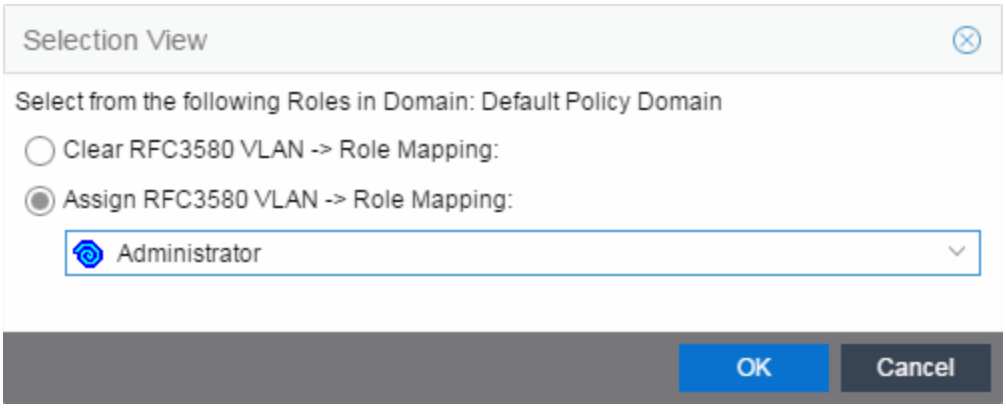
Editing an existing VLAN/Class of Service

OK Button
Creates the VLAN.

Selection View (Roles)

The Roles Selection View displays when you are selecting a role for VLAN to role mapping. It also lets you clear the current VLAN to role mapping. To access this view, select the desired VLAN in the VLANs

> Global VLANs left-panel tab, then select the **Select** button in the VLAN to Role Mapping section on the VLAN tab.



Clear RFC3580 VLAN -> Role Mapping
Select this option to clear the current role selection.

Assign RFC3580 -> Role Mapping
Select this option to assign a new role and make a selection from the list of available roles.

Policy VLAN Islands

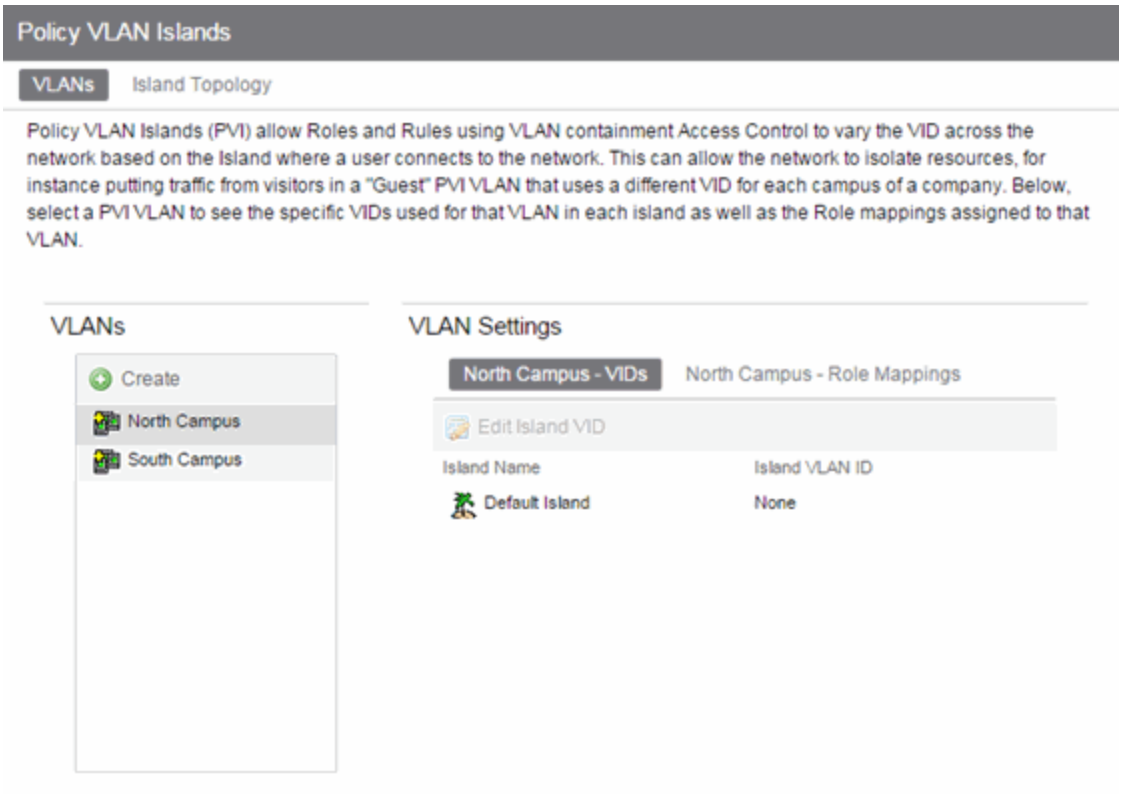
This tab displays a table of the Island VLANs being used in the Policy VLAN Island, and the names created on the devices in the island. To display this tab, select **Control > Policy > VLANs > Policy VLANs Islands**.

The **VLANs Tab** provides two sub-tabs:

- (VLAN) - VIDs Tab
- (VLAN) - Role Mappings Tab

(VLANs) - VIDs Tab

This tab provides information on VIDs assigned to specific islands. When an island is selected, the VIDs tab shows all VIDs for the defined PVI VLANs used for that island.



VLANs

Name of all defined VLANs. Select a VLAN to see the policy VLAN islands in the VLAN Settings section of the window and the VIDs with which that island is associated.

Create

Opens the Create VLAN window from which you can create a PVI VLAN. Unlike global VLANs, PVI VLANs are not created by the Policy tab during enforce. It is left to the user to configure these on the device(s) externally. The Policy tab only associates the appropriate VIDs to the rules during enforce.

Island Name

Shows the names of all VLAN Islands for the PVI VLAN selected in the VLANs section of the window.

Island VLAN ID

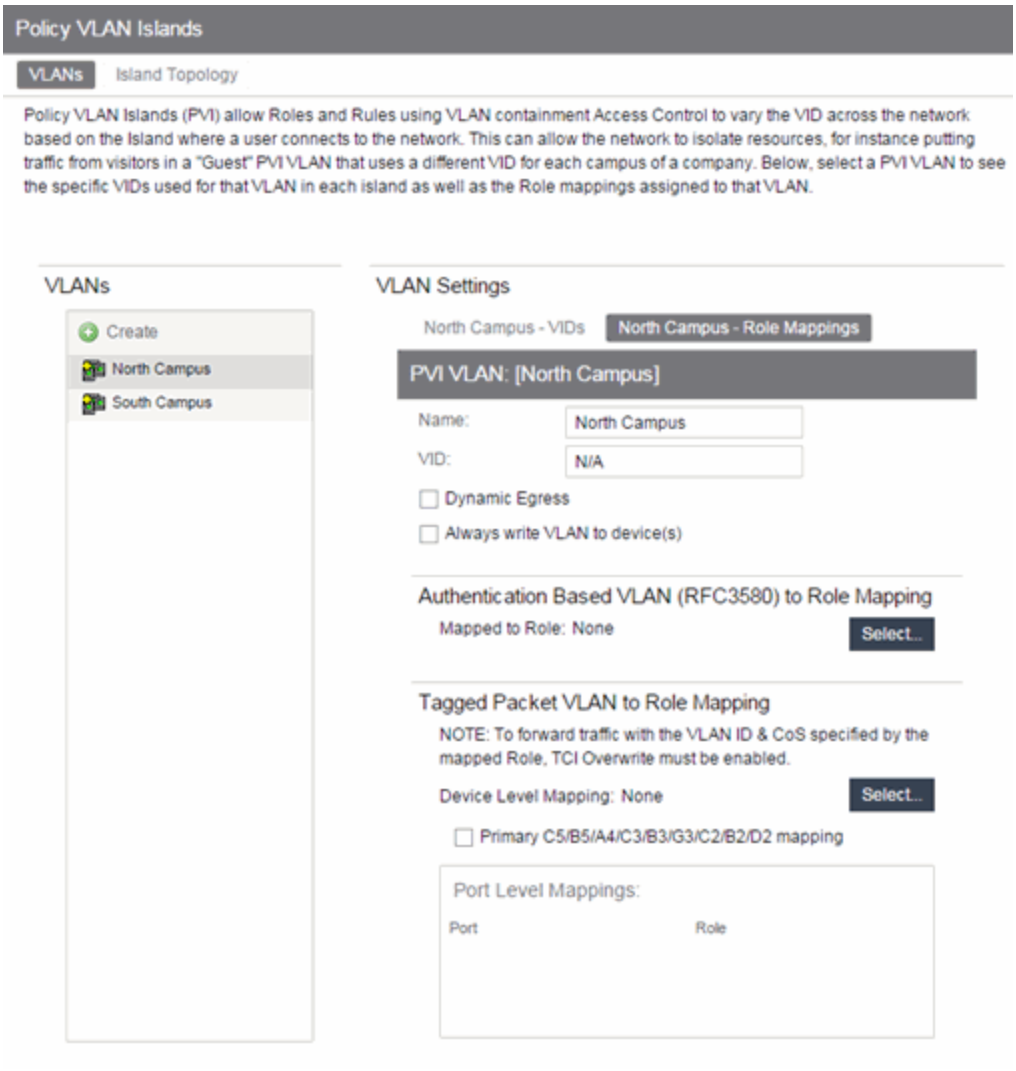
Shows the VID used for this PVI VLAN in this Island.

Edit Island VLAN ID

Selecting an island in the table and selecting this button opens the Edit Island VLAN ID window, where you can change the VID for the Island VLAN.

(VLANs) – Role Mappings Tab

This tab displays the role mappings for the Policy VLAN Island.



General

This area provides general information about the VLAN and allows you to configure the VLAN.

Name

Name of the VLAN selected in the left panel.

VID

Unique number assigned to the VLAN, also called VID (for VLAN ID). This ID was either assigned by an administrator or assigned automatically by the system when the VLAN was created. The value can be anywhere between 1 and 4094, with VID 1 being reserved for the DEFAULT VLAN (a name for a particular VLAN, not to be confused with a role's assigned default VLAN).

Dynamic Egress

Dynamically add all ports which use this VLAN to this VLAN's egress list. Dynamic Egress is

enabled by default in Policy Manager. Leave disabled for discard VLANs. See Dynamic Egress for more information.

Always write VLAN to device(s)

If the box is checked, the VLAN is written to the device whether the VLAN is being used in a rule or role, or not. If it is not checked, the VLAN is not written to the device even though it is being used in a rule or role. Enabling this option is a way of ensuring that the device is aware of a VLAN that is being used for something other than policy configuration, and it allows you to configure that VLAN for Dynamic Egress. If the Default VLAN (VID=1) is selected in the left panel, this option is checked and cannot be edited, as the default VLAN is always on the device.

NOTE: On wireless devices (for example, ExtremeWireless and ExtremeCloud Appliance), the VLAN is always written to the device if it is being used in a rule or role, regardless whether this checkbox is checked or not.

Authentication-Based VLAN to Role Mapping

Authentication-Based VLAN to Role Mapping provides a way to assign a role to a user during the authentication process, based on a VLAN Attribute. (For more information, see VLAN to Role Mapping in the Concepts help topic.) This area displays what role (if any) the VLAN is mapped to (at the device-level) and lets you configure a mapping, if desired.

Mapped to Role

The role to which the VLAN is mapped. To select a role, select **Select**, select the **Assign RFC3580 VLAN -> Role Mapping** radio button, choose a role in the drop-down list, and select **OK**.

Select

Opens the role Selection View, where you can choose a role to associate with the VLAN.

Tagged Packet VLAN to Role Mapping

Tagged Packet VLAN to Role Mapping provides a way to let policy-enabled devices assign a role to network traffic, based on a VLAN ID. (For more information, see VLAN to Role Mapping in the Concepts help topic.) This area displays what role (if any) the VLAN is mapped to at both the device-level and port-level, and lets you configure mappings, if desired.

NOTE: TCI Overwrite Requirement

Tagged Packet VLAN to Role Mapping will apply the Role definition to incoming packets using a mapped VLAN. This definition will apply a CoS and determine if the packet is discarded or permitted, and if TCI Overwrite is enabled will re-specify the VLAN ID defined by the Rule / Role Default. If TCI Overwrite is disabled, the packet will egress (if permitted by the Rule Hit) with the original VLAN ID it ingressed with.

If supported by the device, you can enable TCI Overwrite for an individual role in the role's General tab. The stackable devices support rewriting the CoS values but not the VLAN ID.

Device Level Mapping

The role the VLAN is mapped to at the device level (all devices). To select a role, select **Select**, choose a role, and select **OK**.

Select

Primary C2/B2/D2/C3/B3/G3/C5/B5/A4 mapping

Use this checkbox to specify that this VLAN to role mapping will be the primary mapping for C2/C3/C5 and B2/B3/B5 devices (C2 firmware version 03.02.xx and higher/B2 firmware version 02.00.16 and higher), and D2, A4, and G3 devices (G3 firmware version 6.03.xx and higher). These devices only support one device-level VLAN to role mapping. If you do not make this selection, there will be no device-level mapping for these devices.

Port Level Mappings

This table lists any port-level Tagged Packet VLAN to Role Mappings configured for this VLAN. Port-level mappings override any device-level mapping.

NOTE: This functionality is not yet enabled.

Add Devices (VLAN Islands)

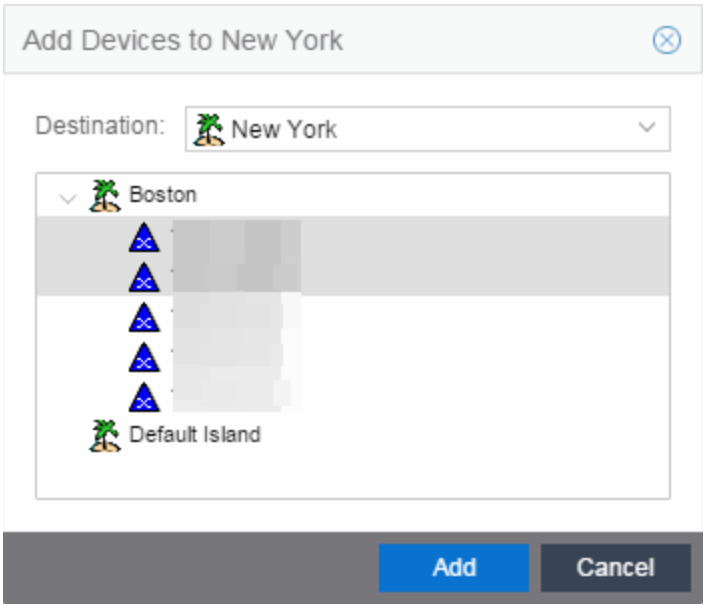
This window enables you to add devices to VLAN islands.

To access the window:

1. Select the **VLANs > Policy VLAN Islands** tab in the left panel.
2. Select the **Island Topology** tab in the Policy VLAN Islands right panel.
3. Select the Default Island - Devices tab in the Island Settings section of the window.
4. Select the **Add Devices** button.

Devices contained in an island are assigned a VID for each Island VLAN unique to the island, allowing roles and rules which use the Island VLANs to isolate users to that island. A device must always belong to an island, and shares a common VID assignment for the Island VLANs with all other devices contained in that island.

To add a device to an island, select the Island to which the device is to be added in the **Destination** drop-down list, select the device in the Devices section, and select **Add**. You can also select and add multiple devices.



Destination
Select the VLAN Island to which the device is to be added.

Devices Section
Expand the Island folder from which the VLAN Island is being selected to add the device or devices.

Add Button
Adds the device(s) selected in the Devices panel to the island selected in the Islands panel.

Island Topology (Policy VLAN Islands)

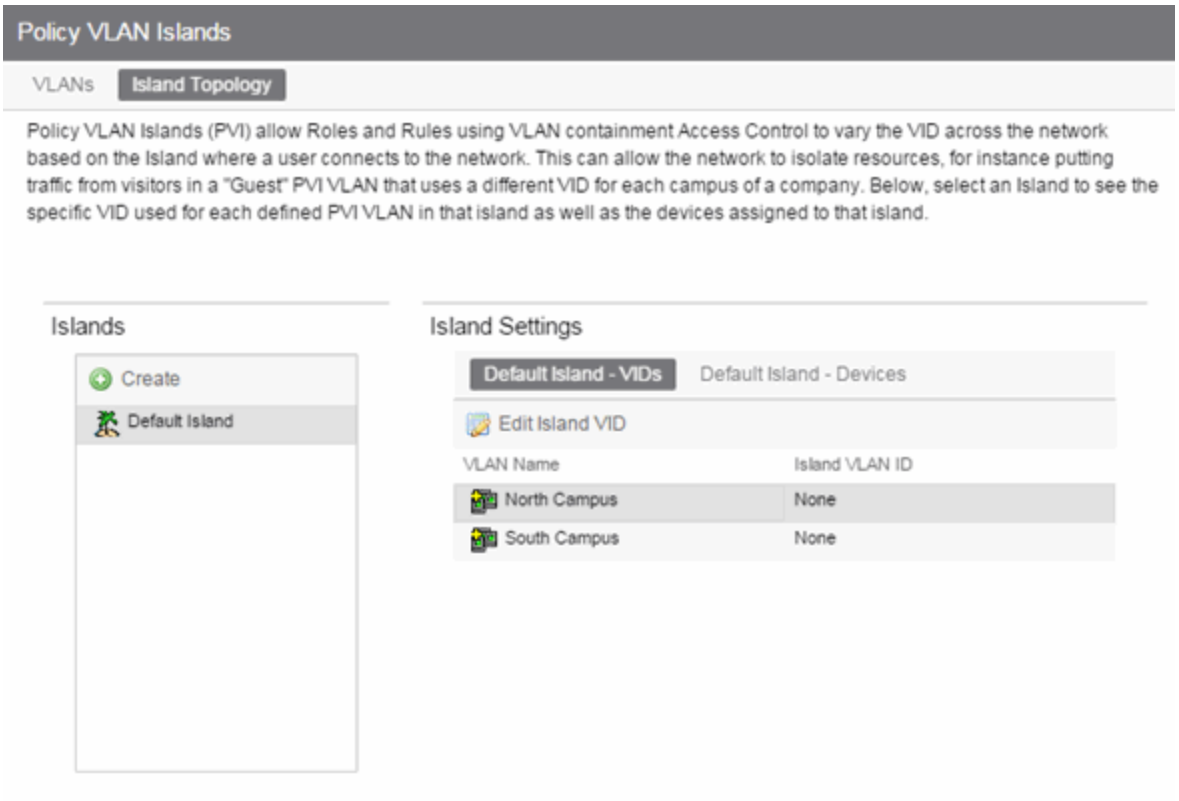
This tab displays a table of information about the Policy VLAN Islands, which shows the VIDs used in the selected island for all defined PVI VLANs. To access this tab, select the Policy VLAN Islands node in the tree of the Access Control Configuration view, and select the Island Topology tab on the right panel.

The **Island Topology** tab provides two sub-tabs:

- (Island) - VIDs Tab
- (Island) - Devices Tab

(Island) - VIDs Tab

This tab provides information on VIDs assigned to specific islands. When an island is selected, the VIDs tab shows all VIDs for the defined PVI VLANs that will be used for that island.



Islands

Name of all defined PVI islands. Select an island to see the VIDs and devices associated with that Island.of the VLAN island in which the Island VLAN is being used.

VLAN Name

Shows the defined PVI VLANs in the Domain. Unlike global VLANs, PVI VLANs are not created by the Policy tab during enforce. It is left to the user to configure these on the device(s) externally. The Policy tab only associates the appropriate VIDs to the rules during enforce.

Island VLAN ID

Shows the VID used for this PVI VLAN in this Island.

Edit Island VLAN ID

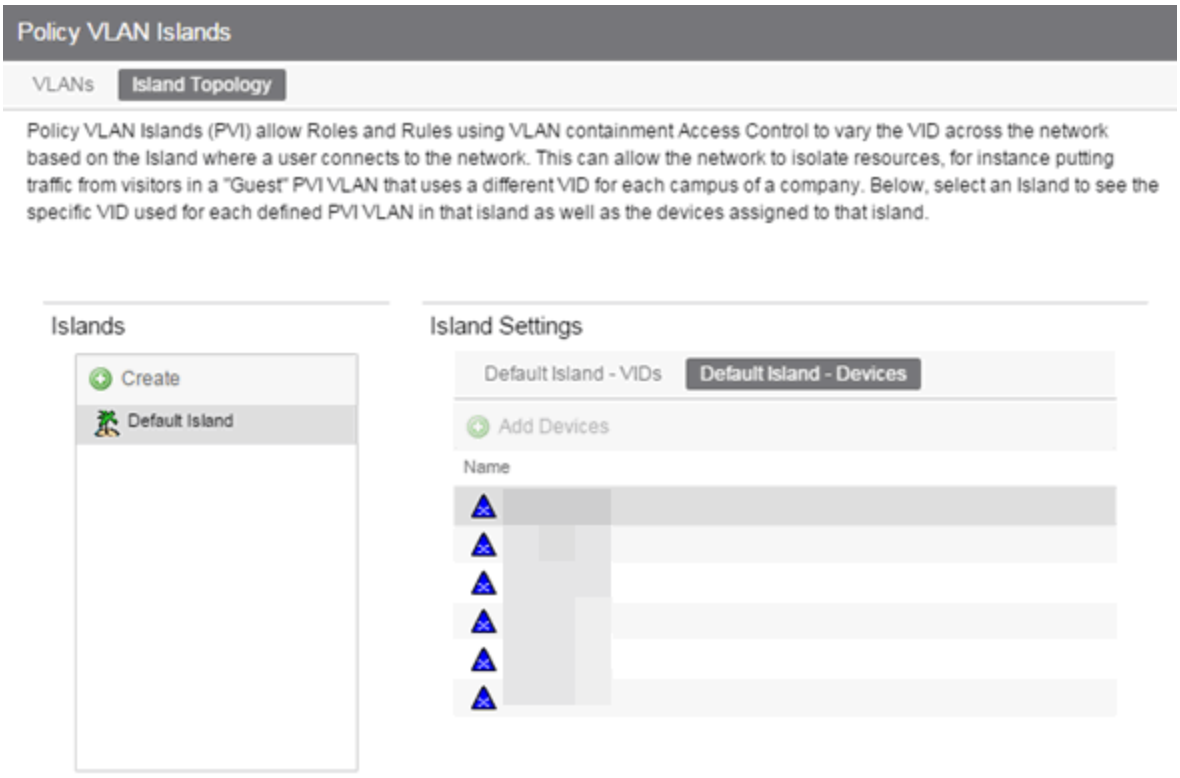
Selecting an island in the table and selecting this button opens the Edit Island VLAN ID window, where you can change the VID for the Island VLAN.

Create

Opens the Create VLAN Island dialog. For more information, see Creating a VLAN Island.

(Island) - Devices Tab

This tab displays the devices that are part of a Policy VLAN Island. To see a menu of options for a device in the table, right-click the device.



Create

Opens the Create VLAN Island dialog. For more information, see Creating a VLAN Island.

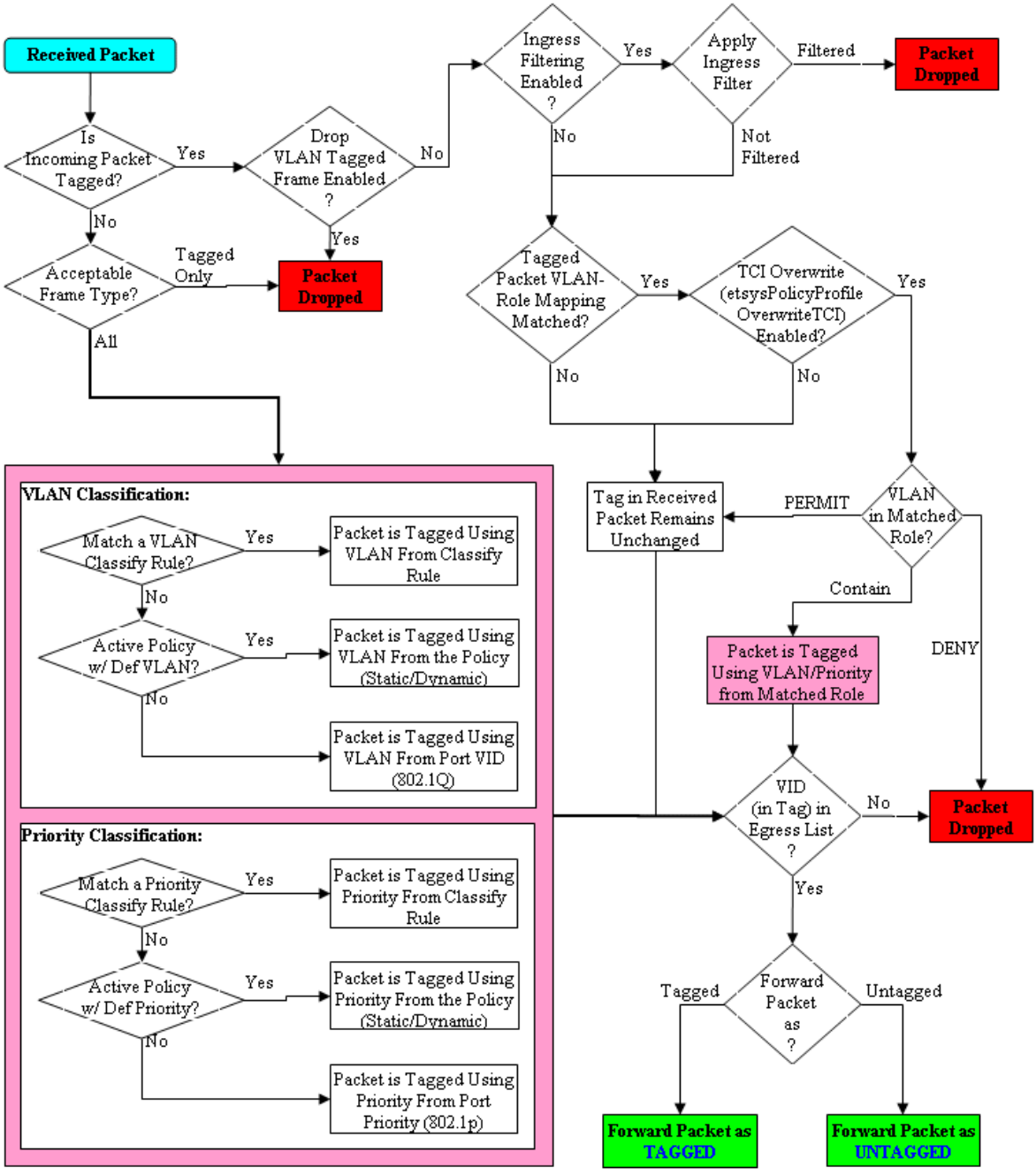
Name

The device's IP address.

Add Devices

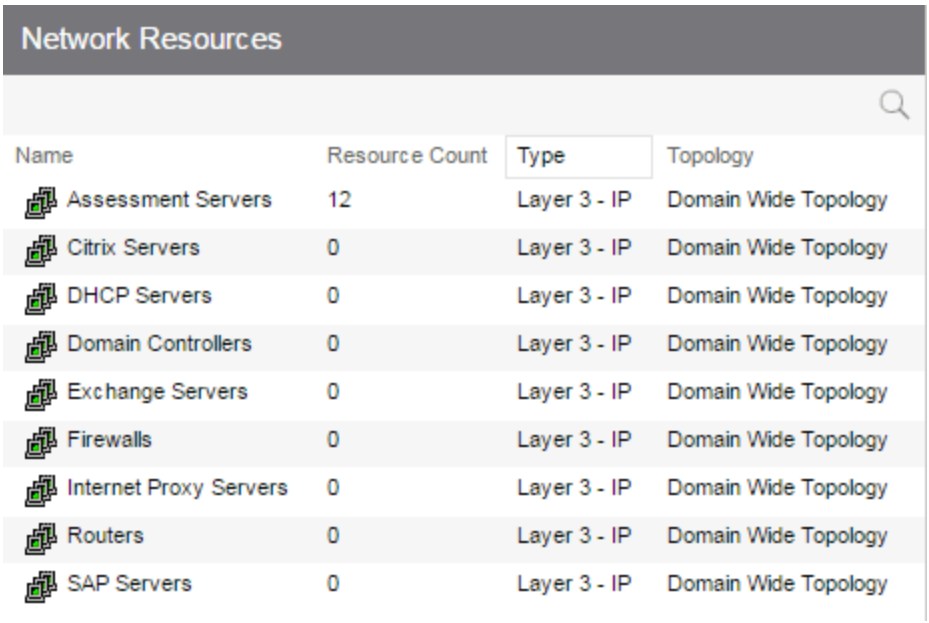
Opens a separate dialog to add devices to specific Islands. For more information, see Add/Remove Devices window.

Packet Flow Diagram



Network Resources Tab Overview

The **Network Resources** tab displays a table of information about all the network resources in the current domain. To access this tab, select the **Network Resources** > **Network Resources** left-panel tab on the **Policy** tab. The Details View is displayed in the right panel. Right-click a network resource to rename or delete it. See How to Create a Network Resource for more information on topologies and islands.



Name

Name of the network resource group.

Resource Count

The number of addresses added to the network resource.

Type

The network resource type:

- Layer 2 MAC - Define a group of network resource MAC addresses.
- Layer 3 IP - Define a group of network resource IP addresses.

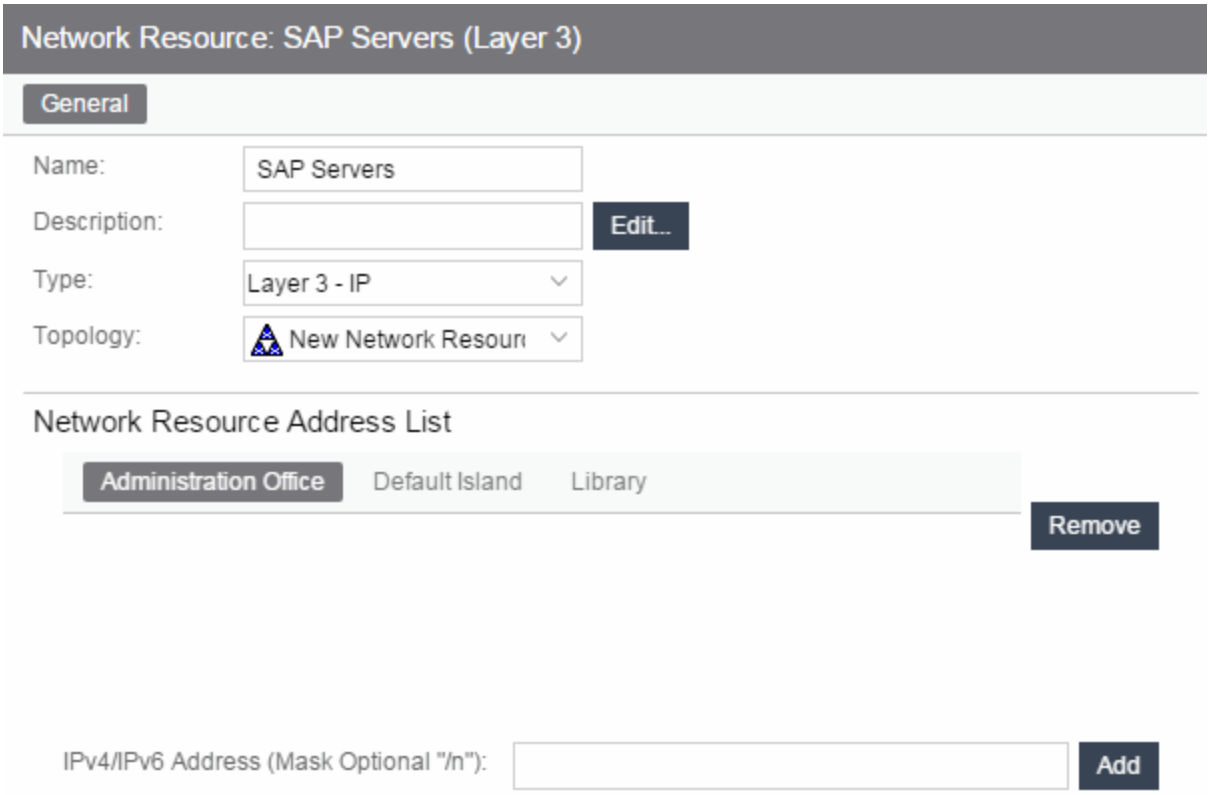
Topology

The network resource topology for this group.

Network Resource Group General Tab

This tab lets you configure a network resource group, which is a group of network resource devices associated with an Automated service. You configure the group by selecting a network resource type (MAC or IP) and typology, and then creating a list of MAC or IP addresses for the resources that are part of the group. When a network resource group is defined, you can associate it with the desired Automated service (see How to Create a Service for more information).

To access this tab, select a network resource group in the **Network Resources** left-panel tab of the **Policy** tab.



Name

Name of the network resource group selected in the left panel.

Description

Use the **Edit** button to open a window where you can add or modify a description for the network resource group.

Type

Select the network resource type:

- Layer 2 MAC - Define a group of network resource MAC addresses.
- Layer 3 IP - Define a group of network resource IP addresses.

Topology

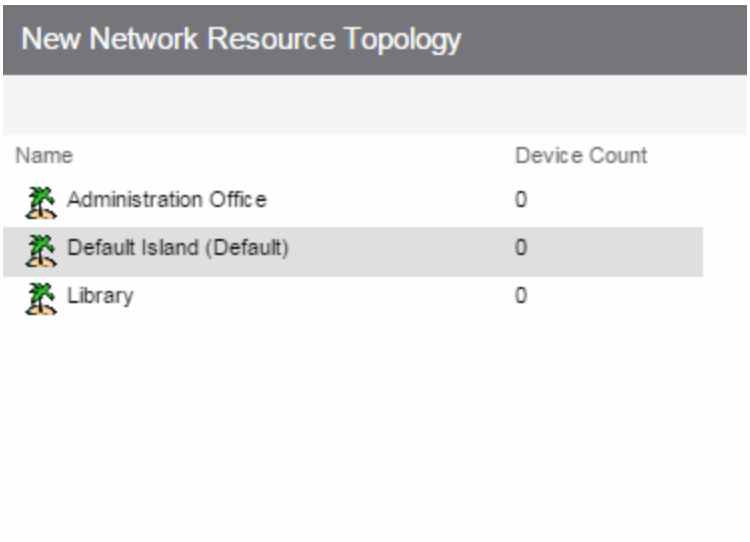
Use this drop-down list to select a network resource topology for this group. Use the configuration menu button on the right to add a new topology or edit an existing topology.

Network Resource Address List

Lists the addresses included in the selected network resource. Use the address field (IPv4 or IPv6, depending on the selected type) and select the **Add** button to add a new resource to the list.

Network Resource Topology Tab

This tab displays when you select a Network Resource Topology in the left panel of the **Network Resources** tab. It displays a list of the islands defined for the topology and the number of devices assigned to each island. See How to Create a Network Resource for more information on topologies and islands.



Name

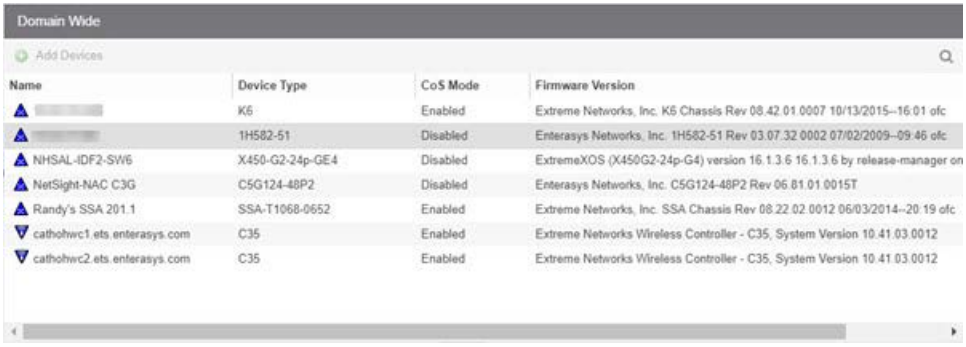
Name of the topology island.

Device Count

The number of devices included in that island.

Network Resource Topology Island Domain Wide

The **Domain Wide** tab displays a table of information about all the devices in an island within the network resource topology selected in the left panel. To access this tab, select a network resource island in a network resource topology on the **Network Resources** > **Network Resource Topologies** left-panel tab on the **Policy** tab. The Domain Wide view is displayed in the right panel. To see a menu of options available for a device, right-click the device.



Name
Name of the device, or its IP address if it does not have a display name.

Device Type
Indicates the type of device. Certain devices can be listed as "Authentication Only" (supports 802.1X and RFC 3580 only; does not support Policy).

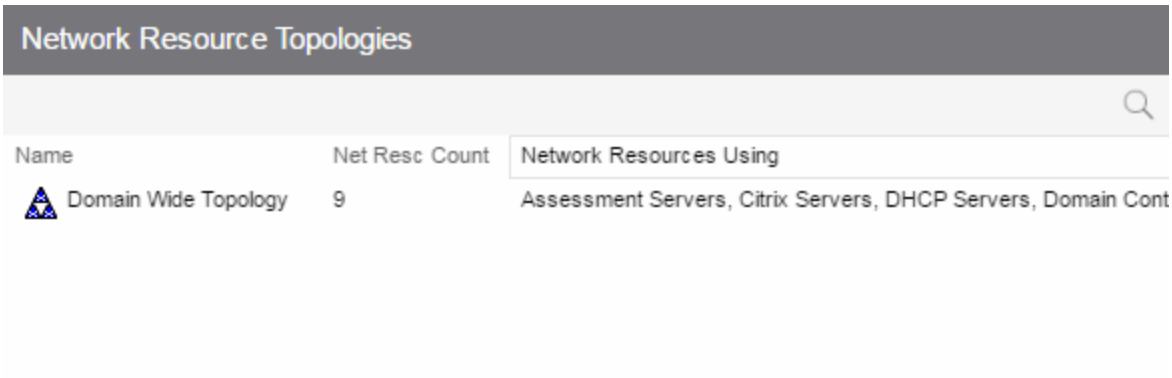
CoS Mode
Shows whether the Class of Service mode has been enabled or disabled on the device.

Firmware Version
Shows the current firmware revision for this device.

Add Devices Button
Select the **Add Devices** button to add devices to the network resource topology.

Details View (Network Resource Topologies Folder)

This tab displays when you select Network Resources > Network Resource Topologies in the left panel of the **Policy** tab. It displays a table of information about the network resource topologies configured in the current domain. See How to Create a Network Resource for more information on topologies.



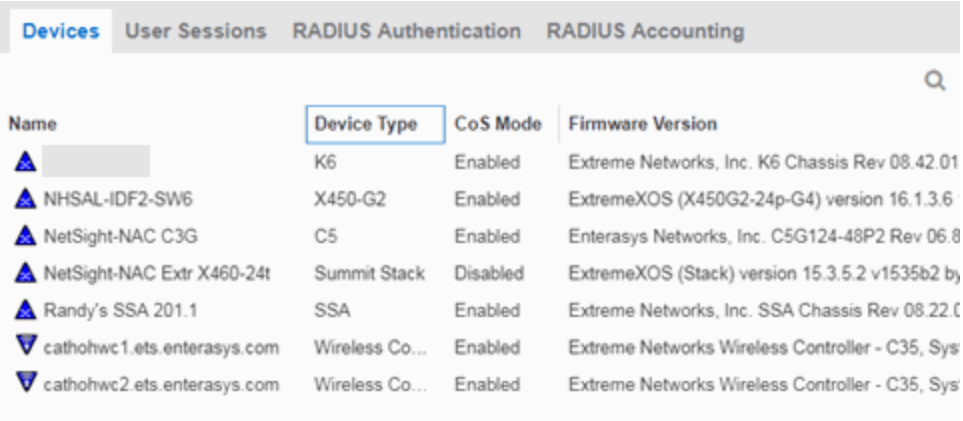
Name
Name of the network resource topology.

Net Resc Count
The number of network resource groups using this topology.

Network Resources Using
The names of the network resource groups using this topology.

Devices (Devices)

The **Devices** tab displays a table of information about all the devices in the current domain. To access this tab, select the **Devices/Port Groups > Devices** left-panel tab on the **Policy** tab. The Details View is displayed in the right panel. To see a menu of options available for a device, right-click the device.



Name
Name of the device, or its IP address if it does not have a display name.

Device Type
Indicates the type of device. Certain devices can be listed as "Authentication Only" (supports 802.1X and RFC 3580 only; does not support Policy).

CoS Mode
Indicates whether Class of Service is enabled or disabled on the device.

Firmware Version
Shows the current firmware revision for this device.

User Sessions (Devices)

The device **User Sessions** panel displays information related to end user login sessions for a device.

This tab can be accessed in a variety of ways:

1. Select a device in the left-panel **Devices** tab, then select the **User Sessions** tab in the right panel.
2. Select the My Network navigation tree in the left panel, select a device in the Devices list, and right-click the device or open the tools menu and select **View** > **User Sessions**.
3. Open the **Control** > **Policy** tab, select **Devices** in the left panel, and select the **User Sessions** tab in the right panel.

User Sessions Tab

This tab displays information about each login session for the ports on the device, including the current values being collected for a session still in progress, or the final values for the last valid session when there is no session currently active.

Checking the **Show Only Active Sessions** checkbox displays only your active sessions. Deselect the checkbox to display all entries. Active sessions applied to traffic are listed in blue text. Active sessions not being applied are listed in green text.

Some devices support multiple authentication sessions simultaneously per interface. This enables a single user to authenticate via 802.1X, Web-Based, MAC, and CEP all at the same time. However, only one authentication type per interface can be *applied* at a single time. The multi-user authentication type precedence (configured on the device Authentication tab) determines which type is applied. The applied session is the one that provides the role and traffic classification information. The remaining non-applied sessions will only be used if the currently applied session is terminated. For example, if a user authenticates on a port that has multi-user authentication enabled (802.1X, Web-Based, and MAC) the active/applied session will be displayed in blue text and the other two sessions will be in green text. Another example would be if the user authenticates using the MAC authentication type but MAC authentication is disabled on the port, the session would be listed in green text. For devices that do not support multi-authentication, by definition the active session is also applied.

NOTE: Devices configured for multi-user authentication always list *only* active sessions even if the **Show Only Active Session** checkbox is deselected.

Session entries are collected up to the maximum permitted. When the maximum is reached, the oldest session entries are replaced with newer ones. The exception to this is the RoamAbout R2, where older session data is not kept.

For devices that support one authenticated user per port, only one user/current role per port appears in the table. For devices that support multiple authenticated users per port, all users authenticated on its ports are listed in the table, along with the roles under which they are authenticated.

Session Status
The status of the device.

Switch IP
The IP address or name of the device.

Switch Port
A description of the port.

Switch Alias
The alias (ifAlias) for the interface, is one is assigned.

Type
The authentication type of this login session: Web-Based, 802.1X, MAC, CEP, Quarantine, Auto Tracking, or Role Override. If Role Override is displayed, it signifies that a rule has been applied to the port, overriding the user's current role with a different role.

- **Role Override (MAC)** signifies that a MAC address rule has been applied to the port, overriding the Default role or any authenticated role assigned to the end user.

- **Role Override (IP)** signifies that an IP address rule has been applied to the port, overriding the Default role or any authenticated role assigned to an end user authenticated with Single User 802.1X. An IP Address rule will **not** override the authenticated role for any authentication type other than Single User 802.1X.

MAC Address
The MAC address of the remote user of this login session.

IP Address
For web-based authentication sessions, this column displays the IP address of the remote user of this login session.

Hostname
The hostname of the remote user of this login session. To determine the hostname, the **Policy** tab takes the IP address (when available) and uses the hostname cache on the ExtremeCloud IQ Site Engine server. The hostname cache must be explicitly enabled by selecting the **Enable Name Resolution** checkbox in the Administration > Options > tab (by default, this option is disabled).

Role
The role under which the user authenticated on the port. If the user authenticated via RFC 3580 VLAN Authorization, this column displays the role the VLAN is mapped to (configured through Authentication-based VLAN to Role Mapping). If VLAN to Role mapping has not been configured, the port's Default role is displayed (if there is one); otherwise, the column displays "N/A."

Default VID Source
When traffic received on a port doesn't match any rules, it is assigned the default VLAN ID. This column indicates the source for the default VLAN ID:

- Policy Default Access Control - The role assigned to the session defines the default VLAN ID via its Default Access Control.
- PVID - If the role assigned to the session has no Default Access Control specified, then the 802.1Q PVID for the port is assigned to the traffic.

Default VID
Displays the VLAN ID that comes from the source listed in the Default VLAN ID Source column: Permit (4095), Deny (VLAN ID #), or Contain (VLAN ID #).

RFC3580 VID
If the user authenticated via RFC 3580 VLAN Authorization, this is the VLAN ID that was returned from the RADIUS server. A VLAN ID value of 0 indicates that no VLAN was assigned. If VLAN authentication is not supported on the device, this column will display "N/A."

VLAN Oper Egress
The modification that will be made to the VLAN egress list for the VLAN ID returned by the RADIUS server, if the user authenticated via RFC 3580 VLAN Authorization.

- None - No modification to the VLAN egress list will be made.
- Tagged - The port will be added to the list with the egress state set to Tagged (frames will be forwarded as tagged).
- Untagged - The port will be added to the list with the egress state set to Untagged (frames will be forwarded as untagged).
- Dynamic - The port will use information returned in the RADIUS response to modify the VLAN egress list.

If VLAN authentication is not supported on the device, this column will display "N/A."

Start Time
The time and date when the login session started.

Duration
The duration of the user's login session, in the format D + HH:MM:SS.

Auth Status
The authentication status of the login session. Possible values are:

- Authentication Successful
- Authentication Failed
- Authentication in Progress
- Authentication Server Timeout
- Authentication Terminated

Terminate Cause
The reason the login session terminated. For web-based authentication, the possible values are:

- Administratively Terminated
- Authorization Revoked
- Link Down
- Not Applicable
- Port Disabled
- Unknown Termination Cause
- User Logged Out

For 802.1X authentication, the possible values are:

- Authorization Revoked
- Client Restarted
- Link Down (or Lost Carrier)

- Not Applicable
- Port Disabled
- Port Reinitialized
- Reauthentication Failed
- Unknown Termination Cause
- User Logged Out

Authentication Server

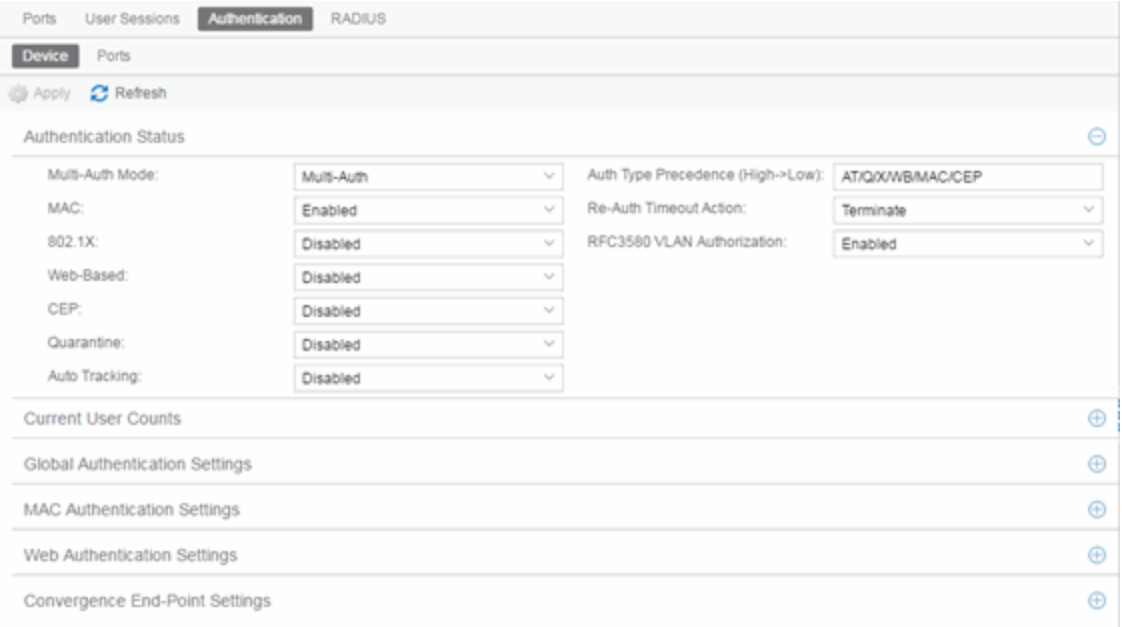
The RADIUS server that authenticated the session.



Authentication (Device)

The device **Authentication** tab enables you to configure and change the authentication settings on the selected device. Authentication must be configured and enabled on the device in order for individual port authentication settings to take effect (see How to Configure Ports).

To access this tab, select a device in the left panel under Devices > Devices, then select the **Authentication** tab in the right panel.



Apply

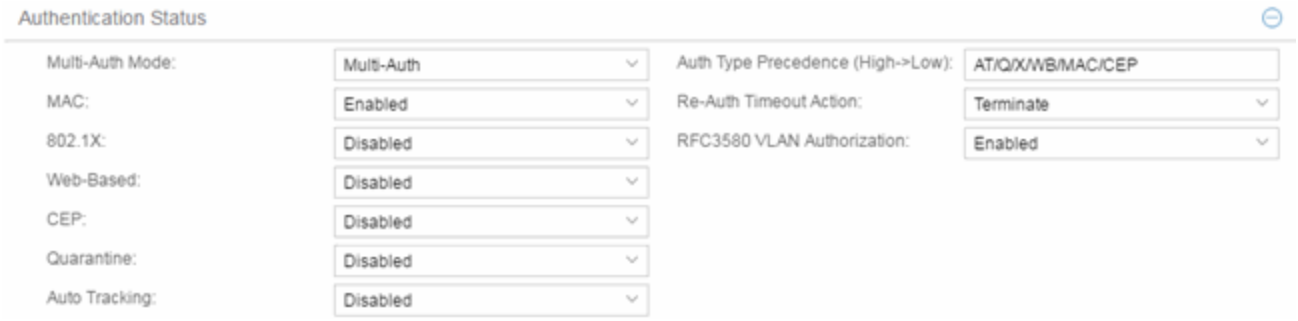
Select this button to save any changes you made to the **Authentication** tab.

Refresh

Select this button to update the tab with your changes.

Authentication Status

Use this section to select the authentication mode and types used on the device.



Use the fields on the left side of this section to select the appropriate single- or multi-user authentication types. Only options supported by the selected device are available for selection. Some devices support multiple authentication types and multiple users (Multi-User Authentication) per port, while others are restricted to only one or two authentication types and single users per port. Refer to the Firmware Support matrix for information on the authentication types supported by each device type.

WARNING: Switching Authentication Types, or changing the Authentication Status from Enabled to Disabled, logs off any currently authenticated users.

Auth Type Precedence (High->Low)

This displays the order in which the authentication types are attempted on the device, with the authentication type on the left having the highest precedence (attempted first). You can edit the precedence order by selecting the field. In the Edit Precedence window, select the authentication type you want to position, and use the **Up** and **Down** buttons to arrange the types in the desired order of precedence.

WARNING: Leave the default precedence, if possible. Changing the Quarantine precedence to be lower than any other type or changing the Auto Track precedence to be higher than any other type can cause problems.

Re-Auth Timeout Action

This setting defines the action for sessions that need to be re-authenticated if the RADIUS server re-authentication request times out. Select the **Terminate** option to terminate the session or the **None** option to enable the current session to continue without disruption.

Maximum Number of Users

This setting applies to devices with Multi-User as their configured authentication type. The maximum number of users that can be actively authenticated or have authentications in progress at one time on this device. You can specify the maximum number of users per port on the port's Port Properties Authentication Configuration tab.

RFC3580 VLAN Authorization

This enables you to enable and disable RFC 3580 VLAN Authorization for the selected device. RFC 3580 VLAN Authorization must be enabled on devices in networks where the RADIUS server is configured to return a VLAN ID when a user authenticates.

When RFC 3580 VLAN Authorization is enabled:

- devices that do **not** support policy tag packets with the VLAN ID.
- devices that support both policy and Authentication-Based VLAN to Role Mapping classify packets according to the role to which the VLAN ID maps.

Current User Counts

This section enables you to specify the maximum number of users on the device and per authentication type.



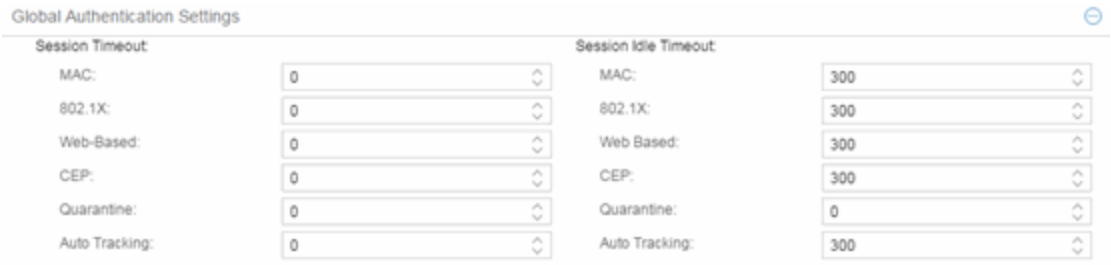
Current Number of Users

For devices with Multi-User as their configured authentication type. The current number of users that are actively authenticated or have authentications in progress, or that the device is keeping authentication termination information for. Any unauthenticated traffic on the port is not included in this count.

NOTE: On E1 and E6/E7 devices, if both 802.1X and MAC authentication are enabled, it is possible for the device to receive a start or response 802.1X packet while a MAC authentication is in progress. If this happens, the device immediately terminates the MAC authentication, and the 802.1X authentication proceeds to completion. Regardless of the success of the 802.1X login attempt, no new MAC authentication logins can occur on the port until 1) the link is toggled; 2) the user executes an 802.1X logout; or 3) the 802.1X session is terminated administratively.

Global Authentication Settings

This section lets you set session timeout and session idle timeout values for each authentication type.



Session Timeout

This setting represents the maximum number of seconds an authenticated session can last before automatic termination of the session. A value of zero indicates that no session timeout applies. This value can be superseded by a session timeout value provided by the authenticating server. For example, if a session is authenticated by a RADIUS server, that server can send a session timeout value in its authentication response.

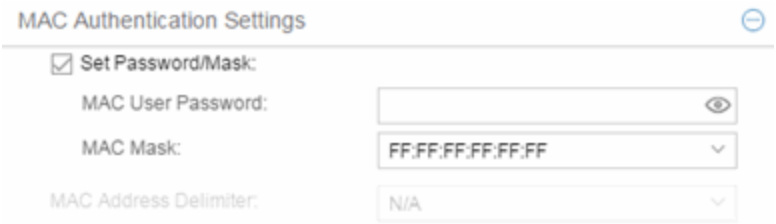
NOTE: Non-zero values are rounded to the nearest non-zero multiple of 10 by the device.

Session Idle Timeout

This displays the maximum number of consecutive seconds an authenticated session can be idle before ExtremeCloud IQ Site Engine automatically terminates the session. A value of zero indicates that no idle timeout applies. This value can be superseded by an idle timeout value provided by the authenticating server. For example, if a session is authenticated by a RADIUS server, that server can send an idle timeout value in its authentication response.

MAC Authentication Settings

This section enables you to set up the MAC password for MAC authentication. In order for MAC authentication to work, you must also configure the RADIUS server with the MAC password as well as the MAC addresses which are permitted to authenticate.



Set Password/Mask

Select this checkbox to set a password and mask for MAC authentication.

MAC User Password

The password passed to the RADIUS server for MAC authentication.

MAC Mask

You can select a mask to provide a way to authenticate end-systems based on a portion of their MAC address. For example, you could specify a mask that would base authentication on the manufacturers ID portion of the MAC address. The MAC Mask is passed to the RADIUS server for authentication after the primary attempt to authenticate using the full MAC address fails.

MAC Address Delimiter

The character used between octets in a MAC address:

- **None** — No delimiter is used in the MAC address (e.g. xxxxxxxxxxxx).
- **Hyphen** — A hyphen is used as a delimiter in the MAC address (e.g. xx-xx-xx-xx-xx-xx).

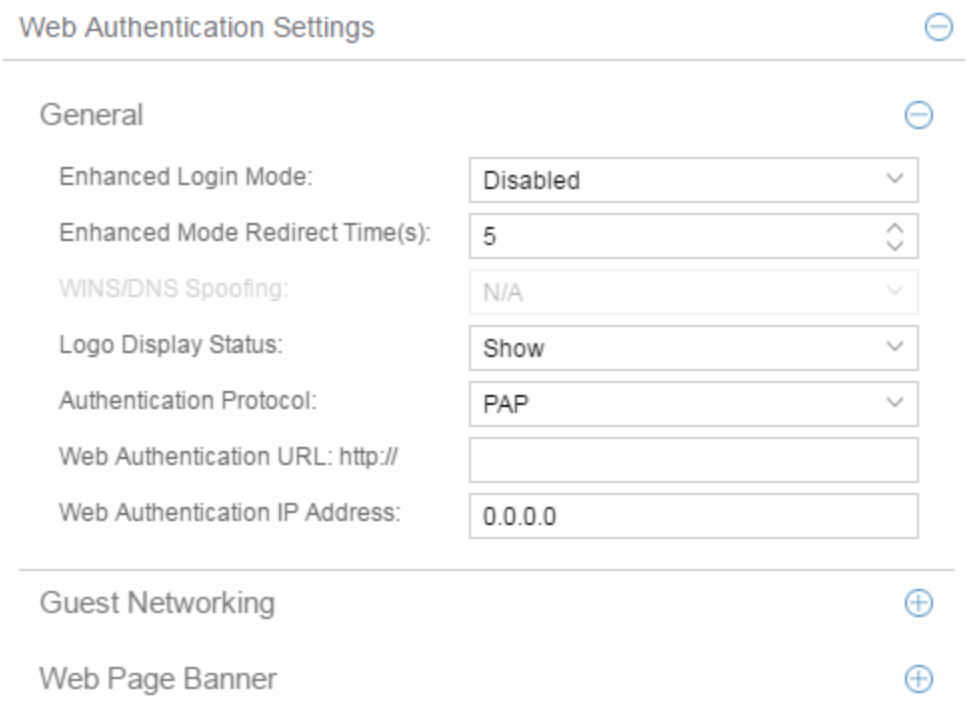
Web Authentication Settings

For users of web-based authentication, this tab lets you specify web authentication parameters using three sections:

- General
- Guest Networking
- Web Login

General

The General section lets you specify the URL of the authentication web page and the IP address of the system where it resides. It also lets you enable certain web authentication features, such as Enhanced Login Mode, on devices that support those features.



Enhanced Login Mode

Enabling the Enhanced Login Mode causes the authentication web page to be displayed regardless of whether the URL or IP address entered into the browser by the end user is the designated Web Authentication URL or IP address. This option is grayed out if the device does not support the mode.

Enhanced Mode Redirect Time(s)

This setting applies for devices with Enhanced Login Mode enabled. It specifies the amount of time (in seconds) before the end-user is redirected from the authentication web page to their requested URL.

An end-system using DHCP requires time to transition from the temporary IP address issued by the authentication process to the official IP address issued by the network. **Enhanced Mode Redirect Time** specifies the amount of time permitted for the end-system to complete this process and begin using its official IP address.

For example, if an end-user (in **Enhanced Login Mode** and a **Redirect Time** of **30 seconds**) enters the URL of "http://ExtremeNetworks.com", the user is presented the authentication web page. When the user successfully authenticates into the network, the user sees a login success page that displays "Welcome to the Network. Completing network connections. You will be redirected to http://ExtremeNetworks.com in approximately 30 seconds."

WINS/DNS Spoofing

This setting enables you to enable and disable WINS/DNS spoofing for the selected device. Spoofing enables the end-user to resolve the Web Authentication URL name to the IP address

using WINS/DNS. The default is Disabled. This option is grayed out if not supported by the device.

Logo Display Status
Specifies whether the Extreme Networks logo is displayed or hidden on the authentication web page window. This option is grayed out if not supported by the device.

Authentication Protocol
This setting is the authentication protocol being used (PAP or CHAP). PAP (Password Authentication Protocol) provides an automated way for a PPP (Point-to Point Protocol) server to request the identity of user, and confirm it via a password. CHAP (Challenge Handshake Authentication Protocol), the more secure of the two protocols, provides a similar function, except that the confirmation is accomplished using a challenge and response authentication dialog.

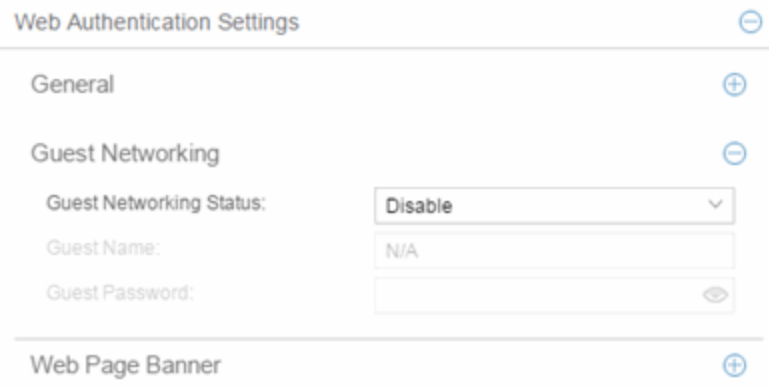
Web Authentication URL
This is the URL for your authentication web page. Users wishing to receive network services access the web page from a browser using this URL. The **http://** is supplied. Alphabetical characters, numerical characters and dashes are permitted as part of the URL, but dots are not. The URL needs to be mapped to the Web Authentication IP address in DNS or in the hosts file of each client. It must be resolvable via DNS/WINS, either on the device or at corporate, assuming the Web Authentication mapping has been set up on the corporate DNS/WINS service. This option is grayed out if not supported by the device.

Web Authentication IP Address
This is the IP address of your authentication web page server. If you have specified a Web Authentication URL, the IP address needs to be mapped to the URL in DNS or in the host file of each client.

Guest Networking

The **Guest Networking** section lets you configure guest networking, a feature that enables any user to access the network and obtain a guest policy without having to know a username or password. The user accesses the authentication web page, where the username and password fields are automatically filled in, enabling them to log access as a guest. If the user does not want to log in as a guest, they can type in their valid username and password to log in.

NOTE: Guest networking is designed for networks using web-based authentication, with port mode set to Active/Discard.



Guest Networking Status

Use the drop-down list to specify guest networking status:

- **Disable** — Guest networking is unavailable.
- **Local Auth** — Guest Networking is enabled. The user accesses the authentication web page where the username field is automatically filled in with the specified Guest Name. When the user submits the web page using this guest name, the default policy of that port becomes the active policy. The port mode must be set to Active/Discard mode.
- **RADIUS Auth** — Guest Networking is enabled. The user accesses the authentication web page, where the username field is automatically filled in with the specified Guest Name, and the password field is masked out with asterisks. When the user submits the web page using these credentials, the value of the Guest Password is used for authentication. Following successful authentication from the RADIUS server, the port applies the policy (role) returned from the RADIUS server. The port mode must be set to Active/Discard mode.

Guest Name

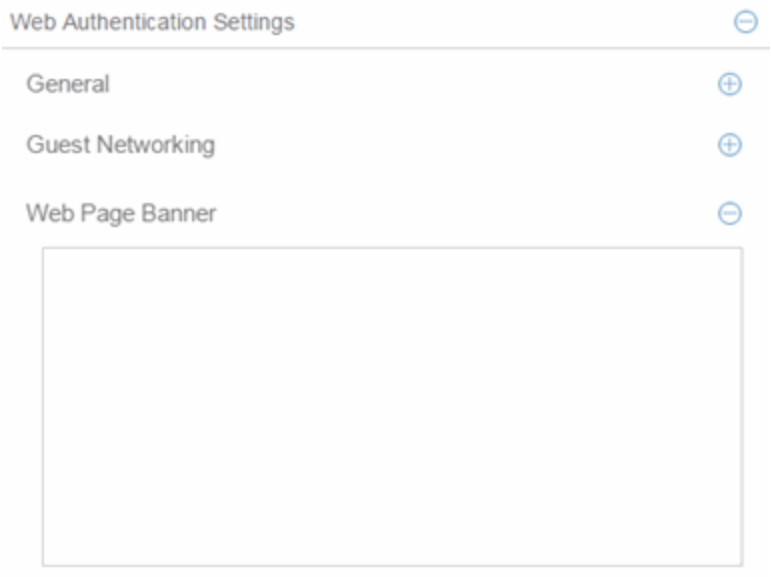
The username that Guest Networking uses to authenticate users. The guest name is displayed automatically on the authentication web page. If the user does not want to log in as a guest, they can type in their valid username to override the guest username.

Guest Password

The password that Guest Networking uses to authenticate users when RADIUS Auth is selected.

Web Page Banner

The Web Page Banner section enables you to customize the banner end users see at the top of the authentication web page and set a Redirect Time, if applicable.



Web Page Banner

Use this area to create a banner end users see at the top of the authentication web page. For example, you might include your company name and information on what to do if the user has questions or problems. Because this banner also appears in messages that occur during successful login and failed authentication, as well as on the "Radius Busy" screen, it is not appropriate to include "Welcome to [Your Company]" in the banner.

The **Default** button enables you to reset the banner to default text provided in a text file (pwa_banner.txt). Initially, the default banner text is the Extreme Networks contact information. However, you can customize the text for your network by editing the pwa_banner.txt file, located in the top level of the Policy Manager install directory. Then, when you select the Default button, the new text will be displayed in the Web Page Banner area.

Convergence End-Point Settings

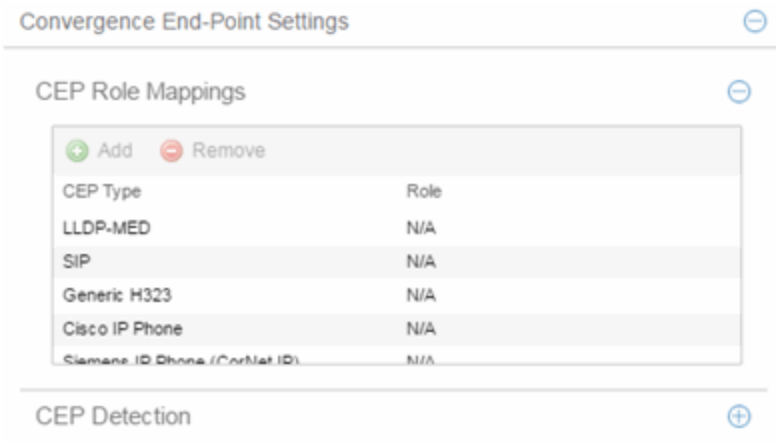
This section provides a way to identify Convergence End-Points (IP phones) connecting to the device, and apply a role to the end-point based on the type of end-point detected. The CEP Detection section lets you create detection rules for identifying the end-points, and the CEP Role Mappings section lets you map a role to each CEP product type.

In addition to configuring CEP on the device, you must also enable CEP protocols on each port using the CEP Access section in the Port Authentication Tab. After you have configured CEP on the device and each port, you can monitor CEP usage on the Port Usage Tab (Port) or Port Usage Tab (Device).

CEP Role Mappings

This section lets you select the CEP product types supported on the device, and map a role for each type. Then, when a convergence end-point (such as an IP phone) connects to the network, the device

identifies the type of end-point (using CEP detection rules) and applies the assigned role.



CEP Type
Lists the CEP types supported by the device.

Role
Lists the role mapped to each **CEP Type**.

Add
Select a CEP Type and select the **Add** button to open the Add Role Mapping window, where you can select a role for the selected **CEP Type**. Your selections are added to the CEP Role Mappings list.

Remove
Select the **CEP Type** and select **Remove** to remove the **CEP Type** in the CEP Role Mappings list.

CEP Detection Tab

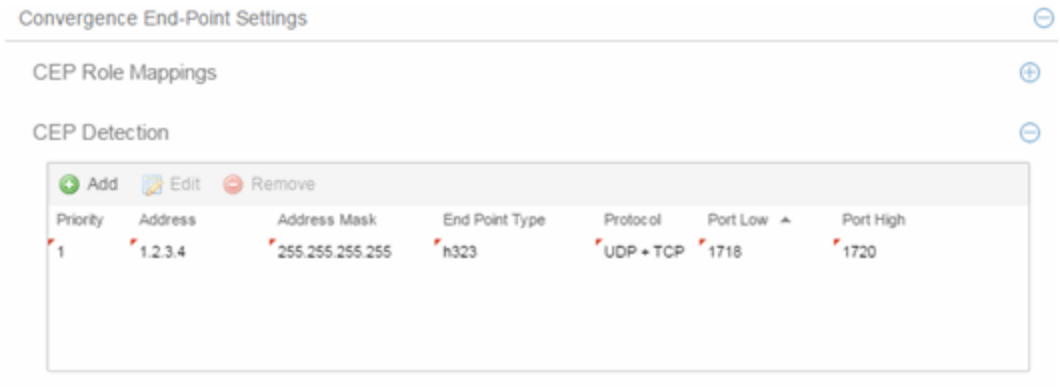
Use this section to create CEP detection rules used to determine if a connecting end-system is a CEP device and the type of CEP device. This enables ExtremeCloud IQ Site Engine to assign the appropriate role to the port based on the type of CEP device detected.

NOTE: CEP detection rules apply only to Siemens, H.323, and SIP (Session Initiation Protocol) phone detection. Cisco detection uses CiscoDP as its detection method.

CEP detection rules are based on two detection methods:

- TCP/UDP Port Number detection — Many CEP vendors use specific TCP/UDP port numbers for call setup on their IP phones. You can create detection rules that identify CEP devices based on specific TCP/UDP port numbers. By default, Siemens Hi-Path phones are detected on TCP/UDP port 4060.
- IP Address detection — H.323 phones use a reserved IP multicast address and UDP port number for call setup. You can create detection rules to detect an IP phone based on its IP

address in combination with an IP address mask. By default, H.323 phones are detected using the multicast address 224.0.1.41 and the TCP/UDP ports 1718, 1719, and 1720. SIP phones are detected using the multicast address 224.0.1.75 and the TCP/UDP port 5060. H.323 and SIP phones are also detected using only their respective multicast addresses without the TCP/UDP ports.



Priority

The rule priority with one (1) being the highest priority. The rule with the highest priority is used first, so it is recommended the highest priority be given to the predominate protocol in the network to provide for greater efficiency.

Address

If the rule is based on IP address detection, this field displays the IP address that incoming packets matched against. By default, H.323 uses 224.0.1.41 as its IP address, SIP uses 224.0.1.75 as its IP address, and Siemens has no IP address configured.

Address Mask

If the rule is based on IP address detection, this field displays the IP address mask against which incoming packets are matched.

End Point Type

Specifies the end-point type assigned (H.323, Siemens, or SIP) if incoming packets match this rule.

Protocol

If the rule is based on TCP/UDP port detection, this field displays the protocol type used for matching, using a port range defined with the Port Low and Port High values:

- UDP + TCP — Match the port number for both UDP and TCP frames.
- TCP — Match the port number only for TCP frames.
- UDP — Match the port number only for UDP frames.

Port Low

The low end of the port range defined for detection on UDP and/or TCP ports.

Port High

The high end of the port range defined for detection on UDP and/or TCP ports.

Add

Opens the Add/Edit CEP Detection Rule window where you can create CEP detection rules.

Remove

To remove a CEP detection rule, select the entry and select **Remove**.

Edit

To edit a CEP detection rule, select the rule and select **Edit**. The Add/Edit CEP Detection Rule window opens where you edit the rule's parameters. You can also double-click an entry in the table to open the edit window.

Add/Edit CEP Detection Rule

Use this window to add or edit CEP detection rules that are used to determine if a connecting end-system is a CEP device, and what type of CEP device it is. This allows Policy Manager to assign the appropriate role to the port based on the type of CEP device detected. Access the window from the CEP Detection sub-tab in the right-panel Device Authentication tab.

NOTE: CEP detection rules apply only to Siemens, H.323, and SIP (Session Initiation Protocol) phone detection. Cisco detection uses CiscoDP as its detection method.

CEP detection rules are based on two detection methods:

- TCP/UDP Port Number detection — Many CEP vendors use specific TCP/UDP port numbers for call setup on their IP phones. You can create detection rules that identify CEP devices based on specific TCP/UDP port numbers. By default, Siemens Hi-Path phones are detected on TCP/UDP port 4060.
- IP Address detection — H.323 phones use a reserved IP multicast address and UDP port number for call setup. You can create detection rules detect an IP phone based on its IP address in combination with an IP address mask. By default, H.323 phones are detected using the multicast address 224.0.1.41 and the TCP/UDP ports 1718, 1719, and 1720. SIP phones are detected using the multicast address 224.0.1.75 and the TCP/UDP port 5060. H.323 and SIP phones are also detected using only their respective multicast addresses without the TCP/UDP ports.



CEP Detection Settings

Priority

Enter the rule priority with one (1) being the highest priority. The rule with the highest priority is used first, so it is recommended the highest priority be given to the predominate protocol in the network to provide for greater efficiency.

IP Address

If the rule is based on IP address detection, enter the IP address against which incoming packets are matched. By default, H.323 uses 224.0.1.41 as its IP address, SIP uses 224.0.1.75 as its IP address, and Siemens has no IP address configured.

Address Mask

If the rule is based on IP address detection, enter the IP address mask against which incoming packets are matched.

End Point Type

Select the endpoint type (H.323, Siemens, or SIP) assigned to incoming packets that match this rule.

Protocol

If the rule is based on TCP/UDP port detection, select the UDP and/or TCP checkbox and define a port range with Port Low and Port High values:

- UDP and TCP — Match the port number for both UDP and TCP frames.
- TCP — Match the port number only for TCP frames.
- UDP — Match the port number only for UDP frames.

Port Low

Define the low end of the port range for detection on UDP and/or TCP ports.

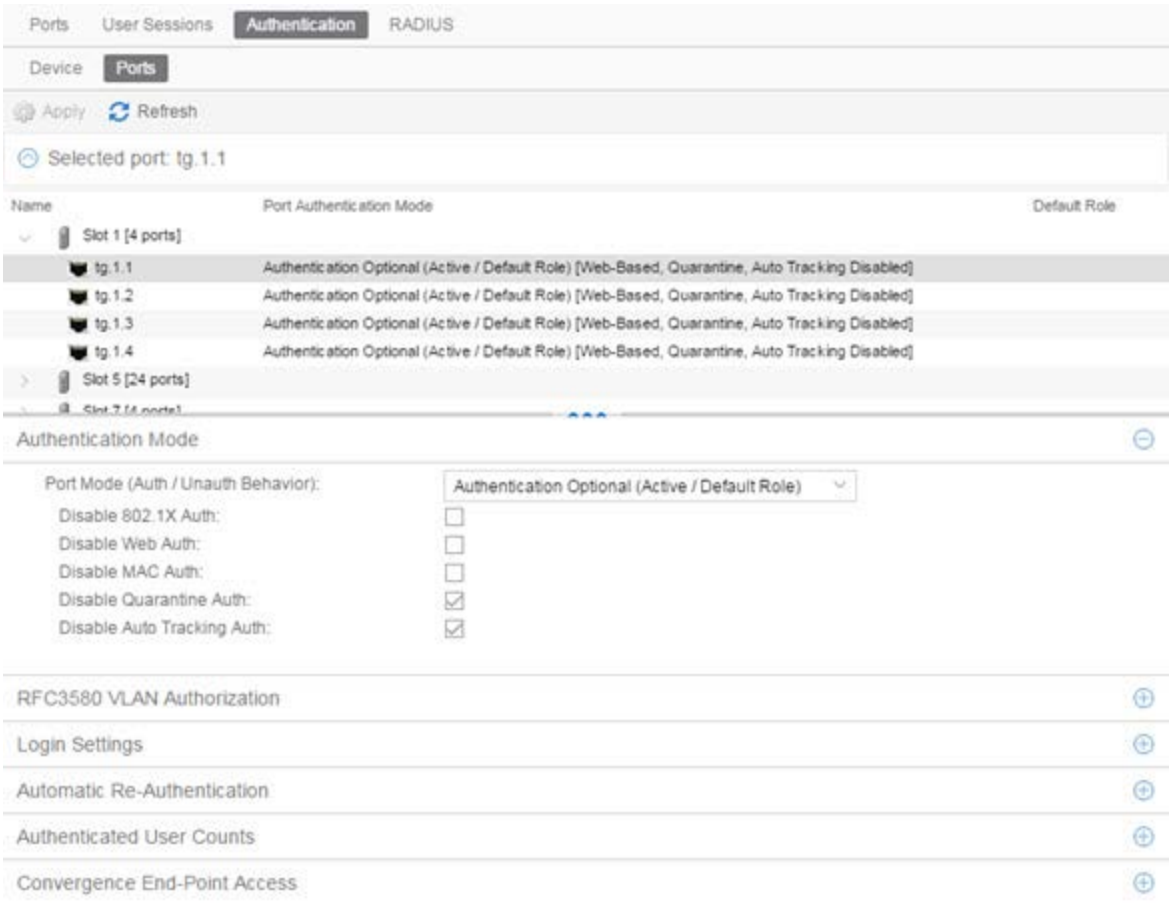
Port High

Define the high end of the port range for detection on UDP and/or TCP ports.

Ports (Authentication)

The **Ports (Authentication)** tab allows you to configure and change the authentication settings for a port. Authentication must be configured and enabled on the device in order for individual port authentication settings to take effect. Only those areas of the tab that relate to the authentication type configured on the device are available for editing.

To access the **Ports (Authentication)** tab, select a device in the left-panel **Devices** > **Devices** tab, then select **Authentication** > **Ports** in the right panel.



Select a port in the top section to display and configure the authentication settings for that port in the bottom of the window.

Select the **Apply** button at the top of the window to save changes to this tab.

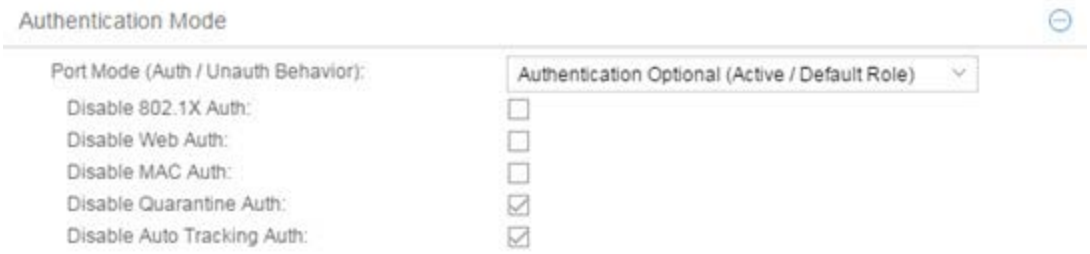
The Authentication Configuration tab has six sections:

- Authentication Mode
- RFC3580 VLAN Authorization

- Login Settings
- Automatic Re-Authentication
- Authenticated User Counts
- Convergence End-Point Access

Authentication Mode

This tab displays general authentication and port mode information about the port.



This area displays the current port mode for the port, and allows you to change the settings if desired. Port mode defines whether or not a user is required to authenticate on a port, and how unauthenticated traffic is handled. It is a combination of Authentication Behavior (whether or not authentication is enabled on the port), and Unauthenticated Behavior (whether unauthenticated traffic is assigned to the port's default role or discarded). See Port Mode for a complete description of each port mode.

In addition, this section provides checkboxes that allow you to disable a specific authentication type at the port level.

Port Mode (Auth/Unauth Behavior)

Select an option to specify whether or not authentication is enabled on the port. (See Port Mode for more information.)

NOTE: Authentication Behavior must be set to **Active** for authentication to be allowed using CEP Protocols.

Disable 802.1X Auth

Select this checkbox to disable 802.1X authentication at the port level. If the device is only configured with 802.1X authentication, selecting this checkbox results in the port Authentication Behavior being set to **Inactive**.

NOTE: For Single User 802.1X+MAC authentication with Active/Default Role as the selected port mode: Disabling 802.1X authentication also disables MAC authentication on the port. An end user connecting to the port is not able to authenticate via 802.1X or MAC. The port behaves as if Inactive/Default Role is the selected port mode.

Disable Web-Based Auth

Select this checkbox to disable web-based authentication at the port level. If the device is only configured with web-based authentication, selecting this checkbox results in the port Authentication Behavior being set to **Inactive**.

NOTE: For Multi-User Web-Based authentication with Active/Discard as the selected port mode: This checkbox is automatically selected because multi-user web-based authentication does not support the Active/Discard port mode.

Disable MAC Auth

Select this checkbox to disable MAC authentication at the port level. If the device is only configured with MAC authentication, selecting this checkbox results in the port Authentication Behavior being set to **Inactive**.

Disable Quarantine Auth

Select this checkbox to disable Quarantine authentication at the port level. If the device is only configured with Quarantine authentication, selecting this checkbox results in the port Authentication Behavior being set to **Inactive**.

Disable Auto Tracking Auth

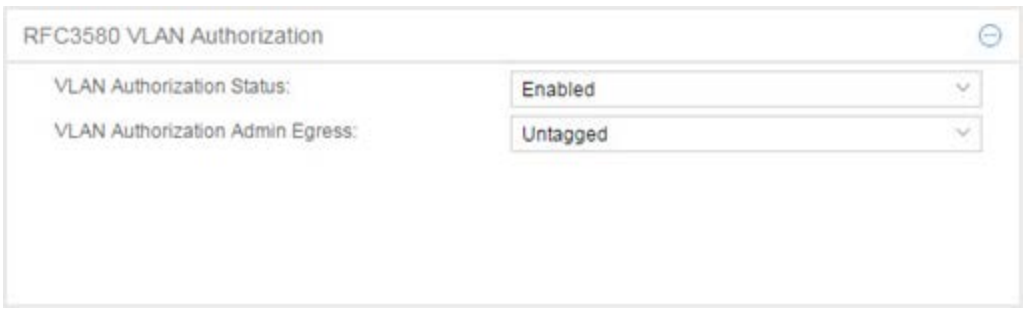
Select this checkbox to disable MAC authentication at the port level. If the device is only configured with Auto Tracking authentication, selecting this checkbox results in the port Authentication Behavior being set to **Inactive**.

RFC3580 VLAN Authorization

This section lets you enable or disable RFC 3580 VLAN Authorization on the port and specify an egress state. RFC 3580 VLAN Authorization must be enabled in networks where the RADIUS server has been configured to return a VLAN ID when a user authenticates. When RFC 3580 VLAN Authorization is enabled:

- ports on devices that do **not** support policy, will tag packets with the VLAN ID.
- ports on devices that do support policy and also support Authentication-Based VLAN to Role Mapping, will classify packets according to the role that the VLAN ID maps to.

You can also enable and disable VLAN Authorization at the device level using the device Authentication tab. If the device does not support RFC 3580, this tab will be grayed out.



VLAN Authorization Status

Allows you to enable and disable RFC 3580 VLAN Authorization for the selected port. This option is grayed out if not supported by the device.

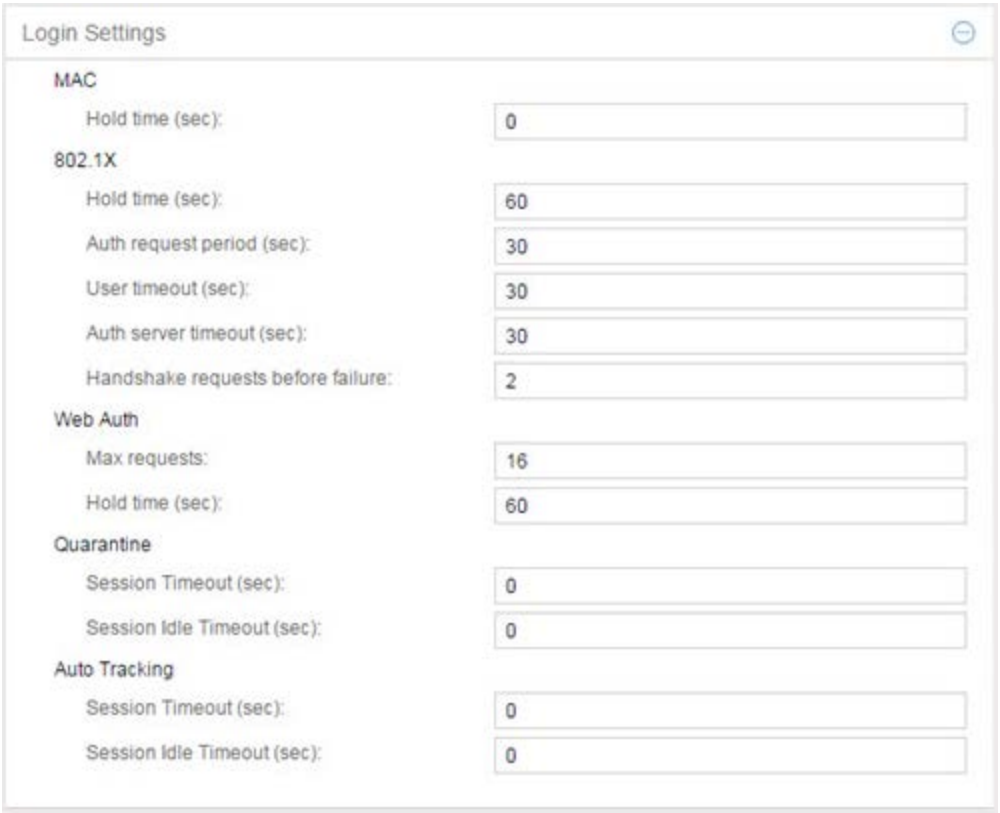
VLAN Authorization Admin Egress

Allows you to modify the VLAN egress list for the VLAN ID returned by the RADIUS server when a user authenticates on the port:

- None — No modification to the VLAN egress list is made.
- Tagged — The port is added to the list with the egress state set to Tagged (frames are forwarded as tagged).
- Untagged — The port is added to the list with the egress state set to Untagged (frames are forwarded as untagged).
- Dynamic — The port uses information returned in the RADIUS response to modify the VLAN egress list. This value is supported only if the device supports a mechanism through which the egress state may be returned in the RADIUS response.

Login Settings

This tab displays the current login settings for the port and allows you to change the settings if desired. The options available depend on what type(s) of authentication are enabled on the device.



MAC

Hold Time (sec)

Amount of time (in seconds) authentication remains timed out after the user fails to login. Valid values are 0-65535. The default is 60. (Hold Time is also known as Quiet Period in web-based and MAC authentication.)

802.1X

Hold Time (sec)

Amount of time (in seconds) authentication remains timed out after the user fails to login. Valid values are 0-65535. The default is 60.

Auth request period (sec)

For 802.1X authentication, how often (in seconds) the device queries the port to see if there is a new user on it. If a user is found, the device then attempts to authenticate the user. Valid values are 1-65535. The default is 30.

User timeout (sec)

For 802.1X authentication, the amount of time (in seconds) the device waits for an answer when querying the port for the existence of a user. Valid values are 1-300. The default is 30.

Auth server timeout (sec)

For 802.1X authentication, if a user is found on the port, the amount of time (in seconds) the device waits for a response from the authentication server before timing out. Valid values are 1-300. The default is 30.

Handshake requests before failure

For 802.1X authentication, the number of times the device tries to finalize the authentication process with the user, before the authentication request is considered invalid and authentication fails. Valid values are 1-10. The default is 2.

Web Auth

Max Requests

Number of times a user can attempt to log in before authentication fails and login attempts are not allowed. For web-based authentication, valid values are 1-2147483647, zero is not allowed, and the default is 2.

Hold Time (sec)

Amount of time (in seconds) authentication remains timed out after the specified **Max Requests** is reached. Valid values are 0-65535. The default is 60.

Quarantine

Session Timeout (sec)

For Quarantine authentication, the maximum number of seconds an authenticated session may last before automatic termination of the session. A value of zero indicates that no session timeout applies.

Session Idle Timeout (sec)

For Quarantine authentication, the maximum number of consecutive seconds an authenticated session may be idle before automatic termination of the session. A value of zero indicates that the device level setting is used.

Auto Tracking

Session Timeout (sec)

For Auto Tracking sessions, the maximum number of seconds a session may last before automatic termination of the session. A value of zero indicates that the device level setting is used.

Session Idle Timeout (sec)

For Auto Tracking sessions, the maximum number of consecutive seconds a session may be idle before automatic termination of the session. A value of zero indicates that the device level setting is used.

Automatic Re-Authentication

This tab is grayed-out if only web-based authentication is enabled on the device. For 802.1X and MAC authentication, the Automatic Re-Authentication tab lets you set up the periodic automatic re-authentication of logged-in users on this port. Without disrupting the user's session, the device repeats the authentication process using the most recently obtained user login information, to see if the same user is still logged in. Authenticated logged-in users are not required to log in again for re-authentication, as this occurs "behind the scenes."



802.1X Re-auth Status

If **Enabled** is selected, the re-authentication feature is enabled. If **Disabled** is selected, the re-authentication feature is disabled.

802.1X Re-auth Frequency (sec)

The length of time (in seconds) the device checks the port to re-authenticate the logged in user. Valid values are 1-2147483647. The default is 3600.

MAC Re-auth Status

If **Enabled** is selected, the re-authentication feature is enabled. If **Disabled** is selected, the re-authentication feature is disabled.

MAC Re-auth Frequency (sec)

The length of time (in seconds) the device checks the port to re-authenticate the logged in user. Valid values are 1-2147483647. The default is 3600.

Authenticated User Counts

This section provides authenticated user count information for devices with Multi-User as their configured authentication type. See the device Authentication tab for information on setting the device authentication type.



Current Number of Users

The current number of users actively authenticated or are in the process of authenticating on this interface. If multi-user authentication is disabled, this number is 0 (zero). Any unauthenticated traffic on the port is not included in this count.

Number of Users Allowed

The maximum number of users that can actively authenticate or be in the process of authenticating at one time on this interface. If you set this value below the current number of users, end user sessions exceeding that number are terminated.

NOTE: B2/C2 Devices. If you are configuring a single user and an IP phone per port, set this value to 2.

Number of MAC Users Allowed

The number of users that can actively authenticate via MAC authentication, or be in the process of authenticating via MAC authentication at one time on this interface. The number of MAC users allowed cannot exceed the number of users allowed. If you set this value below the current number of users, end user sessions exceeding that number are terminated. If MAC is

not selected as a Multi-User authentication type on the device Authentication tab, this field is grayed out.

Number of Quarantine Users Allowed

The number of users that can be actively authenticated via Quarantine authentication, or have Quarantine authentications in progress at one time on this interface. The number of Quarantine users allowed cannot exceed the number of users allowed. If you set this value below the current number of users, end user sessions exceeding that number are terminated. If Quarantine Auth is not enabled on the device Authentication tab, this field is grayed out.

Number of Auto Tracking Users Allowed

The number of Auto Tracking users that can be actively authenticated or have authentications in progress at one time on this interface. The number of Auto Tracking users allowed cannot exceed the number of users allowed. If you set this value below the current number of users, end user sessions exceeding that number are terminated. If Auto Tracking is not enabled on the device Authentication tab, this field is grayed out.

Convergence End-Point Access

This section lists all the Convergence End-Point (CEP) protocols supported by the device that the port resides on, and lets you enable or disable them for that port. For devices that do not support CEP, the section is blank.



Enable Button

Selects all the checkboxes and enables all the CEP protocols for this port.

Disable All Button

Deselects all the checkboxes and disables all the CEP protocols for this port.

CEP Protocols List

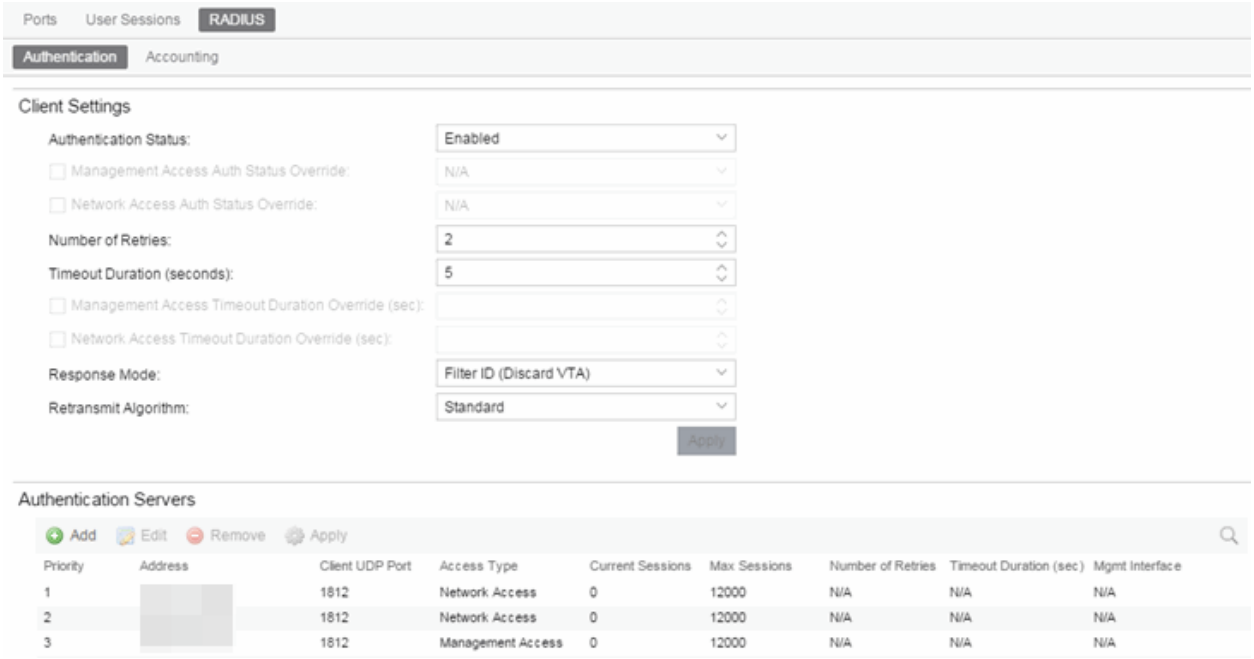
Lists all the CEP protocols supported by the device on which the port resides. Highlight a CEP protocol and select the Enable or Disable button to enable or disable CEP protocols, respectively. If the device does not support the CEP feature, this area is blank.

RADIUS (Device)

The device **RADIUS** tab allows you to configure and enable communication between the selected device (the RADIUS client), a RADIUS server or servers, and ExtremeCloud IQ Site Engine, for the purposes of authentication and accounting.

RADIUS accounting collects various data and statistics, such as the length of time a user has been logged on, and makes that data available to an administrator. It is used by a device to save accounting data on a RADIUS server. The device sends accounting requests to the server. The server acknowledges these requests, and data is passed to the server via accounting updates. For more information on accounting functionality, refer to your RADIUS server documentation.

To display the device **RADIUS** tab, select a device in the left-panel **Devices** tab, then select the **RADIUS** tab in the right panel.



Authentication Tab

Use this tab to view and configure the RADIUS authentication servers with which the device (the RADIUS client) can communicate.

RADIUS Authentication Client Settings

This section lets you enable or disable communication between the selected device (the RADIUS client) and the RADIUS authentication servers, and specify connection attempt information.

Authentication Status

Allows you to enable and disable communication between this device and the RADIUS authentication server(s). If enabled, the device becomes a RADIUS client and communicates with a RADIUS authentication server whenever a user logs on to a port on the device, as long as the port itself is enabled for authentication and the device is set up as a client on the RADIUS authentication server. The default is Disabled. For ExtremeWireless devices, the Client Status is automatically set to Enabled when a RADIUS server exists and Disabled when it does not.

Management Access Auth Status Override

Allows you to override the Authentication Status for users accessing the RADIUS authentication server(s) that have requested management access via the console, Telnet, SSH, or HTTP, etc.

Network Access Auth Status Override

Allows you to override the Authentication Status for users accessing the network via 802.1X, MAC, or Web-Based authentication.

Number of Retries

The number of attempts the device will make in contacting each RADIUS authentication server before giving up and trying the next RADIUS authentication server on the list. Valid values are 1-65535. For ExtremeWireless devices, this value is entered when the RADIUS server is added.

Timeout Duration

The total number of seconds the device will wait for the RADIUS authentication server to respond, before trying again. Valid values are 1-65535. For ExtremeWireless devices, this value is entered when the RADIUS server is added.

Management Access Timeout Duration Override (sec)

The total number of seconds the device waits for the RADIUS authentication server to respond before trying again for users accessing the RADIUS authentication server(s) that have requested management access via the console, Telnet, SSH, or HTTP, etc.

Network Access Timeout Duration Override (sec)

The total number of seconds the device waits for the RADIUS authentication server to respond before trying again for users accessing the network via 802.1X, MAC, or Web-Based authentication.

Response Mode

Select the RADIUS response attribute that the device should use for authentication:

- **Filter ID** — The Filter ID (role) is used. If a VLAN Tunnel Attribute (VTA) is returned, it will be ignored.
- **VLAN Tunnel Attribute** — The VLAN Tunnel Attribute is used and the Authentication-Based VLAN to Role Mappings are applied, if present. If a Filter ID is returned, it will be ignored.
- **Filter ID With VLAN Tunnel Attribute** — Both attributes are applied in the following manner: the role is applied to the user, except that the VLAN Tunnel Attribute replaces the role's Default Access Control VLAN (if present). In this case, the Authentication-Based VLAN to Role

mappings are ignored (as the role was explicitly assigned). VLAN classification rules are still applied, as defined by the assigned role.

Retransmit Algorithm

Select the authentication retransmission algorithm for this device to use with your RADIUS servers. Devices that do not support this functionality will have the option grayed out.

- **Standard** — Specifies that the primary RADIUS server should always be used for authentication, if it is available. The standard RADIUS authentication algorithm focuses on using RADIUS servers for redundancy rather than for scale provisioning. The only time secondary RADIUS servers are used, is when the primary server is unreachable due to a network outage or because server capacity is exceeded.
- **Round-Robin** — The round-robin RADIUS authentication algorithm spreads RADIUS server usage evenly between available RADIUS servers, allowing the load balancing of a large number of authentications across all RADIUS servers. This allows for a maximum authentication throughput for the number of servers configured. Additionally, if a single server is down, only a portion of the authenticating sessions will be affected by the outage.
- **Sticky Round-Robin** — This algorithm uses round-robin when assigning a RADIUS server to each unique authentication session, but specifies that the same RADIUS server should be used for any given authentication session when a session is initiated. In large-scale ExtremeControl deployments, this algorithm is used for switches that are authenticating more users than an ExtremeControl engine supports. For example, an ExtremeControl deployment might have an S-Series device that supports 9000 users deployed at the distribution level and authenticating users to three ExtremeControl engines that support 3000 users each. In this scenario, the sticky round-robin algorithm allows the S-Series device to spread the load across all three ExtremeControl engines while using the same ExtremeControl engine for all RADIUS transactions for a given session (MAC address).

Apply Button

Applies the changes you made in the RADIUS Authentication Client Settings section.

Authentication RADIUS Server(s) Table

This table lists the RADIUS authentication servers with which the device (the RADIUS client) can communicate. Use the buttons to add or remove servers, and edit server parameters. You can also edit a server's parameters by double-clicking the server entry in the list.

Priority

Order in which the RADIUS authentication server is checked, as compared to the other RADIUS authentication servers listed here. The lower the number, the higher the priority.

RADIUS Server IP

IP address of the RADIUS authentication server.

Client UDP Port

UDP port number (1-65535) on the RADIUS authentication server that the device will send authentication requests to; 1812 is the default port number.

Access Type

The type of authentication access allowed for this RADIUS server:

- **Any access** — the server can authenticate users originating from any access type.
- **Management access** — the server can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- **Network access** — the server can only authenticate users that are accessing the network via 802.1X, MAC, or Web-Based authentication.

Devices that do not support this feature will display N/A in this column.

Current Sessions

The current number of sessions associated with this server when the device is using the sticky round-robin RADIUS authentication algorithm. This value is not used when other algorithms are being used.

Max Sessions

The maximum number of sticky round-robin authentication sessions allowed on the server when the sticky round-robin RADIUS authentication algorithm is configured for the device. This value is not used when other algorithms are being used. In sticky round-robin, if a MAC address needs to re-authenticate, the request is sent to the same RADIUS server as the initial authentication request, unless the current number of authentication sessions for the server has reached the specified Max Sessions value. When this value is reached, re-authentication requests will instead default to the standard round-robin behavior to determine which RADIUS server to send the request to.

Number of Retries

The number of times the device will resend an authentication request if the RADIUS authentication server does not respond. For ExtremeWireless devices, this value is configured per RADIUS server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the RADIUS Authentication Client Settings section.

Timeout Duration

The amount of time in seconds the device will wait for the RADIUS authentication server to respond to an authentication request. For ExtremeWireless devices, this value is configured per RADIUS server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the RADIUS Authentication Client Settings section.

Management Interface

The IP address and VRName used when the switch is communicating with a configured RADIUS server.

Apply Button

Applies any changes you made in the RADIUS Authentication Server(s) tab.

Add Button

Opens the Add RADIUS Authentication Server window, where you can enter the parameters for a server you want to add to the list. When you select **OK** on this window, the new server is added.

Remove Button

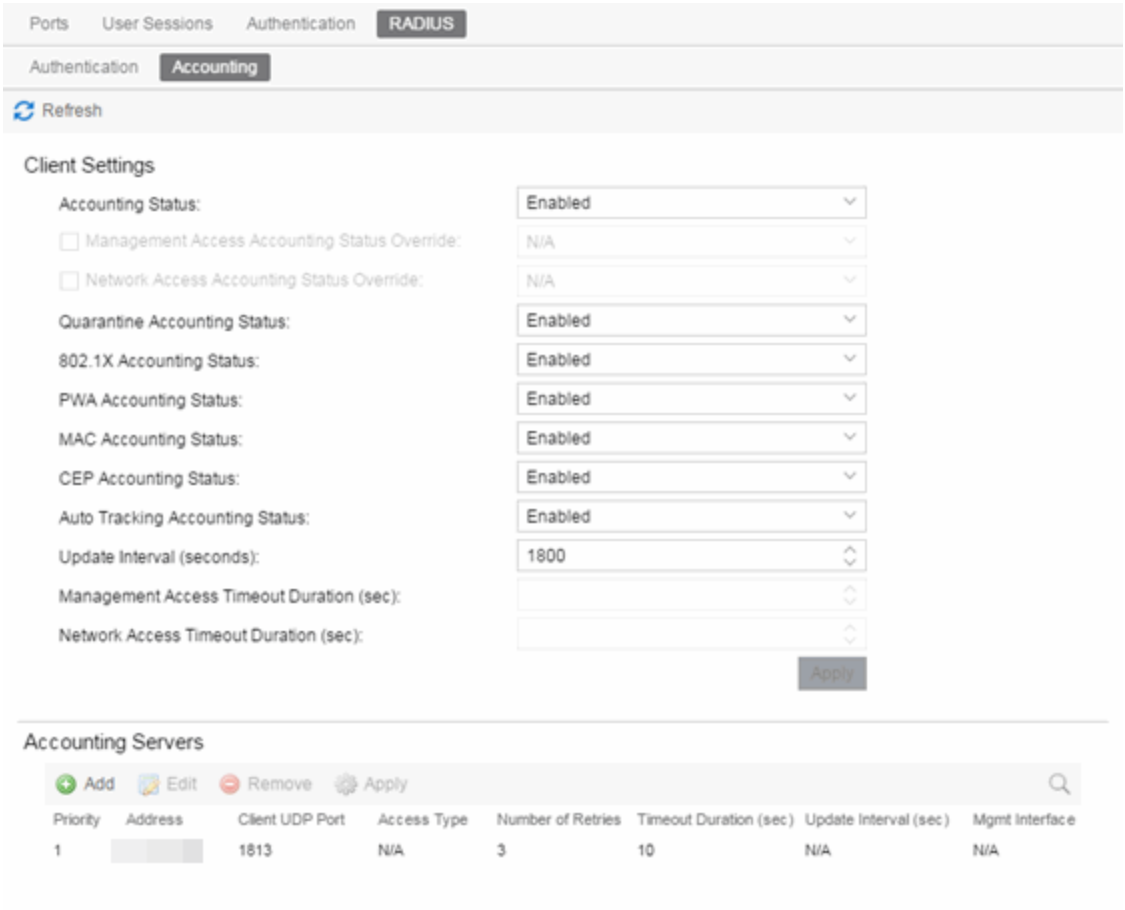
Select a RADIUS authentication server in the list and use this button to remove the server.

Edit Button

Select a RADIUS authentication server in the list and use this button to edit the server's parameters. You can also edit the server parameters by double-clicking the server entry in the list.

Accounting Tab

Use this tab to view and configure the RADIUS accounting servers with which the device (the RADIUS client) can communicate.



RADIUS Accounting Client Settings

This section lets you enable or disable communication between the selected device (the RADIUS client) and the RADIUS accounting servers, and specify the update interval.

Accounting Status

Allows you to enable or disable RADIUS accounting. RADIUS accounting is used by a device to save accounting data on a RADIUS accounting server. If accounting is enabled, an accounting session starts after the user is successfully authenticated by a RADIUS authentication server. The default is Disabled. For ExtremeWireless devices, the status is automatically set to Enabled when a RADIUS server exists and Disabled when it does not. Devices that do not support RADIUS accounting will have this field grayed out.

Management Access Auth Status Override

Allows you to override the Accounting Status for users accessing the RADIUS accounting server(s) that have requested management access via the console, Telnet, SSH, or HTTP, etc.

Network Access Auth Status Override

Allows you to override the Accounting Status for users accessing the network via 802.1X, MAC, or Web-Based authentication.

Per Authentication Type Accounting Status

Allows you to enable/disable RADIUS accounting for individual authentication types. Some authentication types do not have RADIUS accounting enabled by default (when global RADIUS accounting is enabled). Enabling these authentication types will give both ExtremeControl and other RADIUS servers more complete information regarding authentication sessions. These options also allow you to disable accounting messages from certain authentication types, for example, Auto-Tracking, which does not actually authenticate end users. Note that the global Accounting Status option controls accounting on a global basis for all authentication types. Devices that do not support this functionality will have these fields grayed out.

Update Interval (minutes)

Collected accounting data is sent from the device to the RADIUS accounting server via accounting updates. The Accounting Update Interval is the amount of time in minutes between accounting updates. Valid values are 1-65535. It is recommended that the value be greater than 10 minutes, and careful consideration should be given to its impact on network traffic. Devices that do not support RADIUS accounting have this field grayed out (with the exception of an SNMPv1 R2 device, which display accounting values but will not allow you to set them.) For ExtremeWireless devices, this value is entered when the RADIUS server is added.

Management Access Timeout Duration Override (sec)

The total number of seconds the device waits for the RADIUS accounting server to respond before trying again for users accessing the RADIUS accounting server(s) that have requested management access via the console, Telnet, SSH, or HTTP, etc.

Network Access Timeout Duration Override (sec)

The total number of seconds the device waits for the RADIUS accounting server to respond before trying again for users accessing the network via 802.1X, MAC, or Web-Based authentication.

Apply Button

Applies the changes you made in the RADIUS Accounting Client Settings section.

Accounting RADIUS Servers Table

This tab lists the RADIUS accounting servers with which the device (the RADIUS client) can communicate. Use the buttons to add or remove servers, and edit server parameters. You can also edit a server's parameters by double-clicking the server entry in the list.

Priority

Order in which the RADIUS accounting server is checked, as compared to the other RADIUS accounting servers listed here. The lower the number, the higher the priority.

RADIUS Server IP

IP address of the RADIUS accounting server.

Client UDP Port

UDP port number (1-65535) on the RADIUS accounting server that the device will send accounting requests to; 1813 is the default port number. Devices that do not support RADIUS accounting will display N/A in this column (with the exception of an SNMPv1 R2 device, which will display accounting values but will not allow you to set them.)

Access Type

The type of authentication access allowed for this RADIUS server:

- **Any access** — the server can authenticate users originating from any access type.
- **Management access** — the server can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- **Network access** — the server can only authenticate users that are accessing the network via 802.1X, MAC, or Web-Based authentication.

Devices that do not support this feature will display N/A in this column.

Number of Retries

The number of times the device will resend an accounting request if the RADIUS accounting server does not respond. Valid values are 0-20. Devices that do not support RADIUS accounting will display N/A in this column (with the exception of an SNMPv1 R2 device, which display accounting values but does not allow you to set them.)

Timeout Duration

The amount of time in seconds the device will wait for the RADIUS accounting server to respond to an accounting request. Valid values are 2-10 seconds. Devices that do not support

RADIUS accounting will display N/A in this column (with the exception of an SNMPv1 R2 device, which display accounting values but does not allow you to set them.)

Update Interval

The amount of time in minutes between accounting updates. For ExtremeWireless devices, this value is configured per RADIUS server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the RADIUS Accounting Client Settings section.

Management Interface

The IP address and VRName used when the switch is communicating with a configured RADIUS server.

Apply Button

Applies any changes you made in the RADIUS Accounting Server(s) tab.

Add Button

Opens the Add RADIUS Accounting Server window, where you can enter the parameters for a server you want to add to the list. When you select **OK** on this window, the new server is added.

Remove Button

Select a RADIUS accounting server in the list and use this button to remove the server.

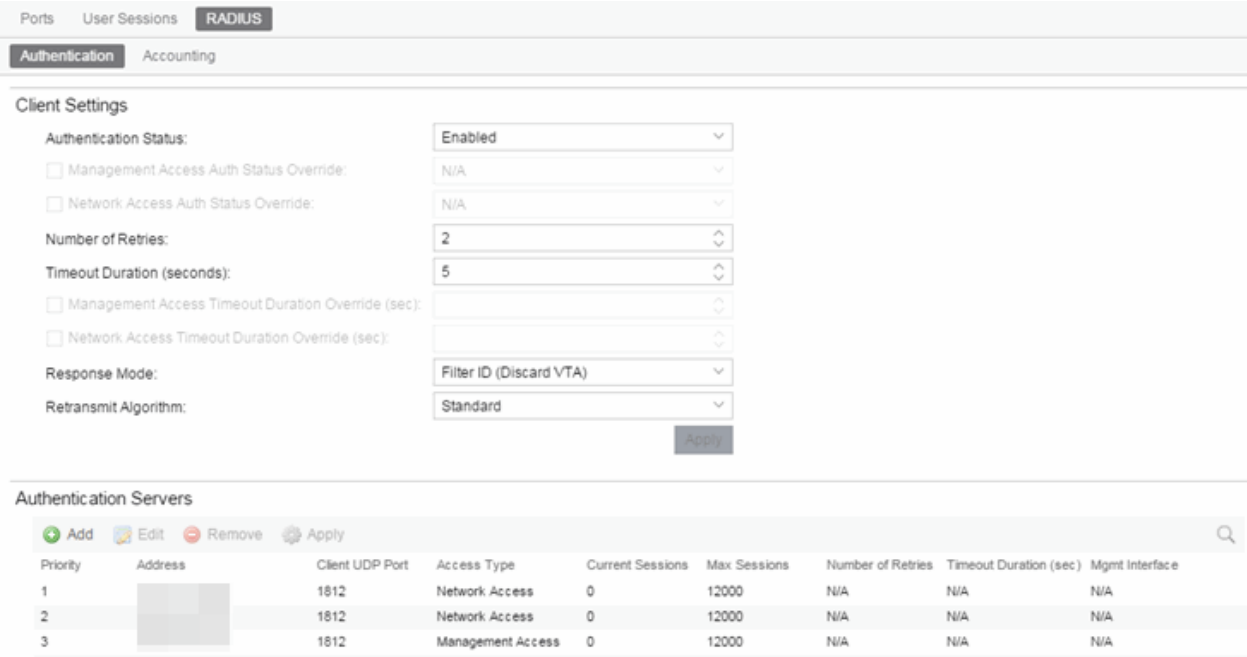
Edit Button

Select a RADIUS accounting server in the list and use this button to edit the server's parameters. You can also edit the server parameters by double-clicking the server entry in the list.

RADIUS Authentication (Device)

The device RADIUS **Authentication** tab enables you to configure and enable communication between the selected device (the RADIUS client), a RADIUS server or servers, and ExtremeCloud IQ Site Engine, for the purposes of authentication and accounting (for your SNMPv3 devices that support it).

Use this tab to view and configure the RADIUS authentication servers with which the device (the RADIUS client) can communicate.



RADIUS Authentication Client Settings

This section lets you enable or disable communication between the selected device (the RADIUS client) and the RADIUS authentication servers, and specify connection attempt information.

Authentication Status

Enables you to enable and disable communication between this device and the RADIUS authentication server(s). If enabled, the device becomes a RADIUS client and communicates with a RADIUS authentication server whenever a user logs on to a port on the device, as long as the port itself is enabled for authentication and the device is set up as a client on the RADIUS authentication server. For ExtremeWireless devices, the Client Status is automatically set to **Enabled** when a RADIUS server exists and Disabled when it does not.

Management Access Auth Status Override

Enables you to override the Authentication Status for users accessing the

RADIUS authentication server(s) that requested management access via the console, Telnet, SSH, or HTTP, etc.

Network Access Auth Status Override
Enables you to override the Authentication Status for users accessing the network via 802.1X, MAC, or Web-Based authentication.

Number of Retries
The number of attempts the device makes in contacting each RADIUS authentication server before giving up and trying the next RADIUS authentication server on the list. For ExtremeWireless devices, this value is entered when the RADIUS server is added.

Timeout Duration (seconds)
The total number of seconds the device waits for the RADIUS authentication server to respond, before trying again. For ExtremeWireless devices, this value is entered when the RADIUS server is added.

Management Access Timeout Duration Override (sec)
The total number of seconds the device waits for the RADIUS authentication server to respond before trying again for users accessing the RADIUS authentication server(s) that requested management access via the console, Telnet, SSH, or HTTP, etc.

Network Access Timeout Duration Override (sec)
The total number of seconds the device waits for the RADIUS authentication server to respond before trying again for users accessing the network via 802.1X, MAC, or Web-Based authentication.

Response Mode
Select the RADIUS response attribute the device uses for authentication:

- **Filter ID (Discard VTA)** — The Filter ID (role) is used. If a VLAN Tunnel Attribute (VTA) is returned, it is ignored.
- **VLAN Tunnel Attribute (Discard Tunnel Attribute)** — The VLAN Tunnel Attribute is used and the Authentication-Based VLAN to Role Mappings are applied, if present. If a Filter ID is returned, it is ignored.
- **Filter ID With VLAN Tunnel Attribute** — Both attributes are applied in the following manner: the role is applied to the user, except that the VLAN Tunnel Attribute replaces the role's Default Access Control VLAN (if present). In this case, the Authentication-Based VLAN to Role mappings are ignored (as the role was explicitly assigned). VLAN classification rules are still applied, as defined by the assigned role.

Retransmit Algorithm
Select the authentication retransmission algorithm for this device to use with your RADIUS servers. Devices that do not support this functionality have the option grayed out.

- **Standard** — Specifies that the primary RADIUS server should always be used for authentication, if it is available. The standard RADIUS authentication algorithm focuses

on using RADIUS servers for redundancy rather than for scale provisioning. The only time secondary RADIUS servers are used, is when the primary server is unreachable due to a network outage or because server capacity is exceeded.

- **Round-Robin** — The round-robin RADIUS authentication algorithm spreads RADIUS server usage evenly between available RADIUS servers, enabling the load balancing of a large number of authentications across all RADIUS servers. This enables a maximum authentication throughput for the number of servers configured. Additionally, if a single server is down, only a portion of the authenticating sessions are affected by the outage.
- **Sticky Round-Robin** — This algorithm uses round-robin when assigning a RADIUS server to each unique authentication session, but specifies that the same RADIUS server is used for any given authentication session when a session is initiated. In large-scale ExtremeControl deployments, this algorithm is used for switches authenticating more users than an Access Control appliance supports. For example, an Access Control deployment might have an S-Series device that supports 9000 users deployed at the distribution level and authenticating users to three Access Control appliances that support 3000 users each. In this scenario, the sticky round-robin algorithm enables the S-Series device to spread the load across all three Access Control appliances while using the same Access Control appliance for all RADIUS transactions for a given session (MAC address).

Apply Button

Applies the changes you made in the RADIUS Authentication Client Settings section.

Authentication RADIUS Server(s) Table

This table lists the RADIUS authentication servers with which the device (the RADIUS client) can communicate. Use the buttons to add or remove servers, and edit server parameters. You can also edit a server's parameters by double-clicking the server entry in the list.

Priority

Order in which the RADIUS authentication server is checked, as compared to the other RADIUS authentication servers listed here. The lower the number, the higher the priority with 1 being the highest priority.

Address

IP address of the RADIUS authentication server.

Client UDP Port

UDP port number (1-65535) on the RADIUS authentication server to which the device sends authentication requests; 1812 is the default port number.

Access Type

The type of authentication access enabled for this RADIUS server:

- **Any access** — the server can authenticate users originating from any access type.
- **Management access** — the server can only authenticate users that requested management access via the console, Telnet, SSH, or HTTP, etc.
- **Network access** — the server can only authenticate users accessing the network via 802.1X, MAC, or Web-Based authentication.

Devices that do not support this feature display N/A in this column.

Current Sessions

The current number of sessions associated with this server when the device is using the sticky round-robin RADIUS authentication algorithm. This value is not used when other algorithms are being used.

Max Sessions

The maximum number of sticky round-robin authentication sessions permitted on the server when the sticky round-robin RADIUS authentication algorithm is configured for the device. This value is not used when other algorithms are selected. In sticky round-robin, if a MAC address needs to re-authenticate, the request is sent to the same RADIUS server as the initial authentication request, unless the current number of authentication sessions for the server has reached the specified **Max Sessions** value. When this value is reached, re-authentication requests instead default to the standard round-robin behavior to determine the RADIUS server to which to send the request.

Number of Retries

The number of times the device resends an authentication request if the RADIUS authentication server does not respond. For ExtremeWireless devices, this value is configured per RADIUS server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the RADIUS Authentication Client Settings section.

Timeout Duration (sec)

The amount of time in seconds the device waits for the RADIUS authentication server to respond to an authentication request. For ExtremeWireless devices, this value is configured per RADIUS server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the RADIUS Authentication Client Settings section.

Management Interface

The IP address and VRName used when the switch is communicating with a configured RADIUS server.

Add Button

Opens the Add/Edit RADIUS Authentication Server window, where you can enter the parameters for a server you want to add to the list. When you select **OK** on this window, the new server is added.

Edit Button

Select a RADIUS authentication server in the list and use this button to edit the server's parameters. You can also edit the server parameters by double-clicking the server entry in the list.

Remove Button

Select a RADIUS authentication server in the list and use this button to remove the server.

Apply Button

Applies any changes you made in the RADIUS Authentication Server(s) tab.

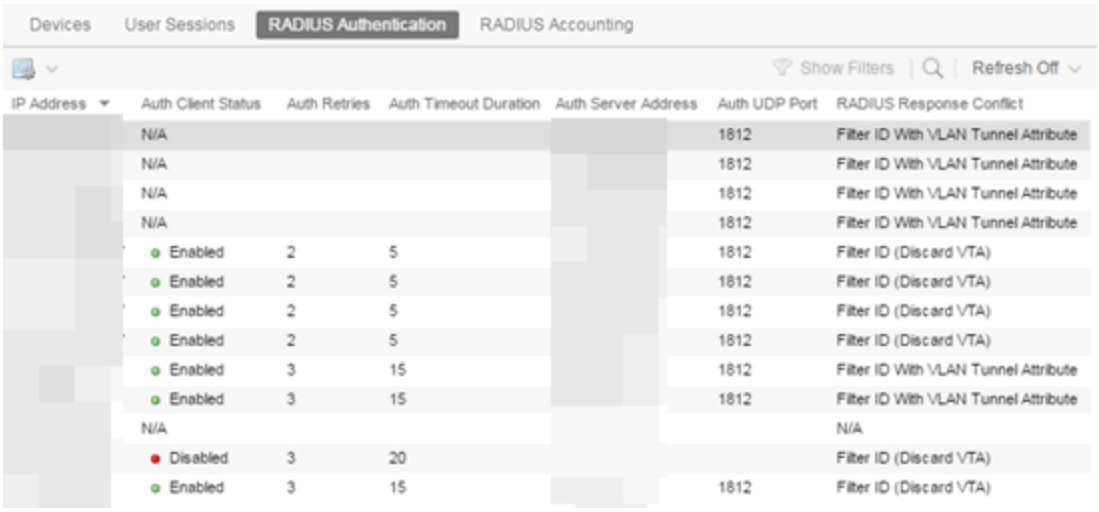
- Authentication
- Port Properties - Authentication Configuration Tab
- Add RADIUS Authentication Server Window
- Add RADIUS Accounting Server Window



RADIUS Authentication (Devices)

The **RADIUS Authentication** tab displays authentication RADIUS server information for all the devices in the current domain. You can configure RADIUS server information for an individual device using the device's RADIUS Tab.

To access this tab, select**Devices/Port Groups**›**Devices**in the left-panel of the**Policy** tab, then select the **RADIUS Authentication** tab in the right panel.



IP Address

IP address of the device.

Auth Client Status

Informs you whether or not the device is enabled as a RADIUS client. If **Enabled**, the device is a RADIUS client and communicates with a RADIUS authentication server whenever a user logs on to a port on the device, as long as the port itself is enabled for authentication. If Disabled, the device is currently not enabled as a RADIUS client.

Auth Retries

Number of attempts the device (RADIUS client) makes to connect to the RADIUS authentication server before giving up and trying the next RADIUS server on the list.

Auth Timeout Duration

Total number of seconds the device (RADIUS client) waits for the RADIUS authentication server to respond before trying again.

Auth Server Address

The IP addresses of the RADIUS servers the client device attempts to contact.

Auth UDP Port

The UDP port number used to send authentication requests.

RADIUS Response Conflict

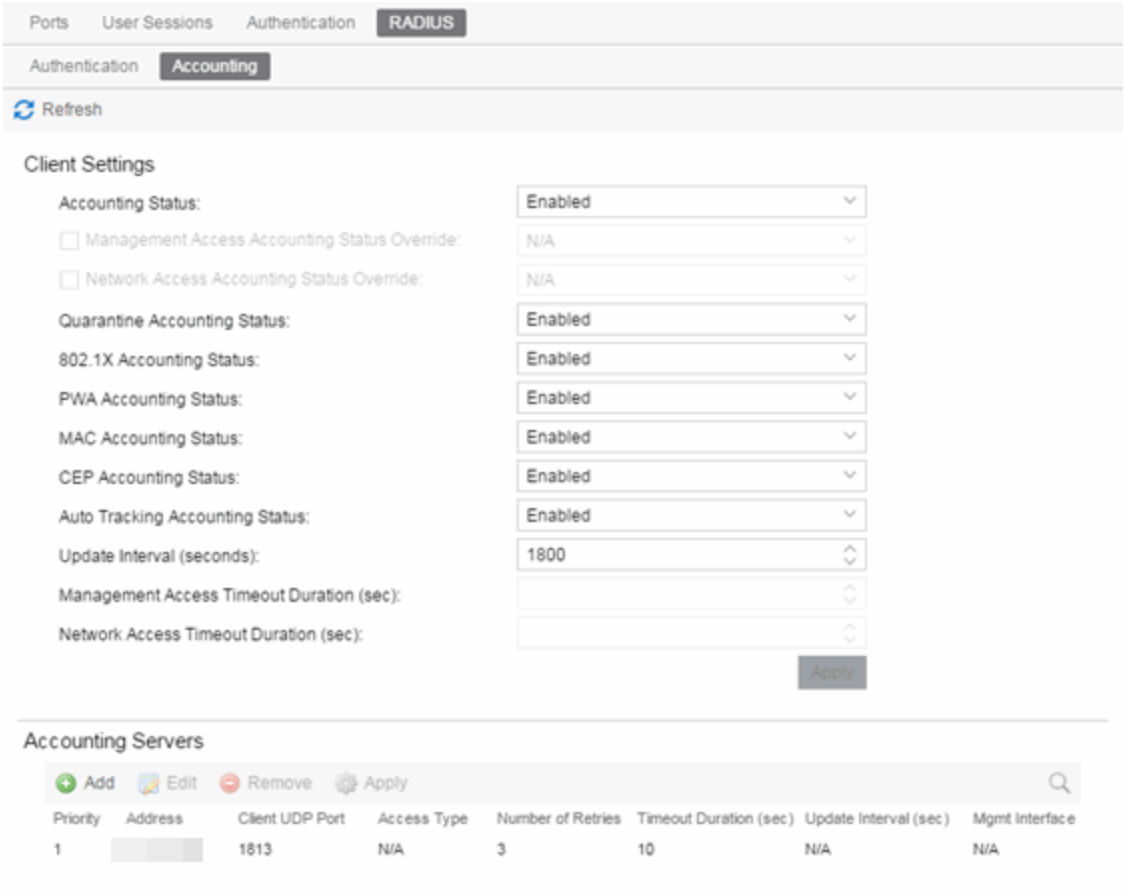
Indicates the RADIUS response attribute that the device uses for authentication. You can configure the Response Mode in the RADIUS tab for the device.

RADIUS Accounting (Device)

The device RADIUS **Accounting** tab enables you to configure and enable communication between the selected device (the RADIUS client), a RADIUS server or servers, and ExtremeCloud IQ Site Engine, for the purposes of accounting (for your SNMPv3 devices that support it).

RADIUS accounting collects various data and statistics, such as the length of time a user has been logged on, and makes that data available to an administrator. It is used by a device to save accounting data on a RADIUS server. Accounting requests are sent from the device to the server. The server acknowledges these requests, and data is passed to the server via accounting updates. For more information on accounting functionality, refer to your RADIUS server documentation.

To display the device RADIUS **Accounting** tab, select a device in the left panel Devices > Devices tree, then select **RADIUS** > **Accounting** in the right panel.



RADIUS Accounting Client Settings

This section lets you enable or disable communication between the selected device (the RADIUS client) and the RADIUS accounting servers, and specify the update interval.

Accounting Status

Enables you to enable or disable RADIUS accounting on SNMPv3 devices that support it. RADIUS accounting is used by a device to save accounting data on a RADIUS accounting server. If accounting is enabled, an accounting session starts after the user is successfully authenticated by a RADIUS authentication server. The default is Disabled. For ExtremeWireless devices, the status is automatically set to Enabled when a RADIUS server exists and Disabled when it does not. Devices that do not support RADIUS accounting have this field grayed out.

Management Access Auth Status Override

Enables you to override the Accounting Status for users accessing the RADIUS accounting server(s) that have requested management access via the console, Telnet, SSH, or HTTP, etc.

Network Access Auth Status Override

Enables you to override the Accounting Status for users accessing the network via 802.1X, MAC, or Web-Based authentication.

Per Authentication Type Accounting Status

Enables you to enable/disable RADIUS accounting for individual authentication types (Quarantine, 802.1X, PWA, MAC, CEP, and Auto Tracking). Some authentication types do not have RADIUS accounting enabled by default (when global RADIUS accounting is enabled). Enabling these authentication types gives both ExtremeControl and other RADIUS servers more complete information regarding authentication sessions. These options also enable you to disable accounting messages from certain authentication types, for example, Auto-Tracking, which does not actually authenticate end users. Note that the global Accounting Status option controls accounting on a global basis for all authentication types. Devices that do not support this functionality have these fields grayed out.

Update Interval (seconds)

Collected accounting data is sent from the device to the RADIUS accounting server via accounting updates. The Accounting Update Interval is the amount of time in seconds between accounting updates. This field is greyed out for devices that do not support RADIUS accounting (with the exception of an SNMPv1 R2 device, which displays accounting values but does not permit you to set them.) For ExtremeWireless devices, this value is entered when the RADIUS server is added.

Management Access Timeout Duration Override (sec)

The total number of seconds the device waits for the RADIUS accounting server to respond before trying again for users accessing the RADIUS accounting server(s) that have requested management access via the console, Telnet, SSH, or HTTP, etc.

Network Access Timeout Duration Override (sec)

The total number of seconds the device waits for the RADIUS accounting server to respond before trying again for users accessing the network via 802.1X, MAC, or Web-Based authentication.

Apply Button

Applies the changes you made in the RADIUS Accounting Client Settings section.

Accounting RADIUS Servers Table

This table lists the RADIUS accounting servers with which the device (the RADIUS client) can communicate. Use the buttons to add or remove servers, and edit server parameters. You can also edit a server's parameters by double-clicking the server entry in the list.

Priority

Order in which the RADIUS accounting server is checked, as compared to the other RADIUS accounting servers listed here. The lower the number, the higher the priority with 1 being the highest priority.

Address

IP address of the RADIUS accounting server.

Client UDP Port

UDP port number (1-65535) on the RADIUS accounting server to which the device sends accounting requests; 1813 is the default port number. Devices that do not support RADIUS accounting display N/A in this column (with the exception of an SNMPv1 R2 device, which displays accounting values, but does not permit you to set them.)

Access Type

The type of authentication access permitted for this RADIUS server:

- **Any access** — the server can authenticate users originating from any access type.
- **Management access** — the server can only authenticate users accessing the network via the console, Telnet, SSH, or HTTP, etc.
- **Network access** — the server can only authenticate users accessing the network via 802.1X, MAC, or Web-Based authentication.

Devices that do not support this feature display N/A in this column.

Number of Retries

The number of times the device resends an accounting request if the RADIUS accounting server does not respond. Valid values are 0-20. Devices that do not support RADIUS accounting display N/A in this column (with the exception of an SNMPv1 R2 device, which displays accounting values, but does not permit you to set them.)

Timeout Duration (sec)

The amount of time in seconds the device waits for the RADIUS accounting server to respond to an accounting request. Valid values are 2-10 seconds. Devices that do not support RADIUS accounting display N/A in this column (with the exception of an SNMPv1 R2 device, which displays accounting values, but does not permit you to set them.)

Update Interval (sec)

The amount of time in seconds between accounting updates. For ExtremeWireless devices, this value is configured per RADIUS server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the RADIUS Accounting Client Settings section.

Management Interface

The IP address and VRName used when the switch is communicating with a configured RADIUS server.

Apply Button

Applies any changes you made in the RADIUS Accounting Server(s) tab.

Add Button

Opens the Add RADIUS Accounting Server window, where you can enter the parameters for a server you want to add to the list. When you select **OK** on this window, the new server is added.

Remove Button

Select a RADIUS accounting server in the list and use this button to remove the server.

Edit Button

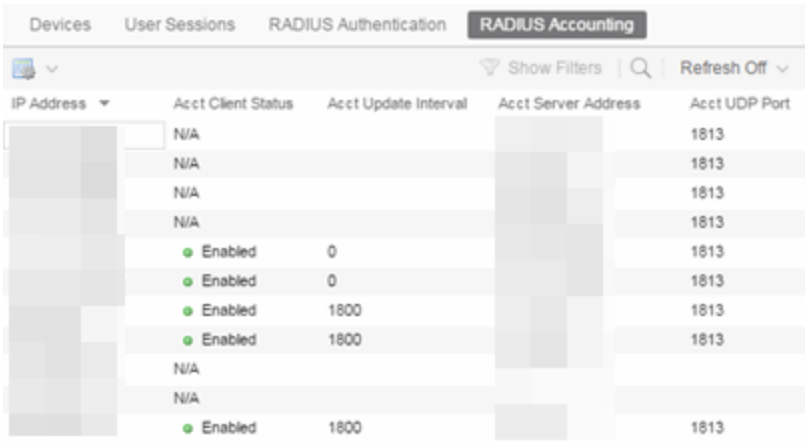
Select a RADIUS accounting server in the list and use this button to edit the server's parameters. You can also edit the server parameters by double-clicking the server entry in the list.



RADIUS Accounting (Devices)

The **RADIUS Accounting** tab displays accounting RADIUS server information for all the devices in the current domain. You can configure RADIUS server information for an individual device using the device's RADIUS Tab.

To access this tab, select **Devices/Port Groups**>**Devices** in the left-panel of the **Policy** tab, then select the **RADIUS Accounting** tab in the right panel.



IP Address

IP address of the device.

Acct. Client Status

Informs you whether or not RADIUS accounting is enabled on the device (the RADIUS client). RADIUS accounting is supported on certain SNMPv3 devices, and is used by the device to save accounting data on a RADIUS server. If accounting is enabled, an accounting session starts after the user is successfully authenticated by a RADIUS server. Devices that do not support RADIUS accounting display N/A in this column (with the exception of an SNMPv1 R2 device, which displays a status.)

Acct. Update Interval

Collected accounting data is sent from the device (RADIUS client) to the RADIUS server via accounting updates. The Accounting Update Interval is the amount of time in minutes between accounting updates. Devices that do not support RADIUS accounting display N/A in this column (with the exception of an SNMPv1 R2 device, which displays a value.)

Acct Server Address

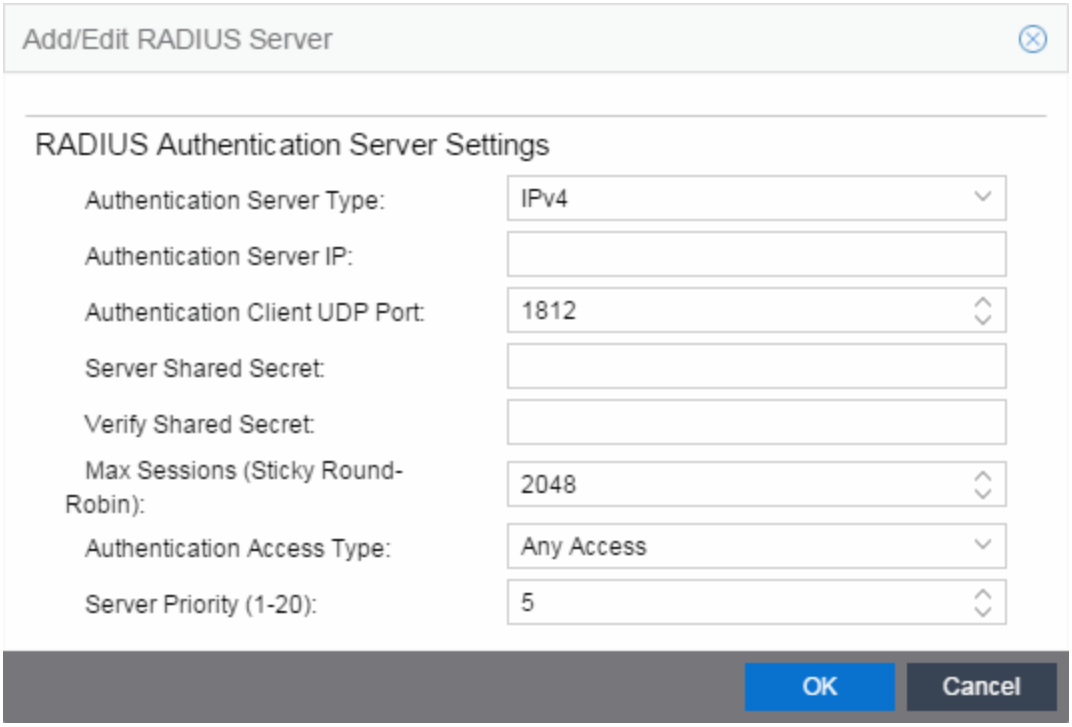
The IP addresses of the RADIUS servers the client device attempts to contact.

Auth UDP Port

The UDP port number used to send accounting requests.

Add/Edit RADIUS Server

This window lets you add a RADIUS server to ExtremeCloud IQ Site Engine for the purpose of authentication. Access this window by selecting **Add** in the RADIUS Server(s) Authentication sub-tab in the RADIUS tab for a device.



Authentication Server Type

Select the authentication type used on the RADIUS server.

NOTE: DNS servers (on supported devices) can only be added when there is a valid DNS server configured on the Device which allows the DNS name to resolve to an IP address at the time of configuration.

Authentication Server IP

Enter the IP or IPv6 address, or the hostname of the RADIUS authentication server. Not all devices support IPv6 address types.

Authentication Client UDP Port

Enter the UDP port number (1-65535) the device (RADIUS client) uses to send authentication requests to the RADIUS authentication server; 1812 is the default port number.

Server Shared Secret

A string of characters used to encrypt and decrypt communications between the device (RADIUS client) and the RADIUS authentication server. This string must match the shared

secret entered when you added the client device on the RADIUS server. Without the shared secret, the server and client are unable to communicate, and authentication attempts fail. The shared secret must be at least 6 characters long; 16 characters is recommended. Dashes are allowed in the string, but spaces are not.

NOTES: If you are configuring multiple RADIUS servers, the same server shared secret must be used for each RADIUS server. This is because most devices (RADIUS clients) only support one shared secret. Matrix N-Series devices with firmware version 5.0 or above are an exception to this, as these devices **do** support a unique shared secret for each server.

This Server Shared Secret is not to be confused with the Application Shared Secret that encrypts communication between the RADIUS client and ExtremeCloud IQ Site Engine, entered in the Application Shared Secret area of the RADIUS tab for a device.

Verify Shared Secret

Re-enter the Server Shared Secret you entered above.

Max Sessions (Sticky Round-Robin)

Specifies the maximum number of sticky round-robin authentication sessions allowed on the server when the sticky round-robin RADIUS authentication algorithm is configured for a device. In sticky round-robin, if a MAC address needs to re-authenticate, the request is sent to the same RADIUS server as the initial authentication request, unless the current number of authentication sessions for the server has reached the specified Max Sessions value. When this value is reached, re-authentication requests will instead default to the standard round-robin behavior to determine which RADIUS server to send the request to. Devices that do not support this functionality will have the option grayed out.

Number of Retries

The number of times the device will resend an authentication request if the RADIUS authentication server does not respond. For ExtremeWireless devices, this value is configured for each server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the RADIUS Authentication Client Settings section of the RADIUS tab.

Timeout Duration

The amount of time in seconds the device will wait for the RADIUS authentication server to respond to an authentication request. For ExtremeWireless devices, this value is configured for each server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the RADIUS Authentication Client Settings section of the RADIUS tab.

Authentication Access Type

Use the drop-down list to select the type of authentication access allowed for this RADIUS server:

- **Any access** - the server can authenticate users originating from any access type.
- **Management access** - the server can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- **Network access** - the server can only authenticate users that are accessing the network via 802.1X, MAC, or Web-Based authentication.

This feature allows you to have one set of servers for authenticating management access requests and a different set for authenticating network access requests. Devices that do not support this feature will have this field grayed out.

Server Priority

Order in which the RADIUS authentication server will be checked, as compared to the other RADIUS authentication servers on the device. The lower the number, the higher the priority.

Management Interface

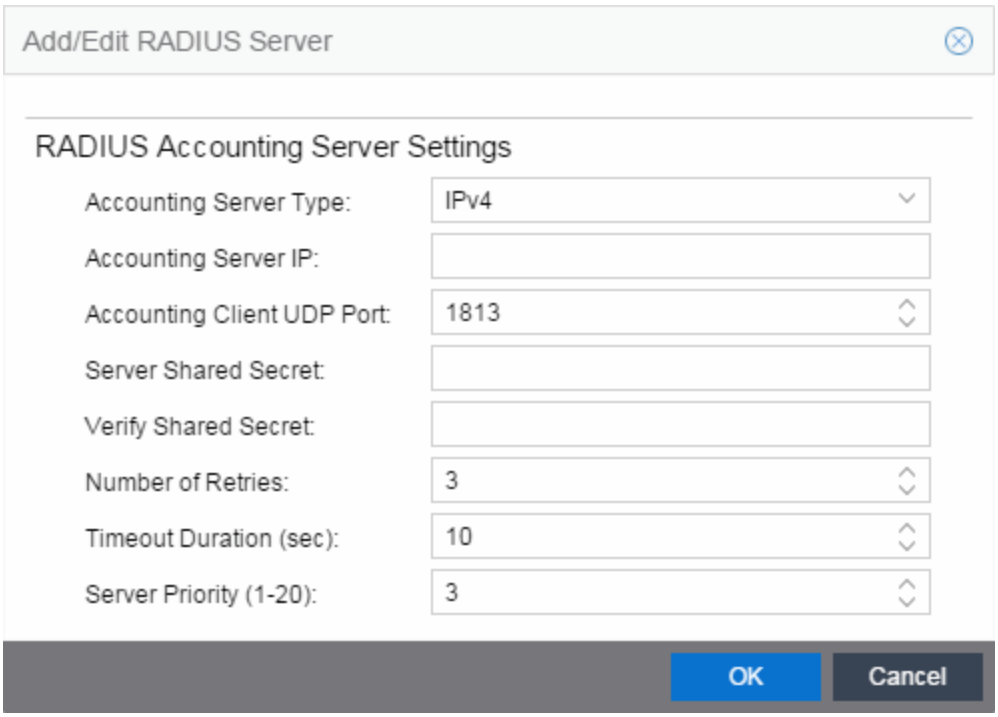
Select the IP address and VRName to use when the switch is communicating with a configured RADIUS server.

NOTE: ExtremeXOS/Switch Engine devices must define a Management Interface.



Add RADIUS Accounting Server

This window lets you add a RADIUS server to ExtremeCloud IQ Site Engine for the purpose of RADIUS accounting. Access this window by selecting **Add** in the RADIUS Server(s) Accounting sub-tab in the RADIUS tab for a device.



Accounting Server Type

Select the accounting type used on the RADIUS server.

NOTE: DNS servers (on supported devices) may only be added when there is a valid DNS server configured on the Device which allows the DNS name to resolve to an IP address at the time of configuration.

Accounting Server IP

Enter the IP or IPv6 address, or the hostname of the RADIUS accounting server. Not all devices support IPv6 address types.

Accounting Client UDP Port

Enter the UDP port number (1-65535) the device (RADIUS client) uses to send accounting requests to the RADIUS server; 1813 is the default port number. Devices that do not support RADIUS accounting will have this field grayed out (with the exception of an SNMPv1 R2 device, which will display accounting values but will not allow you to set them.)

Server Shared Secret

A string of characters used to encrypt and decrypt communications between the device (RADIUS client) and the RADIUS accounting server. This string must match the shared secret entered when you added the client device on the RADIUS server. Without the shared secret, the server and client will be unable to communicate. The shared secret must be at least 6 characters long; 16 characters is recommended. Dashes are allowed in the string, but spaces are not.

NOTES: If you are configuring multiple RADIUS servers, the same server shared secret must be used for each RADIUS server. This is because most devices (RADIUS clients) only support one shared secret. Matrix N-Series devices with firmware version 5.0 or above are an exception to this, as these devices **do** support a unique shared secret for each server.

This Server Shared Secret is different than the Application Shared Secret that encrypts communication between the RADIUS client and ExtremeCloud IQ Site Engine, entered in the Application Shared Secret area of the RADIUS tab for a device.

Verify Shared Secret

Re-enter the Server Shared Secret you entered above.

Number of Retries (0-20)

The number of times the device will resend an accounting request if the RADIUS server does not respond. Valid values are 0-20. Devices that do not support RADIUS accounting will have this field grayed out (with the exception of an SNMPv1 R2 device, which will display accounting values but will not allow you to set them.)

Timeout Duration (2 -10 sec)

The amount of time in seconds the device will wait for the RADIUS server to respond to an accounting request. Valid values are 2-10 seconds. Devices that do not support RADIUS accounting will have this field grayed out (with the exception of an SNMPv1 R2 device, which will display accounting values but will not allow you to set them.)

Update Interval (minutes)

The Accounting Update Interval is the amount of time in minutes between accounting updates. For ExtremeWireless Wireless devices, this value is configured per RADIUS server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the RADIUS Accounting Client Settings section of the RADIUS tab. Devices that do not support RADIUS accounting will have this field grayed out.

Accounting Access Type

Use the drop-down list to select the type of accounting access allowed for this RADIUS server:

- **Any access** - the server can send an accounting request for users originating from any access type.

- **Management access** - the server can only send an accounting request for users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- **Network access** - the server can only send an accounting request users that are accessing the network via 802.1X, MAC, or Web-Based accounting.

This feature allows you to have one set of servers for accounting management access requests and a different set for accounting network access requests. Devices that do not support this feature have this field grayed out.

Server Priority (1-20)

Order in which the RADIUS accounting server will be checked, as compared to the other RADIUS accounting servers on the device. The lower the number, the higher the priority.

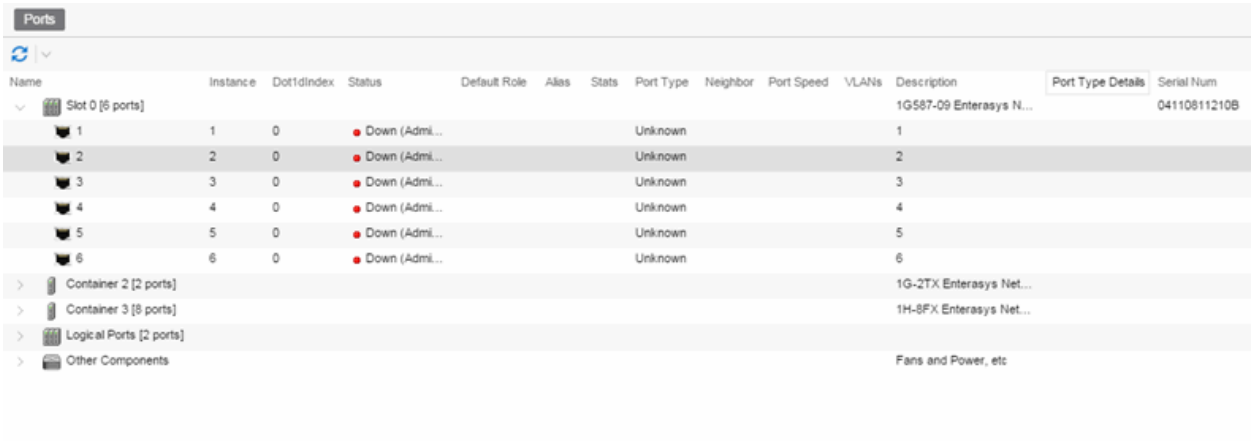
Management Interface

Select the IP address and VRName to use when the switch is communicating with a configured RADIUS server.

NOTE: ExtremeXOS/Switch Engine devices must define a Management Interface.

Ports (Device)

The device **Port Groups** tab displays a table of information about the selected device's ports. To access this tab, select a port group from the left panel's**Devices/Port Groups**>**Port Groups** tab.



Name

Name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

Instance

Shows the instance for the port.

Dot1dIndex
The index value assigned to the port interface.

Status
Shows the status (Up, Down, or Unknown) of the port.

Default Role
Displays the default role for the port. To set the default role, select a port, right-click and select Set Default Role. The Roles Selection view appears where you can select the desired default role. See Default Role in the Concepts topic for information on default roles.

NOTE: Setting a default role on an ExtremeWireless Controller port that is not yet a VNS, creates a new VNS on the HWC.

Alias
Shows the alias (ifAlias) for the interface, if one is assigned.

Stats
Displays information about the port, if configured in PortView.

Port Type
Type of port. Possible values include: Access, CDP, CDP FTM 1 Backplane, FTM 1 Backplane, and Logical.

Neighbor
The port to which the port is connected.

Port Speed
Speed of the port. Possible values include: 10/100, speed in megabits per second (for example, 800.0 Mbps), Unknown (displayed for logical ports).

VLANs
The VLANs to which the port is associated.

Description
A description of the port and the device.

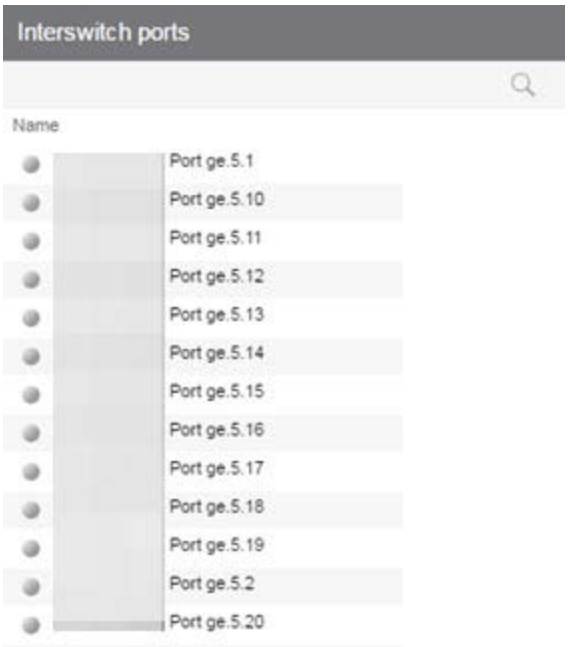
Port Type Details
Additional information about the type of port.

Serial Number
The serial number of the device.

Retrieve Button
Retrieves the most recent information about the ports on the device.

Ports (Port Group)

The Ports panel in the Port Groups navigation tree lists the ports in the selected port group. You can also add and remove ports (user-defined port groups only) by right-clicking the Port Group in the left-hand navigation tree. To access this panel, select a port group in the left-panel **Devices/Port Groups** > **Port Groups** navigation tree.



Name

Name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

Default Role

See Default Role in the Concepts topic for information on default roles. For additional information, see Port Mode.

Alias

Shows the alias (ifAlias) for the interface, if one is assigned.

Port Type

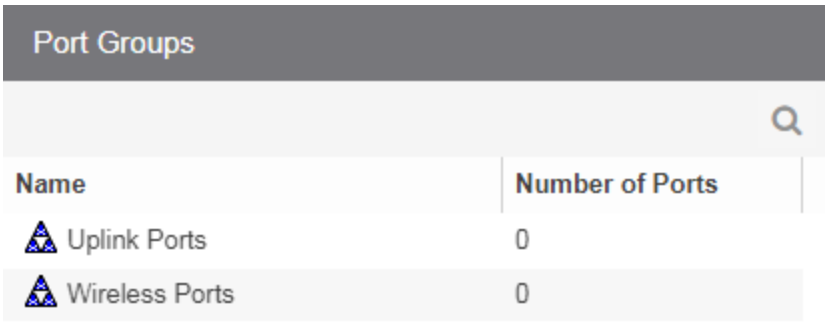
Type of port. Possible values include: Access, Interswitch Backplane, Backplane, Interswitch, and Logical.

Port Speed

Speed of the port. Possible values include: 10/100, speed in megabits per second (for example, 800.0 Mbps), Unknown (displayed for logical ports).

Details View (Port Groups)

This tab displays when you select the **Devices/Port Groups > Port Groups** left-panel tab. It displays a table of information about the existing port groups.



Name
Name of the port group.

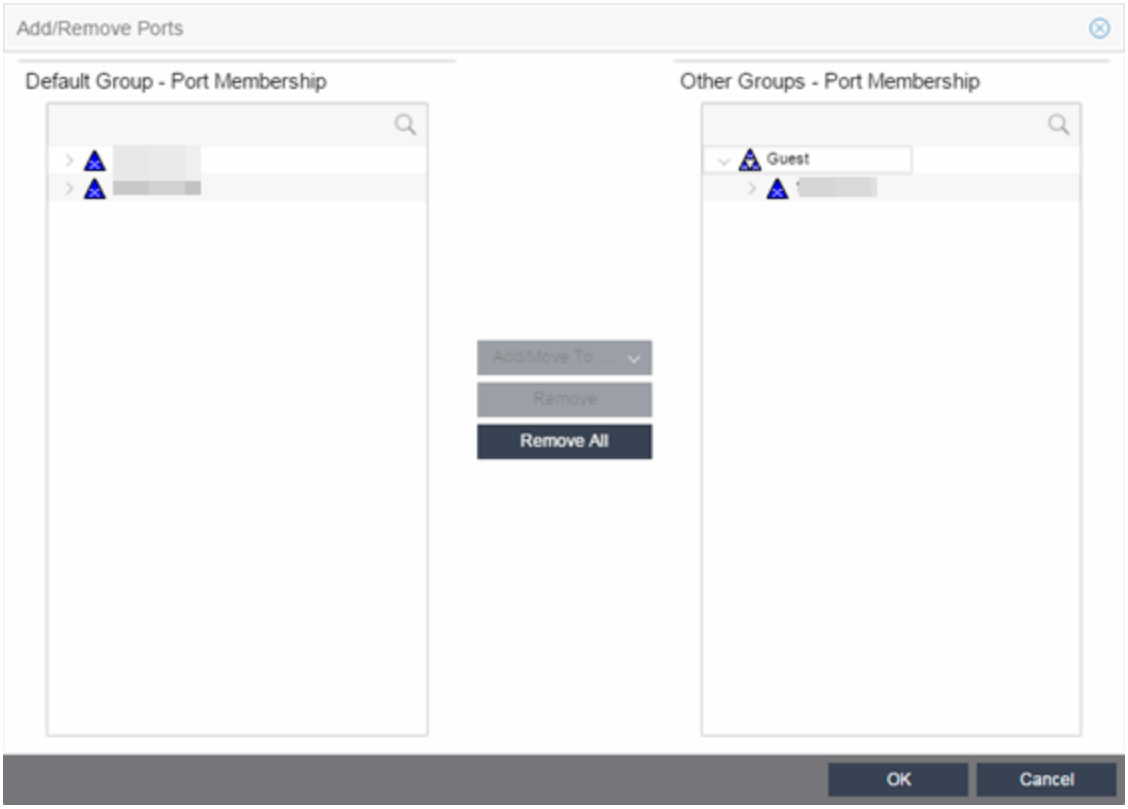
Number of Ports
Number of ports in the port group.

Add/Remove Ports (User-Defined Port Groups)

Use the Add/Remove Ports window to add and remove ports from user-defined port groups.

To access this window, select the left-panel Port Groups tab. Expand the User-Defined Port Groups folder and select a port group. From this window you can:

- Select the **Add/Remove Ports** button in the right-panel **Ports** tab.
- Right-click a Port Group in the left-panel and select **Add/Remove Ports**.



Default Group — Port Membership

This list displays all the device groups, devices, and port groups in the current domain. Select the ports you want to add to the port group. You can select individual ports, devices, or groups of ports.

Other Groups — Port Membership

This field displays all the ports currently defined for the port group. Select the port you want to remove from the port group.

Add/Move To Button

Select **Add/Move To** and select the port group to add the ports selected in the **Default Group — Port Membership** list to the **Other Groups — Port Membership** list.

Remove Button

Select **Remove** to remove the ports selected in the **Other Groups — Port Membership** list from the port group.

Remove All Button

Select **Remove All** to remove all the ports in the **Other Groups — Port Membership** list.

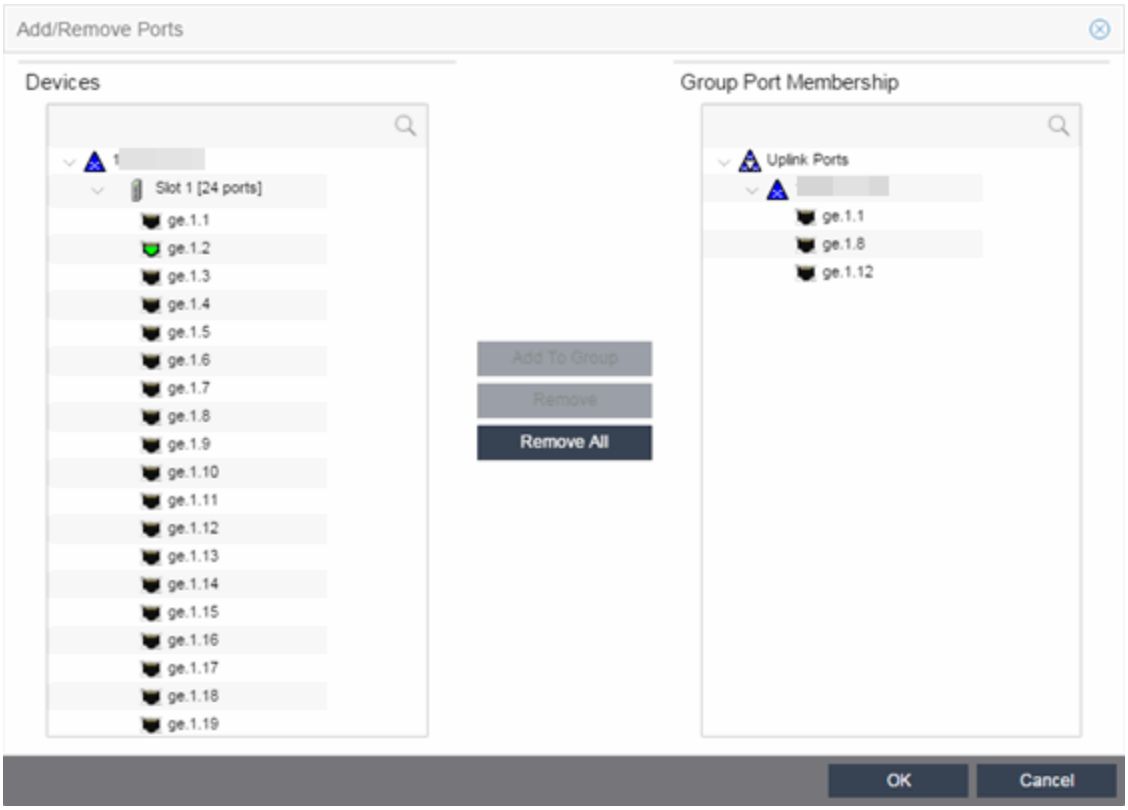
Add/Remove Ports

In this window, you can add and remove ports to and from port groups. Initially, all ports are grouped into a Default port group. When you create new port groups, you add ports from the Default group into your newly defined port groups using this window.

To access this window, open the **Devices > Port Groups** tab. Then, right-click on the port group to which the ports are being added and select **Add/Remove Ports**. The Add/Remove Ports window opens with the ports in the Default port group displayed in the left panel.

Add ports to the port group by selecting the ports in the left-panel, then selecting the port group in the right panel and selecting **Add To Group**.

NOTE: User based ports are not listed because user based port groups can only be one default.



Devices

This field displays the Devices assigned to the Policy Domain. Ports grouped in the Devices list are not members of the Port Group.

Group Port Membership

This field displays any port groups you have created and their currently defined ports.

Add To Group Button

Adds the ports selected under the Devices list to the port group selected on the right.

Remove Button

Select the ports you want to remove from a port group and select **Remove** to return the ports to the Devices list.

Remove All Button

Select a port group and select **Remove All** to remove all ports from the port group and return them to the Devices list.

Port Authentication Configuration

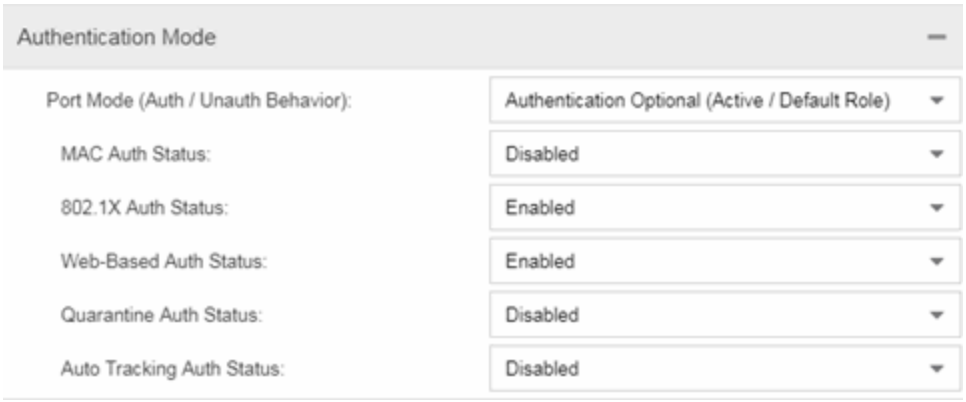
The **Port Configuration** tab allows you to configure and change the authentication settings for a port. Authentication must be configured and enabled on the device in order for individual port authentication settings to take effect. Only those areas of the tab that relate to the authentication type configured on the device are available for editing.

The **Authentication Configuration** tab has six sections:

- Authentication Mode
- RFC3580 VLAN Authorization
- Login Settings
- Automatic Re-Authentication
- Authenticated User Counts
- CEP Access

Authentication Mode

This section displays general authentication and port mode information about the port.



Port Mode

Port mode defines whether or not a user is required to authenticate on a port, and how unauthenticated traffic will be handled. It is a combination of Authentication Behavior (whether or not authentication is enabled on the port), and Unauthenticated Behavior (whether unauthenticated traffic will be assigned to the port's default role or discarded).

- **Authentication Behavior** -- Defines whether or not end users are required to authenticate on the port (device).

    - **Active** -- Normal authentication procedures are implemented. End users are required to authenticate.
    - **Inactive** -- Authentication of end users is not required.
- **Unauthenticated Behavior** -- Defines how the traffic of unauthenticated end users will be handled on the port.
    - **Default Role** -- If the end user is unauthenticated, the port will implement its default role. If there is no default role, there will be no role on the port.
    - **Discard** -- If the end user is unauthenticated, no traffic is allowed on the port.

These two settings can be combined to create four possible port modes.

- **Inactive/Discard Mode**: In this mode, authentication is inactive for the port. All traffic from users connected to the port is discarded. This effectively turns the port off. This port mode is not available for Single User MAC Authentication.

- **Inactive/Default Role Mode**: In this mode, authentication is inactive for the port. All users connecting to this port will use the default role, if one has been assigned to the port, in combination with any existing static classifications. If there is no default role assigned to the port, the port uses only the static classification rules which exist. If there are no static rules, the port uses the PVID and default class of service for the port. This is the default port mode for ports.

- **Active/Discard Mode**: In this mode, authentication is active for the port and end users are required to authenticate. All traffic from unauthenticated users connected to the port is discarded. The Unauthenticated Behavior varies depending on the type of authentication configured on the device.

  Single User Web-based Authentication: If authentication is successful, the port is assigned the end user's role as its current role. If unsuccessful, all traffic is discarded. A default role has no meaning on this Active/Discard port, since all unauthenticated traffic is discarded.

  Single User 802.1X and 802.1X+MAC Authentication: If authentication is successful, the port is assigned the end user's role as its current role. If unsuccessful, all traffic is discarded. This mode requires that there be **no** default role assigned to the port.

  Single User MAC Authentication: This port mode is not available for Single User MAC Authentication.

  Multi-User 802.1X and MAC Authentication: If authentication is successful, the port is assigned the end user's role as its current role. If unsuccessful, all traffic is discarded. A default role has no meaning on this Active/Discard port, since all unauthenticated traffic is discarded.

  Multi-User Web-based Authentication: This port mode is not available for Multi-User Web-

based Authentication.

Advantages of Active/Discard mode: This mode is highly secure, since the end user receives no network services at all until authentication is successful.

Disadvantages of Active/Discard mode: The unauthenticated end user is unable to connect to any network services, such as the Domain Controller (if using a Microsoft operating system), DHCP services, DNS services, or the Web proxy. In single user web-based authentication, the device spoofs WINS/DNS services (if the functionality is enabled) in order to allow the user to communicate with it for authentication.

- **Active/Default Role Mode** - In this mode, authentication is active for the port and end users are required to authenticate. If authentication is successful, the port is assigned the end user's role as its current role. All unauthenticated users connected to the port will use the default role, if one has been assigned to the port, in combination with any existing static classifications. If there is no default role assigned to the port, the port uses only the static classification rules which exist. If there are no static rules, the port uses the PVID and default class of service for the port. For Single User 802.1X and 802.1X+MAC Authentication, this mode **requires** that a default role be assigned to the port.

  Advantages of Active/Default Role mode: In this mode, a default role is applied to the port to allow unauthenticated end users access to basic services such as the DHCP Server, Domain Services, WINS, and the Web proxy. When the end user is authenticated, that user's role is applied to the port, providing a customized set of services allowed by his or her role. Active/Default Role mode is an alternative to Active/Discard mode, which is limiting in that there are no network services available at all until the end user is authenticated.

  Disadvantages of Active/Default Role mode: This mode is less secure than Active/Discard, in that the user receives some network access prior to authentication.

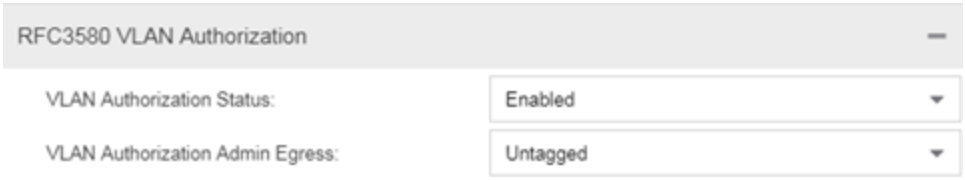
RFC3580 VLAN Authorization Tab

This tab lets you enable or disable RFC 3580 VLAN Authorization on the port and specify an egress state. RFC 3580 VLAN Authorization must be enabled in networks where the RADIUS server has been configured to return a VLAN ID when a user authenticates.

When RFC 3580 VLAN Authorization is enabled:

- ports on devices that do **not** support policy tag packets with the VLAN ID.
- ports on devices that do support policy and also support Authentication-Based VLAN to Role Mapping classify packets according to the role to which the VLAN ID maps.

You can also enable and disable VLAN Authorization at the device level using the device **Authentication** tab. If the device does not support RFC 3580, this tab is grayed out.



VLAN Authorization Status

Allows you to enable and disable RFC 3580 VLAN Authorization for the selected port. This option is grayed out if not supported by the device.

VLAN Authorization Admin Egress

Allows you to modify the VLAN egress list for the VLAN ID returned by the RADIUS server when a user authenticates on the port:

- None - No modification to the VLAN egress list will be made.
- Tagged - The port will be added to the list with the egress state set to Tagged (frames will be forwarded as tagged).
- Untagged - The port will be added to the list with the egress state set to Untagged (frames will be forwarded as untagged).
- Dynamic - The port will use information returned in the RADIUS response to modify the VLAN egress list. This value is supported only if the device supports a mechanism through which the egress state may be returned in the RADIUS response.

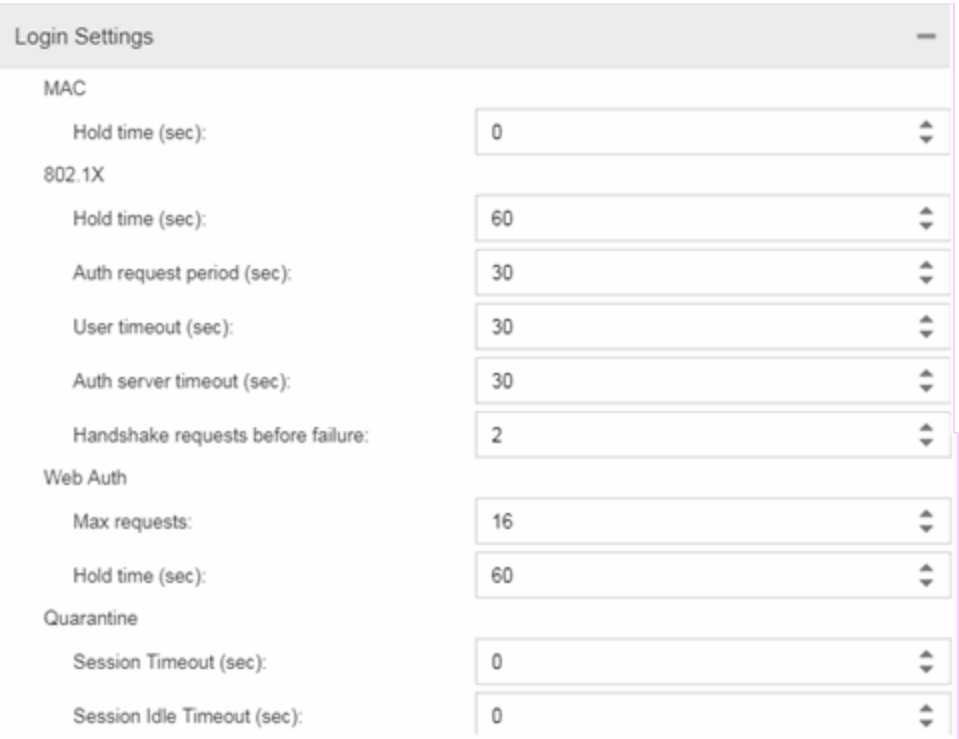
The current egress settings for the port are displayed in the VLAN Oper Egress column in the **User Sessions** tab. These options are grayed out if not supported by the device.

Apply Button

Saves any change you made to the VLAN Authorization settings.

Login Settings

This tab displays the current login settings for the port and allows you to change the settings if desired. The options available depend on what type(s) of authentication are enabled on the device.



Number of Attempts Before Timeout

Number of times a user can attempt to log in before authentication fails and login attempts are not allowed. For web-based authentication, valid values are 1-2147483647, zero is not allowed, and the default is 2. For 802.1X and MAC authentication, this value is permanently set to 1.

Hold Time (seconds)

Amount of time (in seconds) authentication will remain timed out after the specified Number of Attempts Before Timeout has been reached. Valid values are 0-65535. The default is 60. (Hold Time is also known as Quiet Period in web-based and MAC authentication.)

Authentication Request Period

For 802.1X authentication, how often (in seconds) the device queries the port to see if there is a new user on it. If a user is found, the device then attempts to authenticate the user. Valid values are 1-65535. The default is 30.

User Timeout

For 802.1X authentication, the amount of time (in seconds) the device waits for an answer when querying the port for the existence of a user. Valid values are 1-300. The default is 30.

Authentication Server Timeout

For 802.1X authentication, if a user is found on the port, the amount of time (in seconds) the device waits for a response from the authentication server before timing out. Valid values are 1-300. The default is 30.

Port Handshake Requests Before Failure

For 802.1X authentication, the number of times the device tries to finalize the authentication process with the user before the authentication request is considered invalid and authentication fails. Valid values are 1-10. The default is 2.

Quarantine Session Timeout (sec)

For Quarantine authentication, the maximum number of seconds an authenticated session may last before automatic termination of the session. A value of zero indicates that no session timeout will be applied.

Quarantine Session Idle Timeout (sec)

For Quarantine authentication, the maximum number of consecutive seconds an authenticated session may be idle before automatic termination of the session. A value of zero indicates that the device level setting is used.

Auto Tracking Session Timeout (sec)

For Auto Tracking sessions, the maximum number of seconds a session may last before automatic termination of the session. A value of zero indicates that the device level setting is used.

Auto Tracking Session Idle Timeout (sec)

For Auto Tracking sessions, the maximum number of consecutive seconds a session may be idle before automatic termination of the session. A value of zero indicates that the device level setting is used.

Apply Button

Applies the Login Settings changes to the port.

Automatic Re-Authentication

This tab is grayed out if only web-based authentication is enabled on the device. For 802.1X and MAC authentication, the Automatic Re-Authentication tab lets you set up the periodic automatic re-authentication of logged-in users on this port. Without disrupting the user's session, the device repeats the authentication process using the most recently obtained user login information to see if the same user is still logged in. Authenticated logged-in users are not required to log in again for re-authentication, as this occurs "behind the scenes."



802.1X Re-auth Status
If **Active** is selected, the re-authentication feature is enabled for 802.1X authentication. If **Inactive** is selected, the re-authentication feature is disabled.

802.1X Re-auth Frequency (sec)
How often (in seconds) the device checks the port to re-authenticate the logged-in user via 802.1X authentication. Valid values are 1-2147483647. The default is 3600.

MAC Re-auth Status
If **Active** is selected, the re-authentication feature is enabled for MAC authentication. If **Inactive** is selected, the re-authentication feature is disabled.

MAC Re-auth Frequency (sec)
How often (in seconds) the device checks the port to re-authenticate the logged in user via MAC authentication. Valid values are 1-2147483647. The default is 3600.

Authenticated User Counts

This tab provides authenticated user-count information for devices with Multi-User as their configured authentication type. See the device Authentication tab for information on setting the device authentication type.



Current Number of Users
The current number of users actively authenticated or have authentications in progress on this interface. If **Multi-User** authentication is disabled, this number is **0**. Any unauthenticated traffic on the port is not included in this count.

Number of Users Allowed (up to 2048)
The number of users that can be actively authenticated or have authentications in progress at one time on this interface. If you set this value below the current number of users, end-user sessions exceeding that number are terminated.

NOTE: B2/C2 Devices. If you are configuring a single user and an IP phone per port, set this value to **2**.

Number of MAC Users Allowed (up to 2048)

The number of users that can be actively authenticated via MAC authentication, or have MAC authentications in progress at one time on this interface. The number of MAC users allowed cannot exceed the number of users allowed. If you set this value below the current number of users, end user sessions exceeding that number are terminated. If MAC is not selected as a **Multi-User** authentication type on the device Authentication tab, this field will be grayed out.

Number of Quarantine Users Allowed (up to 2048)

The number of users that can be actively authenticated via Quarantine authentication, or have Quarantine authentications in progress at one time on this interface. The number of Quarantine users allowed cannot exceed the number of users allowed. If you set this value below the current number of users, end user sessions exceeding that number are terminated. If Quarantine Auth is not enabled on the device Authentication tab, this field will be grayed out.

Number of Auto Tracking Users Allowed (up to 2048)

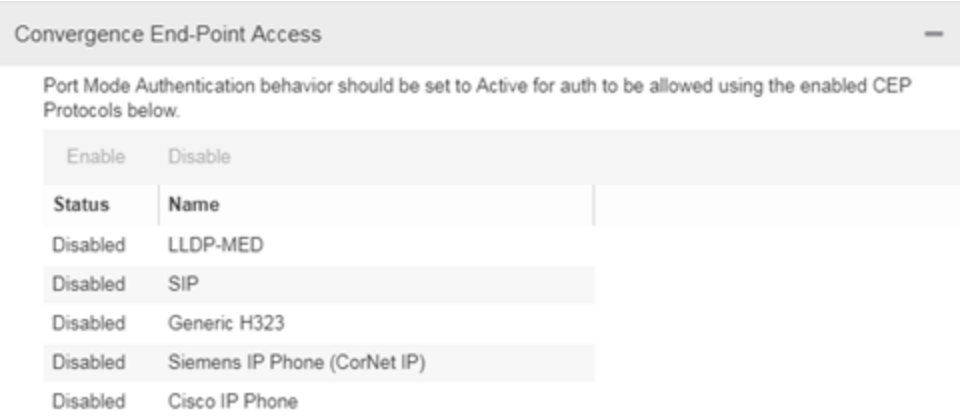
The number of Auto Tracking users that can be actively authenticated or have authentications in progress at one time on this interface. The number of Auto Tracking users allowed cannot exceed the number of users allowed. If you set this value below the current number of users, end user sessions exceeding that number will be terminated. If Auto Tracking is not enabled on the device Authentication tab, this field is grayed out.

Convergence End-Point Access

This tab lists all the CEP (Convergence End-Point) protocols supported by the device on which the port resides, and lets you enable or disable them for that port. For devices that do not support CEP, the tab is blank.

NOTE: **Port Mode Authentication Behavior** must be set to **Active** (on the General sub-tab) for authentication to be allowed using these CEP Protocols.

Enable CEP protocols for multiple ports using the Port Configuration Wizard. In addition to enabling protocols on the port, you must also configure CEP for the device on which the port resides. Configure CEP for a single device using the device Authentication tab (CEP sub-tab) or for multiple devices using the Device Configuration Wizard.



CEP Access
Lists all the CEP protocols supported by the device on which the port resides. Use the checkboxes to enable or disable CEP protocols on this port. If the device does not support the CEP feature, this area is blank.

Enable All Button
Selects all the checkboxes and enables all the CEP protocols for this port.

Disable All Button
Deselects all the checkboxes and disables all the CEP protocols for this port.

Apply Button
Applies CEP access changes to the port.

How To Use Policy

The **How To** section contains Help topics that give you instructions for performing tasks in the **Policy** tab.

How to Select on Add/Remove Windows

The **Policy** tab includes several Add/Remove windows in which you can add items from a left panel to a right panel, and remove items from the right panel. The following procedures explain how to make single and multiple selections in the panels and move the selections to the opposite panel.

Instructions on:

- Selecting single items
- Selecting multiple sequential items
- Selecting multiple non-sequential items

Selecting single items

To select one item from the left panel and add it to the right panel, select the item, then select the **Right Arrow** button.

To remove one item from the right panel, select the item, then select the **Left Arrow** button.

Selecting multiple sequential items

To select a sequence of items in the left panel and add them to the right panel:

1. Hold down the **Shift** key and select the first and last (or last and first) items in the sequence.
2. Select the **Right Arrow** button.

To remove a sequence of items from the right panel:

1. Hold down the **Shift** key and select the first and last (or last and first) items in the sequence.
2. Select the **Left Arrow** button.

Selecting multiple non-sequential items

To select multiple non-sequential items in the left panel and add them to the right panel:

1. Hold down the **Ctrl** key and select each item you want to add.
2. Select the **Right Arrow** button.

To remove multiple non-sequential items from the right panel:

1. Hold down the **Ctrl** key and select each item you want to remove.
2. Select the **Left Arrow** button.

How to Create and Use Domains

ExtremeCloud IQ Site Engine provides the ability to create multiple policy configurations by allowing you to group your roles and devices into Policy Domains. A Policy Domain contains any number of roles and a set of devices that are uniquely assigned to that particular domain. For example, a university can have a Dormitory domain with a policy configuration created for students, and an Administration domain with a policy configuration for staff members.

You can create multiple domains and easily switch from one domain to another. You can also export policy domain configuration data to a .pmd file, (one file per domain) for backup and troubleshooting purposes, and you can import data from a .pmd file into a policy domain.

In order for your network devices to be displayed in the **Policy** tab's left-panel **Devices** tab, they must be assigned to a Policy Domain. Initially, you must use a device Discover to add your devices to the ExtremeCloud IQ Site Engine database. After your devices are in the database, you can assign the

devices to a Policy Domain. As soon as the devices are assigned to a domain, they are automatically displayed in the **Policy** tab's left-panel **Devices** tab. Only devices that support policy are displayed.

ExtremeCloud IQ Site Engine automatically locks the current Policy Domain when you begin to edit the domain configuration. Other users are notified that the domain is locked and they are not be able to save their own domain changes until the lock is released. For more information, see Controlling Client Interactions with Locks. After a modification is made, you must save the domain to notify all clients that are viewing that domain of the change, and automatically update their view with the new configuration.

Instructions on:

- Creating a New Domain
- Opening a Domain
- Assigning Devices to a Domain
- Removing Devices From a Domain
- Importing a File into a Domain
- Exporting a Domain to a File
- Importing Data from a Domain
- Saving a Domain
- Reading a Domain
- Renaming a Domain
- Deleting a Domain

Creating a New Domain

Use these steps to create a new Policy Domain.

1. Select **Open/Manage Domain > Create Domain**.
2. Enter the name for the new domain. Select **OK**.
3. A new (blank) Domain opens.
4. Select the **Global Domain Settings > Do Not Use Global Services** checkbox if you don't want the domain to include and display services common to all domains.
5. Proceed with assigning devices to the domain and then configuring the desired policies.

Opening a Domain

In ExtremeCloud IQ Site Engine, you work in one current domain at a time. To change to a different domain, use the **Open/Manage Domain > Open Domain** menu to select the desired domain. If you have made changes to the current domain, you are prompted to update the database with the current domain configuration prior to opening the new domain.

Assigning Devices to a Domain

Initially, you must perform a device Discover to add a device to the ExtremeCloud IQ Site Engine database. After your devices have been added to the database, you must assign the devices to a Policy Domain. A device can exist in only one Policy Domain. As soon as the devices are assigned to a domain, they are automatically displayed in the **Policy** tab's left-panel **Devices** tab. Only devices assigned to the Policy Domain you are currently viewing are displayed in the tab.

Use these steps to assign devices to a Policy Domain.

1. If necessary, open the domain to which you want to assign devices.
2. Select **Open/Manage Domain > Assign Devices to Domain**. The Assign Devices to Domain window opens.
3. Devices in the database but not assigned to a domain are listed in the left-panel Unassigned folder (including devices that do not support policy). The left panel also displays any other domains and the devices assigned to those domains. Use the drop-down list to select a single domain or All Other Domains. If you select All Other Domains, use the bottom panel to view the domain to which each device is assigned.

   Note: Select the search icon to search for a device. A search box is available to filter through the visible device tree.
4. The right panel displays the current domain and the devices assigned to that domain. To add a device to the current domain, select the device in the left panel and select **Add**. You can also select and add multiple devices.
5. To remove a device from the current domain, select the device and select **Remove**. This removes the device from the current domain and places it back in the device tree as either unassigned or as a member of the domain from which it came. It does not delete the device from the ExtremeCloud IQ Site Engine database.
6. Select **OK**.
7. The selected devices are assigned to the current domain and displayed in the **Policy** tab left-panel **Devices** tab. (Only devices that support policy are assigned to the domain and displayed.)

Removing Devices From a Domain

Removing a device from a domain, removes the device from the **Devices** tab and places it in the Unassigned folder in the Assign Devices to Domain window.

NOTE: Removing a device from a domain does not delete the device from the ExtremeCloud IQ Site Engine database. To delete a device from the database, right-click on the device in the left-panel **Devices** tab, and select **Delete** from the menu. When a device is deleted from the database, it is automatically removed from ExtremeCloud IQ Site Engine and the **Devices** tab.

1. If necessary, open the domain from which you want to remove devices.
2. Select **Open/Manage Domain > Assign Devices to Domain**. The Assign Devices to Domain window opens.
3. The right panel displays the current domain and the devices assigned to that domain. To remove a device from the current domain, select the device from the Current Domain right-panel and select the left arrow. This removes the device from the current domain and places it back in the device tree as either unassigned or as a member of the domain from which it came. It does not delete the device from the ExtremeCloud IQ Site Engine database.
4. Select **OK**.

Importing a File into a Domain

You can import policy data from a PMD file into a Policy Domain.

1. Make sure that the domain you want to import a file into is your current domain.
2. Select **Open/Manage Domain > Import/Export > Import From File**. The Import from File window opens.
3. Enter the name and path for the data file (PMD) you want to import, or browse to the file. Selecting **Select File**, opens a dialog box from which you can select a data file by searching your local drive or a network drive.
4. Select the specific data elements you want to import or select **Select All** to select all the data import options. See Data Elements to Import for important information on each element and how they are imported.
5. To append, update, or overwrite the global rules with the PMD file you are importing, select the **Global Services & Rules** checkbox.
6. Select how you want the imported data applied to your current domain. Select the links below for detailed information on how each specific action affects the import of certain data elements.
    - Append data to existing elements
    - Update existing data with elements from domain
    - Overwrite existing elements
7. Select **OK**. The data elements are imported and see a message regarding import status.

Exporting a Domain to a File

You can export policy data from a Policy Domain to a PMD file.

1. Select **Open/Manage Domain > Import/Export > Export to File**.
2. Select the **Domain** to save as a PMD file.

3. Select **Export**.
4. The Policy Domain is downloaded to the default file download location.

Importing Data from a Domain

You can import policy configuration data from one policy domain into another.

1. Ensure your current domain is the domain into which you want to import data.
2. Select **Open/Manage Domain > Import/Export > Import From Domain**. (This menu option is not available if only one domain exists, as there are no other domains from which to import data.) The Import from Domain window opens.
3. Use the drop-down list to select the domain whose data you want to import.
4. Select the specific data elements you want to import or select **Select All** to select all the data import options. See Data Elements to Import for important information on each element and how they are imported.
5. Select how you want the imported data applied to your current domain. Select the links below for detailed information on how each specific action affects the import of certain data elements.
    - Append data to existing elements
    - Update existing data with elements from domain
    - Overwrite existing elements
6. Select **Import**. The data elements are imported and you see a message regarding import status.

Saving a Domain

After a Policy Domain has been changed, you must save the domain to notify all clients using that domain of the change and automatically update their tab with the new configuration. An asterisk (*) is displayed beside the Policy tab title when you have made changes to the domain that need to be saved. You can save a Policy Domain by selecting Open/Manage Domain > Save Domain. To discard unsaved changes you made to a domain, open the Open/Manage Domains > Open Domain menu and select the domain in which you are currently working.

Renaming a Domain

You can rename the current Policy Domain by selecting Open/Manage Domain > Rename Domain and entering a new name.

Deleting a Domain

You can delete one or more Policy Domains by selecting Open/Manage Domain > Delete Domain.

How to Create a Role

A role is a policy profile consisting of a set of network access services that you can apply at various access points in a policy-enabled network. A port takes on a user's role when the user authenticates.

Creating a role using the role tabs consists of creating a name for the role with the **Create Role** menu option, then defining its characteristics (default class of service, default access control, and/or services) using the role's right-panel tabs. You might also use this method if you are creating a role for which there is default class of service and/or access control, but no services.

If you want to change the characteristics of a role, you can select the role in the left panel and use the right panel to modify it.

Instructions on:

- Using the **Role** Tabs
- Modifying a Role
- Deleting a Role

Using the Role Tabs

Creating a role using the **Role** tab consists of creating a name for the role, then using the right panel to specify the characteristics of the role (default class of service, default access control, and/or services).

1. In the **Policy** tab left panel, select the **Roles/Services > Roles** tab.
2. Right-click the **Roles** tab, and select **Create Role**.
   The Create window opens.
3. Type the role name in the highlighted box. The name can be up to 64 characters in length, and special characters are allowed, with the exception of colons (:) and semicolons (;). Duplicate names are not allowed, regardless of case. For example, if you already have a role `Faculty` and you attempt to name the new role `Faculty` or `faculty`, the **Policy** tab creates the role, but with the name `New Role`, or `New Role`*n* (where *n* is the sequence number, if there is more than one `New Role`). You can then rename the new role. Press **Enter** after you've entered the name. (If you don't press **Enter**, the name remains `New Role`.)
4. Select the role in the left panel, and the role opens in the right panel. Use the right panel to add a role description, enable TCI Overwrite, and set the role's default actions (including access control and class of service).
5. In the Services section in the right panel, select the **Add/Remove Services** button to add services to the role. This opens the role Add/Remove Services window.

> **NOTE:** The **Policy** tab checks for rule conflicts when more than one service is added. See Conflict Checking for more information.

6. To add a VLAN to the Role's Egress list, select the role and use the **VLAN Egress** tab in the right panel.
7. To configure MAC, IP, and VLAN to role mapping lists for the role, select the role and use the **Mappings** tab in the right panel.
8. Now that you have created the role, you can:
    - Assign the role as the default role for a port
    - Modify the role's characteristics
9. Enforce to write the new information to the devices.

Modifying a Role

Once you've created a role, you can change its characteristics by selecting the role in the Policy tab's left panel and using the associated tabs in the right panel.

Instructions on:

- Adding Services to Roles
- Modifying a Role's Default Class of Service
- Modifying a Role's Default Access Control
- Modifying a Role's Description
- Modifying a Role's Ports
- Removing Services from Roles

Adding Services to Roles

To add services to roles:

1. Select the left panel **Roles/Services > Roles** tab and expand the **Roles** tab. Select the role to which you want to add services in the left panel, then select the **General** tab in the right panel.
2. Select **Add/Remove Services**. This opens the Add/Remove Services window.
3. Make sure the role to which you wish to add services is displayed in the Role selection box.
4. In the Groups and Services panel, select the services and/or service groups you wish to add to the role, and select the **Right Arrow** button. To remove services, select them in the Selected Services panel and select the **Left Arrow** button.

NOTE: The Policy tab checks for rule conflicts when more than one service is added. See Conflict Checking for more information.

---

5. If you wish, you can select another role, and add or remove services from it.

6. Select **OK**.
7. Enforce to write the new information to the devices.

Removing Services from a Role

1. Select the left panel **Roles/Services > Roles** tab and expand the Roles folder.
2. Select the role from which you want to remove services, then select the **General** tab in the right panel.
3. Select **Add/Remove Services**. This opens the Add/Remove Services window.
4. Make sure the role from which you wish to remove services is displayed in the Role selection box.
5. In the Selected Services panel, select the services and/or service groups you wish to remove from the role, and select the **Left Arrow** button. To add services, select them in the Groups and Services panel and select the **Right Arrow** button.
6. If you wish, you can select another role, and remove services from or add services to it.
7. Select **OK**.
8. Enforce to write the new information to the devices.

Modifying a Role's Default Class of Service

Use the role's General tab to change its default class of service settings. Be sure to enforce to write the new information to the devices.

Modifying a Role's Default Access Control

Use the role's General tab to change its default access control. Be sure to enforce to write the new information to the devices.

Modifying a Role's Description

You can edit the description for the role on the role's General tab. Select OK to save the change to the database.

Modifying a Role's Ports

You can select a port and choose the default role on the Ports tab. You can also select PortView to open the PortView for the port or make changes to the port settings themselves.

1. In the **Policy** tab left panel, select a device in the **Devices** left-panel tab.
2. Select the port on which you want to set a default role.
3. Right-click the port and select **Policy > Set Default Role**.
4. Select the **Assign/Replace Default Role** checkbox. The drop-down list is available.

5. Select the default role for the port from the drop-down list.
6. Select **OK**.
7. Enforce to write the new information to the devices.

Mapping a Role to an HTTP Redirect Group

The HTTP Redirect action allows the role/rule to be mapped to an HTTP Redirect group index. The action widgets contain a menu to edit the group configuration.

Deleting a Role

1. In the **Policy** tab left panel, select a device in the **Devices** left-panel tab.
2. Select the port on which you want to delete the default role.
3. Right-click the port and select **Policy > Set Default Role**.
4. Select the **Clear Default Role** checkbox.
5. Select the default role for the port.
6. Select **OK**.
7. Enforce to write the new information to the devices.

How to Assign a Default Role to a Port

In the **Policy** tab, you can specify a default role for the port. To configure ports you use the Set Default Role window.

Assigning and Clearing a Default Role

Configuring a port allows you to set the port mode, establish login settings, set the default role, and enables you to view the current configuration on the port.

- Assigning Default Roles to Ports
- Clearing Default Roles from Ports

Assigning Default Roles to Ports

NOTE: Setting a default role on an ExtremeWireless Controller port that is not yet a VNS, creates a new VNS on the wireless controller.

1. Select a device in the left-panel **Devices** tab and expand a slot or ports grouping in the right-panel Details view.

2. Right-click the desired port and select **Policy > Set Default Role** from the menu. The Set Default Role window opens.
3. Select **Assign/Replace Default Role** and select a role in the drop-down list.
4. Select **OK**.

Clearing Default Roles from Ports

You can clear the default role from a single port, or from multiple ports.

1. Select a device in the left-panel **Devices** tab and expand a slot or ports grouping in the right-panel Details view.
2. Right-click the desired port and select **Policy > Set Default Role** from the menu. The Set Default Role window opens.
3. Select **Clear Default Role**.
4. Select **OK**.

NOTE: If you are replacing the current default role with another one, you don't need to clear the current default role. Selecting the new default role and selecting **OK** clears the previous default role automatically.

How to Create a Quarantine Role

The Quarantine role is a highly restrictive role used to isolate users and restrict network access.

The Quarantine role is used in conjunction with the Extreme Networks Intrusion Prevention System (IPS) to create an automatic response to threats detected on the network. After the Quarantine role has been enforced to the network and the Extreme Networks IPS is properly configured, this role can be automatically set as the default role on any port where a threat has been detected. Normally, roles are applied to ports via authentication.

You can also set the Quarantine role as a port's default role if, for example, you have modified the role to provide some limited access and you want to use it as a "guest" role.

The **Policy** tab default domain includes the Quarantine role. However, if you add a new domain, you need to create the Quarantine role. For information on how to create a role, see How to Create a Role.

After you have created the role, you can modify the role's default class of service and access control settings, and make changes to the role's services and rules using the right-panel tabs, just like any other role. If you make any changes to the Quarantine role, keep in mind that the role can be used by other applications and should remain highly restrictive in nature.

Instructions on:

- Modifying the Quarantine Role: Use the right-panel tabs to modify the Quarantine role's default values and add or remove services.
- Setting the Quarantine Role as the Default Role on a Port: Use the right-panel General tab or the Port Configuration wizard to set the Quarantine role as a default role on a port.

Modifying the Quarantine Role

When you've created a Quarantine role, you can change its characteristics by selecting the role in the **Policy** tab's left panel and using the associated tabs in the right panel.

NOTE: You cannot rename the Quarantine role.

Modifying Default Values

Use the General tab to change the Quarantine role's default class of service and default access control settings, and to add or edit a description.

1. Select the Quarantine Role in the left-panel **Roles** tab.
2. In the right-panel **General** tab, select the desired default class of service and default access control settings.
3. If desired, add or edit the role's description.
4. Be sure to perform an Enforce to write the new Quarantine role to the devices.

Adding/Removing Services

Use the General tab to add or remove services to the Quarantine role.

1. Select the Quarantine Role in the left-panel Roles tab.
2. In the right-panel General tab, select **Add/Remove Services**. This opens the Add/Remove Services window.
3. Make sure the Quarantine role is displayed in the Role selection box.
4. Select the service or service group in the All Services & Service Groups and select the **Right Arrow** button to add them to the Selected Services & Service Groups list. To remove services, select them in the Selected Services & Service Groups list and select the **Left Arrow** button. To remove all services, select the **Double Left Arrow** button.

   NOTE: The **Policy** tab checks for rule conflicts when more than one service is added. See Conflict Checking for more information.
5. Select **OK**.
6. Be sure to perform an Enforce to write the new Quarantine role to the devices.

Setting the Quarantine Role as the Default Role on a Port

There can be circumstances when you would like to use the **Policy** tab to assign the Quarantine role as the default role on one or more ports. For example, if you have modified the Quarantine role to provide limited access, you can use it as the default role for guest users on your network.

The Quarantine role is assigned as a default role just like any other role. Refer to Assigning Default Roles to Ports for instructions.

How to Create a Service

Services are sets of rules that define how network traffic for a particular network service or application should be handled by a network access device. A service might consist of only one rule governing, for example, email priority, or it might consist of a complex set of rules combining class of service, filtering, rate limiting, and access control (VLAN) assignment. ExtremeCloud IQ Site Engine policy allows you to create Local Services (services unique to the current domain) and Global Services (services common to all domains). Global Services let you easily create and manage services shared between all your domains.

Services can be one of two types: Manual Service or Automated Service.

- **Manual Service** — This service consists of one or more traffic classification rules you create based on your requirements. Manual services are good for applying customized sets of rules to roles.
- **Automated Service** — This service automatically creates a rule with a specified action (class of service and/or access control), for each device in a particular network resource group or groups. You create a network resource group using a list of MAC or IP addresses, and then associate the group with the Automated service (see How to Create a Network Resource for more information). Automated rule types include Layer 2 MAC Address rules, Layer 3 IP Address and IP Socket rules, and Layer 4 IP UDP Port and IP TCP Port rules.

To create a service using the service tabs, right-click the Services tab and select **Create Service**. If you are creating a Manual service, you can then use the Create Rule menu option and the tabs for the rule to define the rules for the service. You can also use the service tabs and rule tabs to modify an existing service and its rules.

Once you've created a service, you can apply it to any number of roles in the **Policy** tab. A role may utilize both Manual and Automated services.

Instructions on:

- Using the Service Tabs
- Modifying a Service
- Deleting a Service

Using the Service Tabs

The following steps depend on whether you are creating a Manual or an Automated service. For an Automated service, you create the service, select the newly created service, and define the class of service and/or access control for the service in the right-panel. For a Manual service, you create the service and then use the Create Rule menu option and the tabs for the rule to define the rules for the service.

Creating an Automated Service

1. In the left panel, select the **Service Repository** tab.
2. Expand either the **Local Services** tab or the **Global Services** tab depending on whether you want the service to be local (unique to the current domain) or global (shared between all your domains).
3. Right-click on the **Services** tab and select **Create Automated Service**. A New Service item is created in the left panel in a highlighted box.
4. Type the service name in the Create window. The service name is case-sensitive; therefore, ExtremeCloud IQ Site Engine policy sees `Engineer` and `engineer` as two different service names. Select **OK**. If you don't do this, the name remains `New Service`. The right-panel displays the service you created.
5. Define the rule's traffic description and actions, and enter a description of the service, if desired. For information on configuring the fields on this tab, see the Automated Service window Help topic.
6. Enforce to write the new information to your devices.

Creating a Manual Service

1. In the left panel, select the **Service Repository** tab.
2. Expand either the **Local Services** tab or the **Global Services** tab depending on whether you want the service to be local (unique to the current domain) or global (shared between all your domains).
3. Right-click on the **Services** tab and select **Create Service**. A New Service item is created in the left panel in a highlighted box.
4. Type the service name in the Create window. The service name is case-sensitive; therefore, the Policy view sees `Engineer` and `engineer` as two different service names. Select **OK**. If you don't do this, the name remains `New Service`. The service is created.
5. Define rules for the service. For more information, see Using the Rule General Tab.

NOTE: When you add more than one rule to a service, ExtremeCloud IQ Site Engine checks for conflicts with other rules in the service. See Conflict Checking for more information.

---

6. Enforce to write the new information to your devices.

Modifying a Service

Once you've created a service, you can change its characteristics by selecting the service or its rules in the left-panel **Services** tab and using the menu options or associated right-panel tabs.

- Modifying a Service Description
- Modifying a Service Name
- Modifying the Roles for a Service
- Modifying the Rules for a Manual Service
- Modifying an Automated Service

Modifying a Service Description

You can edit the description for the service by selecting it and selecting the **Edit** button beside the **Description** field in the right-panel. Enter a description in the Edit Description window and select **Save** to save the change to the database.

Modifying a Service Name

1. In the left panel, select the **Service Repository** tab.
2. Expand the **Local** or **Global Services** tab and then the **Services** tab, and select the service you want to modify.

   NOTE: If the service is a member of a service group and it's more convenient, you can find the service under the service group in the Service Groups folder. Any change you make to the name there are also reflected in the **Services** tab.

3. Right-click the service whose name you want to change, and select **Rename**.
4. Type the new name in the Rename window.
5. Select **OK** to save the change to the database.

Modifying the Roles for a Service

You can see all the roles associated with a particular service in the Role/Service Usage window.

1. In the left-panel **Roles** tab, select the Role to which you are adding or removing a service.
2. Select the Add/Remove button in the Services section of the window to open the Add/Remove Services window.
   - Add a service by selecting it from the All Services & Service Groups column and moving it to the Selected Services & Service Groups column by selecting the right arrow.

- Remove a service by selecting it from the Selected Services & Service Groups column and moving it to the All Services & Service Groups column by selecting the left arrow.

3. Select **OK** to save the changes.
4. Enforce to write the new information to your devices.

Adding a Service to Roles

A newly created service can be added to multiple roles using the Add to Role(s) menu.

1. In the left panel, select the **Roles/Services** drop-down list.
2. Right-click the service or service group(s) and select **Add to Role(s)**.
3. Select one of more Roles to add to the selected Service/Service Group(s) to.
4. Select **OK** to save the changes.

Modifying the Rules for a Manual Service

1. Select the left-panel **Services** tab and locate the service you want to modify.

   NOTE: If the service is a member of a service group and it's more convenient, you can find the service under the service group in the **Service Groups** tab. Any change you make to the rule there will also be reflected in the **Services** tab.

2. Select the service to display its rules.
3. Select the rule you want to change, then use the right-panel tabs to make your changes.
4. Enforce to write the new information to your devices.

Modifying an Automated Service

1. Open the left-panel **Services** tab.

   NOTE: If the service is a member of a service group and it's more convenient, you can find the service under the service group in the **Service Groups** tab. Any change you make to the service there are also reflected in the **Services** tab.

2. Select the service you want to modify. The Automated Service window opens in the right panel.
3. Modify the characteristics of the Automated service as required.
4. Enforce to write the new information to your devices.

Deleting a Service

Deleting a service removes the service and its rules. If copies of the rules exist for other services, those copies are not affected by the deletion. However, deleting the service removes it from any service

groups and roles with which it was associated, so be sure the service is not needed before you delete it. Deleting a Global service deletes the service from all your domains.

1. Select the left-panel **Roles/Services > Service Repository** tab.
2. Expand the **Services** tab in either the **Local Services** or **Global Services** tab, depending on the type of service you are deleting.

   NOTE: If the service is a member of a service group and it's more convenient, you can find the service under the service group in the **Service Groups** tab. Any change you make to the service there are also reflected in the **Services** tab.

3. Right-click the service you want to delete, and select **Delete**.
4. Select **Yes** to confirm, then **OK** to clear the confirmation message.
5. Enforce to write the change to your devices.

How to Create a Service Group

ExtremeCloud IQ Site Engine Policy lets you create service groups into which you can group Local and Global services. A service group can contain any number of services, as well as other service groups. A service can be a part of more than one group.

Instructions on:

- Creating a Service Group
- Adding Services to a Service Group
- Removing Services from a Service Group

Creating a Service Group

1. In ExtremeCloud IQ Site Engine, select the **Control** tab.
2. Open the **Policy** tab and select **Roles/Services** > **Service Repository** left-panel tab. Expand the **Local Services** or **Global Services** tab.
3. Right-click on the Service Groups folder and select **Create Service Group**. This opens the Create window where you can enter a name for the new service group.
4. Type the service group name in the highlighted box and select **OK**. You can now add services to the service group. After a service group has been created at the top level under the Service Groups folder, it can be added to another service group.

Adding Services to a Service Group

A service group can contain any number of services, as well as other service groups. You can add services to a service group by

1. Right-click the service group from which you wish to remove services, and select **Add/Remove Services**.
2. In the Add/Remove Services window, select the services or service groups you want to add to the service group, and select the **Right Arrow** button.
3. Select **OK**.

Removing Services from a Service Group

Use the following steps to remove a service or service group from a service group. Removing a service from a service group does not delete the service itself. If you want to delete the service itself, see Deleting a Service. Keep in mind that if you change the contents of a service group, ExtremeCloud IQ Site Engine automatically updates the services list for any role that the service group is associated with, affecting the rules in the role.

1. Right-click the service group from which you wish to remove services, and select **Add/Remove Services**.
2. In the Add/Remove Services window, select the services or service groups you want to remove from the service group, and select the **Left Arrow** button.
3. Select **OK**.

How to Create or Modify a Rule

Traffic Classification rules enable you to assign a class of service and/or access control (VLAN membership) to network traffic, depending on the traffic's classification type. Classification types are based on layers 2, 3, and 4 of the OSI model, and traffic is classified according to specific layer 2/3/4 information contained in each frame. For more information, see Traffic Classification Rules.

A rule has two main parts: Traffic Description and Actions. The Traffic Description identifies the type of traffic to which the rule pertains. Actions specify whether that traffic is assigned class of service, access control, or both.

In order to create a rule, you must first create a service with which to associate it.

Instructions on:

- Creating a Rule
- Disabling/Enabling a Rule
- Deleting a Rule

Creating a Rule

When you create a rule using the Rule tab, you first create and name the rule using the **Create Rule** menu option, then define its characteristics in the right panel. You can also use the right panel to

modify an exiting rule's characteristics.

1. In the **Policy** tab left panel, select the **Roles/Services > Service Repository** tab.
2. Expand either the **Local** or **Global Services** folder, depending on whether the rule is going to be used locally or by all users.
3. Expand either the **Service Groups** or **Services** folder and select the service for which you want to create a rule.
4. Right-click the service and select **Create Rule**.
5. In the Create Rule window, enter a name for the rule and select the rule type. Select **OK**. The rule is created in the left-panel tree.
6. Select the rule to and use the associated right-panel **Rule** tab to define the rule. Refer to the Rule tab Help topic for information on configuring the rule.
7. Enforce to write the new information to the devices.

Disabling/Enabling a Rule

In the Policy tab, you can disable and enable individual or multiple rules. You can also disable and enable all the rules associated with a service, or all the rules for all the services in a service group. The rule icon in the left panel displays a red X if the rule is disabled.

Disabling a rule is an alternative to deleting and recreating it. If you disable a rule, it is temporarily unavailable for use by the service with which it is associated. However, the rule can be copied to another service and enabled for that service.

Disabling/Enabling an Individual Rule

You can enable or disable a rule on the Rule tab or by right-clicking on the rule in the Service Repository tab and selecting Disable Rule(s) or Enable Rule(s).

1. In the **Policy** tab left panel, select the **Roles/Services > Service Repository** tab.
2. Expand either the **Local** or **Global Services** folder, depending on whether the rule is going to be used locally or by all users.
3. Expand either the **Service Groups** or **Services** folder and select the service for which you want to create a rule.
4. Select the rule you want to disable or enable.
   The Rule tab opens in the right panel.
5. Select **Enable** or **Disable** in the **Rule Status** field. Disabling the rule turns on the red X on the rule icon in the left panel, and re-enabling it turns it off.
6. Enforce to write the new information to the devices.

Disabling/Enabling the Rules for a Service or Service Group

If a service is associated with more than one service group, disabling or enabling the rules for the

service in one service group will disable/enable the rules for the service in the other service groups of which the service is a part.

1. In the **Policy** tab left panel, select the **Roles/Services > Service Repository** tab.
2. Expand either the **Local** or **Global Services** folder, depending on whether the rule is used locally or by all users.
3. Right-click the service or service group containing the rules you want to disable or enable and select **Disable Rule(s)** or **Enable Rule(s)**.
4. Select **Yes** to confirm the change.
5. Enforce to write the new information to the devices.

Deleting a Rule

Deleting a rule removes the rule from a service. If the service is also part of a service group, the rule is deleted there as well, so be sure the rule is not needed before you delete it.

1. In the **Policy** tab left panel, select the **Roles/Services > Service Repository** tab.
2. Expand either the **Local** or **Global Services** folder, depending on whether you are deleting a rule used locally or by all users.
3. Right-click the rule you want to delete, and select **Delete**.
4. Select **Yes** to confirm, then **OK** to clear the confirmation message. The rule is deleted wherever it exists.
5. Enforce to write the new information to the devices.

- Traffic Classification Rules
- Edit Rule Window
- Rule Tab

How to Define Rate Limits

The Policy tab allows you to create and define rate limits as components of a class of service. Rate limits are used to control the transmit rate at which traffic enters and exits ports in your network.

The Policy tab uses role-based rate limits that are tied directly to roles and rules, and are written to a device when the role/rule is enforced.

Instructions on:

- Defining Rate Limits
- Removing a Rate Limit

Defining Rate Limits

Rate limits are defined within a class of service and associated with a specific role via a rule action or as a role default. When role-based rate limits are implemented, all traffic on the port that matches the rule with the associated rate limit cannot exceed the configured limit. If the rate exceeds the configured limit, frames are dropped until the rate falls below the limit.

The rate limit remains on the port only as long as the role using the rate limit is active on the port either as the authenticated role or as the port's default role.

1. Open the **Class of Service > CoS Components** left-panel tab on the **Policy** tab.
2. Right-click the **Rate Limits** left-panel tab and select **Create Rate Limit**.
3. Create a new rate limit using the **Rate Limit** tab.
4. Select the desired CoS and in the **Class of Service** left-panel tab. Select the **View/Edit** button for the appropriate rate limit to open the Create Rate Limit/Shaper window.
5. Fill out the Create Rate Limit/Shaper window:
    a. Specify the desired rate limit.
    b. Select the action you would like performed if the rate limit is exceeded:
        - Generate System Log on Rate Violation — a syslog message is generated when the rate limit is first exceeded.
        - Generate Audit Trap on Rate Violation — an audit trap is generated when the rate limit is first exceeded.
        - Disable Port on Rate Violation — the port is disabled when the rate limit is first exceeded.

        NOTE: N-Series Gold devices do not support rate limit notification.

    c. Select **OK**.

    The rate limit appears in the CoS Configuration table mapped to the CoS.

Role-based rate limits are written to your devices when you enforce the role that includes them.

Removing a Rate Limit

Rate limits remain on a port only as long as the role using the rate limit is active on the port either as the authenticated role or as the port's default role. To remove a rate limit, you must delete it from the Policy tab and then enforce. This removes the rate limit from any roles with it is associated.

1. Select the **Class of Service > CoS Components > Rate Limits** left-panel tab on the **Policy** tab.
2. In the right-panel table, right-click on the rate you want to remove.

3. Select **Delete**.
4. Enforce.

NOTE: If you simply select **None** from the drop-down list, it un-maps the rate from the class of service but it does not remove the rate limit.

How to Create a Class of Service

The **Policy** tab lets you define classes of service (CoS) that can include one or more of the following components: an 802.1p priority, an IP type of service (ToS) value, drop precedence, rate limits, and transmit queue configuration.

Initially, the Class of Service Configuration window (available from the **Policy** tab **Class of Service** left-menu tab) is pre-populated with eight static classes of service, each associated with one of the 802.1p priorities (0-7). You can use these classes of service as is, or configure them to include ToS, rate limit, and/or transmit queue values. In addition, you can also create your own classes of service.

After you have created and defined your classes of service, they are then available when you make a class of service selection for a rule action (**Rule** tab), a role default (**General** tab), or an automated service (**Automated Service** window).

It is recommended that you read Getting Started with Class of Service before creating your classes of service.

Instructions on:

- Creating a Class of Service
- Creating Class of Service Port Groups
- Deleting a Class of Service

Creating a Class of Service

The basic components for a class of service include an 802.1p priority, an IP type of service (ToS) value, drop precedence, rate limits, and transmit queue configuration.

Use the following instructions to create a new class of service using the Class of Service Configuration window.

1. Open ExtremeCloud IQ Site Engine and select **Control** tab > **Policy** tab > **Class of Service** left-menu tab.
2. Right-click the **Class of Service** tab tree and select **Create COS** from the menu.
   The Create window opens.
3. Enter the name for the CoS in the **Name** field and select **OK**.
   The new class of service opens in the right panel.

4. Select the **Edit** button to enter a description for the CoS.
5. Select the **Edit** button next to the **Transmit Queue** field to open the Edit Transmit Queue window, from which you can select a transmit queue for the class of service. If you would like to select a different transmit queue for each port type, select the **Select Q/Port Type** option. Then, when you select **OK**, a window opens where you can specify a different transmit queue for each port type.
6. Select an 802.1p priority from the drop-down list to choose the priority (0-7 with 7 being the highest priority).
7. Select the **Edit** button to select the ToS option to associate an IP ToS (Type of Service) value with the class of service, if desired (see IP Type of Service for more information). Enter a value in the **Type of Service (ToS)** field.
8. Specify a Drop Precedence, if necessary. The Drop Precedence is used in conjunction with the Flex-Edge feature available on K-Series and S-Series (Release 7.11 or higher) devices. Flex-Edge provides the unique capability to prioritize traffic in the MAC chip as it enters the switch. When the Class of Service is assigned to a policy role, and that role is applied to a port via a MAC source address mapping or the port default role, the drop precedence dictates the internal priority (within the MAC chip) that will be used for packets received on the port. If congestion occurs, packets with a high drop precedence are discarded first. Therefore, if a packet is important, it should have a low drop precedence. Refer to the K-Series or S-Series Configuration Guide for more information on the Flex-Edge feature and drop precedence.
9. If desired, use the Rate Limiting/Rate Shaping section to select a port inbound, outbound, and transmit queue rate limit to associate with the class of service. Select **View/Edit** next to the **IRL Port Group Mappings** or **ORL Port Group Mappings** to open the **CoS - Rate Limit Mappings** tab of the Rate Limit Port Groups window where you can add, edit, or delete a rate limit. The rate limit you select here applies to all IRL/ORL port groups. Select the **View/Edit** button next to **TXQ Port Group Shapers** field to open the **CoS - Transmit Queue Mappings tab** to configure transmit queue mappings.
10. If you have ExtremeWireless Controllers on your network, you see an option to select inbound and outbound user rate limits to associate with the class of service. User rate limits specify the bandwidth given to each individual user on a port. Currently, user rate limits are only available for wireless controllers.
11. Select **Open/Manage Domain > Save Domain**. The class of service is created and is listed in the **Class of Service** tab.

After a class of service has been created, you can double-click in the Class of Service Configuration table to modify its characteristics, if necessary.

Creating Class of Service Port Groups

The Policy tab provides the ability to create rate limit port groups that let you group together ports with similar rate limiting requirements. For example, you might want to create a class of service where your edge ports would receive one rate limit while your core ports would receive a different rate limit.

With port groups, you can create a single class of service that assigns a different rate limit to each group.

It also provides the ability to create transmit queue shaper port groups that enable you to isolate certain kinds of sensitive network traffic so that you can give it a high transmit queue priority. For example, ports on a router might be grouped together and configured with a specific rate shaping parameter. A transmit queue port group can contain multiple port queue types (for example, 4-queue ports and 16-queue ports) depending on the type of devices on your network.

Initially, all ports are grouped into a Default port group. When you create new port groups, you add ports from the Default group into your newly defined port groups.

The following instructions are for creating new port groups for an existing class of service.

1. Open the **Class of Service** left-panel tab and select the **Inbound Rate Limit Port Groups**, **Outbound Limit Port Groups**, or **Transmit Queue Port Groups** tab, depending on the type of port group you want to create.
2. Right-click the tab and select **Create Port Group** to create the desired group type: rate limit (RL) port group or transmit queue (TxQ) shaper port group.
   The Create window opens.
3. Enter a name for the port group and select **OK**.
4. The new port group displays in the **Class of Service** left-panel tab under the appropriate port group type.
5. Right-click on the new port group in the left-panel tab and select **Add/Remove Ports**.
6. The Add/Remove Ports window opens with the ports in the Default port group displayed in the left panel. Add ports to the new port group by selecting the ports in the left-panel, then selecting the port group in the right panel, and selecting **Add/Move To**. Select **OK** to save the changes and close the window.
7. Select **Save Domain** in the **Open/Manage Domain** drop-down list.

Deleting a Class of Service

1. Open the **Class of Service** tab.
2. Right-click the class of service you want to remove, and select **Delete**.
3. Select **OK** to confirm that you want the class of service removed.
4. Select **Save Domain** in the **Open/Manage Domain** drop-down list.

How to Configure Transmit Queues

The **Policy** tab allows you to configure transmit queues as a component of a class of service (CoS).

There are two transmit queue configuration capabilities:

- Transmit Queue Configuration — Allows you to set the transmit queue associated with the class of service.
- TxQ Shaper — Transmit Queue Rate Shapers let you pace the rate at which traffic is transmitted out of a transmit queue.

These two capabilities are configured in the Class of Service tab available from the **Policy** tab.

For more information, see the section on transmit queues in Getting Started with Class of Service.

Instructions on:

- Transmit Queue Configuration
- Transmit Queue Rate Shapers

Transmit Queue Configuration

Transmit queues represent the hardware resources for each port used in scheduling packets for egressing the device. By default, the static classes of service 0-7 map to transmit queues 0-7. The actual transmit queue number can vary depending on the number of queues supported by the port.

The Priority column in the Class of Service Configuration window displays the actual transmit queues associated with the class of service for each port type. Double-click in the column to see a drop-down list where you can select a new transmit queue for all port types, or select a different transmit queue for each individual port type.

TIP: For more detailed information, refer to the tooltip that displays when you hover the cursor over the Queue column.

Transmit Queue Rate Shapers

Rate shapers let you pace the rate at which traffic is transmitted out of a transmit queue. Packets received above the configured rate are buffered rather than dropped. Only when the buffer fills are packets dropped.

The following steps describe how to configure rate shapers in the **Policy** tab:

1. In the **Class of Service** left-panel tab, select the class of service where you want to configure the transmit queue.
2. Select the **Edit** button beside the **Transmit Queue** field and select the desired Transmit Queue from the drop-down list.
3. Select **Open/Manage Domain > Save Domain** to save the configuration change to the database.

For more information, see the section on transmit queues in Getting Started with Class of Service.

NOTE: A rate shaper is associated to a specific transmit queue, not a CoS. This means that the 1) you should select the queue you want to use for a CoS first, then set the shaper and 2) all CoS using that queue uses the same rate shaper. Associating a rate shaper to a transmit queue is accomplished via the **CoS - Transmit Queue Mappings** tab. For additional information, see the CoS - Transmit Queue Mappings Tab (Transmit Queue Port Group) Help topic.

How to Define Traffic Descriptions

Traffic Classification rules allow you to assign VLAN membership and/or class of service to network traffic based on the traffic's classification type. Traffic descriptions are the part of a rule that defines this classification type. For more information, see Traffic Classification Rules.

The Edit Rule window accessed via the Traffic Description section of the Rule window is used to define traffic descriptions for new rules.

Use the following steps to create a new rule:

1. Open the **Control** tab.
2. Select the **Policy** tab.
3. In the Policy tab left panel, select the **Roles/Services** tab.
4. Open the Service Repository tab and open either the **Local** or **Global Services** tab, depending on the location of the rule being edited.
5. Open either the **Service Groups** or **Services** tab and select the service for which you want to create a rule.
6. From the menu bar, select **Tools > Create Classification Rule**. You can also right-click the service and select the option from the menu.
   The Rule opens in the right panel.
7. Select the **Edit** button in the Traffic Description area.
   The Edit Rule window opens.
8. Enter the information for the Traffic Description rule. For additional information, see Edit Rule window.
9. Enforce to write the new information to the devices.

How to Use Compressed Dynamic ACLs

Compressed Dynamic ACLs reduce the size of RADIUS Access-Accept messages sent to Fabric Engine (VOSS) devices running VOSS 8.9 or later. VOSS 8.9 increased the maximum length of an individual ACE command from 128 to 255 characters, enabling longer compressed commands. Compression combines multiple ACE entries into a single entry and abbreviates command keywords, allowing more

rules to fit within the approximately 4 KB RADIUS packet size limit. For example, seven uncompressed ACE entries totaling 819 characters can be reduced to a single compressed and abbreviated entry of 103 characters, an 87% reduction in RADIUS VSA payload size.

NOTE: Compressed Dynamic ACLs are supported on all Fabric Engine (VOSS) platforms except XA1400, VSP8600, and Digital Twin. Supported port types include regular ports (tagged or untagged), Flex-UNI ports, and Auto-Sense ports. MLT and SMLT ports are not supported. VSP4450 does not support EAP on Flex-UNI ports.

Use the following steps to create a new rule using a port list classification type, which combines multiple port values into a single ACE:

1. Open the **Control** tab.
2. Select the **Policy** tab.
3. In the Policy tab left panel, select the **Roles/Services** tab.
4. Open the Service Repository tab and open either the **Local** or **Global Services** tab, depending on the location of the service.
5. Open either the **Service Groups** or **Services** tab and select the service for which you want to create a rule.
6. From the menu bar, select **Tools > Create Classification Rule**. You can also right-click the service and select the option from the menu.
   The Rule opens in the right panel.
7. Select the **Edit** button in the Traffic Description area.
   The Edit Rule window opens.
8. In the Layer area, select Layer 4 — Application Transport.
9. In the Traffic Classification Type dropdown, scroll to the bottom of the list and select one of the List types (for example, IP TCP Port Destination List).
10. In the Traffic Classification Value area, select the List radio button and enter the port numbers separated by commas (for example, 37, 38, 1427).
11. Select OK.
12. Configure the appropriate action for the rule in the **Actions** area.
13. Enforce to write the new information to the devices.

When enforced to a Fabric Engine device, ExtremeControl generates a single ACE entry containing all specified ports. For example, a TCP Destination Port List rule with ports 37, 38, and 1427 generates one ACE instead of three separate ACEs.

NOTE: Port values in Range and List fields must be valid numeric values between 0 and 65535. Entering invalid characters may result in unexpected values being saved.

Using Range Compression

Existing TCP/UDP Port Range rules are automatically compressed when enforced to a Fabric Engine (VOSS) device. No additional configuration is required. Access Control converts the range into optimized port/mask pairs combined into a single ACE entry using the mask list keyword syntax. For example, a TCP Destination Port Range of 1000–2000 generates one compressed ACE instead of eight separate ACEs.

The Enforcement Preview window displays the compressed ACL as it will be sent to the switch, including the combined port/mask segments for the full range.

Automatic Command Appreviation

When compression is enabled, ExtremeControl automatically abbreviates ACE command keywords to further reduce the DACL size. The following list shows each command keyword and the abbreviated form generated by ExtremeControl.

Full Command	**Abbreviated**
ethernet	eth
ether-type	et
ip-protocol-type	ip-pr
protocol	pr
dst-port	dst
scr-port	src
dst-ip	dst
scr-ip	src
action	ac
permit	per

NOTE: The abbreviated forms dst and src are used for both port and IP address commands. The switch disambiguates based on the preceding keyword: pr dst refers to dst-port, while ip dst refers to dst-ip. The Fabric Engine CLI accepts other abbreviated forms, but ExtremeControl consistently generates the forms listed in this table. Do not manually modify the abbreviated commands in the RADIUS VSA.

Viewing Compressed ACLs on the Fabric Engine Switch

When a Fabric Engine switch receives a compressed ACE containing a port list or mask list, it expands the list into individual ACEs and renumbers all ACE IDs sequentially. The ACE IDs visible on the switch (for example, when using the show filter acl config command) may differ from the ACE IDs sent by ExtremeControl.

How to Configure Flood Control

Flood Control provides rate limiting capabilities to CoS to enable certain types of flooded traffic to be dropped. The flood control traffic types are:

- unknown - unicast
- multicast
- broadcast

When Flood Control is enabled, incoming traffic is monitored over one second intervals. A traffic control rate sets the acceptable flow for each type, specified in packets per second. If, during a one second interval, the incoming traffic of a configured type reaches the traffic control rate on the port, the traffic is dropped until the interval ends. Packets are then permitted to flow again until the limit is reached.

By default, Flood Control is disabled for each CoS. Similarly to CoS Port Groups, a different configuration can be assigned for each group. Since Flood Control is shared across all CoS, when Flood Control is enabled on at least one CoS, those rates apply to all ports that have Flood Control enabled.

How to Display Flood Control Port Groups on the CoS Components Tab

1. Select the **CoS Components** left-panel tab on the **Class of Service** left-panel tab. The **CoS Configuration** tab opens.
2. Verify that the **Flood Control** checkbox is selected.

How to Create a Flood Control Port Group

1. From the left-panel menu, open the **CoS Components** tab and select the **Flood Control Port Groups** tab.
2. Right-click the **Flood Control Port Groups** tab and select **Create Port Groups**.
3. In the Create window, enter a name for the Flood Control Port Group and select **OK**. A New Flood Control item is added to the CoS Configuration Window.

How to Enable/Disable Flood Control for a CoS

Flood Control Rate Limits are shared across all CoS. When a Flood Control rate has been enabled on at least one CoS, that is the rate specified for all Flood Control enabled CoS.

1. Open the **Flood Control Port Groups** tab (**Class of Service > CoS Components** tab) and select a Port Group.
2. Select a rate from the drop-down list for the desired Flood Control broadcast traffic type Unicast, Multicast, or Broadcast.
3. Select an existing rate or create a new one.
4. Open a CoS in the **Class of Service** left-panel tab, and enable Flood Control for the CoS by selecting the **Enable** in the **Flood Ctrl Status** drop-down list.

How to Add/Remove Ports to Flood Control Port Groups

1. From the **Class of Service** left-panel tab, select the **CoS Components > Flood Control Port Groups** tab.
2. Right-click a Flood Control Port Group, and select **Add/Remove Ports**.
3. Add or remove the ports in the Add/Remove Ports window.

- Getting Started with Class of Service
- Class of Service Configuration Tab
- How to Create a Class of Service
- How to Define Rate Limits
- How to Configure Transmit Queues
- General Tab (Rate Limit)
- General Tab (Class of Service)

How to Create Global and Island VLANs

The **Policy** tab **VLANs** left-panel tab used for access control are displayed in the Access Control Configuration window. If you have enabled the Policy VLAN Islands feature, there are two tabs in the VLANs tab: Global VLANs and Policy VLAN Islands . Otherwise, only the Global VLANs folder is displayed. For more information on Policy VLAN Islands, see How to Create a Policy VLAN Island.

The **Policy** tab provides you with one Global Default VLAN, available when you first access the **Policy** tab. You can create additional VLANs by selecting the **Create VLAN** option available when you right-click on the **Global VLANs** tab.

Once a VLAN is created, you can use it as follows:

- as the default access control for a role, using the role **General** tab.
- as an access control action for a rule using the **Rule** tab.
- as an access control action for an automated service, using the **Automated Service** tab.
- in a Policy VLAN Island, if that feature is enabled.

See Create VLAN Window and Roles for additional information.

Instructions on:

- Creating a VLAN
- Editing an Island VLAN ID
- Deleting a VLAN

Creating a VLAN

1. Open the **Policy** tab.
2. Select the left-panel **VLANs > Global VLANs** tab.
3. Right select the **Global VLANs** tab and select **Create VLAN** from the menu.
4. Fill out the Create VLAN Window to your specifications.
5. Select **OK** to create the VLAN and close the Create VLAN window.
6. Enforce to write the new information to the devices.

Editing an Island VLAN ID

1. Open the **Policy** tab.
2. Expand the **VLANs > Policy VLAN Islands** left-panel tab.
3. Select the **VLANs** tab in the right panel.
4. Select the VLAN with which the policy VLAN island is associated in the VLANs section of the window.
5. Select the Island VLAN in the VLAN Settings section of the window and select **Edit Island VID**.
6. Enter the new VLAN ID and select **OK**.
7. Enforce to write the new information to the devices.

Deleting a VLAN

Deleting a VLAN removes it and its associations with any roles and services from the NetSight database and from the devices.

WARNING: The delete operation immediately removes the VLAN(s) from the devices in the **Devices** tab and could result in serious consequences if the VLANs are used outside the scope of the **Policy** tab.

---

1. Open the **Policy** tab and select the **VLANs** left-panel tab.
2. Expand the **Global VLANs** left-panel tab.
3. Right-click on the VLAN you wish to delete and select **Delete** from the menu. A confirmation window opens.
4. Select **Yes** to delete the VLAN.
5. Enforce to write the new information to the devices.

How to Create a Policy VLAN Island

VLAN islands enable you to set up, for example, a guest VLAN that restricts the guests in one facility from communicating with guests in another facility. See Policy VLAN Islands for more information.

Instructions on:

- Creating a VLAN Island
- Modifying a VLAN Island
- Deleting a VLAN Island

Creating a VLAN Island

You can create a Policy VLAN Island as follows:

Note: VLANs used in VLAN islands must be Island VLANs.

1. Open the **Policy** tab and select the **VLANs** left-panel tab.
2. In the left-panel **VLANs** tab, select the **Policy VLAN Islands** tab.
3. In the right-panel, select the **VLANs** Tab and select **Create** in the VLANs section.
4. In the **Create VLAN** window, enter a name for the VLAN. Select **OK**.
5. Select **Open/Manage Domains > Save Domain**.

Modifying a VLAN Island

Once you've created a VLAN island, you can change its characteristics using the right-panel tabs as follows:

- *To change a VLAN island name*: Right-click the island in the VLANs section of the **VLANs > Policy VLAN Islands** and select **Rename**.
- *To change a VLAN island description*: Use the island's **Island Topology** tab.
- *To edit an Island VLAN ID*: Use the **Edit Island VLAN ID** button on the island's **VLANs** tab.
- *To change a VLAN Island Configuration (Base ID, Offset, Naming Convention)*: Use the **Policy VLAN Islands** tab **Island Topology** tab .
- *To add or remove devices from a VLAN island*: Use the VLAN Islands Add/Remove Devices window.

Deleting a VLAN Island

You cannot delete the Default Island.

1. Open the **Policy** tab and select the **VLANs > Policy VLAN Islands** left-panel tab.
2. Select the VLAN island you want to delete in the VLANs section of the right panel.

3. Right-click the island you want to delete and select **Delete**.
4. Select **Yes** to confirm the deletion.

How to Create a Network Resource

Network Resource groups provide a quick and easy way to define traffic classification rules for groups of network resources such as routers, VoIP (Voice over IP) gateways, and servers. You create a network resource group by defining a list of MAC or IP addresses for the resources you want included in the group.

In addition, you can use Network Resource Topologies to define a different resource list for different groups of devices in your domain. This enables you to set up network resource access based on the location where end users authenticate.

After a network resource group has been defined, you can associate it with an Automated service (see How to Create a Service for more information). The Automated service automatically creates a rule with a specified action (class of service and/or access control), for each resource address in the network resource group. Automated rule types include Layer 2 MAC Address rules, Layer 3 IP Address and IP Socket rules, and Layer 4 IP UDP Port and IP TCP Port rules.

You can also create Global Network Resources shared between all your domains and can be used by global automated services. Network Resource Topologies are not available for Global Network Resources.

TIP: The **Policy** tab Demo.pmd file contains examples of network resource groups that you might want to create, such as Internet Proxy Servers and SAP Servers.

How to Create a Network Resource

1. From the **Policy** tab, select the **Network Resources** left-panel tab.
2. Right-click the Network Resources folder and select **Create Network Resource**. A New Network Resource item is created in the left panel in a highlighted box. (If you want to create a Global Network Resource, select the Global Network Resources folder.)
3. Type the resource name in the Create window and select **OK**.
4. In the right-panel **General** tab, use the **Edit** button to add a description of the network resource, if desired.
5. Select the network resource Type:
    - Layer 2 MAC - Define a group of network resources using MAC addresses.
    - Layer 3 IP - Define a group of network resources using IP addresses.
6. Select the appropriate network resource topology. Network Resource Topologies are used to divide the devices in a domain into groups called islands. You can then define a unique

resource list for each island within that topology, allowing user access to resources on the network based on the physical location at which they authenticate. If you are not using topologies to group your devices, select the Domain Wide topology, which contains just one island for all your domain devices.

7. For each topology island included in the selected topology, a tab is available where you can list the resources for that specific island. Use the address field (MAC or IP, depending on the selected type) and select the **Add** button to add a new resource to the list.

After a network resources group has been created and defined, it can be associated with an Automated service (see How to Create a Service for more information).

How to Create a Network Resource Topology

1. From the **Policy** tab, select the **Network Resources** left-panel tab.
2. Right-click the **Network Resource Topologies** left-panel tab and select **Create Network Resource Topology**. A New Network Resource Topology item is created in the left panel in a highlighted box.
3. Type the topology name in the highlighted box.
4. Expand the topology to see the Default Island, which contains all the devices in the domain.
5. Right-click on the topology and select **Create Network Resource Island**. Type in the island name in the highlighted box and select **OK**. Use this step to create all the islands for this topology.
6. Select an island and select the **Add Devices** button to open the Add Devices to Resource Island window, where you can move devices from the Default Island to the islands you just created. Select **Add**.
7. Set any island as the [Default] island for new devices that are added to the domain by right-clicking the island and selecting **Set Default**.

The Network Resource Topology is available for selection when you create your network resources.

How to Add and Delete Devices

The ExtremeCloud IQ Site Engine database contains all the devices in your network and displays them in the left-panel device tree. The Network tab and the Policy tab share a common view of the device tree, except that only devices that support policy are displayed in the Policy tab tree. Any changes you make to the devices are reflected in both trees.

Initially, perform a device Discover to populate the database. After devices have been added to the ExtremeCloud IQ Site Engine database, you must assign the devices to a Policy Domain using the Policy tab. As soon as the devices are assigned to a domain, they are automatically displayed in the Policy tab device tree. Only devices assigned to the domain you are currently viewing are displayed. For more information, see How to Create and Use Domains.

After you have initially added your devices, you can use the **Policy** tab's Add Device window to add a single device to the database and the current domain.

Instructions on:

- Adding a Single Device
- Deleting Devices from the Database

Adding a Single Device

You can add a single device to the ExtremeCloud IQ Site Engine database using the **Policy** tab's Add Device window. When you add a device, it is assigned to the current domain and automatically listed in the left-panel device tree. Specify the device's SNMP profile. This information is used by the **Policy** tab to access and manage the device.

1. Select the **Devices** tab.
2. Select Devices folder, right-click and select **Assign Devices to Domain**. The Add Device window opens.
3. Enter the IP address of the device you want to add.
4. Use the drop-down list to select one of the SNMP profiles that have been defined for device access. The **Edit** button lets you create a profile if one does not already exist.
5. Select the checkbox and enter an SNMP context, if desired.
6. Select whether to use the default nickname or select **Specify** to assign a unique nickname to this device.
7. To add the device and leave the window open, select **Apply**. To add the device and close the window, select **OK**.

Deleting Devices from the Database

When a device is deleted from the ExtremeCloud IQ Site Engine database, it is removed from all groups where it is a member in both the **Policy** tab device tree (and any other ExtremeCloud IQ Site Engine plugin applications).

NOTE: If you want to remove a device from a domain without deleting it from the database, you must use the Assign Devices to Domain window. For more information, see Removing Devices from a Domain.

To delete devices from the ExtremeCloud IQ Site Engine database:

1. Open the **Network** tab, select the device being deleted from the Devices table.
2. Right-click the device and select **Device > Delete Device** from the menu. A confirmation message advises that you are deleting the device from the ExtremeCloud IQ Site Engine

database.

3. Select **Yes** to delete the device.

How to Create a Port Group

The **Policy** tab allows you to group ports into user-defined port groups, similar to the way you can group services into service groups. Port groups enable you to configure multiple ports on the same device or on different devices, simultaneously. A port can be a member of more than one group.

When you create a user-defined port group, you select individual ports to add to the group.

The **Policy** tab also provides you with Pre-Defined Port Groups which are automatically populated according to port characteristics. See Pre-Defined Port Groups for more information.

Instructions on:

- Creating a Port Group
- Adding Ports to a Port Group
- Removing Ports from a Port Group

Creating a Port Group

1. In the left panel, select the **Devices > Port Groups** tab.
2. Right-click on the Port Groups folder and select **Create Port Group**. This opens the Create window.
3. Enter a **Name** and select **OK**.

Adding Ports to a Port Group

You can add ports directly from the port group:

1. Select the left-panel **Devices > Port Groups** tab. Expand the User-Defined Port Groups folder and select a port group.
2. Right-click the port group and select **Add/Remove Ports** from the menu.
3. In the Add/Remove Ports window, select the ports you want to add to the port group in the Devices list and select **Add to Group** to move the port to the Group Port Membership list.
4. Select **OK**.

Removing Ports from a Port Group

This procedure applies to user-defined port groups.

1. In the left-panel **Devices > Port Groups** tab, right-click the port group from which you wish to remove a port, and select **Add/Remove Ports**.

2. In the Add/Remove Ports window, select the ports you want to remove from the port group, and select **Remove**.
3. Select **OK**.

Alternatively, you can right-click a single port under the port group in the left panel or multiple ports in the right-panel Ports tab, and select **Remove Port(s) from Group**.

ExtremeControl Access Control

The **Access Control** tab provides secure, policy-based management for the ExtremeControl solution. It configures and manages Access Control engines, provides user to device location mapping services, generates network endpoint audit reports and interfaces with other security management applications.

Contact your sales representative for information on obtaining an ExtremeCloud IQ Site Engine software license.

The **Access Control** tab contains three main navigation trees in the left-panel:

- Access Control Configuration
- Access Control Group Editor
- All Access Control Engines

Access Control Configuration

The Access Control Configuration lets you manage the end-user connection experience and control network access based on a variety of criteria including authentication, user name, MAC address, time of day, and location. ExtremeCloud IQ Site Engine comes with a default Access Control Configuration which is automatically assigned to your Access Control engines. You can use this default configuration as is, or make changes to the default configuration, if desired.

Configure a registration that forces any new end-system connected on the network to provide the user's identity in a web page form before being allowed access to the network. End users are automatically provisioned network access on demand without time-consuming and costly network infrastructure reconfigurations. In addition, IT operations gains visibility into the end-systems and their associated users (for example, guests, students, contractors, and employees) on the network.

Via the Access Control **Configuration**, you can also configure agent-less or agent-based security posture assessment of endpoints. The **Access Control** tab uses assessment servers to assess and audit connecting end-systems and provide details about an end-system's patch levels, running processes, anti-virus definitions, device type, operating system, and other information critical in determining an end-system's security compliance. End-systems that fail assessment can be dynamically quarantined with restrictive network access to prevent security threats from entering the

network.

Assisted remediation is a process that informs end users when their end-systems have been quarantined due to network security policy non-compliance, and allows end users to safely remediate their non-compliant end-systems without assistance from IT operations. After the remediation steps have been successfully performed and the end-system is compliant with network security policy, the appropriate network resources are allocated to the end-system, again without the intervention of IT operations.

Access Control Group Editor

The Access Control Engine Groups tree presents groups of Access Control engines you configure into engine groups. Information for engine groups is organized into four tabs in the right-panel, each showing different information relating to the engine group selected:

- **Details** — Displays basic information about the engine group as well as information about how the engines in the group are configured.
- **Switches** — Shows the switches monitored by the engines in the group and allows you to add, delete, and edit the switch configuration.
- **End-Systems** — Displays end-systems monitored by the Access Control engines in the selected engine group.
- **Access Control Engines** — Displays the Access Control engines added to the engine group. Right-clicking an engine in the table displays a menu from which you can configure the engine. You can also preview the changes you are making to an engine when you enforce by selecting **Enforce Preview**.

All Access Control Engines

The All Access Control Engines tree displays all of your Access Control engines. Selecting an engine displays information in three tabs:

- **Details** — Displays basic information about the engine, provides a summary of the interface, and allows you to disable Access Control authentication and assessment.
- **End-Systems** — Displays end-systems monitored by the Access Control engine.
- **Switches** — Shows the switches monitored by the engine and allows you to add, delete, and edit the switch configuration.

Access Control Configuration Considerations

Review the following configuration considerations when installing and configuring ExtremeCloud IQ Site Engine ExtremeControl.

- ExtremeControl Configuration Tables
- General Considerations
- Considerations When Implementing Policy Roles
- Considerations when Implementing Compound Rules
- ExtremeWireless Controller Configuration
- DNS Proxy Functionality for Registration and Remediation
- Backup DNS Server
- Troubleshooting

ExtremeControl Configuration Tables

The following tables provide valuable information to help guide you through the deployment of Extreme Networks ExtremeControl for your network. The first table displays suggested Access Control configurations to use for different network deployment circumstances (e.g. type of end-systems on the network, network topology, authentication method deployed, etc.). The second table displays details and information for each of the different suggested Access Control configurations. The information in the tables assumes that DHCP is deployed on the network.

Suggested Access Control Configuration for Different Deployments

Policy/VLAN Switch Configuration	Number of Devices Allowed to Connect to Authentication-enabled Edge Port	Type of End-Systems	Authentication Method Deployed	Switch Support IEEE 802.1X MIB	Switch Support, Session Timeout and Termination Action RADIUS Attributes	Suggested Configuration
- Policy Only (*without* changing of VLANs)	*	*	*	*	*	A

Policy/VLAN Switch Configuration	Number of Devices Allowed to Connect to Authentication-enabled Edge Port	Type of End-Systems	Authentication Method Deployed	Switch Support IEEE 802.1X MIB	Switch Support, Session Timeout and Termination Action RADIUS Attributes	Suggested Configuration
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs)	Multiple	Microsoft XP SP1 with KB822596 installed[1]	802.1X[2]	Yes	*	A
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs)	Multiple	*	802.1X[2]	Yes	*	B
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs)	Multiple	*	802.1X[2]	No	Yes	C
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs)	Multiple	*	802.1X[2]	No	No	D

Policy/VLAN Switch Configuration	Number of Devices Allowed to Connect to Authentication-enabled Edge Port	Type of End-Systems	Authentication Method Deployed	Switch Support IEEE 802.1X MIB	Switch Support, Session Timeout and Termination Action RADIUS Attributes	Suggested Configuration
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs) *[for Enterasys switch]*	Multiple	*	MAC Authentication	*	*	B
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs) *[for non-Enterasys switch]*	Multiple	*	MAC Authentication	*	Yes	C
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs) *[for non-Enterasys switch]*	Multiple	*	MAC Authentication	*	No	D

Policy/VLAN Switch Configuration	Number of Devices Allowed to Connect to Authentication-enabled Edge Port	Type of End-Systems	Authentication Method Deployed	Switch Support IEEE 802.1X MIB	Switch Support, Session Timeout and Termination Action RADIUS Attributes	Suggested Configuration
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs)	Single	Microsoft or MAC OS	*	*	*	E
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs)	Single	Linux	*	*	*	F
Wireless Device	Multiple	*	*	*	*	G

* = Any value.
N/A = Not applicable.
[1]For more information on this patch, see the following link: http://support.microsoft.com/default.aspx?scid=kb;en-us;KB822596
[2]When 802.1X is implemented to authenticate multiple users on a single switch port, the downstream device providing connectivity to the users must support the forwarding of EAP frames. Unintelligent devices such as repeaters and switches with newer firmware releases should forward EAP frames. However, some switches do not forward EAP frames therefore preventing the 802.1X authentication of multiple users on a single port.

Access Control Configuration Details

Configuration	Port Link Control	Assessing Session Timeout	Assessing Policy Configuration	DHCP Server Configuration Considerations	Other Considerations
A	Disabled	Disabled	*	No	N/A
	NOTE: This is the simplest of configurations.				
B	Disabled	Disabled	Initial Scan Only	- Set short lease times (e.g. 1 min) for the unauthenticated, Assessing, and Quarantine VLANs - Normal lease times can be configured for the Accept (Production) VLANs	N/A
	NOTES: When an end-system transitions from the unauthenticated, Assessing, or Quarantine VLAN to another VLAN, the end-system will soon renew its IP address via DHCP to automatically re-establish connectivity to the network. When a compliant end-system on the Production VLAN is subsequently quarantined after failing a re-assessment, the end-system's connectivity to the network will be lost until expiration of the DHCP lease for the Accept (Production) VLANs.				

Configuration	Port Link Control	Assessing Session Timeout	Assessing Policy Configuration	DHCP Server Configuration Considerations	Other Considerations
C	Disabled	Enabled	Initial Scan Only	- Set short lease times (e.g. 1 min) for the unauthenticated, Assessing, and Quarantine VLANs - Normal lease times can be configured for the Accept (Production) VLANs	N/A
	NOTES: When an end-system transitions from the unauthenticated, Assessing, or Quarantine VLAN to another VLAN, the end-system will soon renew its IP address via DHCP to automatically re-establish connectivity to the network. Furthermore, the end-system will continually reauthenticate to the network while it is being scanned. When a compliant end-system on the Production VLAN is subsequently quarantined after failing a re-assessment, the end-system's connectivity to the network will be lost until expiration of the DHCP lease for the Accept (Production) VLANs.				
D	Disabled	Disabled	Initial Scan Only	- Set short lease times (e.g. 1 min) for the unauthenticated, Assessing, and Quarantine VLANs - Normal lease times can be configured for the Accept (Production) VLANs	Set short reauthentication interval manually on edge switches (e.g. 2 min)
	NOTE: This is not a very scalable configuration model, and therefore should not be implemented for a network with a large number of end-systems.				
E	Enabled	Disabled	*	No	N/A
	NOTE: End-system will be reauthenticated and will renew its IP address via DHCP with link down/up execution.				

Configuration	Port Link Control	Assessing Session Timeout	Assessing Policy Configuration	DHCP Server Configuration Considerations	Other Considerations
F	Enabled	Disabled	Initial Scan Only	- Set short lease times (e.g. 1 min) for the unauthenticated, Assessing, and Quarantine VLANs - Normal lease times can be configured for the Accept (Production) VLANs	N/A
	NOTES: End-system will be reauthenticated with link down/up execution and will automatically re-establish network connectivity via DHCP upon lease expiration of the IP address in the unauthenticated, Assessing, and Quarantine VLANs. When a compliant end-system on the Production VLAN is subsequently quarantined after failing a re-assessment, the end-system will be reauthenticated and will renew its IP address via DHCP with link down/up execution.				
G	Disabled	*	*	*	RFC 3576 Reauthentication Enabled
	NOTES: ExtremeCloud IQ Site Engine supports RFC 3576 which provides for forced reauthentication (Force Reauth) of end-systems connected to an RFC 3576-capable switch. RFC 3576 defines new RADIUS messaging that enables the Access Control Engine to send Disconnect or Change of Authorization (CoA) RADIUS messages to the authenticating switch or AP to force reauthentication on a currently authenticated end-system.				

* = Any value.
N/A = Not applicable.

General Considerations

- **RADIUS Attributes to Send - Send RFC 3580 Only Feature.** This feature (configured in the Add/Edit Switches to Identity and Access Appliance Group panel) lets you specify that an Access Control Engine sends a VLAN (instead of a policy) via RFC 3580-defined RADIUS Tunnel attributes to the RFC 3580-enabled switches in your network. Keep in mind the following considerations when configuring this feature:

- **Send RFC 3580 Only is not supported on Matrix E7 Devices.** Matrix E7 devices should not be configured with the "RADIUS Attributes to Send" parameter set to RFC 3580 Only.
- **Send RFC 3580 Only does not support end-systems with static IP addresses.** The Send RFC 3580 Only feature is not-supported for end-systems with static IP addresses. This is because end-systems transitioned between VLANs must be assigned an IP address on the appropriate subnet to maintain IP connectivity to the network, which is facilitated dynamically through DHCP.
- **Send RFC 3580 Only requires a particular DHCP configuration for Active/Default Role port mode.** When the Send RFC 3580 Only feature is configured, the Active/Default Role port mode on network devices requires a particular DHCP configuration. The DHCP lease time for the pool of IP addresses that corresponds to the default role's VLAN must be short (e.g. less than 1 minute) because the Active/Default Role port mode enables end-systems to obtain IP addresses via the DHCP protocol before they are authenticated to a VLAN.
- **Switch management fails with Send RFC 3580 Only and certain Auth Access Types.** Switch management via TELNET/WebView fails with the following configuration in the Add/Edit Switches to Identity and Access Appliance Group window:
  Auth Access Type = "Management Access" or "Any Access"
  RADIUS Attributes to Send = "RFC 3580 Only"
  This is because switches check the "mgmt" attribute in the Filter-ID for Telnet management. To avoid this problem, set the Auth Access Type to "Network Access."

- **Enable Port Link Control Option.** Port link control is required if you are using VLAN only (RFC 3580) switches or if you are using policy with VLANs on policy-enabled switches. When an end-system is transitioned between VLANs with a new VLAN being assigned to a switch port, the end-system is required to obtain a new IP address for the assigned VLAN. To do this, the Access Control Engine links down the port (using the ifAdmin MIB), waits the configured amount of time, and then links up the port, causing the end-system to make a new DHCP request and get a new IP address.
  - **Port Link Control is not supported on authentication-enabled switch ports providing connectivity to multiple end-systems.** Do not enable port link control for switches authenticating multiple users per port. When an Access Control Engine is configured to return only the VLAN RADIUS attribute, the engine links down the authenticated port to force the end-system to release and then renew the DHCP IP address when port link control is enabled. This action interrupts IP connectivity of other authenticated end-systems on the port. If the switch is an Enterasys switch, protection is automatically provided by reading the number of users currently on the port prior to linking down an port.
  - **Port Link Control is only supported on Windows XP or later.** Port link control is only supported for end-users that are authenticating from end-systems running Windows

XP or later. When an Access Control Engine is configured to return only the VLAN RADIUS attribute, the engine links down the authenticated port to force the end-system to release and then renew the DHCP IP address when port link control is enabled. However, other systems such as NT workstations, do not release their DHCP IP address when the port is linked down. To account for this scenario, disable port link control, set the Access Control Profile to "Use Assessment Policy During Initial Assessment Only," and set the DHCP lease time for the IP address pools that correspond to the VLAN(s) associated to the Quarantine and Assessing access policies, as well as the default VLAN associated to the unauthenticated state of the port, to a low value (e.g. 1 minute). This forces an end-system to send DHCP Request messages every 30 seconds while it is unauthenticated, being assessed, and quarantined. Upon passing assessment, the end-system is dynamically assigned an IP address on the production VLAN shortly after assessment is complete, establishing connectivity to the network on the production VLAN.

- **Access Control Engine DHCP Snooping:**
  - **Option 1: Locate the Access Control Engine on the same subnet as the DHCP server.** If the Access Control engine is in the same subnet (relay router interface) as the end-system, it is able to hear ACK responses from the DHCP server, enabling it to have more accurate DHCP entries unless the relay router (or DHCP server) sends unicast ACK responses directly to the end-system.
    Note: Whether the ACK response is sent using unicast or broadcast is normally determined by how the end-system requests the packet. If the end-system sends out a DHCP discover/request with a unicast bootp flag, then the DHCP server (or relay router) sends the ACK response using unicast. This is typically what happens. Sometimes, the end-system can request the DHCP discover/request with a broadcast bootp flag set. In this case, the end-system gets the ACK response with broadcast, and the Access Control engine hears the ACK response if it is in the same broadcast domain.
    The benefit of using option 1 over the helper-address implementation described in option 2, is that the helper-address implementation only gets the requests from the end-systems that might not have the correct IP address. When an Access Control Engine learns a MAC/IP address pair, it sends a message to all other Access Control Engines, so only one Access Control Engine needs to live on each subnet with a DHCP server on it, to leverage this technique.
  - **Option 2: Add the Access Control Engine IP address as a helper address on default gateway routers.** To increase the accuracy of the MAP-to-IP resolution, the Access Control Engine listens for DHCP traffic on port 67 and saves the MAC/IP address pairs it learns. In order to receive DHCP traffic, the IP address of any Access Control Engine must be added as a helper address on default gateway routers on the network. Routers permit multiple IP helper address entries, so the Access Control engines IP address can be added along with the actual DHCP server IP addresses. When an Access Control Engine learns a MAC/IP address pair, it sends a message to all other Access Control Engines, so only one Access Control engine IP address needs to be added.

- **Configure RADIUS settings on 3rd-party switches.** You must manually configure the RADIUS settings on your third-party switches communicating to the Access Control Engine. In addition, make sure that the shared secret on the switches matches the shared secret you entered in the Advanced Switch Settings window. This is the shared secret the switches uses to communicate with Access Control Engines.

- **Configuring Agent-based Assessment Test Sets with Hotfix Checks.** When configuring an Agent-based test set to perform multiple hotfix checks, make sure that the Monitoring Interval is set to at least 5 minutes, so that the assessment agent does not take a lot of CPU cycles trying to monitor these settings.

- **Supported desktop browsers for end-systems connecting through Access Control.** The following browsers are supported for desktop end-systems connecting to the network through Extreme Networks Access Control:
    - Microsoft Edge
    - Mozilla Firefox 34 and later
    - Google Chrome 33.0 and later
- **Supported mobile browsers for end-systems connecting through Access Control.** The following browsers are supported for mobile end-systems connecting to the network through the Mobile Captive Portal of Extreme Networks Access Control:
    - Microsoft Edge
    - Microsoft Windows 10 Touch Screen Native (Surface Tablet)
    - iOS 9+ Native
    - Android 4.0+ Chrome
    - Android 4.4+ Native
    - Dolphin
    - Opera

NOTES:

A native browser indicates the default, system-installed browser. Although this can be Chrome (Android), this also includes the default, system-controlled browser used for a device's Captive Network Detection. Typically, this is a non-configurable option for Wi-Fi Captive Network Detection, but default Android, Microsoft of iOS devices are tested for compatibility with the Mobile Captive Portal.

A mobile device can access the standard (non-mobile) version of the Captive Portal using any desktop-supported browsers available on a mobile device.

    - For other browsers, the Mobile Captive Portal requires the browser on the mobile device be compatible with Webkit or Sencha Touch. To confirm compatibility with Webkit or Sencha Touch, open http://*<ip_of_engine>*/mobile_screen_preview using your mobile web browser. If the browser is compatible, the page displays properly.
- **RADIUS Configuration on E1 Devices.** The Access Control engine opens an SSH/Telnet session on the E1 device and enable RADIUS by running a script of CLI commands. CLI credentials for the device are obtained from the device profile and must be configured in the Authorization/Device Access tool.

- **RADIUS Authentication and Accounting Configuration on ExtremeXOS/Switch Engine Devices.** ExtremeCloud IQ Site Engine uses CLI access to perform RADIUS configuration operations on ExtremeXOS/Switch Engine devices. CLI credentials for the device are obtained from the device profile and must be configured in the Authorization/Device Access tool.
- **RADIUS Accounting Configuration on Fixed Switching Devices.** Access Control uses CLI to configure RADIUS accounting on Enterasys fixed switching devices (A-Series, B-Series, C-Series, D-Series, G-Series, and I-Series). CLI credentials for the device are obtained from the device profile and must be configured in the Authorization/Device Access tool. This does not apply to A4, B5, and C5 devices running firmware version 6.81 and higher. Those devices support RADIUS accounting configuration using SNMP. For more information, see How to Enable RADIUS Accounting.

Considerations When Implementing Policy Roles

This section describes the communication that takes place between Access Control engines and end-systems connecting to the network. This communication should be taken into account when defining and deploying policy roles and rules on your network. It is particularly critical because certain policy roles and rules can discard traffic that is necessary for communication between the end-system and the engine. For example, in a Guest policy role, NetBIOS traffic is probably discarded, but doing so could impact the MAC to IP resolution process.

Review the following information and verify that the policy roles and rules deployed on your network will permit the required communication between end-systems and your Access Control engines.

IP resolution via NetBIOS
MAC Resolution via NetBIOS
    Access Control engine UDP Port 137 <==> End-System Port 137

Remediation and Registration
    Access Control engine (TCP or UDP) Port 80 <==> End-System Port (determined on the client) - HTTP
    Access Control engine (TCP or UDP) Port 443 <==> End-System Port (determined on the client) - HTTPS

Access Control Agent Discovery via HTTP
    Access Control engine Port TCP 8080 <==> End-System Port (determined on the client)

Access Control Agent Heartbeat via HTTPS
Access Control engine Port TCP 8443 <==> End-System Port (determined on the client)

Access Control Agent-less Assessment
All ports determined by the selected test set.

The following software is optional and can be installed with agent-less Assessment:
SAMBA add-on enabled
TCP Ports 149 and 195, and UDP Ports 137 and 138.

End-System Reachability Test (Assessment Configurations - does not apply to agent-based assessment)
ICMP Ping Test => ICMP Protocol (1), ICMP Type (8)
TCP Ping Test => Default TCP Ports: 21, 22, 23, 25, 79, 80, 111, 135, 139, 445, 497, 515, 548, 1025, 1028, 1029, 1917, 5000, 6000, 9100

Considerations when Implementing Compound Rules

When you use Compound Rules (multi-select criteria in User Groups or End-System Groups), the AND logic requires the end-system to satisfy all selected group conditions. Plan your group membership hierarchy accordingly to avoid overly restrictive rules that no end-system can match.

- Existing single-condition policies continue to function without modification. There is no regression to existing rule configurations when you upgrade to a version that supports Compound Rules.
- The Compound Rules feature currently supports multi-select for User Groups and End-System Groups criteria categories only. Multi-select is not currently available for other categories in the UI or NBI services.
- When you configure Compound Rules, use the Configuration Evaluation Wizard to verify rule behavior. The wizard displays granular per-value pass or fail results for compound criteria, which is useful for troubleshooting complex rule configurations.

ExtremeWireless Controller Configuration

- The NAS IP address used for the wireless controller should be either the management IP address or an IP address of one of its physical data ports, or all zeros to force ExtremeControl (Access Control) to use the source IP. If a logical IP address is used, then Access Control is unable to reauthenticate end-systems.
- If you have configured Assisted Remediation, you must perform the following steps if your network includes wireless controllers:
    - Enable the "ToS override for Access Control" option configured through Wireless Manager in the Edit WLAN Service > Authentication Mode Configuration > Settings window.

- If Policy Manager is **not** being used to configure policy on the wireless controller, use Wireless Manager to manually add the following rule to the VNS Quarantine, Assessing, and Unregistered filters to permit HTTP traffic to pass through (IN/OUT) the controller when end-systems are proxied to the Internet during remediation.
  `0.0.0.0/0 tcp port 80 (Allow traffic In/Out)`
- If Policy Manager **is** being used to configure policy for the wireless controller, use the Classification Rule Wizard to add an "Allow HTTP" rule to a service currently included in your Quarantine, Assessing, and Unregistered policy roles. The rule would be a traffic classification type "IP TCP Port Destination" with the TCP type set to HTTP (80) and the Access Control set to "Permit Traffic."

DNS Proxy Functionality for Registration and Remediation

ExtremeControl (Access Control) engines provide DNS proxy functionality for use in networks that are deploying registration and/or remediation, but cannot configure the policy-based routing that is required to redirect network traffic to the web portal. Using DNS proxy, any end-system that needs to be redirected to the remediation and registration web portal has its DNS packets spoofed to direct all web page requests to the Access Control engine. This enables networks that do not have a router to deploy registration and remediation.

Basic Operation

To set up DNS proxy, the Access Control engine is configured as a secondary DNS server in the DHCP scope, in addition to the primary DNS server on the network. When an end-system is required to register or undergo remediation, access to the primary DNS server is blocked and the end-system sends its DNS requests to the DNS proxy on the Access Control engine.

The DNS proxy must determine whether to spoof the packet or forward the request to the primary DNS server. If the end-system is unregistered or quarantined, the DNS proxy spoofs the DNS packet and send back a DNS response to the end-system with the Access Control engine IP address. This redirects the end-system traffic to the web portal where the end user can register or remediate. After the end user has registered or remediated their end-system, their DNS requests are forwarded to the primary DNS server.

For third-party devices, a dynamic ACL is configured to block access to the primary DNS server for end-systems undergoing registration or remediation. This causes the DNS requests to be sent to the DNS proxy. The DNS proxy determines whether spoofing is necessary or not by checking the state of the end-system in the database. If the end-system is unregistered or quarantined, the DNS proxy spoofs the DNS packet.

To permit access to hosts or domains for any protocol other than http, you must add the host or domain to the list of allowed web sites configured in the Network Settings view of the Access Control Edit Portal Configuration window. The DNS proxy uses this list of permitted domains to determine if the end-system is permitted access to the requested domain. This can be useful if you want to enable end-systems to perform specific functions such as anti-virus updates or software updates that run over TCP/UDP ports.

You can also define post authorization assessment behavior using DNS proxy. End-systems in the scan state are granted access according to the assessment settings in your Access Control profile.

- If an assessment policy is **not** defined, the user is permitted access while being scanned.
- If an assessment policy is defined for initial assessment only, the user is permitted access if they passed the last scan. If the first or last scan resulted in quarantine, the user is redirected to the Access Control Engine.
- If an assessment policy is defined for all assessments, the user is redirected to the Access Control Engine.

Enabling DNS Proxy

Use the following steps to enable DNS proxy:

1. Enable Registration and/or Remediation via the Edit Access Control Configuration window and enforce. Note that it is important to wait a couple of minutes after enabling or disabling registration and remediation for the DNS proxy to be notified of the enable/disable change, and to start or stop proxying DNS requests.
2. Uncomment the "#DNS_PROXY_ENABLE=true" in the config.properties file on the Access Control engine by deleting the # symbol at the beginning of the line.
3. Restart the Access Control engine using the `nacctl restart` command.
4. Start the DNS Proxy process on the engine using the `/opt/nac/server/dnsProxy.sh start` command.

Backup DNS Server

Because the DNS proxy forwards DNS requests to the primary DNS server, it is important to configure a backup DNS server on your network, in case the primary server is down. The DNS proxy polls the primary DNS server every minute. If the primary server is down, a backup DNS server is used. If both servers are down, all DNS requests forwarded by the DNS proxy are dropped.

Troubleshooting

DNS proxy error messages are logged in the /var/log/dnsProxy.log file on the Access Control engine. You can enable diagnostics for DNS proxy by going to the Access Control engine administration web page and enabling the DNS Proxy diagnostic group to provide troubleshooting information. Launch the Access Control engine administration web page by using the following URL: https://<Access ControlengineIP>:8443/Admin. The default user name and password for access to this web page is "admin/Extreme@pp." Select the Diagnostics page and then the Server Diagnostics page. View the output in the /var/log/dnsProxy.log file or on the Log Files > Server Log web page.

Install the Assessment Agent Adapter on a Nessus Server

This document provides instructions to install the Extreme Networks Assessment Agent Adapter software on a Nessus Server. The Assessment Agent Adapter is required for communication between the ExtremeControl engine and the Nessus server.

NOTE: As of ExtremeCloud IQ Site Engine version 26.11.10, only Nessus Version 6 is officially supported.

1. Go to the Network Management Suite (NMS) Download web page to download the Assessment Agent Adapter: https://extranet.extremenetworks.com/downloads/Pages/NMS.aspx. Select the version of ExtremeCloud IQ Site Engine you are using.
2. Scroll down to find the Identity and Access Tools section of the web page. The install file is named "Assessment Adapter (for 3rd party assessment integration)". Download the file and copy it to the Nessus server.
3. Open a shell and "cd" to the directory where you downloaded the install file.
4. Change the permissions on the install file by entering the following command at the shell prompt:
   ```
   chmod 755 EXTRAssessmentServerAgentAdapter_x.x.x.x.bin
   ```
5. Run the install program by entering the following command at the shell prompt:
   ```
   ./EXTRAssessmentServerAgentAdapter_x.x.x.x.bin
   ```
6. The Introduction screen displays. Press **Enter**.
7. Enter Nessus as the agent type to install. Press **Enter**.
8. The Choose Install Folder screen displays, where you can choose the installation folder or directory. Enter an absolute path or press **Enter** to accept the default installation folder /root/AssessmentAgent. The installer requires 100 MB of memory. If the installation folder does not have enough memory, an error displays.
9. The Pre-Installation Summary screen displays. This screen shows you the locations you have chosen for the installation process and disk space requirements. Review this information to ensure its accuracy. Press **Enter**.
10. The Nessus Server Information screen displays. You must enter information in several fields in this screen.
11. Enter the port on which the Nessus daemon is running. The default value is 1241. Press **Enter**.
12. Enter the username you created when you installed the Nessus server. Press **Enter**.
    If you did not create a user when you installed the Nessus server, from a shell prompt, type:
    ```
    cd /nessus installation directory/sbin
    ```
    followed by

```
nessuscli adduser username
```

and follow the prompts to add a user to the application. Press **Enter**.

13. Enter the password for the Nessus user. Press **Enter**.
14. The SSL Server Information screen displays. Enter the port on which the HTTPS daemon is running. The default port number is 8445. Press **Enter**. The Assessment Agent Adapter begins installing.
15. If you are upgrading to a newer version of the Assessment Agent Adapter, you are asked if you want to overwrite several files: launchAS.sh, bin/nessus_cmd, and version.txt. Enter the letter "y" to answer yes and press **Enter**.
16. The Installation Complete screen displays. The installation is complete and the Assessment Agent Adapter has been installed on the server.
17. Start the Assessment Agent Adapter as a background process by entering the following command at the shell prompt:

    ```
    /assessmet agent adapter installation directory/launchAS.sh &
    ```

18. Make sure that the Nessus daemon and the Assessment Agent Adapter are started each time the system is started, by adding this command into your rc.local script:

    ```
    /assessment agent adapter installation directory/launchAS.sh &
    ```

19. To verify the Assessment Agent Adapter is running on the system, from the shell prompt enter:

    ```
    netstat -an | grep port number
    ```

    where port number is the port you entered that has the HTTPS daemon running on it. The default value for this is 8445. Returned entries containing ESTABLISHED or LISTEN is displayed.
20. To verify the Nessus application is running on the system, from the shell prompt enter:

    ```
    ps -eaf | grep nessusd
    ```

    A return entry similar to: "nessusd: waiting for incoming connections" is displayed. This is an indication that the Nessus process is running correctly on the system.

How to Configure Local RADIUS Termination at the ExtremeControl Engine

This Help topic provides information on how to configure authentication using the ExtremeControl engine RADIUS server to locally terminate 802.1X EAP authentication requests. There are three methods that can be used to do this, depending on the protocol that is used:

- LDAP Authentication - Uses a backend Active Directory server or LDAP server, and RADIUS server and client certificates (if required) to authenticate users.
- Local Authentication - Uses a local password repository, and RADIUS server and client certificates (if required) to authenticate users.
- RADIUS Certificates only - Uses only RADIUS server and client certificates to authenticate users (no password is required).

The following chart lists the protocols that are supported for local RADIUS termination, and shows whether the protocol uses RADIUS certificates and/or passwords to authenticate users. If passwords are required, you can then decide whether to use LDAP or local authentication for password verification. The chart also lists the hash types supported by each protocol for user password encryption. Note that PEAP (TLS) is not supported for local RADIUS termination and is only supported in a proxy RADIUS configuration.

Protocol	RADIUS Certificates Required	Password Required	Supported Password Hash Types
PAP	No	Yes	PKCS5 Reversible, SHA1, NT Hash
CHAP	No	Yes	PKCS5 Reversible
MsCHAP	Yes	Yes	PKCS5 Reversible, NT Hash
PEAP (EAP-MsCHAPv2)	Yes	Yes	PKCS5 Reversible, NT Hash
EAP-TTLS	Yes	Yes	PKCS5 Reversible, SHA1, NT Hash
EAP-TLS	Yes	No	N/A
EAP-MD5	No	Yes	PKCS5 Reversible

Instructions on:

- LDAP Authentication
  - User Authentication Considerations
- Local Authentication
  - User Password Considerations
- Certificate Configuration
  - EAP-TLS Certificate Requirements

LDAP Authentication

LDAP authentication uses a backend Active Directory server or LDAP server defined in your AAA Configuration to authenticate users. Additionally, some protocols also require RADIUS server and client certificates to be used in conjunction with LDAP authentication (see Certificate Configuration).

Before configuring LDAP authentication, read through the User Authentication considerations described below.

User Authentication Considerations

If you are using LDAP authentication, the type of LDAP server you select depends on the protocol you are using. With Active Directory, NAC Manager provides a more feature-rich integration and supports a large number of protocols, while with other LDAP servers such as OpenLDAP, NAC Manager provides a more basic integration with limited protocol support.

Active Directory

Supported Protocols: PAP, MsCHAP, PEAP, EAP-MsCHAPV2, and EAP-TTLS with tunneled PAP.

PAP or EAP-TTLS with tunneled PAP protocols

During the authentication process, the Access Control engine sends an LDAP bind request to the Active Directory domain controller using the password retrieved from the end user's authentication request. Therefore, the LDAP protocol must be permitted between the Access Control engine and the Active Directory domain controller for the authentication process to take place.

MsCHAP, PEAP, and EAP-MsCHAPv2 protocols

These three protocols work with Active Directory (and not other LDAP servers) because they use NT Hash for password encryption, which is the same password hash type used by the Microsoft Active Directory domain controller.

Authentication requests are made by the Access Control engine sending an ntlm_auth request to the Active Directory domain controller. The Access Control engine attempts to join the Active Directory domain using the LDAP configuration and the administrator username and password. In your LDAP configuration, the administrator username used to connect to the LDAP server must be a member of the built-in Domain Administrator group or Account Operators group. (See the Active Directory Permissions section below.)

Additionally, the DNS configuration must be set up so that the Access Control engine can resolve the domain by name. To do this, you should configure the DNS server to be one of the domain controllers for that domain, and verify that the domain name is configured correctly on the Access Control engine. If users authenticate to multiple domains, you must also configure the domains to fully trust each other. Refer to the following Microsoft documentation for information on how to set up domain trusts: https://technet.microsoft.com/en-us/library/cc740018%28WS.10%29.aspx.

Note: For these protocols to work when the active directory domain server is set to only permit NTLMv2 authentication, your version of Samba must pass a flag during authentication to permit NTLMv1 to work for 802.1x MSCHAPv2 when the AD is set to the highest security setting (NTLMv2 only). On earlier versions, these protocols do not work if the active directory is set to only permit NTLMv2 because these protocols do not use NTLMv2 and the hash passed to NAC Manager is rejected by the active directory server. Permitting only NTLMv2 authentication only works if NAC Manager proxies the 802.1x request to Microsoft IAS/NPS. Microsoft IAS/NPS permits this lower level of authentication because it is in a TLS session, which Microsoft believes makes it as secure as NTLMv2. For more information, see https://technet.microsoft.com/en-us/library/cc772468.aspx

Active Directory Permissions

Active Directory is supported on Windows 2008, Windows 2012, and Windows 2016 systems. ExtremeControl can fail to join Active Directory when accessing as a **Standard Domain User with Descendant Computer Objects** group member.

To enable this functionality, add the following permissions:

- Reset Password
- Validated write to DNS host name
- Validated write to service principal
- Read and write account restrictions
- Read and write DNS host name attributes
- Write servicePrincipalName

Active Directory with User Log On Restrictions

In Active Directory, it is possible to configure an option that restricts a user domain log on to specific computers. This configuration is enforced during the domain log on process.

In an Access Control environment where users authenticate using 802.1X and NAC Manager is configured to proxy RADIUS requests, no additional configuration is required. The 802.1X authentication process completes normally and the determination of whether the user is permitted to log on to the domain from the specific computer is enforced at that time.

In an Access Control environment where NAC Manager is terminating 802.1X authentications locally, NAC Manager performs an NTLM authentication to authenticate the 802.1X session. This process simulates the domain log on process. Therefore, NAC Manager indicates the incoming authentication request for the user is coming from a computer (the Access Control engine) that the user is not permitted to log on to, and the authentication attempt is rejected.

The solution in this scenario is to add the Access Control engines to the list of computers the user is permitted to log on to. This enables the 802.1X authentication process to complete and successfully authenticate the user. The enforcement of whether the user is permitted to log on to the specific computer takes place during the domain log on process.

Other LDAP Servers

Supported Protocols: PEAP, PAP, and EAP-TTLS with tunneled PAP.

During the authentication process, the Access Control engine attempts an LDAP(S) bind with the LDAP server to authenticate the end user's credentials. Ensure that LDAP(S) between the Access Control engine and LDAP server is not blocked by an ACL or firewall.

Local Authentication

Local authentication uses a local password repository defined in your AAA Configuration to authenticate users. Additionally, some protocols also require RADIUS server and client certificates to be used in conjunction with local authentication (see Certificate Configuration). Before configuring local authentication, read through the user password considerations described below.

User Password Considerations

When you add or edit a user in your local password repository, you can specify the password hash type used to encrypt the user's password in the ExtremeCloud IQ Site Engine and NAC Manager databases. Select from two supported hashing algorithms, depending on the protocol you are using:

- SHA 1 – a non-reversible hashing algorithm
  Supported Protocols: PAP and EAP-TTLS with tunneled PAP
- PKCS5 – a reversible hashing algorithm
  Supported Protocols: PAP, CHAP, MsCHAP, PEAP, EAP-MsCHAPV2, EAP-TTLS with tunneled PAP, and EAP-MD5

Certificate Configuration

If the protocol you are using requires RADIUS certificates for authentication (see the table above), review the certificate configuration information in this section.

During installation, Access Control generates a unique private key and server certificate for the NAC Manager RADIUS server. This certificate provides basic functionality while you are configuring and testing your NAC Manager deployment. To integrate with the certificate structure you already have on your network, update to a certificate generated by a Certificate Authority that your connecting end-systems are already configured to trust.

In addition, configure the AAA Trusted Certificate Authorities to designate which client certificates can be trusted.

Note: The EAP-TLS Certificates with SHA1 are considered weak and are not accepted anymore. The radius server fails to start with the SHA1 certificate. You can use a more secure certificate, such as SHA256.

EAP-TLS Certificate Requirements

Server Certificate:

Enhanced Key Usage:
Server Authentication (1.3.6.1.5.5.7.3.1)

Key Usage:
Digital Signature, Key Encipherment

Client Certificate:

Enhanced Key Usage:
Client Authentication (1.3.6.1.5.5.7.3.2)

Key Usage:
Digital Signature, Key Encipherment

Deploy ExtremeControl in an MSP or MSSP Environment

This topic describes deploying ExtremeControl within an MSP (Managed Service Provider) or MSSP (Managed Security Service Provider) environment,. It includes the following information:

- Configuring ExtremeCloud IQ Site Engine Behind a NAT Router
- Defining Interface Services

Configuring ExtremeCloud IQ Site Engine Behind a NAT Router

If the ExtremeCloud IQ Site Engine server is located behind a NAT (Network Address Translation) router, use the following steps to add an entry to the nat_config.text file that defines the real IP address for the ExtremeCloud IQ Site Engine server. This allows the ExtremeCloud IQ Site Engine server to convert the NAT IP address received in the Access Control engine response to the real IP address used by the ExtremeCloud IQ Site Engine server.

NOTE: The text in the nat_config.text file refers to a remote IP address and a local IP address. For this configuration, the NAT IP address is the remote IP address and the real IP address is the local IP address.

1. On the ExtremeCloud IQ Site Engine server, add the following entry to the <install directory>/appdata/nat_config.text file.
   ```
   <NAT IP address>=<real IP address>
   ```
2. Save the file.
3. Configure your Access Control engines to use the NAT IP address for the IP address of the ExtremeCloud IQ Site Engine server. For information on how to configure or change your engine settings, refer to your Access Control engine Installation Guide.

If you have remote ExtremeCloud IQ Site Engine clients connecting to the NAT IP address, perform the following additional steps.

1. On the ExtremeCloud IQ Site Engine server, add the following text to the <install directory>/appdata/NSJBoss.properties file. In the second to last line, specify the hostname of the ExtremeCloud IQ Site Engine server.
   ```
   # In order to connect to a ExtremeCloud IQ Site
   Engine server behind a NAT firewall or a
   # ExtremeCloud IQ Site
   Engine server with multiple interfaces you must define these two
   # variables on the ExtremeCloud IQ Site
   ```

```
Engine server. The java.rmi.server.hostname
# should be the hostname (not the IP) if multiple IPs are being used
# so that each client can resolve the hostname to the correct IP that
# they want to use as the IP to connect to.
java.rmi.server.hostname=<hostname of ExtremeCloud IQ Site Engine server>

java.rmi.server.useLocalHostname=true
```

2. Save the file.
3. Add the ExtremeCloud IQ Site Engine server hostname to your DNS server.

Defining Interface Services

The advanced interface configuration mode available in ExtremeCloud IQ Site Engine allows you to define which services are provided by each of the Access Control engine's interfaces. This provides the very granular out-of-band management that is often required in MSP or MSSP environments.

For instructions, see the Interface Configuration Window Help topic.

ExtremeControl Concepts

This Help topic explains some of the concepts you'll need to understand in order to make the most effective use of **Access Control** tab and the ExtremeControl solution.

Information on:

- Overview of the Access Control Tab
- Access Control Engines
  - Use Scenario
  - ExtremeControl VPN Deployment
- Access Control Tab Structure
  - ExtremeControl Configuration
  - Rule Components
  - ExtremeControl Profiles
  - AAA Configurations
  - Portal Configurations
- Access Policies
- Registration
- Assessment
  - Assessment Remediation
- End-System Zones
- Enforcing
- MAC Locking
- Notifications

Overview of the Access Control Tab

Extreme Networks Access Control is a centralized network access control solution located in the **Access Control** tab that combines authentication, vulnerability assessment, and location services to authorize network access and determine the appropriate level of service for an end-system. The Access Control solution ensures that only valid users and devices with appropriate security postures at the proper location are granted access to your network. For end-systems which are not compliant with defined security guidelines, the Access Control solution provides assisted remediation, enabling end users to perform self-service repair steps specific to the detected compliance violation.

The **Access Control** tab is the management component in the Extreme Networks Access Control solution. The **Access Control** tab and Access Control engines work in conjunction to implement network access control. The **Access Control** tab provides one centralized interface for configuring the authentication, authorization, assessment, and remediation parameters for your Access Control engines. After these configurations are enforced, the Access Control engines can detect, authenticate, assess, authorize, and remediate end-systems connecting to the network according to those configuration specifications.

Access Control Engines

The Access Control engine is required for all Extreme Networks Access Control deployments. It provides the ability to detect, authenticate, and effect the authorization of end devices attempting to connect to the network. It also integrates with, or connects to, vulnerability assessment services to determine the security posture of end-systems connecting to the network. After authentication and assessment are complete, the Access Control engine effects the authorization of devices on the network by allocating the appropriate network resources to the end-system based on authentication and/or assessment results.

If authentication fails and/or the assessment results indicate a non-compliant end-system, the Access Control engine can either totally deny the end-system access to the network or quarantine the end-system with a highly restrictive set of network resources, depending on its configuration. The Access Control engine also provides the remediation functionality of the Access Control solution by means of the remediation web server that runs on the engine. Remediation informs end users when their end-systems have been quarantined due to network security policy non-compliance, and enables end users to safely remediate their non-compliant end-systems without assistance from IT operations.

Use Scenario

The Access Control engine provides out-of-band network access control for networks where intelligent wired or wireless edge infrastructure devices are deployed as the authorization point for connecting end-systems. End-systems are detected on the network through their RADIUS authentication interchange. Based on the assessment and authentication results for a connecting device, RADIUS attributes are added/modified during the authentication process to authorize the end-system on the authenticating edge switch. Therefore, the Access Control Engine can be positioned anywhere in the network topology with the only requirement being that IP connectivity between the authenticating edge switches and the Access Control Engines is operational.

It is important to note that if the wired edge of the network is non-intelligent (unmanaged switches and hubs) and is not capable of authenticating and authorizing locally connected end-systems, it is possible to augment the network topology to enable implementation of inline Access Control with the Access Control Engine. This can be accomplished by adding an intelligent edge switch that possesses specialized authentication and authorization features. The Extreme Networks K-, S-, or N-Series switch is capable of authenticating and authorizing numerous end-systems connected on a single port through its Multi-User Authentication (MUA) functionality, and can be positioned upstream from non-

intelligent edge devices to act as the intelligent edge on the network. In this configuration, the K-, S-, or N-Series switch acts as the intelligent edge switch on the network, although not physically located at the access edge.

For end-systems connected to EOS policy-enabled switches, a *policy role* is specified in the **Access Control** tab (policy roles are defined and distributed to those switches by the **Policy** tab) to authorize connecting end-systems with a particular level of network access. For end-systems connected to RFC 3580-compliant switches (Enterasys and third-party), a VLAN is specified in the **Access Control** tab to authorize connecting end-systems with a particular level of network access, facilitated using dynamic VLAN assignment via Tunnel RADIUS attributes.

When a user or device attempts to connect to the network, the end-system is authenticated and assessed according to configurations defined in the **Access Control** tab. The **Access Control** tab uses the results of the authentication and assessment to determine if that device meets the requirements for a compliant end-system. If the results of the authentication and security assessment are positive, ExtremeCloud IQ Site Engine authorizes the end-system with network access by assigning a designated policy role or VLAN on the switch port to which the end-system is connected. If the result of the security assessment is negative, ExtremeCloud IQ Site Engine restricts network access by assigning the user or device to a Quarantine policy role or VLAN on the switch port until the end-system is remediated and brought into a compliant state. If the result of the authentication is negative, ExtremeCloud IQ Site Engine can deny all network access for the endpoint as an invalid device or user on the network, setting the switch port to the unauthenticated state.

Depending on the engine model, the Access Control Engine provides either on-board (integrated) vulnerability assessment server functionality and/or the ability to connect to external assessment services, to determine the security posture of end-systems connecting to the network. (On-board assessment requires a separate license.)

The number of Access Control Engines you deploy on the network depends on the number of end-systems on the network. The following table displays the number of end-systems supported per Access Control Engine model. Use this table to help determine the number of engines to deploy.

Model	Number of End-Systems Supported	Notes
IA-A-20	6000	Configured Access Control Features: Authentication and OS/Device Fingerprinting, but no Registration or Assessment.
	4500	Configured Access Control Features: All features excluding Assessment.
	3000	Configured Access Control Features: All features including Assessment.

Model	Number of End-Systems Supported	Notes
IA-A-300	12000	Configured Access Control Features: Authentication and OS/Device Fingerprinting, but no Registration or Assessment.
	9000	Configured Access Control Features: All features excluding Assessment.
	6000	Configured Access Control Features: All features including Assessment.
IA-V	See Notes	The IA-V is used in conjunction with an Access Control Enterprise license (IA-ES-12K).
NAC-V-20	3000	The NAC-V-20 is a virtual engine and requires an Access Control VM license in the ExtremeCloud IQ Site Engine Server.
NAC-A-20	3000	
SNS-TAG-ITA	3000	
SNS-TAG-HPA	3000	
SNS-TAG-LPA	2000	

It is important to configure Access Control Engine redundancy for each switch. This is achieved by configuring two different Access Control engines as a primary and secondary engine for each switch. When connection to the primary engine is lost, the secondary engine is used. Note that this configuration supports redundancy but not load-sharing, as the secondary engine is only used in the event that the primary engine becomes unreachable. To achieve redundancy with load-sharing for two Access Control engines, it is suggested that one half of the switches connecting to the engines are configured with "Access Control Engine A" as the primary and "Access Control Engine B" as the secondary, and the second half are configured with "Access Control Engine B" as the primary and "Access Control Engine A" as the secondary. In this way, the Access Control Engines are configured in redundant active-active operation on the network.

ExtremeControl VPN Deployment

Extreme Networks ExtremeControl provides out-of-band support for VPN remote access with specific VPN concentrators (see the Release Notes for a list of supported VPN concentrators). Out-of-band VPN support provides visibility into who and what is accessing the network over VPN. If RADIUS accounting is used, you also have the ability to determine who was on the network at any given time. In the VPN remote access use scenario, the VPN concentrator acts as a termination point for remote access VPN tunnels into the enterprise network. In addition, the Extreme Networks Access Control engine is deployed to authenticate and authorize connecting end-systems on the network and implement network access control.

The process begins when the user's end-system successfully establishes a VPN tunnel with the VPN concentrator, and the VPN concentrator sends a RADIUS authentication request with the associated credentials to the Access Control Engine. The Access Control Engine proxies the authentication request to a backend authentication server (RADIUS or LDAP) to validate the identity of the end user/device or can authenticate with a local password repository within ExtremeCloud IQ Site Engine. If authentication fails, the Access Control Engine can deny the end-system access to the network by sending a RADIUS access reject message to the VPN concentrator.

After the end-system is authenticated, the Access Control Engine requests an assessment of the end-system, if assessment is configured. After authentication and assessment are complete, the Access Control Engine allocates the appropriate access control to the end-system based on authentication and/or assessment results. Access control can be implemented using one of two methods. With the first method, access control is applied directly at the VPN concentrator via RADIUS response attributes, if the VPN concentrator supports this. For example, with a Cisco ASA security engine, this can be accomplished by using the filter-ID response attribute to specify the name of a valid ACL.

With the second method, an Extreme Networks K-Series, S-Series, or N-Series device is added between the VPN's internal port and the internal network as a Policy Enforcement Point (PEP). This enables the Access Control Engine to provide a more granular access control mechanism using IP to Policy Mappings. This method must be used if you are implementing remediation on your network. If the end-system fails assessment, the Access Control Engine can apply a Quarantine policy on the PEP to quarantine the end-system. When the quarantined end user opens a web browser to any web site, its traffic is dynamically redirected to a Remediation web page that provides steps for the user to execute in order to achieve compliance. After executing the steps, the end user can reattempt network access and start the process again.

Access Control Tab Structure

The **Access Control** tab components are contained in three major navigation trees.

At the top are the following navigation trees:

- Engine Groups — Lists the Access Control engines added to the selected engine group, the end-systems connected to those engines, the switches added to the engines in the engine group, and general information about the engine group.
- All Access Control Engines — Lists all Access Control engines added to ExtremeCloud IQ Site Engine, the end-systems connected to those engines, the switches added to the engines, and general information about the engine.
- Access Control Configurations — Provides options to configure the end-user connection experience and control network access based on a variety of criteria including authentication.

ExtremeControl Configuration

The ExtremeControl Configuration lets you manage the end user connection experience and control network access based on a variety of criteria. The **Access Control** tab comes with a default Access Control Configuration which is automatically assigned to your Access Control engines. You can use this default configuration as is, or make changes to the default configuration, if desired.

The Access Control Configuration determines what Access Control Profile will be assigned to an end-system connecting to the network. It contains an ordered list of rules that are used by the configuration to assign an Access Control Profile to a connecting end-system based on rule criteria. It also specifies the Default Profile which serves as a "catch-all" profile for any end-system that doesn't match one of the rules. By default, all end-systems match the Default Profile.

When an end-system connects to the network, the rules are evaluated in a top-down fashion, similar to the way an ACL would be evaluated. End-systems that do not match any of the rules are assigned the Default Profile.

Rule Components

The rules defined in an Access Control Configuration provide very granular control over how end-systems are treated as they come onto the network. The following criteria can be used to define the rules used in your Access Control Configuration:

- Authentication Type - for example, 802.1X or MAC authentication.
- End-System Groups - enables you to group together devices that have similar network access requirements or restrictions. For example, a list of MAC addresses, IP addresses, or hostnames.
- Device Type - enables you to group together end-systems based on their device type. The device type can be an operating system family, an operating system, or a hardware type, such as Windows, Windows 7, Debian 3.0, and HP Printers.
- Locations - enables you to specify network access requirements or restrictions based on the network location where the end user is connecting. For example, a list of switches, wireless devices, switch ports, or SSIDs.
- Time of Day - enables you to specify network access requirements or restrictions based on the day and time when the end user is accessing the network. For example, traditional work hours or weekend work hours.
- User Groups - enables you to group together end users having similar network access requirements or restrictions. For example, a list of usernames, an LDAP users group, or a RADIUS user group.

For more information, see the Manage Rule Groups window.

Compound Rules

Compound Rules define multiple conditions in a single NAC rule criteria category for more precise and context-aware Access Control policy decisions. The User Groups and End-System Groups criteria categories in a NAC rule support multi-select, you can select more than one value for a single criteria category in a rule.

When you select multiple values in a User Groups or End-System Groups criteria category, the rule engine applies AND logic. The end-system must satisfy all selected group criteria to match the rule. For example, if you select both Group A and Group B in the User Groups category, the end-system must be a member of both groups.

The following are key characteristics of Compound Rules:

- Multi-select is available only for the **User Groups** and **End-System Groups** criteria categories. All other criteria categories allow only a single selection.
- The rule engine uses AND logic when evaluating multiple values within a single criteria category. An end-system must match all selected values to satisfy the condition.
- The existing **Invert** check box behavior extends to multi-value selections. When you select **Invert** on a multi-value category, the end-system must match none of the selected values.
- Existing single-condition policies are not affected. Selecting a single value in a criteria category produces the same behavior as in earlier versions.

ExtremeControl Profiles

ExtremeControl Profiles specify the authorization and assessment requirements for the end-systems connecting to the network. Profiles also specify the security policies applied to end-systems for network authorization, depending on authentication and assessment results.

The **Access Control** tab comes with ten system-defined Access Control Profiles:

- Administrator
- Allow
- Default
- Guest Access
- Notification
- Pass Through
- Quarantine
- Registration Denied Access
- Secure Guest Access
- Unregistered

If desired, you can edit these profiles or you can define your own profiles to use for your Access Control Configurations. For more information, see the Manage ExtremeControl Profiles window.

AAA Configurations

The AAA Configuration defines the RADIUS servers, LDAP configurations, and Local Password Repository that provide the authentication and authorization services for all end-systems connecting to your ExtremeControl engines. The **Access Control** tab comes with a default Basic AAA Configuration that ships with each Access Control engine. You can use this default configuration as is, or make changes to the default configuration, if desired. For more information, see the Edit Basic AAA Configurations window.

Portal Configurations

If your network is implementing Registration or Assisted Remediation, the Portal Configuration defines the branding and behavior of the website used by the end user during the registration or remediation process. ExtremeControl engines are shipped with a default Portal Configuration. You can use this default configuration as is, or make changes to the default configuration, if desired. For more information, see Portal Configuration.

Access Policies

Access policies define the authorization level that the ExtremeControl assigns to a connecting end-system based on the end-system's authentication and/or assessment results. There are four access policies used in the **Access Control** tab: Accept policy, Quarantine policy, Failsafe policy, and Assessment policy. In your Access Control Profiles, these access policies define a set of network access services that determine exactly how an end-system's traffic is authorized on the network. How access policies are implemented depends on whether your network utilizes Access Control Controller engines and/or Access Control engines.

For end-systems connected to EOS policy-enabled switches, Access Control engines inform the switch to assign a policy role to a connecting end-system, as specified by the access policy. These policy roles must be defined in **Policy** tab and enforced to the EOS policy-enabled switches in your network.

For end-systems connected to RFC 3580-enabled switches, policy roles are associated to a VLAN ID. This enables your Access Control Engines to send a VLAN ID instead of a policy role to those switches using Tunnel RADIUS attributes.

For Access Control Controller engines, authorization of the end-system is implemented locally on the Access Control Controller engine by assigning a policy role to the end-system, as specified by the access policy. In this scenario, all policy roles must be defined in the Access Control Controller policy configuration.

Here is a description of each the **Access Control** tab access policy, and some guidelines for creating corresponding policy roles in the **Policy** tab.

Accept Policy: The Accept access policy is applied to an end-system when it has been authorized locally by the Access Control Engine and when an end-system has passed an assessment (if an assessment was required), or if the Accept policy has been configured to replace the Filter-ID information returned in the RADIUS authentication messages. For EOS policy-enabled switches, a corresponding policy role (created in the **Policy** tab) would allocate the appropriate set of network resources for the end-system depending on their role in the enterprise. For example, you might associate the Accept policy in the **Access Control** tab to the "Enterprise User" role that is defined in the **Policy** tab demo.pmd file. For RFC 3580-compliant switches, the Accept access policy can be mapped to the Production VLAN. Access Control Controllers are shipped with a default policy configuration that includes an Enterprise User policy role.

Quarantine Policy: The Quarantine access policy is used to restrict network access to end-systems that have failed assessment. For EOS policy-enabled switches, a corresponding Quarantine policy role (created in the **Policy** tab) should deny all traffic by default while permitting access to only required network resources such as basic network services (e.g. ARP, DHCP, and DNS) and HTTP to redirect web traffic for Assisted Remediation. For RFC 3580-compliant switches, the Quarantine access policy can be mapped to the Quarantine VLAN. Access Control Controllers are shipped with a default policy configuration that includes a Quarantine policy role.

Failsafe Policy: The Failsafe access policy is applied to an end-system when it is in an Error connection state. An Error state results if the end-system's IP address could not be determined from its MAC address, or if there was an assessment error and an assessment of the end-system could not take place. For EOS policy-enabled switches, a corresponding policy role (created in the **Policy** tab) allocates a nonrestrictive set of network resources to the connecting end-system so it can continue its connectivity on the network, even though an error occurred in the Access Control Solution operation. For RFC 3580-compliant switches, the Failsafe access policy can be mapped to the Production VLAN. Access Control Controllers are shipped with a default policy configuration that includes a Failsafe policy role.

Assessment Policy: The Assessment access policy can be used to temporarily allocate a set of network resources to end-systems while they are being assessed. For EOS policy-enabled switches, a corresponding policy role (created in the **Policy** tab) should allocate the appropriate set of network resources needed by the Assessment server to successfully complete its end-system assessment, while restricting the end-system's access to the network.

Typically, the Assessment access policy enables access to basic network services (e.g. ARP, DHCP, and DNS), permits all IP communication to the Assessment servers so the assessment can be successfully completed (using destination IP address "Permit" classification rule), and HTTP to redirect web traffic for Assisted Remediation. For RFC 3580-compliant switches, the Assessment access policy can be mapped to the Quarantine VLAN. Access Control Controllers are shipped with a default policy configuration that includes an Assessing policy role.

It is not mandatory to assign the Assessment policy to a connecting end-system while it is being assessed. The policy role received from the RADIUS server or the Accept policy can be applied to the end-system, enabling the end-system immediate network access while the end-system assessment is occurring in the background. In this case, the policy role or Accept policy (or the associated VLAN for

RFC 3580-compliant switches) must be configured to permit access to the appropriate network resources for communication with the Assessment servers.

NOTE: The Assessment server sends an ICMP Echo Request (a "ping") to the end-system before the server begins to test IP connectivity to the end-system. Therefore, the Assessment policy role, the router ACLs, and the end-system's personal firewall must permit this type of communication between end-systems and Assessment servers in order for the assessment to take place. If the Assessment server cannot verify IP connectivity, the Failsafe policy is assigned to the end-system.

For more information, refer to the How to Set Up Access Policies Help topic.

Registration

The Extreme Networks ExtremeControl Solution provides support for Registration, a solution that forces any new end-system connected on the network to provide the user's identity in a web page form before being permitted access to the network, without requiring the intervention of network operations. This means that end users are automatically provisioned network access on demand without time-consuming and costly network infrastructure reconfigurations. In addition, IT operations has visibility into the end-systems and their associated users (e.g. guests, students, contractors, and employees) on the network without requiring the deployment of backend authentication and directory services to manage these users. This binding between user identity and machine is useful for auditing, compliance, accounting, and forensics purposes on the network.

End-system or user groups can be configured to exempt certain devices and users from having to register to the network, based on authentication type, MAC address, or user name. For example, a end-system group for the MAC OUI of the printer vendor for the network can be configured to exempt printers from having to register for network access.

The Registration solution has minimal impact on the end user's experience by initially redirecting guests, contractors, partners, students, or other pre-defined end users to a web page for registering their end-system when it is first connected to the network. After successful registration, the end-system is permitted access, and possibly assessed for security posture compliance checking, until the registration is administratively revoked.

Registration is supported on Access Control engines and/or Layer 2 Access Control Controller engines. (Registration is not supported on the Layer 3 Identity and Access Controller engines.) Registration provides flexibility in implementation by offering the following capabilities:

- Determine "valid" end users by prompting each end user for a username with additional information such as full name and email address, or a username and password (for example, email address and student ID number) which can be validated against an existing database on the network.

- Enable end users to register to the network when approved by a "sponsor" who is an internal trusted user to the organization. This is referred to as "Sponsored Registration." With sponsored registration, end users are only permitted to register to the network when approved by a sponsor. Sponsorship can provide the end user with a higher level of access than just guest or web access and enables the sponsor to fine-tune the level of access for individual end users.
- Configure the introductory message for the Registration web page (displayed to end-systems before registering to the network) to state that the end user is agreeing to the Acceptable Use Policy for the network upon registering their device.
- Specify the maximum number of registered MAC addresses per user.
- Control areas on the network where Registration is enabled.
- Provide a web-based administrative interface served over HTTPS where registrations can be viewed, manually added, deleted, and modified by administrators and sponsors without requiring access to the **Access Control** tab.

The Extreme Networks Access Control Solution utilizes a Registration Web Server installed on the Access Control engine to provide this registration functionality to end-systems. Note that an Access Control engine can implement both assisted remediation and registration concurrently.

There are specific network configuration steps that must be performed when using Registration in your Access Control Solution. In addition, you must configure Registration in the **Access Control** tab.

How Registration Works

Here is a description of how Registration works in the Extreme Networks ExtremeControl (Access Control) Solution:

- An unregistered end-system attempts to connect to the network and is assigned the unregistered access profile without being assessed by the Access Control engine. For example, if connected to a Layer 2 Access Control Controller, the end-system can be assigned to the "Unregistered" policy as defined in the Access Control Controller's default policy configuration. If connected to an EOS policy-enabled switch, the end-system can be assigned to the "Unregistered" policy as defined in the ExtremeCloud IQ Site Engine **Policy** tab and enforced to the policy-enabled switches. Or, if connected to an RFC 3580-compliant switch, the end-system can be assigned to the "Unregistered" VLAN.
- The user on the unregistered end-system opens up a web browser to any URL and is redirected to the Registration Web Page served by the Access Control engine.
- The end user registers its end-system on the network by entering information such as username, full name, email, and possibly a password or sponsor's email address into the Registration Web Page, and selecting the "Complete Registration" button.
- The Registration Web Server assigns the end user to an end-system group based on the Registration Behavior configured in the Access Control Configuration.

- The end-system is then automatically re-authenticated to the network by the Access Control engine. Upon re-authentication, the end-system is authenticated, assessed, and authorized as defined by the profile specified in the Access Control Configuration for the newly registered system. If the profile specifies to assess the end-system, an assessment of the end-system takes place at this time.

Assessment

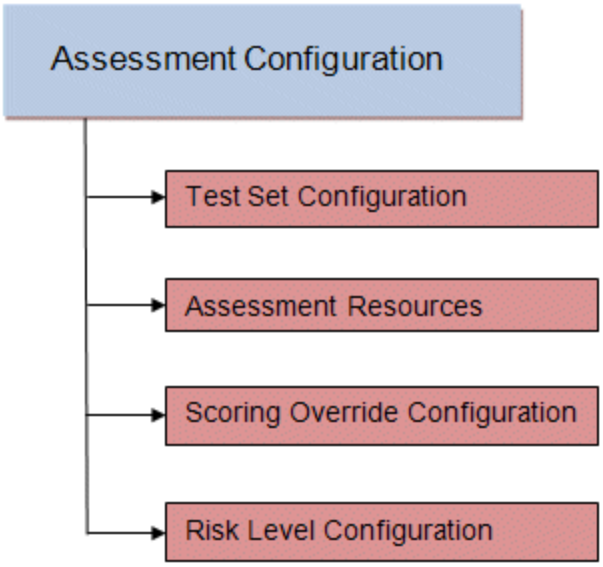
The Extreme Networks ExtremeControl Solution integrates with assessment services to determine the security posture of end-systems connecting to the network. It uses assessment servers to assess and audit connecting end-systems and provide details about an end-system's patch levels, running processes, anti-virus definitions, device type, operating system, and other information critical in determining an end-system's security compliance. End-systems that fail assessment can be dynamically quarantined with restrictive network access to prevent security threats from entering the network.

When an assessment is performed on an end-system, a *Health Result* is generated. For each health result, there can be several *Health Result Details*. A health result detail is a result for an individual test performed during the assessment. Each health result detail is given a score ranging from 1 to 10, and based on this score, the health result is assigned a risk level. The Access Control tab uses this risk level to determine whether or not the end-system will be quarantined.

In addition, assessment tests are assigned a *scoring mode* which determines whether the resulting health result detail is applied towards the quarantine decision, or is used only for informational or warning purposes. Informational health result details can be used to gather information about the security risks on your network, while warning health result details enable you to notify end users when they have security risks that should be remediated. Informational or warning health result details have scores, however these health result details do not impact the end-system's overall risk level.

The Access Control tab lets you create multiple *assessment configurations* that can define different assessment requirements for end-systems. Assessment configurations define the following information:

- What assessment tests to run (determined by the selected test sets).
- What resources to use to run the tests (determined by the selected Assessment Resources).
- How to score assessment results (determined by the selected Risk Level and Scoring Override configurations).



Test sets let you define what type of assessment to execute, what parameters to pass to the assessment server, and which assessment server resources to use. The **Access Control** tab provides three default test sets; one for each type of assessment agent that is either supplied or supported by the **Access Control** tab. You can use these default test sets "as is" or edit them, if desired.

When you define your assessment server resources for a test set, you can specify to balance the assessment load between your all your assessment servers, or, you can specify an assessment server pool. For example, if you have four Nessus assessment servers, you can put server A and server B in server pool 1, and server C and server D in server pool 2. Then, in your test set configuration you can specify which server pool that test set should use.

You can use risk level and scoring override configurations to define how each assessment configuration will interpret an end-system's health results. The risk level configuration determines what risk level is assigned to an end-system (high, medium, or low) based on the end-system's health result details score. The scoring override configuration lets you override the default score and scoring mode assigned to a particular assessment test ID.

After you have defined your assessment configurations, they are available for selection when creating your Access Control Profiles. In addition, the **Access Control** tab provides a default assessment configuration that is already set up with default assessment parameters and is ready to use in your Access Control Profiles.

Before beginning to configure assessment on your network, read through the following information presented in the **Access Control** tab online Help.

- How to Set up Assessment – Provides information on the steps that must be performed in the **Access Control** tab prior to deploying assessment on your network, including managing your assessment servers and adding external assessment servers. It also includes basic information

on how to use the default assessment configurations provided by the **Access Control** tab, and enable assessment for your Access Control Configuration.

- ExtremeControl Assessment Phased Deployment Guide - This guide describes the phased approach to introducing assessment into your Access Control deployment using Informational, Warning, and Quarantine assessment. The guide also provides information on the **Access Control** tab tools that can be used to monitor and evaluate assessment results, and diagnose and troubleshoot problems.
- How to Configure Assessment - Provides step-by-step instructions for configuring assessment using the phased approach described in the Access Control Assessment Phased Deployment Guide. Instructions are provided for configuring phased assessment using agent-less or agent-based assessment, or a combination of both.
- How to Deploy Agent-Based Assessment - If you are deploying agent-based assessment, this Help topic provides the configuration steps specific to deploying agent-based assessment in a Windows and Mac network environment. It includes instructions for configuring agent deployment and provides information about the agent icon and notification messages that appear on the end-user's system. It also includes instructions on performing a managed deployment or installation of the agent.
- How to Set Up Assessment Remediation - Because Warning and Quarantine assessment provides end-system remediation, you must enable remediation for your Access Control Configuration. This Help topic provides the specific steps that must be performed when setting up assisted remediation in your network.

Assessment Remediation

Remediation is a process that informs end users when their end-systems have been quarantined due to network security policy non-compliance, and enables end users to safely remediate their non-compliant end-systems without assistance from IT operations. The process takes place when an end-system connects to the network and assessment is performed. End users whose systems fail assessment are notified that their systems have been quarantined, and are instructed in how to perform self-service remediation specific to the detected compliance violation. After the remediation steps have been successfully performed and the end-system is compliant with network security policy, the appropriate network resources are allocated to the end-system, again without the intervention of IT operations.

The Extreme Networks ExtremeControl Solution implements local Remediation Web Server functionality to provide web notification to end users indicating when their end-systems are quarantined and what remediation steps the end user must take. The Remediation Web Server is installed on the Access Control engine.

There are specific network configuration steps that must be performed when using assisted remediation in your Access Control Solution. In addition, you must configure assisted remediation in the **Access Control** tab. For more information, see How to Set up Assessment Remediation and Portal Configuration Help topics.

How Remediation Works

Here is a description of how assisted remediation works in the Extreme Networks ExtremeControl Solution:

- An end-system connects to the network (where assessment has been configured) and is authorized with the level of network access defined by the Assessment access policy configuration.
- The end-system is assessed by the assessment server for security threats and vulnerabilities.
- When the end-system opens a web browser to any web site, the HTTP traffic is redirected to the Access Control engine and a web page indicating that the end-system is currently being assessed is displayed.
- When the assessment is complete, the assessment server sends the results to the Access Control engine. If the end-system failed assessment, the end-system is authorized with the level of network access defined by the Quarantine access policy configuration.
- When the quarantined end user opens a web browser to any web site, its traffic is dynamically redirected to the Access Control engine.
- The Access Control engine returns a web page formatted with self-service remediation information for the quarantined end-system. This web page indicates the reasons the end-system was quarantined and the remediation steps the end user must take.
- After taking the appropriate remediation steps, the end-user selects a button on the web page and attempts to reconnect to the network. A re-assessment of the end-system is initiated. If the end-system is now compliant with network security policy, the Access Control engine authorizes the end-system with the appropriate access policy. If the end-system is not compliant, the Quarantine access policy is again utilized to restrict the authorization level of the end-system and the process starts again.
- After a specified number of attempts and/or maximum time to remediate have expired, the end user can be redirected to a web page requiring them to contact the helpdesk for further assistance, and a notification is sent to the helpdesk system with information regarding the non-compliant end-system.

End-System Zones

The **Access Control** tab end-system zones enable you to group end-systems into zones, and then limit an ExtremeCloud IQ Site Engine user's access to ExtremeCloud IQ Site Engine end-system information and configuration based on those zones.

End-system zones are configured and managed in the **Access Control** tab, and are enforced for ExtremeCloud IQ Site Engine end-system information and configuration.

When an end-system authenticates to the network, Access Control rules are used to assign an Access Control profile and an end-system zone to the end-system. This enables you to use a variety of rule

components (such as End-System Groups, Location Groups, and User Groups) to determine which zone an end-system should be assigned to.

You can create any number of end-system zones in your network. An end-system can only be assigned to one zone (but does not have to be assigned to a zone). You can view which zone an end-system is currently assigned to in the end-systems table in the **Access Control** tab in ExtremeCloud IQ Site Engine.

A user's authorized zones are determined by their ExtremeCloud IQ Site Engine user group membership. User groups are created and configured in the ExtremeCloud IQ Site Engine Authorization/Device Access Tool (accessed from the Tool menu), and authorized zones are assigned to each user group in the **Access Control** tab.

In addition to using end-system zones, you can also limit a user's access to ExtremeCloud IQ Site Engine operations by assigning authorized rule groups. Whenever a user initiates a change to a rule group, such as adding or removing an end-system to or from a group, a check is performed to verify that the user is authorized to change that rule group. Similar to end-system zones, a user's authorized rule groups are determined by their ExtremeCloud IQ Site Engine user group membership.

A third component that should be taken into consideration is the ability to limit user access to ExtremeCloud IQ Site Engine using authorization group capabilities. For example, you can assign a user group the ExtremeCloud IQ Site Engine End-Systems Read Access capability to enable read-only access to ExtremeCloud IQ Site Engine end-system information, and use end-system zones to limit which end-systems can be viewed. You can assign a user group the ExtremeCloud IQ Site Engine End-Systems Read/Write Access capability to enable the ability to modify rule groups, and use rule group authorization to limit which rule groups the user can perform these operations on.

Capabilities are assigned to user groups using the Authorization/Device Access Tool. The Netsight Administrator group is always assigned all capabilities.

For more information, see Authorization Group Capabilities.

End-System Zone Use Cases

Here are several network scenarios where using end-system zones could be beneficial.

- **A Service Provider with multiple tenants.** If a service provider serves multiple tenants and each tenant has a clearly delineated set of switches, user access can be configured to enable each tenant's IT staff to only view the end-systems connecting to their own switches.
- **A large enterprise with network administrator groups.** In a large enterprise where specific groups of network administrators are responsible for specific groups of switches on shared engines, user access can be configured so that each administrator can view reports and other information only for their switches and end-systems.
- **A large business segmented by business function.** In a large enterprise where division of control is not closely tied to switches or engines, user access can be configured so that administrators only have the ability to view and manage the appropriate end user groups.

In each of these scenarios, a restricted set of authorization group capabilities must be used to prevent users from viewing and accessing information that does not pertain to their area.

Enforcing

In the **Access Control** tab, enforcing means writing Access Control configuration information to one or more Access Control engines. Any time you add or make a change to the Access Control Configuration, the engines need to be informed of the change through an enforce, otherwise the changes do not take effect. When an engine needs to be enforced, the Enforce icon displays on that engine in the left-panel tree.

To enforce, use the **Enforce All** button in the **Enforce** menu at the bottom of the left-hand panel which writes the information to all the Access Control engines. You can enforce to an individual engine or engine group by selecting the **Enforce** menu and selecting **Selection**.

TIP: For a preview of ExtremeCloud IQ Site Engine is enforcing/updating on an individual engine, right-click the engine and choose **Enforce Preview** from the menu. The Access Control Engine Enforce Preview window displays, which indicates the information changing.

The enforce operation is performed in two stages: first an engine configuration audit is performed and then the actual enforce to engines is performed.

The configuration audit takes place automatically after you start the enforce operation. It looks for a wide-range of engine configuration problems including a review of the Access Control Configuration, Access Control Profile, rule configuration, AAA configuration, and portal configuration. The audit results are displayed in the Enforce window, enabling you to view any warning and error information. To see warning or error details, use the + icon in the left column to expand the Details information (as shown below) or select **Show Details** to open the information in a new window.

If you choose to correct any problems at this point, you must close the Audit Results window. When you have made your changes, select the Enforce All button to start the enforce operation and perform a new audit.

From the Enforce window, you can select the **Enforce All** button to enforce all engines, or use the checkboxes in the Select column to select some of the engines to enforce and select the **Enforce** button. In order for the enforce operation to be carried out, none of the selected engines can have an error associated with it. Even if one of the selected engine has passed the audit, it will not be enforced if other selected engines have errors.

If none of the selected engines have errors, but a selected engine has a warning associated with it, you are given the option to acknowledge the warning and proceed with the enforce anyway. When you acknowledge the warning and select **OK**, the enforce is performed.

TIP: If there are warning messages that are regularly displayed during Enforce engine audits, you can use the Enforce Warning Settings to specify that these messages should be ignored and not be displayed.

The Enforce window displays the enforce operation status, as shown below.

Advanced Enforce Options

In the Enforce window, there are two Advanced enforce options available. The two options can be used for the following situations:

- **Force Reconfiguration for All Switches** - This option can be used if the switch RADIUS settings were manually changed via CLI or the **Policy** tab. Since Identity and Access does not reconfigure the switches every time there is an enforce, selecting this option forces reconfiguration of RADIUS settings on all switches to ensure they are configured correctly.
- **Force Reconfiguration for Captive Portal** - During an enforce, captive portal settings are not enforced unless they have changed. You can use this option to force reconfiguration of the portal to ensure the state of the captive portal processes.

MAC Locking

MAC Locking lets you lock a MAC address to a specific switch or port on a switch so that the end-system can only access the network from that port or switch. If the end-system tries to authenticate on a different port or switch, it is rejected or assigned a specific policy based on an action that you specify when you create the MAC Lock. Access the Add MAC Lock window to set up your MAC Locks.

NOTE: MAC Locking to a specific port on a switch is based on the port interface name (e.g. fe.5.1). If a switch board is moved to a different slot in a chassis, or if a stack reorders itself, this name will change and break the MAC Locking settings.

Here are some examples of ways to use MAC Locking:

- A university might lock end-users on a specific floor in a dormitory to a switch that services that floor.
- A printer, server, or other end-system could be permitted network access only when it is connected to a port specified by IT operations. This prevents security issues that could result if the device was moved to a different area of the network.
- A company could lock an IP phone to a specific port on a switch. This would enable exact identification of the phone's location in case an emergency (911) call was placed from the phone.

NOTE: For ExtremeControl Controller Engines.

-- On Layer 3 ExtremeControl Controllers, do not use MAC Locking to lock a MAC address to the Controller PEP IP address **and** a port on the PEP. You can however, lock a MAC address to the PEP IP and **not** the port, which would restrict movement of the MAC address away from the Layer 3 Controller.

-- On Layer 2 Access Control Controllers, a MAC address can be locked to the Controller PEP IP address and port, or just the PEP IP address, but this only controls the movement of the end-system between the downstream ports on the PEP (IP address and port) and not the actual edge of the network.

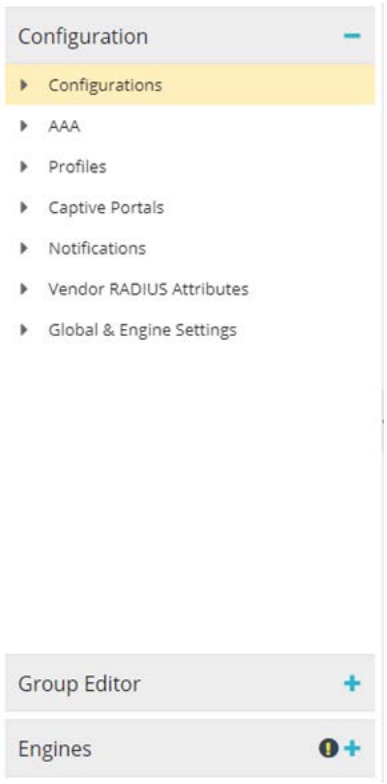
-- On Layer 3 Access Control Controllers, there can be cases where the **Access Control** tab cannot determine the MAC address of the connecting end-system (for example, DHCP is disabled and a firewall is enabled on the end-system, or the end-system is connecting through a VPN), and the MAC address for the end-system is displayed as "Unknown." In these cases, the MAC Locking feature is not supported.

Notifications

Notifications provide the ability for the Identity and Access tab to notify administrators or helpdesk personnel of important information through email, Trap, or Syslog messages. These notifications help administrators understand what is going on in their system on a real-time basis. For example, the Access Control tab could be configured to send a notification when a new end-system is learned on the network, when a MAC lock is violated, or when a new MAC address is registered on the network.

Access Control

Access Control Configuration provides a central location to view the configuration parameters for all aspects of your ExtremeControl system. Access this window by selecting Control > Access Control. Expand the tab to display the options:

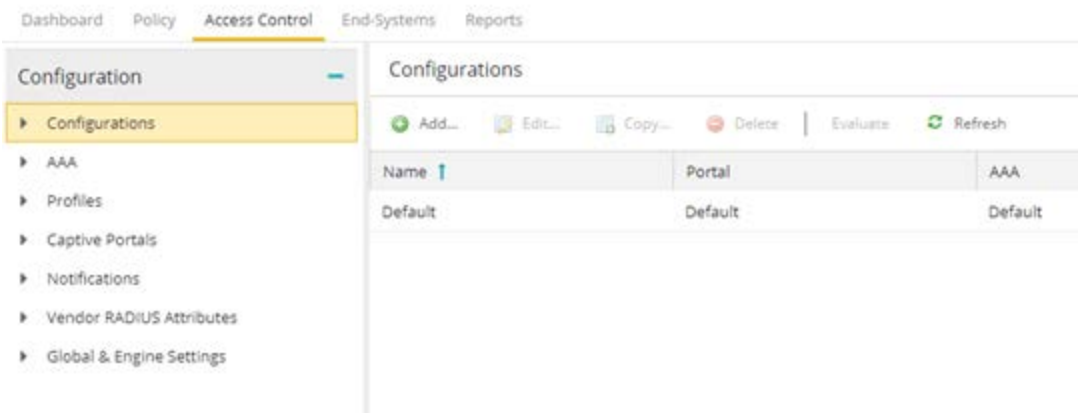


The following tabs are included in the Configuration tree:

- Configurations
- AAA
- Profiles
- Captive Portals
- Notifications
- Vendor RADIUS Attributes
- Global & Engine Settings

Configurations

Expand Configurations to access to the following Access Control system components.



Each engine group uses one Access Control configuration that contains an ordered list of rules used to determine which Access Control profile is assigned to the end-systems connecting to the engines in that group. Access Control configurations include the following components:

Name

The **Name** by which the Access Control Configuration is known.

Portal

If your network is implementing Registration or Assisted Remediation, use the Portal Configuration to define the branding and behavior of the website used by the end user during the registration or remediation process.

AAA

AAA configurations define the RADIUS and LDAP configurations, and Local Password Repository that provide the authentication and authorization services to your Access Control engines.

AAA

The AAA tab defines the RADIUS and LDAP configurations that provide the authentication and authorization services to your ExtremeControlengines.

Profiles

The Profiles tab displays ExtremeCloud IQ Site Engine's system-defined ExtremeControl profiles that define the authorization and assessment requirements for the end-systems connecting to the network.

Captive Portals

The Captive Portals tab enables you to define the branding and behavior of the portal website used by the end user, if your network is implementing registration or Assessment/Remediation.

Notifications

The Notifications tab displays all the notifications you create, and enables you to add, edit, and test specific notification rules. Notifications enable you to create alert actions performed when specific events or triggers take place in ExtremeCloud IQ Site Engine

Vendor RADIUS Attributes

The **Vendor RADIUS Attributes** tab displays all the vendors and a list of known vendor RADIUS dictionary attributes that have been discovered from the managed engines. Select a vendor name in the table to display the vendor attribute details, including Attribute Name, Attribute Data Type, Attribute Type, and Options.

Add Radius Dictionary to ExtremeControl.

1. Upload the custom RADIUS dictionary to all Access Control engines:

   ```
   /opt/tag/radius/share/freeradius
   ```

2. Update the permissions for the file:

   ```
   chmod 644 /opt/tag/radius/share/freeradius/*
   ```

3. Restart the service:

   ```
   nacctl restart
   ```

NOTES:

- Custom radius dictionaries are not part of the backup. The procedure may need to be repeated after the software upgrade.
- A non-compatible radius dictionary can cause the solution to be non-operational.
- Renaming existing VSAs in radius dictionaries can cause the system to be non-operational.
- Duplicating existing VSAs in radius dictionaries can cause the system to be non-operational.
- Extreme can not guarantee that third party radius dictionary will work.

Global & Engine Settings

The **Global & Engine Settings** tab provides you access to the following additional tabs:

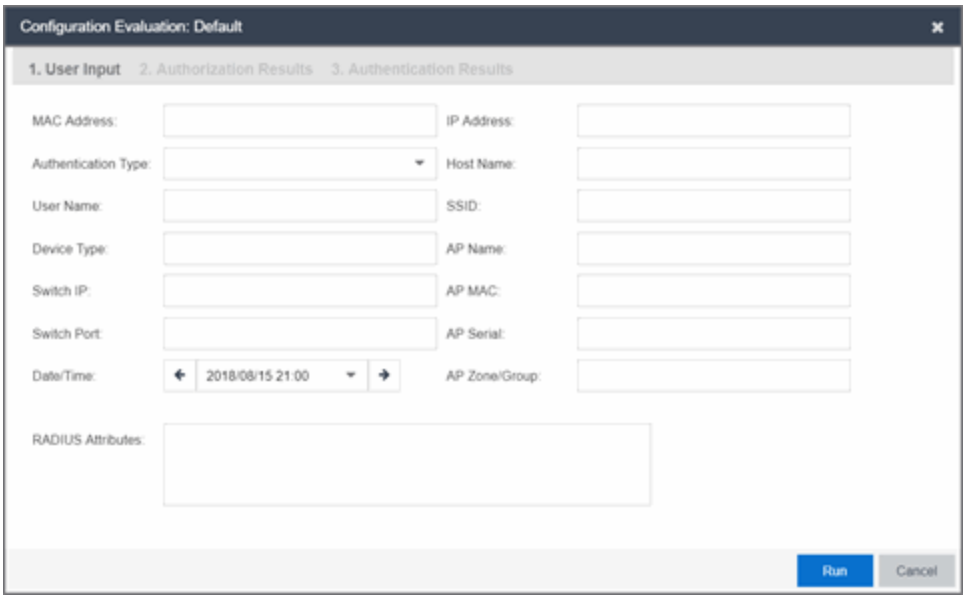
- MAC Locking - Use this tab to view settings for locked MAC addresses or to lock a MAC address to a specific switch or port on a switch so that the end-system can only access the network from that port or switch.

- MAC to IP Mappings – Use this tab to view MAC to IP address mappings for devices with statically assigned IP addresses, and import a file of MAC to IP mappings to the list. You can also Add, Edit, Delete, and Export mappings from this tab.
- Manage End System Zones

The Engine Settings tab, which is accessible when you expand the Global & Engine Settings tab, to view and configure advanced configuration options for ExtremeControlengines. ExtremeCloud IQ Site Engine includes a default engine settings configuration. You can also define your own settings to use for your Access Controlengines.

Configuration Evaluation Wizard

This Configuration Evaluation Wizard is used to test the rules defined in your Access Control Configuration in order to determine what behavior an end-system encounters when it is authenticated on an Access Control engine. To access this window, select Configurations in the left-panel of the **Access Control** tab, select an Access Control Configuration in the main panel, and select the **Evaluate** button in the toolbar.

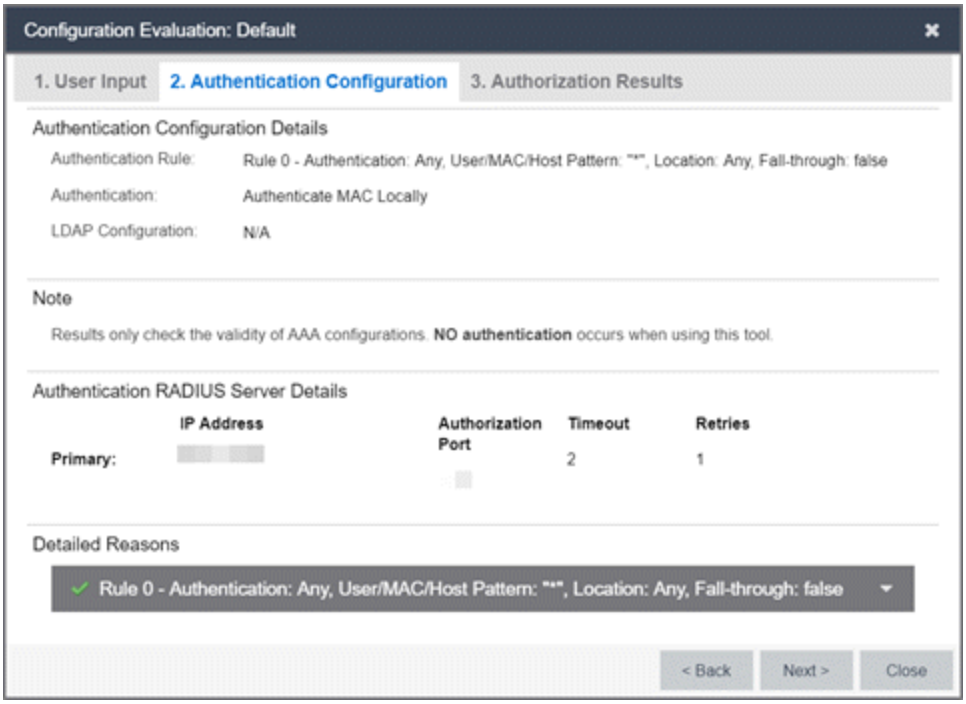


User Input

Enter the end-system data on which you are evaluating the Access Control configuration in this tab.

Authentication Results Tab

This tab displays the set of RADIUS servers and LDAP servers by which ExtremeControl processes an end-system request.



Authentication Result Details

- Authentication Rule - A description of the authentication type and user name expression used for the AAA entry that the ExtremeControlengine uses to authenticate the end-system. For a Basic AAA Configuration, this is always: Authentication: Any, User Pattern"*". Additionally, indicates whether fall-through functionality is enabled for the Configuration.
- Authentication - For MAC authentication requests, this field displays whether the request is authenticated locally or proxied to the RADIUS server.
- LDAP Configuration - The LDAP configuration used to obtain any LDAP data for the end-system, if applicable.

Authentication RADIUS Server Details

This section lists the IP address, port, shared secret, timeout, and retries listed for all the RADIUS servers used to authenticate the end-system request, if it needs to be proxied.

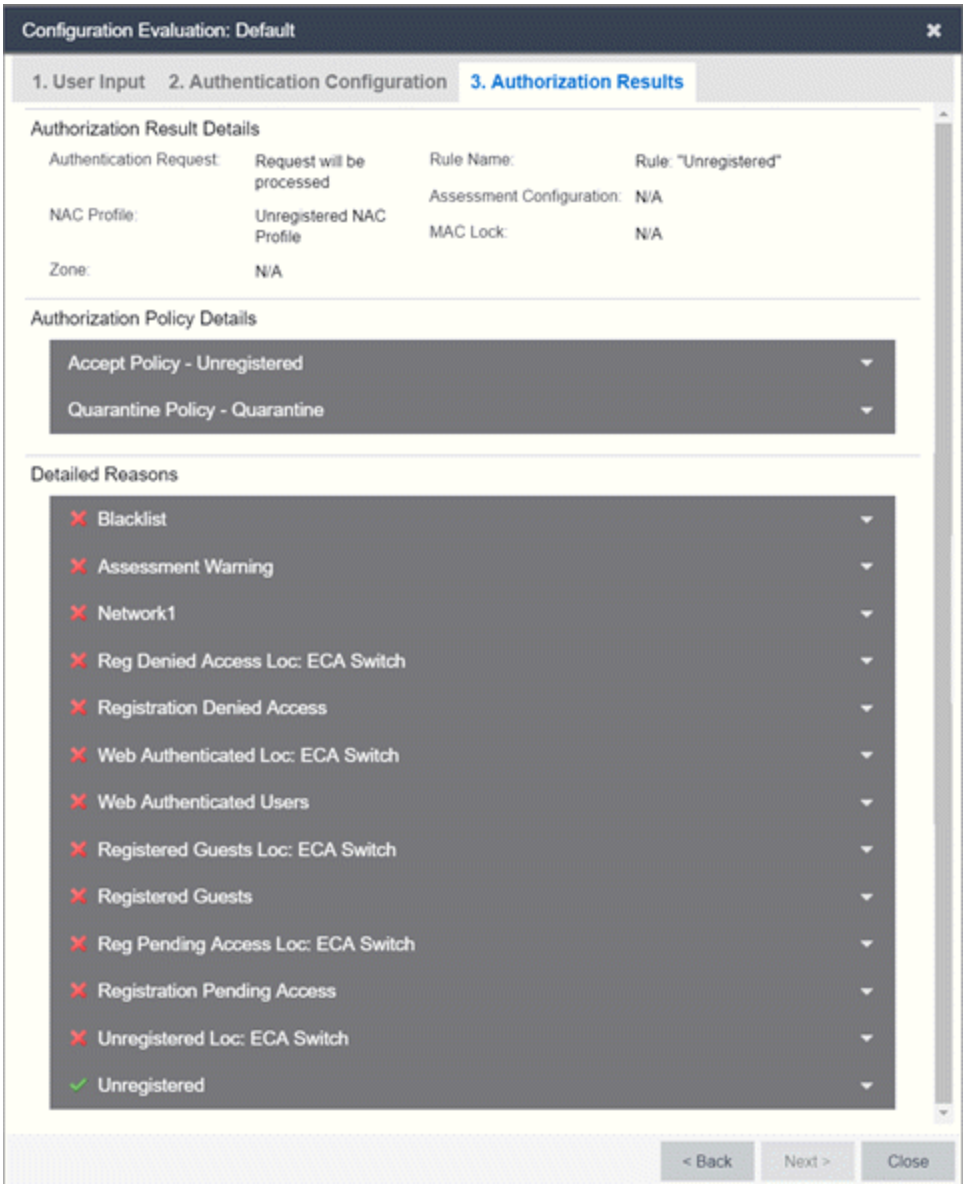
Detailed Reasons

This section is only applicable for an Advanced AAA Configuration. It lists why a request passed or failed the definition of each AAA entry as well as whether fall-through functionality is enabled.

Authorization Results Tab

This tab displays information detailing the method by which the end-system is authorized, according to the parameters and rules of the selected Access Control Configuration. The results also factor in any

RADIUS user attributes you enter on the **User Input** tab when the evaluation is run.



Authorization Result Details

- Authentication Request - Displays whether the ExtremeControl engine processes the request, or reject the request based on a MAC Lock or a rule that assigns an Access Control Profile configured to reject the user.
- Rule Name - The name of the rule that the end-system passed.
- NAC Profile - The Access Control Profile assigned to the end-system by the rule.
- Assessment Configuration - The assessment configuration used by the Access Control

Profile, if any.

- MAC Lock - The MAC Lock assigned to the end-system, if any.

Authorization Policy Details

This section displays the RADIUS response attributes returned for end-systems in specific states. Possible states are Accept, Quarantine, Assessing, and Failsafe. Expand each state to view the RADIUS attributes. These are the RADIUS attributes returned for the switch IP that is listed in the End-System Details section.

Detailed Reasons

This section lists all the rules from the Access Control Configuration that were evaluated during the end-system authentication. Rules are only evaluated until one of them is passed. Each rule listing can be expanded to view why the end-system passed or failed that rule.

Compound Criteria Evaluation Results

When a NAC rule contains Compound Rules criteria with multiple values selected in the User Groups or End-System Groups category, the Configuration Evaluation Wizard displays granular pass or fail results for each individual value in the category. For each criteria category that contains multiple values, the **Authorization Results** tab shows individual child rows for each selected value in the category display separate pass or fail results. Use these child rows to identify which group conditions matched or did not match during evaluation.

The granular breakdown provides detailed visibility into the specific conditions that passed or failed during rule engine evaluation of compound criteria.

NOTE: For criteria categories containing only a single value, the evaluation results display the same pass or fail behavior as in earlier versions.

Access Control Configuration Rules

The Rules panel in the **Access Control** tab displays a list of rules used by the Access Control Configuration to assign an Access Control Profile to a connecting end-system based on rule criteria.

This Help topic provides information for accessing and configuring Access Control Configuration Rules:

- Accessing ExtremeControl Configuration Rules
- Viewing Rules in the Table
- Creating and Editing Rules
- Advanced Location-Based Registration and Web Access - Allows you to configure different access features for end users based on the location of a connecting end-system, as determined by the location groups you have defined for your network.

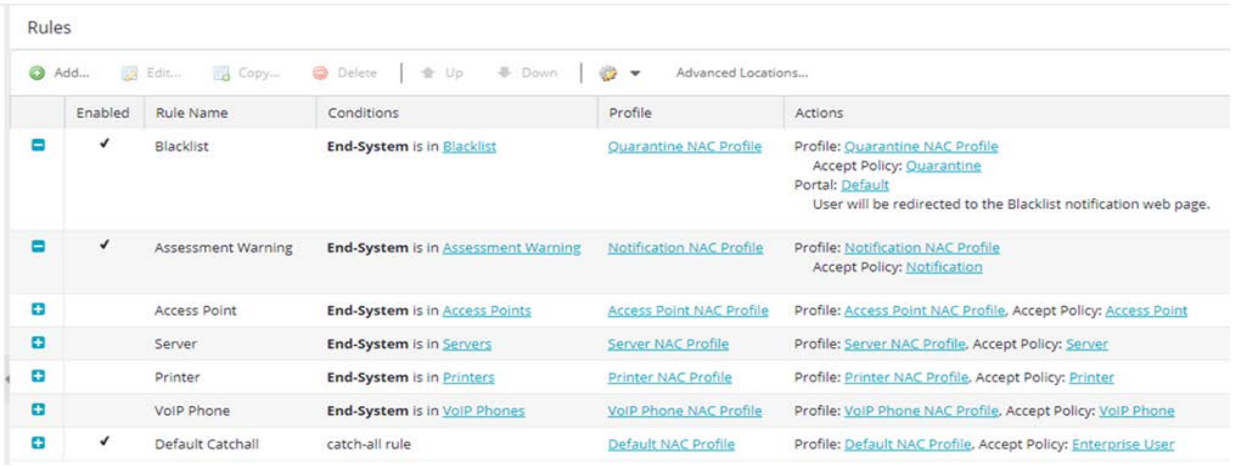
Accessing ExtremeControl Configuration Rules

Use the following steps to view and edit your Access Control Configuration rules.

1. Open the **Control** tab in ExtremeCloud IQ Site Engine.
2. Select the **Access Control** tab.
3. In the left-panel tree, expand the Access Control Configurations tree.
4. Expand an Access Control Configuration and select Rules. The table of your Access Control rules is displayed in the right panel. See below for an explanation of the table columns.
5. Use the toolbar buttons at the top of the right-panel to create a new rule or edit existing rules. See below for a description of each button.

Viewing Rules in the Table

The Rules table displays the rule name, whether the rule is enabled, and summary information about the rule. It also shows the Access Control Profile assigned to any end-system that matches the rule and the portal redirection action, if applicable. Rules are listed in order of precedence. End-systems that do not match any of the listed rules are assigned the Default Catchall rule.



TIP: Right-click a rule in the table to access a menu of options including the ability to edit the Access Control profile and any user groups included in the rule.

Expand (⊞) and Collapse (⊟) Icons

Select the ⊞ icon to expand a Rule in the table to display additional conditions, end-system, profile, and portal details. Select the ⊟ icon to collapse a row and hide the additional Rule details.

Enabled

This column displays whether the rule is enabled by displaying a check mark icon ✓ or disabled, with no check mark. Select the **Edit** button to enable or disable the rule. You cannot disable any of the system rules provided by ExtremeCloud IQ Site Engine.

Rule Name

This column displays the rule name. Double-click on the rule to open the Edit Rule window where you can edit the rule name, if desired. You cannot change the name of the system rules provided by ExtremeCloud IQ Site Engine.

Conditions

This column displays the criteria an end-system must meet in order to be assigned the rule, including the authentication method and rule groups that the end-system or user must match. Double-click on the rule to open the Edit Rule window where you can edit the rule criteria, if desired. You cannot change the criteria for the system rules provided by ExtremeCloud IQ Site Engine. Select a rule group name to open a window where you can edit the group's parameters.

User Group

This column, hidden by default, displays the user group you configured. User groups limit an ExtremeCloud IQ Site Engine user's access based on the LDAP, RADIUS, or Username group to which they are assigned. To edit the **User Group**, select the user group in the **Conditions** column, which opens the **Add/Edit User Group** window.

Zone
: This column displays the end-system zone you configured. End-system zones allow you to group end-systems into zones, and then limit an ExtremeCloud IQ Site Engine user's access to end-system information and configuration based on those zones.

Actions
: This column displays the actions the rule takes when an end-system matches the rule's criteria. This includes the profile assigned to the end-system, the network policy, and the portal configuration the end user sees. If you want to edit an action, select the profile, policy, or portal to open a window where you can make the changes.

Add or remove a column by selecting the down arrow at the right of a column header and selecting a checkbox associated with a column from the Columns menu.

Creating and Editing Rules

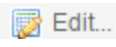
Use the Rules toolbar buttons to create, edit, and modify the rules in the table. Any changes made in this table are written immediately to the ExtremeCloud IQ Site Engine database.



Add New Rule

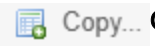
Opens the Create Rule window where you can define a new rule to use in the Access Control configuration.

TIP: To add a new rule at a specific location in the table, select the rule that you want the new rule to follow, right-click and select **Add Rule** after Selection. When you create the new rule and select **OK**, it is added after the selected rule. The selected rule must be a custom (user-defined) rule, or it can be the blocked list or Assessment Warning rule.



Edit Rule

Opens the Edit Rule window where you can edit the rule criteria for a selected rule.



Copy Rule

Opens the Copy Rule window where you can copy the rule criteria of an existing rule for a new rule.



Delete Selected Rules

Deletes any rules selected in the table.



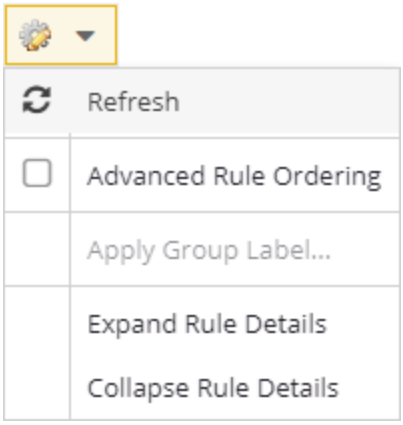
Move Rule Up/Down

Move rules up and down in the list to determine rule precedence.



Configuration

Opens the Configuration drop-down list:

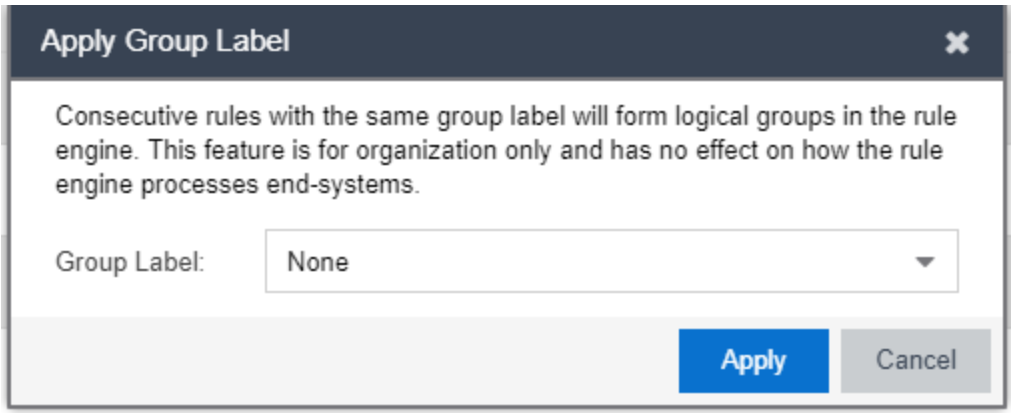


Refresh

Updates the Rules details.

Apply Group Label

Opens the Apply Group Label window where you can add a group label to selected rules to create a new group. When the group label is applied, the new group appears in the Rules window and is collapsible.



Expand Rule Details

Expands all Rules in the table to display additional conditions, end-system, profile, and portal details.

Collapse Rule Details

Collapses all expanded Rules in the table.

Advanced Locations **Advanced Locations**

Use the Advanced Locations tab to define location-based access configurations.

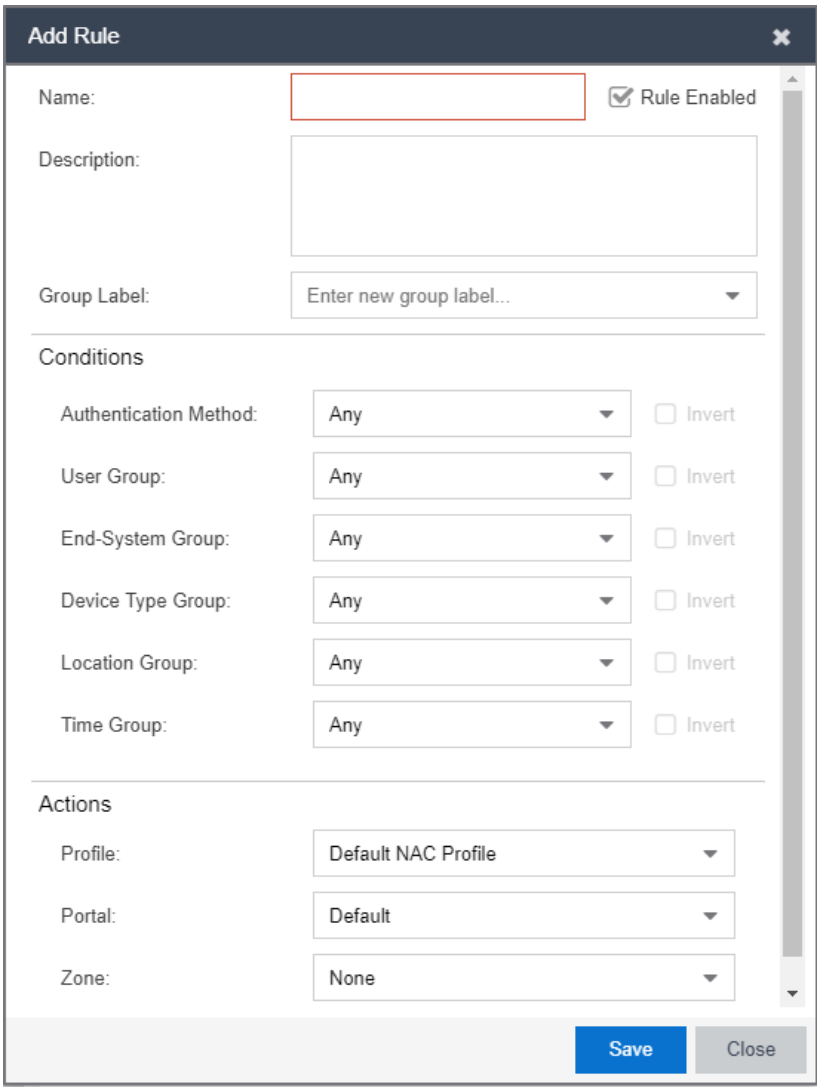
Add/Edit Rule

Use this window to add a new rule or edit an existing rule in an ExtremeControl configuration. End-systems that match the criteria selected for the rule are assigned the Access Control profile that is specified.

To access this window:

1. Open the **Control** tab in ExtremeCloud IQ Site Engine.
2. Select the **Access Control** tab.
3. In the left-panel tree, select Access Control Configurations > Default > Rules. A table of rules for the Access Control configuration is displayed in the right panel.
4. Select the **Add** button in the table toolbar to open the Create Rule window.
   or
   Select a rule in the table and select the **Edit** button in the toolbar to open the Edit Rule window.

The image below shows a rule created to provide a different Access Control profile for authenticated registered users on mobile devices. Descriptions of the different fields and options in the window are provided below.



NOTES: For the following rule criteria:

-- If you select **Any** then the criteria is ignored during the rule match process.

-- If you select the **Invert** checkbox, it is considered a rule match if the end-system does **not** match the selected value.

Name

Enter a name for a new rule or change the name of an existing rule, if desired.

Rule Enabled

Select this checkbox to enable this rule in the Access Control configuration.

Description

Enter a description of the rule.

Group Label
If this rule is part of a group, select the group name from the drop-down list or enter a new group label here.

Authentication Method
Select the authentication method that end-systems must match for this rule.

User Group
Select the user group that the end user must be a member of to match this rule. Select the Edit button to edit the selections available in this drop-down list.

End-System Group
Select the end-system group that the end-system must be a member of to match this rule. Select the **Edit** button to edit the selections available in this drop-down list.

Device Type Group
Select the device type group that the end-system must be a member of to match this rule. Select the **Edit** button to edit the selections available in this drop-down list.

Location Group
Select the network location (switch and interface) that the end-system must originate from to match this rule.

Time Group
Select a time frame that the connection request must match for this rule.

Profile
Select the Access Control profile assigned to any end-system matching this rule from the drop-down list. Select New to add a new profile in the Create New Profile window. Select Manage from the drop-down list to be redirected to the Engine Group > Switches tab and allows you to make additions or edits to the switches in this engine group.

Portal
Select the portal configuration from the drop-down list to any end-system matching this rule. Select New to add a new portal configuration in the Add New Portal Configuration window. Select Manage from the drop-down list to be redirected to the Engine Group > Switches tab and allows you to make additions or edits to the switches in this engine group.

Zone
This field only displays if you have displayed the Zone column in the Access Control Configuration Rules table. Select the end-system zone assigned to any end-system matching this rule. Enter a new zone name if none exists. See End-System Zones for more information.

Select **Save** to save your changes.

Multi-Select Criteria for Compound Rules

The User Groups and End-System Groups criteria categories support multi-select. You can select multiple values in a single criteria category to configure Compound Rules.

Use the following steps to configure Compound Rules:

1. In the **Add/Edit Rule** window, locate the User Groups or End-System Groups criteria category.
2. Select the criteria type from the drop-down list.
3. Select multiple values from the value selector. The selector provides the option to choose more than one group. Selected values are displayed in the criteria field.
   When multiple values are selected, a helper text label displays below the selector indicating that AND logic is applied. The end-system must match all selected values to satisfy the condition.
4. (Optional) Select the **Invert** check box to invert the matching logic. When you select Invert with multiple values, the end-system must not match any of the selected values.
5. Select **OK** to save the rule.

When you view rules in the rules table, criteria categories with multiple values display a summary of the selected values. You can use the summary to identify which rules contain compound criteria.

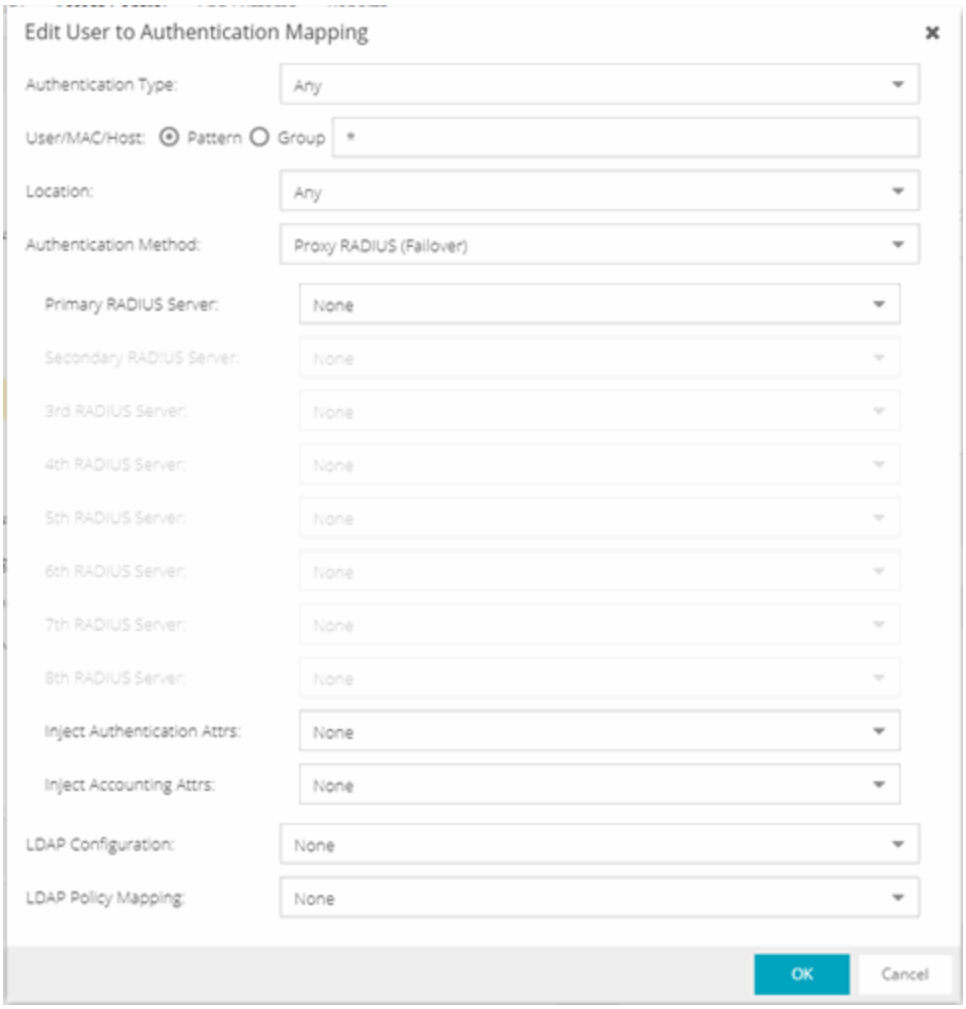
Important: All other criteria categories, such as Location Groups, Time Groups, and Device Type Groups, continue to support only single-value selection. Multi-select is available only for the User Groups and End-System Groups criteria categories.

NOTE: Compound Rules use AND logic within a single criteria category. The relationship between different criteria categories in a rule, such as between User Groups and End-System Groups, continues to follow the existing rule evaluation logic.

Compound Rules remain fully backward compatible with existing single-condition rules. When a criteria category contains only a single value, the behavior remains the same as in earlier versions. Existing rule configurations do not require modification.

Authentication Rules and Add User to Authentication Mapping Window

This window lets you add or edit the user to authentication mappings that define your Advanced AAA configurations. You can access this window from the **Add** or **Edit** buttons in the AAA Configuration window.



Authentication Type

Select the authentication type that the end-system must match for this mapping. Note that individual types of 802.1X authentication are not available for selection because at this point in the authentication process, the fully qualified 802.1X authentication type cannot be determined. Select **Any** if you don't want to require an authentication match. Select **802.1X (TTLS-INNER-TUNNEL)** or **802.1X (PEAP-INNER-TUNNEL)** to authenticate via another RADIUS server using an inner tunnel to protect the authentication request.

The Management Login authentication type enables you to set up a mapping specifically for authenticating management login requests, when an administrator logs into a switch's CLI via the console connection, SSH, or Telnet. This enables you to send management requests to a different authentication server than network access requests go to. This authentication type can be used to authenticate users locally, or proxy them to specific RADIUS or LDAP servers. Make sure that the Management Login mapping is listed above the "Any" mapping in the list of mappings in your Advanced AAA Configuration. In addition, you must set the Auth. Access Type to either "Management Access" or "Any Access" in the Add/Edit Switches window for this authentication type.

User/MAC/Host

Select the **Pattern** radio button and enter the username, MAC address, or hostname that the end-system must match for this mapping. Or, select the **Group** radio button and select a user group or end-system group from the drop-down list. If you enter a MAC address, you can use a colon (:) or a dash (-) as an address delimiter, but not a period (.).

Location

Select the location group that the end-system must match for this mapping, or select "Any" if you don't want to require a location match. You can also add a new location group or edit an existing one.

Authentication Method

Select the authentication method that the end-system must match for this mapping: Proxy RADIUS, LDAP Authentication, or Local Authentication.

Primary RADIUS Server — Use the drop-down list to select the primary RADIUS server for this mapping to use. You can also add or edit a RADIUS server, or manage your RADIUS servers.

Secondary RADIUS Server — Use the drop-down list to select the backup RADIUS server for this mapping to use. You can also add or edit a RADIUS server, or manage your RADIUS servers.

3rd - 8th RADIUS Server — Use the drop-down list to select the backup RADIUS server for this mapping to use. You can also add or edit a RADIUS server, or manage your RADIUS servers.

Inject Authentication Attrs — Use the drop-down list to select attributes to inject when proxying authentication requests to the back-end RADIUS servers. You can also add or edit a RADIUS attribute configuration, or manage your RADIUS attribute configurations. Select **ExtremeGuest** when configuring a Captive Portal that redirects users to ExtremeGuest.

Inject Accounting Attrs — Use the drop-down list to select attributes to inject when proxying accounting requests to the back-end RADIUS servers. You can also add or edit a RADIUS attribute configuration, or manage your RADIUS attribute configurations. Select **ExtremeGuest** when configuring a Captive Portal that redirects users to ExtremeGuest.

LDAP Authentication — If you select LDAP Authentication, specify the LDAP configuration for

this mapping to use.

Local Authentication — If desired, select the option to configure a password for all authentications that match the mapping. This option could be used with MAC authentication where the password is not the MAC address. For example, you can have MAC (PAP) authentication configured for all your switches, with the exception of MAC (MsCHAP) authentication configured for a wireless controller. For the wireless controller, you would add a new AAA mapping with the authentication type set to MAC (MsCHAP), the location set to the wireless controller location group, and the authentication method set to Local Authentication with the password for all authentications set to the static password configured on the wireless controller.

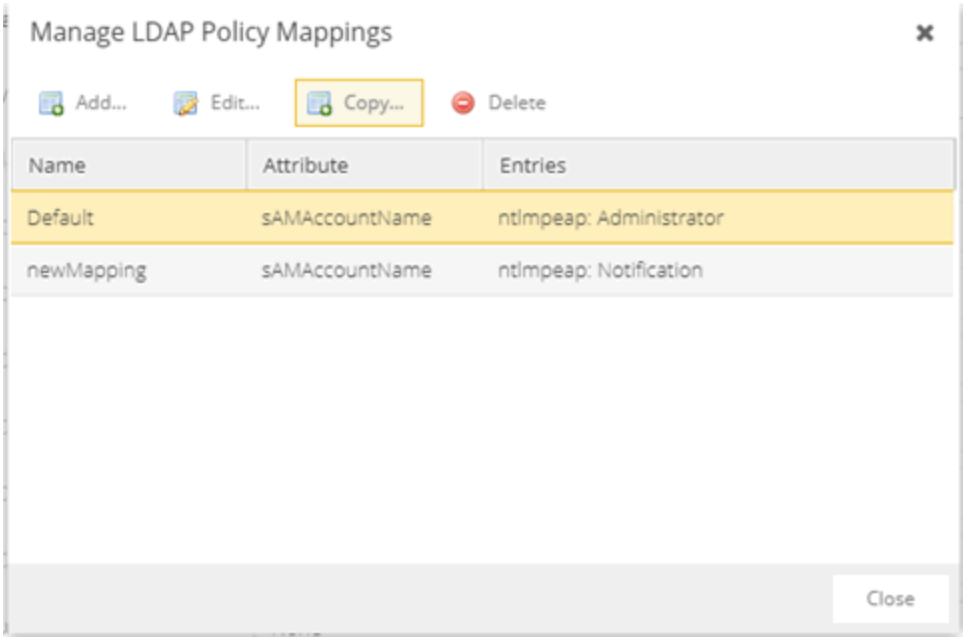
LDAP Configuration

Use the drop-down list to select the LDAP configuration for the LDAP servers on your network that you want to use for this mapping. You can also add or edit an LDAP configuration, or manage your LDAP configurations. You must specify an LDAP configuration if you have selected LDAP Authentication as your authentication method. However, you might also specify an LDAP configuration if you use Proxy RADIUS to a Microsoft NPS server that is running on a domain controller. The domain controller is also an LDAP server that can do RADIUS requests and LDAP requests for users on that server.

LDAP Policy Mapping

Select the LDAP Policy Mapping for this mapping from the drop-down list. If you have selected an LDAP configuration, this option enables you to use a different LDAP policy mapping. This is useful if the LDAP configuration uses user attribute values that overlap with another LDAP configuration. For example, in the case of multiple companies where company A's Sales department uses one policy, but company B's Sales department uses a different policy.

Select Manage from the drop-down list to Add, Edit, Copy, or Delete the LDAP policy mappings for the LDAP configuration:



Fall-through if Authentication Failed

Select the checkbox to authenticate against the next AAA authentication rule in the event the authentication configured as the first AAA authentication rule results in authentication failure or the Directory Service is unreachable. The fall-through functionality only occurs for those rules on which the checkbox is selected and only in the event the first authentication rule fails. When this checkbox is enabled and an authentication rule fails, the Access Control engine continues checking the end-user against the remaining rules until it finds a matching rule. If it does not find a matching rule, authentication continues using the previous authentication response.

NOTE:	When using EAP-TEAP the fall-through option requires the computer authentication as EAP-TLS and the user authentication as MsCHAP to function.

AAA Configurations Panel

The AAA Configurations panel provides a list of your AAA configurations and buttons to add, edit, or delete configurations. AAA configurations define the RADIUS and LDAP configurations that provide the authentication and authorization services to your ExtremeControl engines.

Access the Access Control Configurations panel in the **Control** > **Access Control** tab by expanding the **Access Control Configurations** tree in the left-panel and expanding the AAA Configurations tree. Your configurations are listed within the tree.

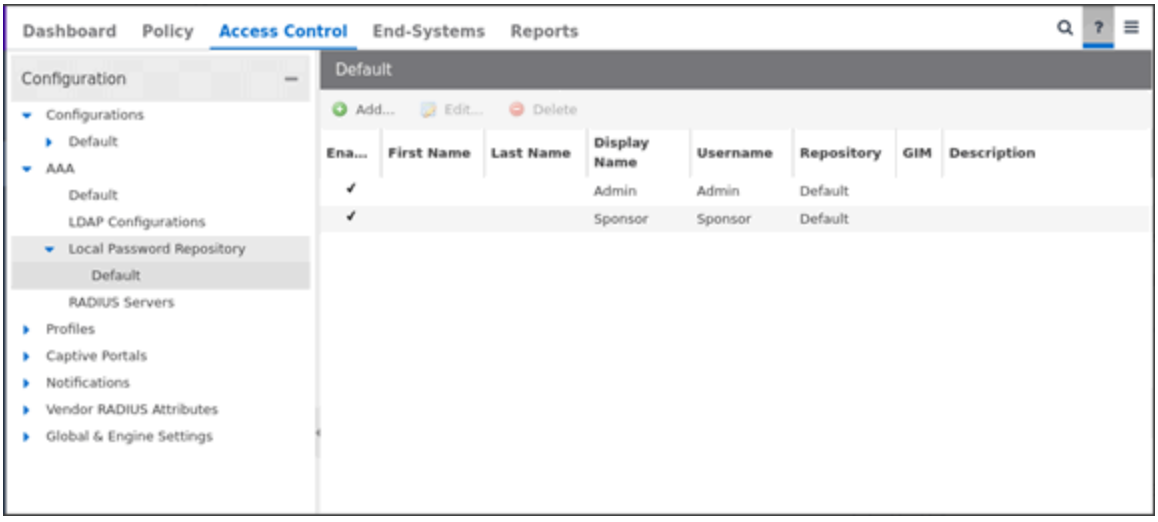
The following configurations are available in the left-panel tree:

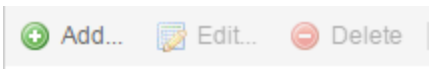
LDAP Configuration

This panel lets you view and define the LDAP configurations used in ExtremeCloud IQ Site Engine. Any changes made are written immediately to the ExtremeCloud IQ Site Engine database. For more information about LDAP Configuration, visit the Manage LDAP Configuration topic.

Local Password Repository

The local password repository specified for this AAA configuration. ExtremeCloud IQ Site Engine supplies a default repository that can be used to define passwords for administrators and sponsors accessing the Registration administration web page and the sponsor administration web page. The default password is Extreme@pp.





Use these buttons to add, edit, or delete local repository in the table. Select the **Add button** to open the Add User window, where you can define a new user and password

for the Repository. Select the **Edit button** to open the Edit User, window where you can edit the selected user entry. Use the **Delete button** to delete the selected user entry. You cannot delete a user that is referenced by an Administrative Login Configuration (as configured in the Edit Portal Configuration Window > Administration).

The following columns are displayed in the default Local Password Repository table:

Enabled
Displays whether the user is enabled or disabled. If a user is disabled, they are not able to log in. This feature is useful if you want to enable a user only at certain times, such as when they are on-site. You can enable or disable a user by editing the user entry (select the entry and select the **Edit** button).

First Name
The user's first name (for administrative information only).

Last Name
The user's last name (for administrative information only).

Display Name
The display name is used on the voucher for pre-registration in the captive portal.

Username
The user's login user name.

Repository
The name of the Local Password Repository of which the user is a member.

GIM
Indicates if the local repository is used by the Guest and IoT Manager (GIM).

Description
A description of the repository.

RADIUS Servers
This panel lets you view and define the RADIUS servers used in ExtremeCloud IQ Site Engine. RADIUS servers can be used in ExtremeCloud IQ Site Engine server authentication configurations and in ExtremeControl AAA configurations. For more information about RADIUS Servers, visit the Manage RADIUS Server topic.

RADSec Certificates
This panel lets you view and define the CA certificates and certificates that the Access Control engine pushes to switches to configure RadSec, and the mappings that determine which CA certificates and certificate each switch receives. For more information about RADSec Certificates, visit the Manage RADSec Certificates topic.

AAA Configurations

The AAA Configuration defines the RADIUS and LDAP configurations that provide the authentication and authorization services to your ExtremeControl engines. A AAA Configuration can be a basic or advanced configuration. Basic AAA Configurations define the authentication and authorization services for all end-systems connecting to your Access Control engines Advanced AAA configurations allow you to define different authentication and authorization services for different end users based on end-system to authentication server mappings.

This Help topic provides the following information for accessing and configuring the AAA Configuration:

- Accessing the AAA Configuration
- Basic AAA Configuration
- Advanced AAA Configuration

NOTE: Users with a AAA configuration using NTLM authentication to a back-end active directory domain whose passwords expire are prompted via windows to change their domain password.

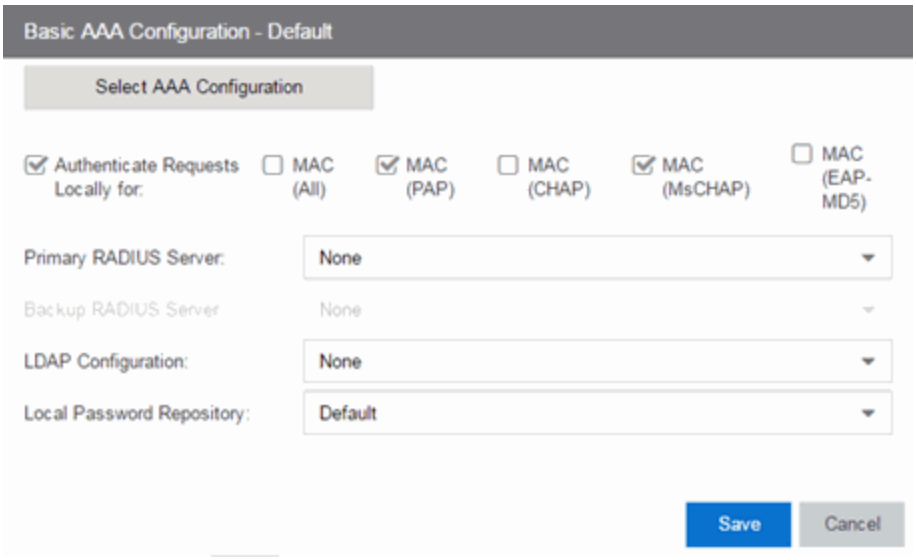
Accessing the AAA Configuration

Use the following steps to edit or change your AAA Configuration.

1. Open the **Control** tab in ExtremeCloud IQ Site Engine.
2. Select the **Access Control** tab.
3. Select **AAA Configurations** within the left-panel tree. The AAA Configuration is displayed in the right panel.
4. Use the fields in the right panel to edit or modify the configuration. See the sections below for a description of each field and option in the panel.
5. Select **Save** to save your changes.

Basic AAA Configuration

Basic AAA Configurations define the RADIUS and LDAP configurations for all end-systems connecting to your ExtremeControl engines.



Authenticate Requests Locally

This option lets you specify that MAC authentication requests are handled locally by the Access Control engine. Select this option if all MAC authentication requests are to be authorized, regardless of the MAC authentication password (except MAC (EAP-MD5) which requires a password that is the MAC address). The Accept policy is applied to end-systems that are authorized locally.

Select one or more MAC authentication types:

- MAC (All) — includes MAC (PAP), MAC (CHAP), MAC (MsCHAP), and MAC (EAP-MD5) authentication types.
- MAC (PAP) — this is the MAC authentication type used by Extreme Networks wired and wireless devices.
- MAC (CHAP)
- MAC (MsCHAP)
- MAC (EAP-MD5) — this MAC authentication type requires a password, which must be the MAC address.

Primary/Backup RADIUS Servers

If your Access Control engines are configured to proxy RADIUS requests to a RADIUS server, use these fields to specify the primary and backup RADIUS servers to use. Use the drop-down list to select a RADIUS server, add or edit a RADIUS server, or manage your RADIUS servers.

LDAP Configuration

Use this field to specify the LDAP configuration for the LDAP server on your network that you want to use in this AAA configuration. Use the drop-down list to select an LDAP configuration, add or edit an LDAP configuration, or manage your LDAP configurations.

Local Password Repository

Use this field to specify the local password repository you want for this AAA configuration. ExtremeCloud IQ Site Engine supplies a default repository to define passwords for administrators and sponsors accessing the Registration administration web page and the sponsor administration web page. The default password is Extreme@pp. Use the drop-down list to select a repository.

Advanced AAA Configuration

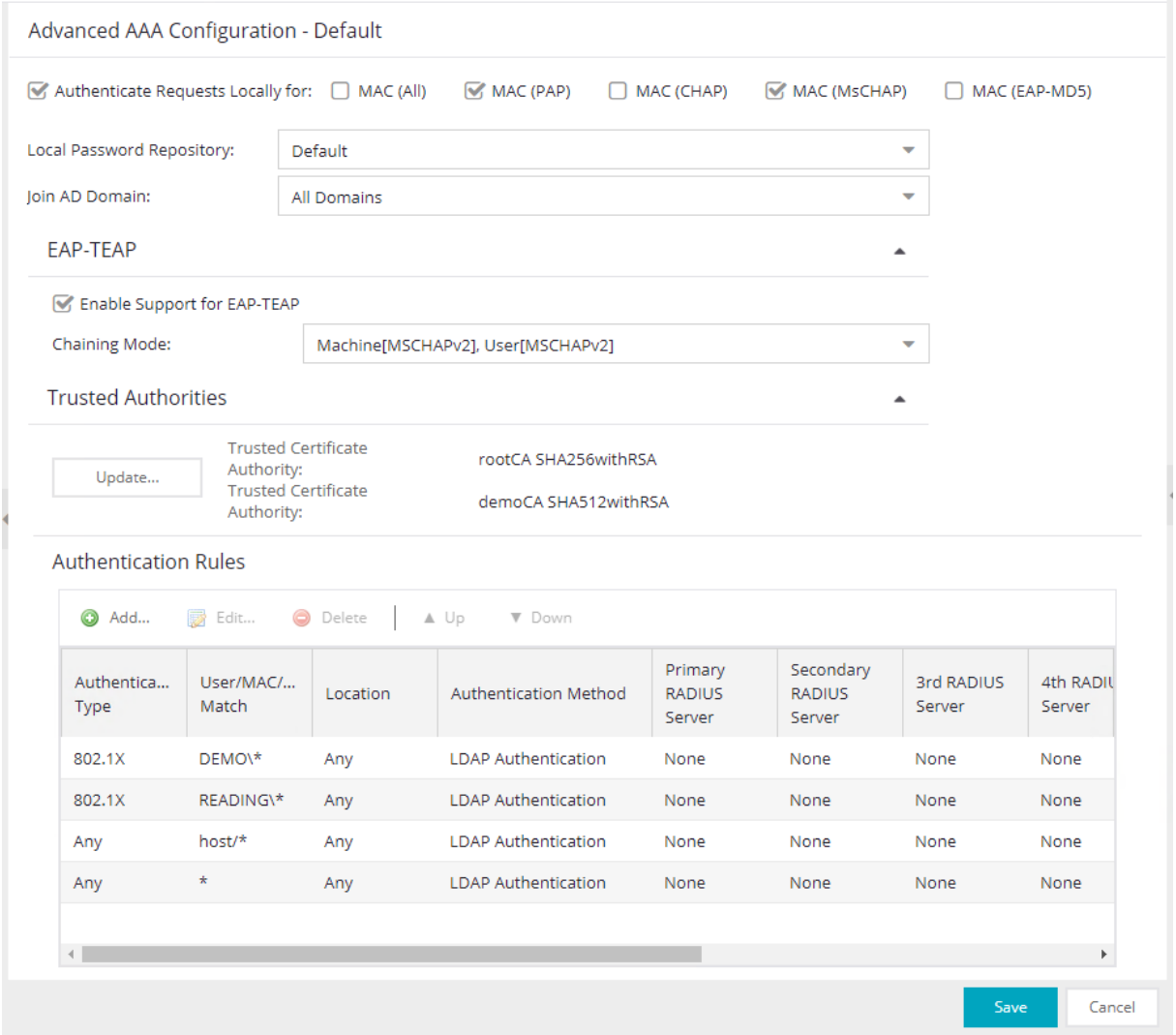
Advanced AAA configurations allow you to define different authentication and authorization services for different end users based on end-system to authentication server mappings. Mappings can be based on:

- authentication type
- username/user group
- MAC address/end-system group
- hostname/hostname group
- location group
- authentication method
- RADIUS user group
- LDAP user group

NOTE: LDAP User Group is only available with an **Authentication Type** of **Registration**.

For example, in a higher education setting, you may want faculty members authenticating to one RADIUS server and students authenticating to another. You can also create mappings specifically for authenticating management login requests, when an administrator logs into a switch's CLI via the console connection, SSH, or Telnet.

Mappings are listed in order of precedence from the top down. If an end-system does not match any of the listed mappings, the RADIUS request is dropped. Because of this, you might want to use the "Any" mapping (created automatically when you add a new advanced AAA configuration) as your last mapping in the list.



Authenticate Requests Locally for

This option lets you specify that MAC authentication requests are handled locally by the ExtremeControl engine. Select this option if all MAC authentication requests are to be authorized, regardless of the MAC authentication password (except MAC (EAP-MD5) which requires a password that is the MAC address). The Accept policy is applied to end-systems authorized locally.

Use the drop-down list to specify a particular type of MAC authentication:

- MAC (All) - includes MAC (PAP), MAC (CHAP), and MAC (EAP-MD5) authentication types.
- MAC (PAP) - this is the MAC authentication type used by Extreme Networks wired and wireless devices.
- MAC (CHAP)

- MAC (MsCHAP)
- MAC (EAP-MD5) - this MAC authentication type requires a password, and the password must be the MAC address.

Local Password Repository

Use this field to specify the local password repository you want for this AAA configuration. ExtremeCloud IQ Site Engine supplies a default repository that can be used to define passwords for administrators and sponsors accessing the Registration administration web page and the sponsor administration web page. The default password is Extreme@pp. Use the drop-down list to select a repository.

Join AD Domain

Use the drop-down list to explicitly select which LDAP configuration of the Active Directory domain the Access Control engine joins in order to authenticate users to all Active Directory domains configured for that engine or select **Auto Detect** to let the Access Control engine determine the domain. Auto Detect starts at the first entry set to LDAP Authentication in the table and attempt to join that domain. If it cannot join that domain, it goes to the next entry set to LDAP Authentication and attempt to join that domain, and so on until one succeeds.

You can also join multiple Active Directory domains by selecting **All Domains** and configuring multiple authentication rules with an **Authentication Method** of **LDAP Authentication** in the **Advanced AAA Configuration** tab.

NOTE: There are configuration considerations when joining multiple Active Directory Domains.

RadSec

Enable RadSec (RADIUS over TLS) Server

Use the **Enable RadSec (RADIUS over TLS) Server** option to specify whether the Access Control engine accepts RADIUS over TCP (secured by TLS) connections from network devices, in addition to RADIUS over UDP connections. Authentication rules, policy assignment, and end-system group logic apply to RadSec connections in the same way as they apply to RADIUS over UDP connections. RadSec connections always use TCP port 2083. You cannot configure the port.

NOTE: RadSec uses the RADIUS Server Certificate that you configure for the Access Control engine. A separate RadSec certificate is not required. For the Access Control engine to accept the RadSec connection, the Access Control engine must trust the certificate. To establish trust, add the CA that signed the certificate to the Trusted Authorities of the AAA configuration. The switch must also trust the CA that issued the RADIUS Server Certificate. Add the CA that issued the RADIUS Server Certificate to the RADSec Client CA Certificate table and assign the CA to the switch. You cannot use self-signed certificates, including the default RADIUS Server Certificate, to secure RadSec communication. Use a RADIUS Server Certificate that your CA issues. For more information, see Manage Certificates.

EAP-TEAP

Enable Support for EAP-TEAP
Use this option to enable or disable support for the standard-based chaining protocol EAP-TEAP.

Chaining Mode
Use the drop-down list to specify what method to use for Machine authentication and for User authentication. Machine authentication must be first (primary) and User authentication must follow (secondary):

- Machine[MSCHAPv2], User[MSCHAPv2] -The primary authentication uses MSCHAPv2 to authenticate the computer. The secondary authentication uses MSCHAPv2 to authenticate the user.
- Machine[MSCHAPv2], User[TLS] -The primary authentication uses MSCHAPv2 to authenticate the computer. The secondary authentication uses TLS to authenticate the user.
- Machine[TLS], User[MSCHAPv2] -The primary authentication uses TLS to authenticate the computer. The secondary authentication uses MSCHAPv2 to authenticate the user.
- Machine[TLS], User[TLS] -The primary authentication uses TLS to authenticate the computer. The secondary authentication uses TLS to authenticate the user.

NOTE: Machine-only TEAP authentication is supported, allowing authentication to succeed when machine authentication passes, but no user identity is provided.

Logging records the final authentication outcome (for example, **MACHINE_AUTH_PASSED, USER_AUTH_FAILED**) for troubleshooting and NAC processing visibility.

Trusted Authorities
Configure the AAA Trusted Certificate Authorities to designate which client certificates can be trusted. For more information see,
Use the **Update...** button to update the AAA trusted Certificate Authorities for your AAA configuration:

- Provide one or more CA certificates for Certificate Authorities that are trusted to issue client certificates for 802.1X authentication. Client certificate issued by an untrusted Certificate Authority are not accepted and the authentication session will be rejected.
- Optionally, provide one or more URLs for Certificate Revocation Lists (CRLs), or Online Certificate Status Protocol (OCSP) configuration to check for revoked certificates. You must provide one for every used Certificate Authority, or none.

  CRL
  Use this option to define the URLs where the Certificate Revocation List can be downloaded.

  Allow expired CRLs to be used when checking CRLs - Defines the system behavior if the CRL is expired.

  Allow CRLs to be missed when checking CRLs - Defines the system behavior if the CRL is missing.

  OCSP
  Use this option to configure the Online Certificate Status Protocol to check for revoked certificates. Access Control Engine validates the client certificate during authentication by sending requests to the OCSP responder. The OCSP responder URL can be configured manually or obtained from the client certificate.

  Always Override Certificate URL with Default Responder URL - Defines if the OCSP Responder URL is used regardless of the potential URL in the certificate.

  Default Responder URL - Defines that the Default Responder URL is used if the certificate does not contain the URL, or the Always Override Certificate URL with Default Responder URL is checked.

  Secondary Responder URL - If defined, the Access Control Engine periodically checks the reachability of the Default responder. The Secondary responder is used If the Default responder is not reachable. Once the Default responder is back in service and reachable, the Default responder is used again. OCSP Responder Health Check is configured in **Access Control > Configuration > Global & Engine Settings > Engine Settings > Miscellaneous**.

  Responder URL Timeout - Defines the timeout for the Responder URL, in seconds.

  Verify Nonces Uniqueness - Defines if the nonce value must be unique.

  Continue Processing Requests After Responder Error - Defines the system

behavior if a responder error occurs. If checked and the responder returns an error the authentication continues to be processed. If unchecked and the responder returns an error the authentication is rejected.

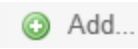
Authentication Rules

This table lists mappings between groups of users and authentication configurations. The table displays the username to match along with the defined configuration parameters for that mapping. Mappings are listed in order of precedence from the top down. If an end-system does not match any of the listed mappings, the RADIUS request is dropped. Because of this, you might want to use an "Any" mapping as your last mapping in the list. Use the Mappings toolbar buttons to perform actions on the mappings.



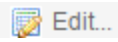
Move Mappings Up/Down

Move mappings up and down in the list to determine mapping precedence. Mappings are listed in order of precedence from the top down.



Add New Mapping

Opens the Add User to Authentication Mapping window where you can define a new mapping.



Edit Mapping

Opens the Edit User to Authentication Mapping window where you can edit the selected mapping.



Delete Selected Mappings

Deletes any mappings selected in the table.

AAA Configurations Panel

The AAA Configurations panel provides a list of your AAA configurations and buttons to add, edit, or delete configurations. AAA configurations define the RADIUS and LDAP configurations that provide the authentication and authorization services to your ExtremeControl engines.

Access the Access Control Configurations panel in the **Control** > **Access Control** tab by expanding the **Access Control Configurations** tree in the left-panel and expanding the AAA Configurations tree. Your configurations are listed within the tree.

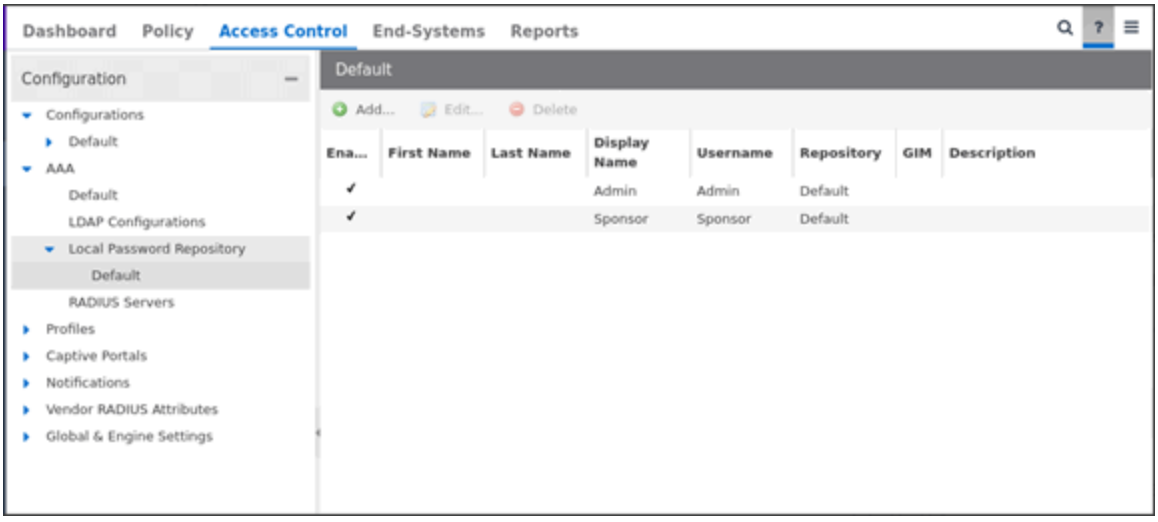
The following configurations are available in the left-panel tree:

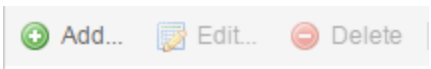
LDAP Configuration

This panel lets you view and define the LDAP configurations used in ExtremeCloud IQ Site Engine. Any changes made are written immediately to the ExtremeCloud IQ Site Engine database. For more information about LDAP Configuration, visit the Manage LDAP Configuration topic.

Local Password Repository

The local password repository specified for this AAA configuration. ExtremeCloud IQ Site Engine supplies a default repository that can be used to define passwords for administrators and sponsors accessing the Registration administration web page and the sponsor administration web page. The default password is Extreme@pp.





Use these buttons to add, edit, or delete local repository in the table. Select the **Add button** to open the Add User window, where you can define a new user and password

for the Repository. Select the **Edit button** to open the Edit User, window where you can edit the selected user entry. Use the **Delete button** to delete the selected user entry. You cannot delete a user that is referenced by an Administrative Login Configuration (as configured in the Edit Portal Configuration Window > Administration).

The following columns are displayed in the default Local Password Repository table:

Enabled
Displays whether the user is enabled or disabled. If a user is disabled, they are not able to log in. This feature is useful if you want to enable a user only at certain times, such as when they are on-site. You can enable or disable a user by editing the user entry (select the entry and select the **Edit** button).

First Name
The user's first name (for administrative information only).

Last Name
The user's last name (for administrative information only).

Display Name
The display name is used on the voucher for pre-registration in the captive portal.

Username
The user's login user name.

Repository
The name of the Local Password Repository of which the user is a member.

GIM
Indicates if the local repository is used by the Guest and IoT Manager (GIM).

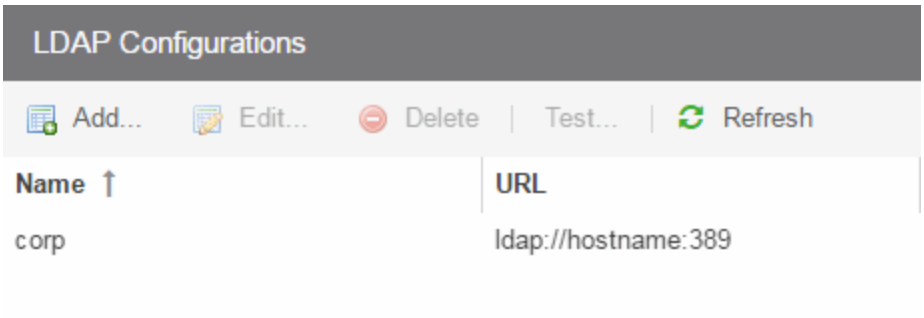
Description
A description of the repository.

RADIUS Servers
This panel lets you view and define the RADIUS servers used in ExtremeCloud IQ Site Engine. RADIUS servers can be used in ExtremeCloud IQ Site Engine server authentication configurations and in ExtremeControl AAA configurations. For more information about RADIUS Servers, visit the Manage RADIUS Server topic.

RADSec Certificates
This panel lets you view and define the CA certificates and certificates that the Access Control engine pushes to switches to configure RadSec, and the mappings that determine which CA certificates and certificate each switch receives. For more information about RADSec Certificates, visit the Manage RADSec Certificates topic.

Manage LDAP Configurations

This panel lets you view and define the LDAP configurations used in ExtremeCloud IQ Site Engine. You can access this panel by selecting LDAP Configurations from the left-panel in the Access Control Configurations > AAA Configurations tree or from AAA Configuration, by selecting the drop-down list in the LDAP Configuration field. Any changes made are written immediately to the ExtremeCloud IQ Site Engine database.



LDAP Configurations Table

The name of the configuration and the LDAP server connection URLs specified for that configuration.

Test Configuration Button

Use this button to run a connection test for the selected configuration. The connection to the LDAP server is tested and a report on connection test results is provided. There is also a user search that lets you search on a user entry value and display the attributes associated with the user.

Add Configuration Button

Opens the Add LDAP Configuration window where you can define a new LDAP configuration.

Edit Configuration Button

Opens the Edit LDAP Configuration window where you can edit the selected LDAP configuration.

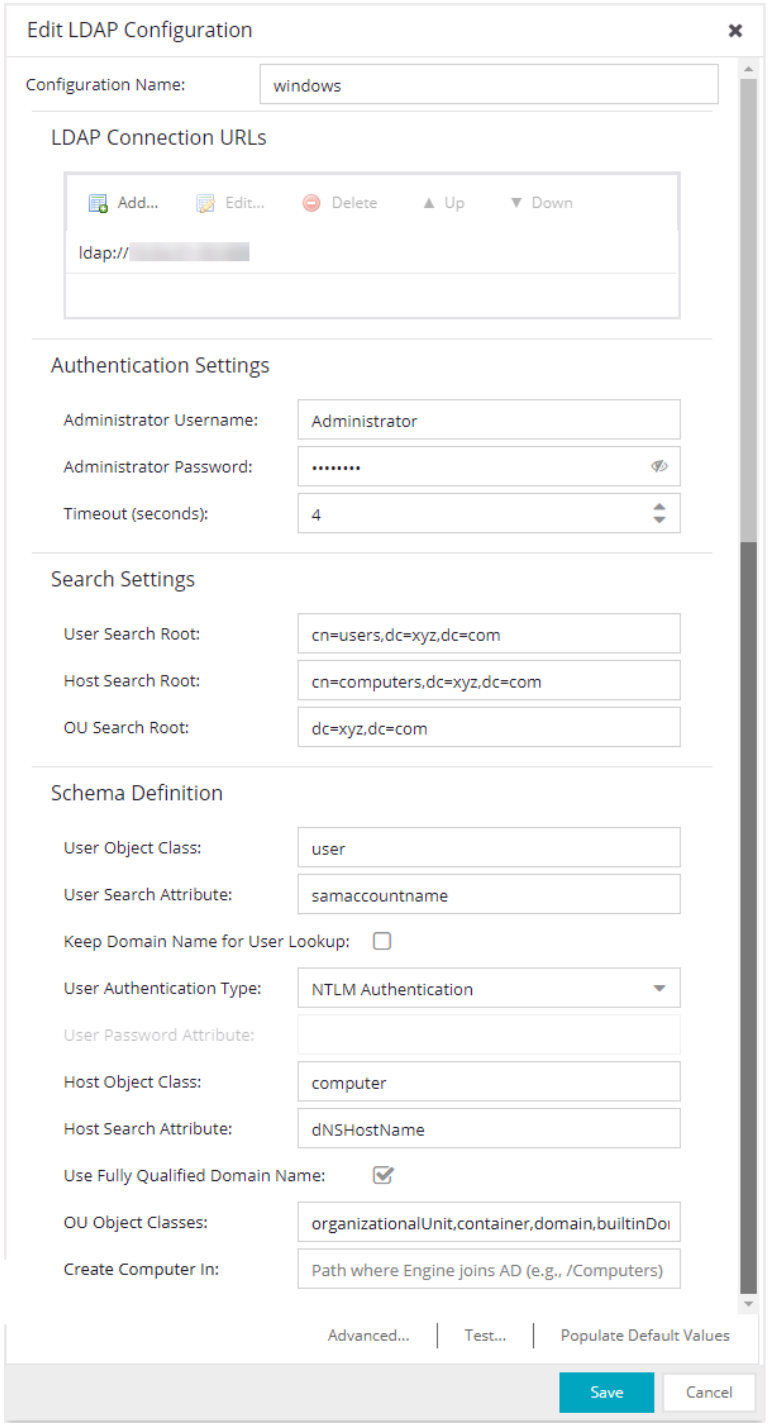
Delete Configuration Button

Deletes the selected LDAP configuration(s).

Add LDAP Configuration

Use the Add LDAP Configuration window to configure the LDAP servers on your network. You can access this window from the **Control > Access Control** tab. Expand the **Configuration > Configurations > AAA > LDAP Configurations** folder in the right panel and select **Add**. You can also access this window from the Manage LDAP Configurations tab. Any changes made in this window are written immediately to the ExtremeCloud IQ Site Engine database.

NOTE:	If you are using LDAPS, your ExtremeCloud IQ Site Engine/ExtremeControl environment must be configured to accept the new LDAPS server certificate. For information, see Server Certificate Trust Mode in the Secure Communications Help topic.



Configuration Name

Enter a name for the LDAP configuration.

LDAP Connection URLs

Use this table to add, edit, or delete connection URLs for the LDAP server and any backup servers you have configured. (The backup servers are redundant servers containing the same directory information.) Use the Up and Down arrows to arrange the order that the URLs are listed.

The format for the connection URL is`ldap://host:port`where host equals hostname or IP address, and the default port is 389. For example, `ldap://10.20.30.40:389`. If you are using a secure connection, the format is `ldaps://host:port`and the default port is 636. For example, `ldaps://10.20.30.40:636`. If you are using LDAPS, yourExtremeCloud IQ Site Engine/Access Control environment must be configured to accept the new LDAPS server certificate. For information, see Server Certificate Trust Mode in the Secure Communications Help topic.

If you are creating an LDAP configuration for Novell eDirectory, be aware that the eDirectory may require that the universal password lookup be done using LDAPS. If you configure the URL for LDAP only, the lookup may fail.

Authentication Settings

Enter the Administrator Username and Administrator Password for the Active Directory. These credentials are used for queries if the Read Only Username and Read Only Password are not provided. The Administrator credentials only need to provide read access to the LDAP server. The timeout field lets you specify a timeout value in seconds for the LDAP server connection.

Search Settings

For the three fields, enter the root node of the LDAP server. To improve search performance, you can specify a sub tree node to confine the search to a specific section of the directory. The search root format should be a DN (Distinguished Name). If Nested Group Search is enabled, then groups are processed recursively which can impact the authorization delay.

Schema Definition

Provide information that describes how entries are organized in the LDAP server.

Schema Definition fields:

- **User Object Class**- enter the name of the class used for users.
- **User Search Attribute**- enter the name of the attribute in the user object class that contains the user's login ID.
- **Keep Domain Name for User Lookup**- If selected, this option will allow the full username to be used when looking up the user in LDAP. For example, you should select this option when using the User Search Attribute: userPrincipalName.

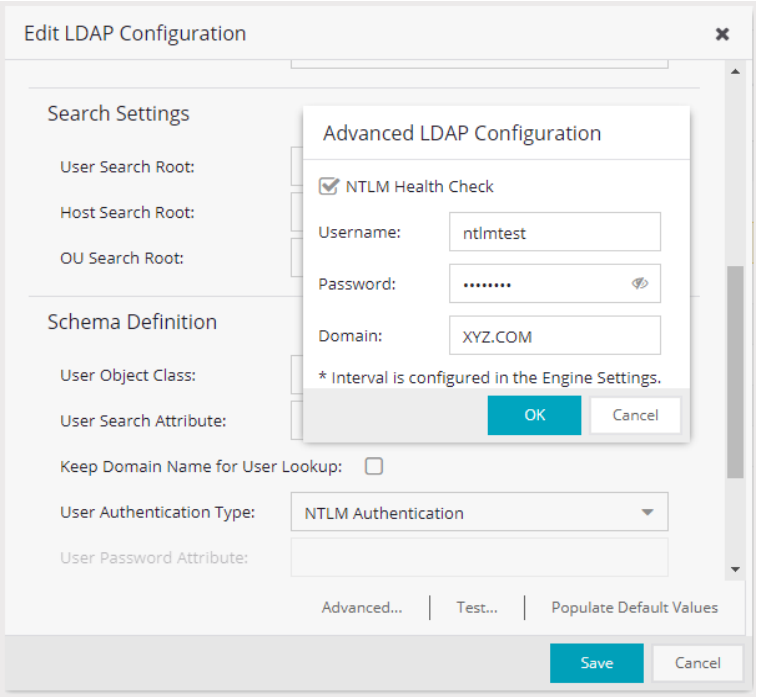
  If the option is not selected, the domain name will be stripped off the username prior to performing the lookup. For example, you should deselect this option when using the User

Search Attribute: sAMAccountName. Two examples of the domain name being stripped off would be:
user@domain.com -> user
DOMAIN\user -> user

- **User Authentication Type**- Specify how the user is authenticated. There are 4 options:
  - LDAP Bind– This is the easiest option to configure, but only works with a plain text password. It is useful for authentication from the captive portal but does not work with most 802.1x authentication types.
  - NTLM Authentication– This option is only useful when the backend LDAP server is really a Microsoft Active Directory server. This is an extension to LDAP bind that uses ntlm_auth to verify the NT hash challenge responses from a client in MsCHAP, MsCHAPV2, and PEAP requests. If you want to run a NTLM Health Check, see NTLM Health Check and Advanced for the additional configuration steps.
  - NT Hash Password Lookup– If the LDAP server has the user's password stored as an NT hash that is readable by another system, you can have Access Control read the hash from the LDAP server to verify the hashes within an MsCHAP, MsCHAPV2, and PEAP request.
  - Plain Text Password Lookup– If the LDAP server has the user's password stored unencrypted and that attribute is accessible to be read via an LDAP request, then this option reads the user's password from the server at the time of authentication. This option can be used with any authentication type that requires a password.
- **User Password Attribute**- This is the name of the password used with the NT Hash Password Lookup and Plain Text Password Lookup listed above.
- **Host Object Class**- enter the name of the class used for hostname.
- **Host Search Attribute**- enter the name of the attribute in the host object class that contains the hostname.
- **Use Fully Qualified Domain Name**checkbox - use this checkbox to specify if you want to use the Fully Qualified Domain Name (FQDN) or just hostname without domain.
- **OU Object Classes**- the names of the classes used for organizational units.
- **Create Computer In** - the path in the Active Directory where Access Control Engines will be created (OU where Access Control Engines join the domain). The default value is empty. It translates to /Computers in the common AD.

Advanced

Advanced LDAP Configurationis only accessible when **User Authentication Type** is set to **NTLM Authentication**.The LDAP configuration information you enter here specifies a user account and domain to the user for the NTLM Health Check. To configure the Health Check tests:



1. Configure the interval and timeout for the test. See NTLM Health Check.
2. Select **NTLM Health Check**.
3. Enter the **Username**, **Password**, and the**Domain** to use for the health check tests.
4. Select **OK**.

The Access Control Engine expects a positive response from the domain controller for the health check authentication. If timeout happens or a negative response is received, the failover occurs and the **Access Control Lost Partial Contact with LDAP Service** alarm is generated.

WARNING:

- You should only use the health check in an environment where you have multiple domain controllers deployed.
- The health check should only be enabled if you have experienced this issue.
- The Domain password policy requirement for periodic password check should be disabled for the health check account. The credentials used by the health check should always be working.

Test Button

The connection to the LDAP server is tested and a report on connection test results is provided. There is also a user/host search that lets you search on a user entry or host entry value and display the attributes associated with those values.

Populate Default Values Button

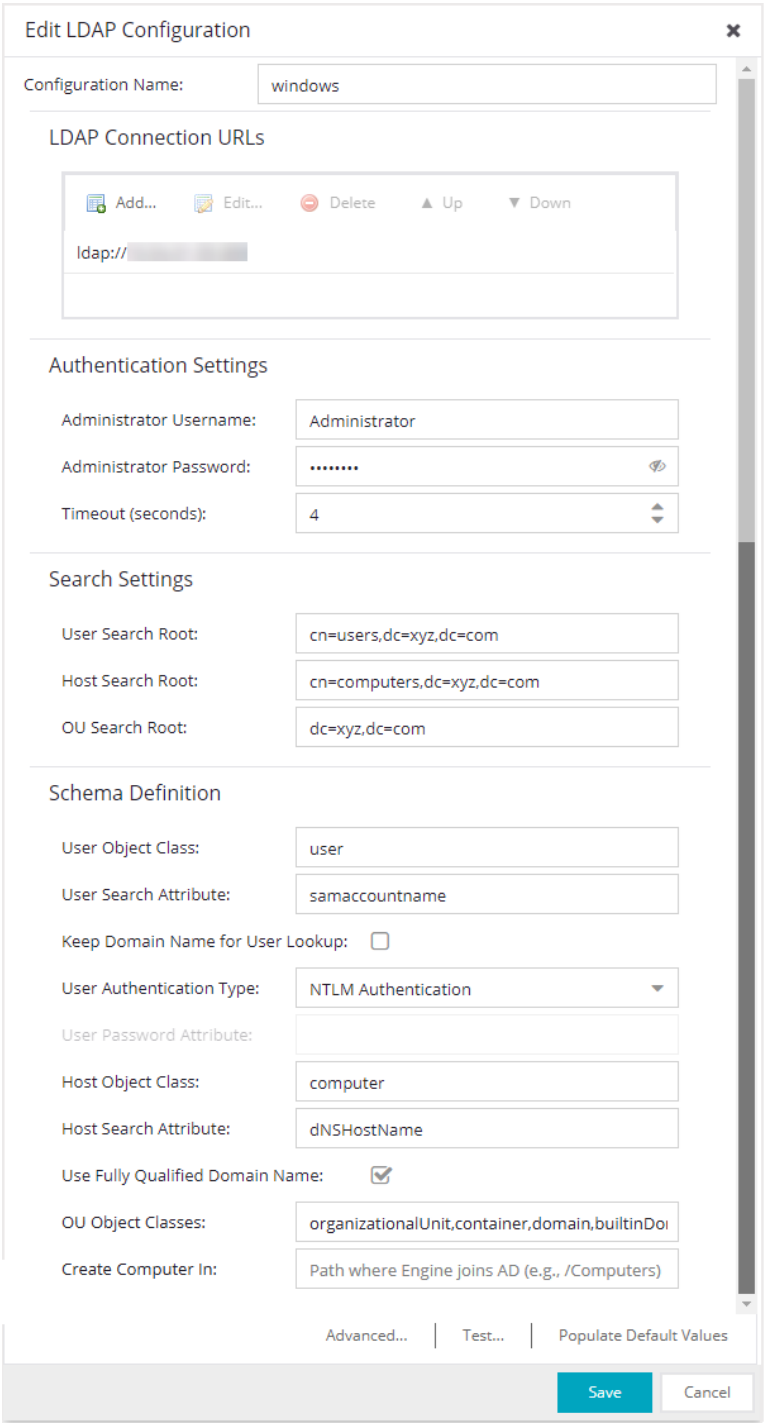
Select from the defaults available from the menu:

- **Active Directory: User Defaults**- Settings that allow user authentication when Access Control is set to proxy to LDAP and the server is an Active Directory machine.
- **Active Directory: Machine Defaults**- Settings that allow machine authentication when Access Control is set to proxy to LDAP and the server is an Active Directory machine.
- **Open LDAP Defaults -**Settings that allow Access Control to verify the user's password via an OpenLDAP server. See the NAC Manager How to Configure PEAP Authentication via OpenLDAP Help topic for information.
- **Novell eDirectory Defaults**- Settings that allow Access Control to read the universal password from Novell eDirectory. You must configure eDirectory to allow that password to be read. See the NAC Manager How to Configure PEAP Authentication via eDirectory help topic for information.

Edit LDAP Configuration

Use the Edit LDAP Configuration window to configure the LDAP servers on your network. You can access this window from the **Users** tab in the Authorization/Device Access tool, or in NAC Manager from the AAA Configuration window, by selecting an LDAP configuration from the drop-down list in the LDAP Configuration field. Any changes made in this window are written immediately to the ExtremeCloud IQ Site Engine database.

NOTE:	If you are using LDAPS, your ExtremeCloud IQ Site Engine/ExtremeControl environment must be configured to accept the new LDAPS server certificate. For information, see Server Certificate Trust Mode in the Secure Communications Help topic.



Configuration Name

The name for the LDAP configuration you defined.

LDAP Connection URLs

Use this table to add, edit, or delete connection URLs for the LDAP server and any backup servers you have configured. (The backup servers are redundant servers containing the same directory information.) Use the Up and Down arrows to arrange the order that the URLs are listed.

The format for the connection URL is `ldap://host:port` where host equals hostname or IP address, and the default port is 389. For example, `ldap://10.20.30.40:389`. If you are using a secure connection, the format is `ldaps://host:port` and the default port is 636. For example, `ldaps://10.20.30.40:636`. If you are using LDAPS, your ExtremeCloud IQ Site Engine/Access Control environment must be configured to accept the new LDAPS server certificate. For information, see Server Certificate Trust Mode in the Secure Communications Help topic.

If you are creating an LDAP configuration for Novell eDirectory, be aware that the eDirectory may require that the universal password lookup be done using LDAPS. If you configure the URL for LDAP only, the lookup may fail.

Authentication Settings

Enter the Administrator Username and Administrator Password for the Active Directory. These credentials are used for queries if the Read Only Username and Read Only Password are not provided. The Administrator credentials only need to provide read access to the LDAP server. The timeout field lets you specify a timeout value in seconds for the LDAP server connection.

Search Settings

For the three fields, enter the root node of the LDAP server. To improve search performance, you can specify a sub tree node to confine the search to a specific section of the directory. The search root format should be a DN (Distinguished Name). If Nested Group Search is enabled, then groups are processed recursively which can impact the authorization delay.

Schema Definition

Provide information that describes how entries are organized in the LDAP server.

Schema Definition fields:

- **User Object Class** - enter the name of the class used for users.
- **User Search Attribute** - enter the name of the attribute in the user object class that contains the user's login ID.
- **Keep Domain Name for User Lookup** - If selected, this option will allow the full username to be used when looking up the user in LDAP. For example, you should select this option when using the User Search Attribute: userPrincipalName.

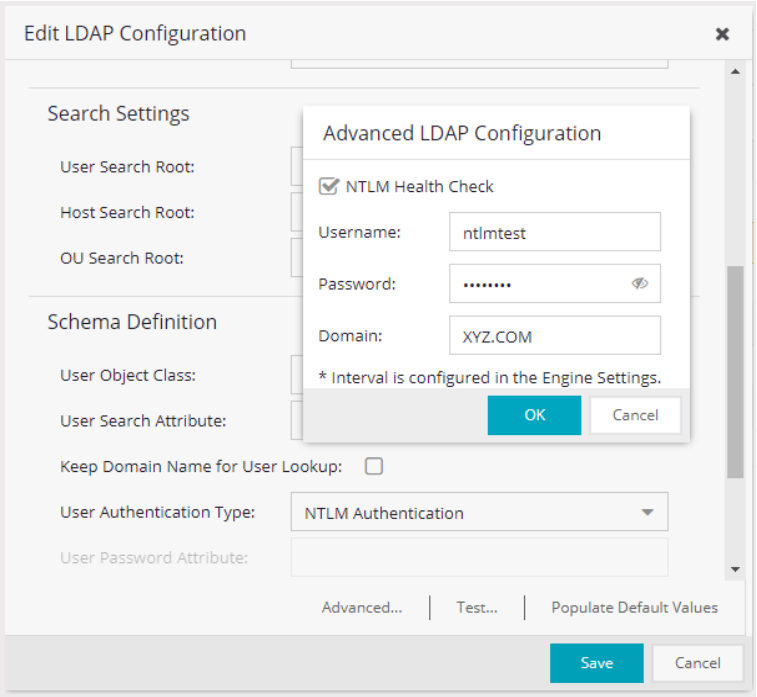
  If the option is not selected, the domain name will be stripped off the username prior to performing the lookup. For example, you should deselect this option when using the User Search Attribute: sAMAccountName. Two examples of the domain name being stripped

off would be:
user@domain.com -> user
DOMAIN\user -> user

- **User Authentication Type** - Specify how the user is authenticated. There are 4 options:
    - LDAP Bind – This is the easiest option to configure, but only works with a plain text password. It is useful for authentication from the captive portal but does not work with most 802.1x authentication types.
    - NTLM Auth – This option is only useful when the backend LDAP server is really a Microsoft Active Directory server. This is an extension to LDAP bind that uses ntlm_ auth to verify the NT hash challenge responses from a client in MsCHAP, MsCHAPV2, and PEAP requests.
    - NT Hash Password Lookup – If the LDAP server has the user's password stored as an NT hash that is readable by another system, you can have Access Control read the hash from the LDAP server to verify the hashes within an MsCHAP, MsCHAPV2, and PEAP request.
    - Plain Text Password Lookup – If the LDAP server has the user's password stored unencrypted and that attribute is accessible to be read via an LDAP request, then this option reads the user's password from the server at the time of authentication. This option can be used with any authentication type that requires a password.
- **User Password Attribute** - the name of the password used with the NT Hash Password Lookup and Plain Text Password Lookup listed above.
- **Host Object Class** - enter the name of the class used for hostname.
- **Host Search Attribute** - enter the name of the attribute in the host object class that contains the hostname.
- **Use Fully Qualified Domain Name** checkbox - use this checkbox to specify if you want to use the Fully Qualified Domain Name (FQDN) or just hostname without domain.
- **OU Object Classes** - the names of the classes used for organizational units.
- **Create Computer In** - the path in the Active Directory where Access Control Engines will be created (OU where Access Control Engines join the domain). The default value is empty. It translates to /Computers in the common AD.

Advanced

Advanced LDAP Configurationis only accessible when **User Authentication Type** is set to **NTLM Authentication**.The LDAP configuration information you enter here specifies a user account and domain to the user for the NTLM Health Check. To configure the Health Check tests:



1. Configure the interval and timeout for the test. See NTLM Health Check.
2. Select **NTLM Health Check**.
3. Enter the **Username**, **Password**, and the**Domain** to use for the health check tests.
4. Select **OK**.

The Access Control Engine expects a positive response from the domain controller for the health check authentication. If timeout happens or a negative response is received, the failover occurs and the **Access Control Lost Partial Contact with LDAP Service** alarm is generated.

WARNING:

- You should only use the health check in an environment where you have multiple domain controllers deployed.
- The health check should only be enabled if you have experienced this issue.
- The Domain password policy requirement for periodic password check should be disabled for the health check account. The credentials used by the health check should always be working.

Test

The connection to the LDAP server is tested and a report on connection test results is provided. There is also a user/host search that lets you search on a user entry or host entry value and display the attributes associated with those values.

Populate Default Values

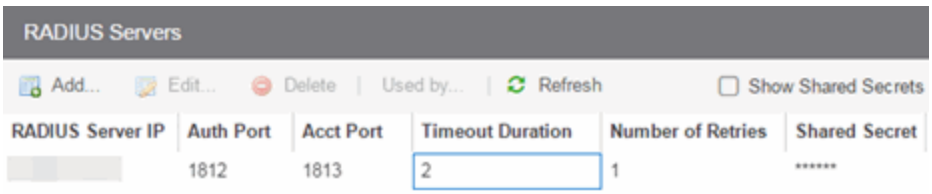
Select from the defaults available from the drop-down list:

- **Active Directory: User Defaults** - Settings that allow user authentication when Access Control is set to proxy to LDAP and the server is an Active Directory machine.
- **Active Directory: Machine Defaults** - Settings that allow machine authentication when Access Control is set to proxy to LDAP and the server is an Active Directory machine.
- **OpenLDAP Defaults -** Settings that allow Access Control to verify the user's password via an OpenLDAP server. See the NAC Manager How to Configure PEAP Authentication via OpenLDAP Help topic for information.
- **Novell eDirectory Defaults** - Settings that allow Access Control to read the universal password from Novell eDirectory. You must configure eDirectory to allow that password to be read. See the NAC Manager How to Configure PEAP Authentication via eDirectory Help topic for information.

Manage RADIUS Servers

This panel lets you view and define the RADIUS servers used in ExtremeCloud IQ Site Engine. RADIUS servers can be used in ExtremeCloud IQ Site Engine server authentication configurations and in ExtremeControl AAA configurations.

You can access this panel by selecting RADIUS Servers from the Access Control Configurations > AAA Configurations > RADIUS Servers in the left-panel tree, or from the Configure Device window or AAA Configuration window. Any changes made are written immediately to the ExtremeCloud IQ Site Engine database.



RADIUS Server IP

The IP address of the RADIUS server.

Auth Port

The UDP port number (1-65535) on the RADIUS server to which the ExtremeCloud IQ Site Engine server or Access Control engine sends authentication requests; 1812 is the default port number.

NOTE: If you are enforcing to an ExtremeControl engine for an Extreme Management Center version prior to Version 8.5, you must use different ports to configure UDP Auth. and Accounting. UDP will not function if the Auth and Accounting are configured for the same port for previous versions of ExtremeCloud IQ Site Engine.

The TCP port number (1-65535) on the RADIUS server that the ExtremeCloud IQ Site Engine server or Access Controlengine sends authentication requests to; 1812 is the default port number.

The TLS port number (1-65535) on the RADIUS server that the ExtremeCloud IQ Site Engine server or Access Controlengine sends authentication requests to; 2083 is the default port number.

NOTE: For versions prior to ExtremeCloud IQ Site Engine Version 8.5, TCP and TLS settings are not supported and cannot be enforced to ExtremeControl engines.

Acct Port

The UDP port number (1-65535) on the RADIUS server to which the Access Control engine sends accounting requests; 1813 is the default port number.

NOTE: If you are enforcing to an ExtremeControl engine for an Extreme Management Center version prior to Version 8.5, you must use different ports to configure UDP Auth. and Accounting. UDP will not function if the Auth and Accounting are configured for the same port for previous versions of ExtremeCloud IQ Site Engine.

The TCP port number (1-65535) on the RADIUS server that the Access Control engine sends accounting requests to; 1813 is the default port number.

The TLS port number (1-65535) on the RADIUS server that the Access Control engine sends accounting requests to; 2083 is the default port number.

NOTE: For versions prior to ExtremeCloud IQ Site Engine Version 8.5, TCP and TLS settings are not supported and cannot be enforced to ExtremeControl engines.

Timeout Duration

The amount of time, in seconds, the ExtremeCloud IQ Site Engine server or Access Control engine waits for the RADIUS server to respond to an authentication or accounting request. Valid values are 2-60 seconds.

Number of Retries

The number of times the ExtremeCloud IQ Site Engine server or Access Control engine resends an authentication or accounting request if the RADIUS server does not respond. Valid values are 0-20.

Shared Secret

The shared secret used to encrypt and decrypt communication between the ExtremeCloud IQ Site Engine server or Access Control engine and the RADIUS server. In Access Control, this is also the shared secret used between the switch and the RADIUS server if the Access Control engine is bypassed or if you configured the Management RADIUS Server options when you added the switch.

Show Shared Secrets

When checked, the shared secrets are shown in text. When unchecked, the shared secrets are shown as a string of asterisks.

Used By Button

This button is only available when the panel is launched from Access Control. Opens the RADIUS Server(s) Used By window which shows where the selected servers are in use by AAA configurations.

Add Button

Opens the Add RADIUS Server window where you can define a new RADIUS server.

Edit Button

Opens the Edit RADIUS Server window where you can edit the values for the selected RADIUS server.

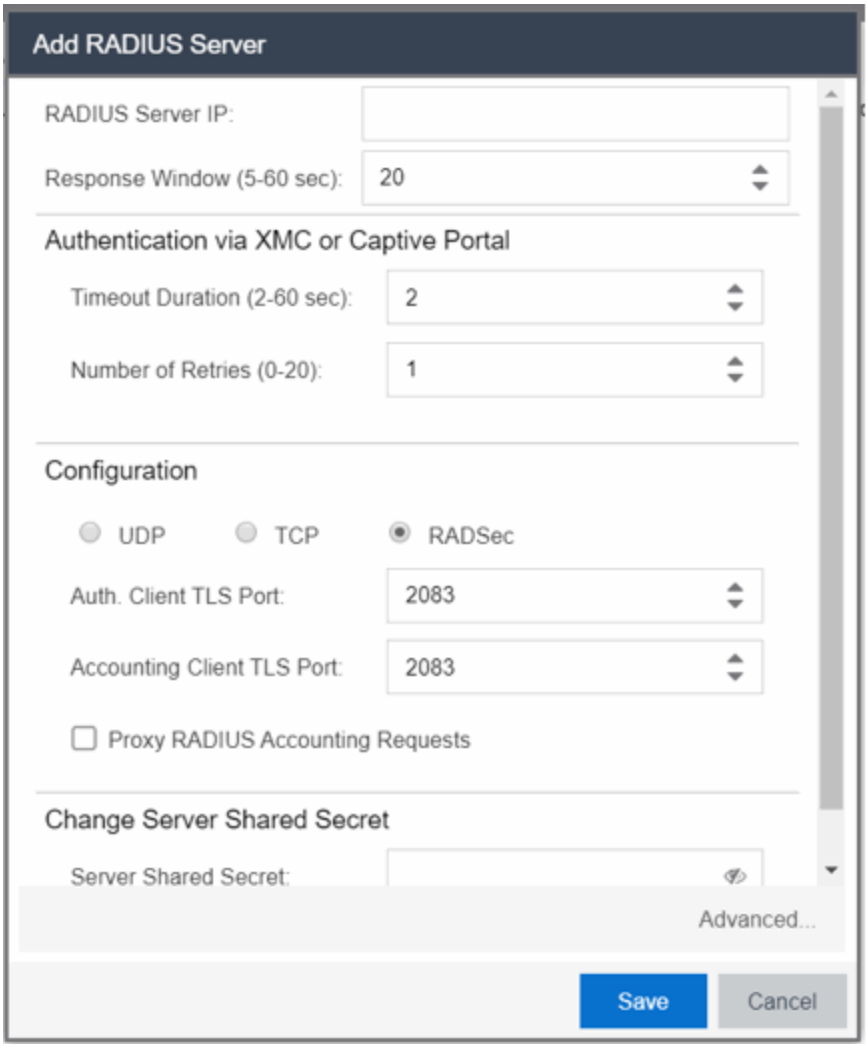
Delete Button

Deletes the selected RADIUS server. You cannot delete servers currently in use.

Add/Edit RADIUS Server

Use the Add/Edit RADIUS Server window to configure the RADIUS servers used in your ExtremeCloud IQ Site Engine applications. RADIUS servers can be used in ExtremeCloud IQ Site Engine server authentication configurations and in ExtremeControl AAA configurations.

You can access this window from the Manage RADIUS Servers window. Any changes made in this window are written immediately to the ExtremeCloud IQ Site Engine database.



RADIUS Server IP

The IP address of the RADIUS server.

Response Window

This setting is used by Access Control when proxying a RADIUS request to a backend RADIUS server. Access Control keeps a status on all backend RADIUS servers instead of going to the

primary RADIUS server for every request. If a RADIUS server does not respond in the amount of time specified here, that server is marked as down until it can be verified as being up. See the Health Check section of the Advanced RADIUS Server Configuration window for information on how Access Control determines the health of a RADIUS server.

Authentication Via ExtremeCloud IQ Site Engine or Captive Portal

Timeout Duration

The amount of time in seconds the ExtremeCloud IQ Site Engine server or Access Control waits for the RADIUS server to respond to an authentication or accounting request. Valid values are 2-60 seconds. This setting is only used for logging into ExtremeCloud IQ Site Engine via RADIUS or logging into the Access Control Captive Portal via RADIUS.

NOTE: The Access Control engine times out a RADIUS server if it takes more than "(retries +1) * timeout" or 20 seconds, whichever is greater, for the server to respond. For example, if the number of retries is set to 1 and the timeout duration is set to 2 (the default values), then the engine times out a RADIUS server if it takes longer than 20 seconds to respond, because that is the greater value (20 to 4). If the RADIUS server times out, then Access Control fails over to the backup RADIUS server until it determines that the primary server is back up. At that point, Access Control starts proxying RADIUS requests to the primary server again.

Number of Retries

The number of times the ExtremeCloud IQ Site Engine server or Access Control engine resends an authentication or accounting request if the RADIUS server does not respond. Valid values are 0-20. This setting is only used for logging into ExtremeCloud IQ Site Engine via RADIUS or logging into the Access Control Captive Portal via RADIUS.

Configuration

UDP Button

Select the UDP button to configure the UDP port on the RADIUS server to receive authentication and accounting requests.

NOTE: If you are enforcing to an ExtremeControl engine for an Extreme Management Center version prior to Version 8.5, you must use different ports to configure UDP Auth. and Accounting. UDP will not function if the Auth and Accounting are configured for the same port for previous versions of ExtremeCloud IQ Site Engine.

Auth. Client UDP Port

The UDP port number (1-65535) on the RADIUS server that the ExtremeCloud IQ Site Engine server or Access Control engine sends authentication requests to; 1812 is the default port number.

Accounting Client UDP Port

The UDP port number (1-65535) on the RADIUS server that the Access Control engine sends accounting requests to; 1813 is the default port number.

TCP Button

Select the TCP button to configure the TCP port on the RADIUS server to receive authentication and accounting requests.

NOTE: For versions prior to ExtremeCloud IQ Site Engine Version 8.5, TCP settings are not supported and cannot be enforced to ExtremeControl engines.

Auth. Client TCP Port

The TCP port number (1-65535) on the RADIUS server that the ExtremeCloud IQ Site Engine server or Access Control engine sends authentication requests to; 1812 is the default port number.

Accounting Client TCP Port

The TCP port number (1-65535) on the RADIUS server that the Access Control engine sends accounting requests to; 1813 is the default port number.

RADSec Button

Select the RADSec button to configure the TLS (Transport Layer Security) port on the RADIUS server to receive authentication and accounting requests.

NOTE: For versions prior to ExtremeCloud IQ Site Engine Version 8.5, TLS settings are not supported and cannot be enforced to ExtremeControl engines.

Auth. Client TLS Port

The TLS port number (1-65535) on the RADIUS server that the ExtremeCloud IQ Site Engine server or Access Control engine sends authentication requests to; 2083 is the default port number.

Accounting Client TLS Port

The TLS port number (1-65535) on the RADIUS server that the Access Control engine sends accounting requests to; 2083 is the default port number.

Proxy RADIUS Accounting Requests

Select this checkbox to enable the Access Control engine to proxy RADIUS accounting requests to the RADIUS server. This option must be enabled if you are doing RADIUS accounting in an Access Control environment where the primary RADIUS server is being used for redundancy in a single Access Control engine configuration (Basic AAA configuration only).

Change Server Shared Secret

Server Shared Secret

The shared secret is a string of characters used to encrypt and decrypt communication between the ExtremeCloud IQ Site Engine server or Access Control and the RADIUS server. In ExtremeCloud IQ Site Engine, this is also the shared secret used between the switch and the RADIUS server if the Access Control engine is bypassed or if you configured the Management RADIUS Server options when you added the switch. The shared secret must be at least 6 characters long; 16 characters is recommended. Dashes are allowed in the string, but spaces are not.

Verify Shared Secret

Re-enter the Server Shared Secret you entered above.

Show Shared Secret

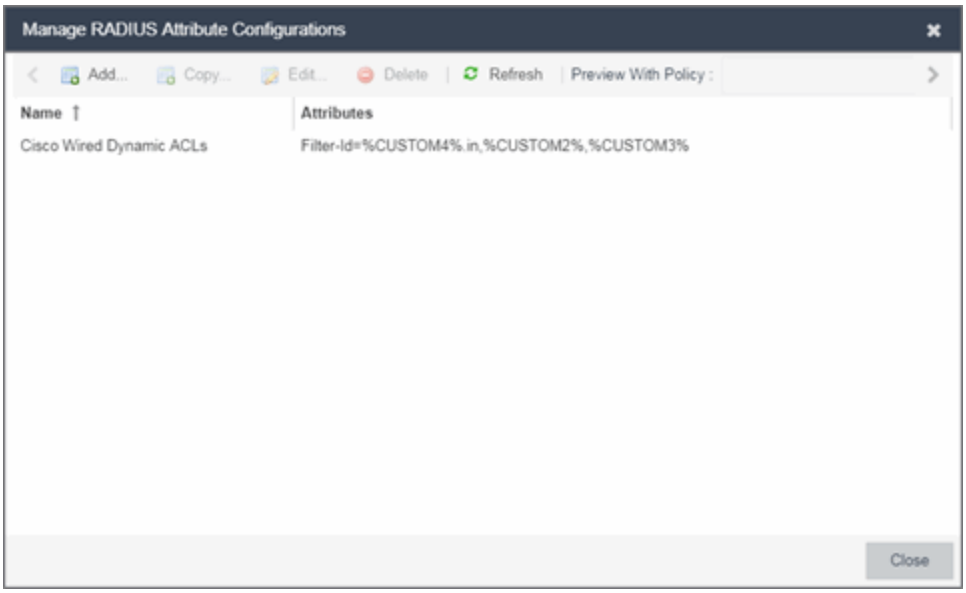
Displays the secret in the **Server Shared Secret** and **Verify Shared Secret** fields.

Advanced Button

Use this button to open the Advanced RADIUS Server Configuration window, where you can configure advanced RADIUS settings used by Access Control when proxying access requests to a backend RADIUS server.

Manage RADIUS Attribute Configurations Window

Use this window to view attributes injected when authentication or accounting requests are proxied to a back-end RADIUS server. Attributes you inject provide additional information about the users on your network. You can access the RADIUS Attribute Configurations window from the Add/Edit User To Authentication Mapping window.



Preview With Policy

Presents a preview of the attributes defined for selected attribute configuration.

Name

The names of the available attribute configurations. You cannot edit the name of a configuration.

Add

Select the **Add** button to open the Create New RADIUS Attribute Settings window, which allows you to create a new attribute configuration.

Edit

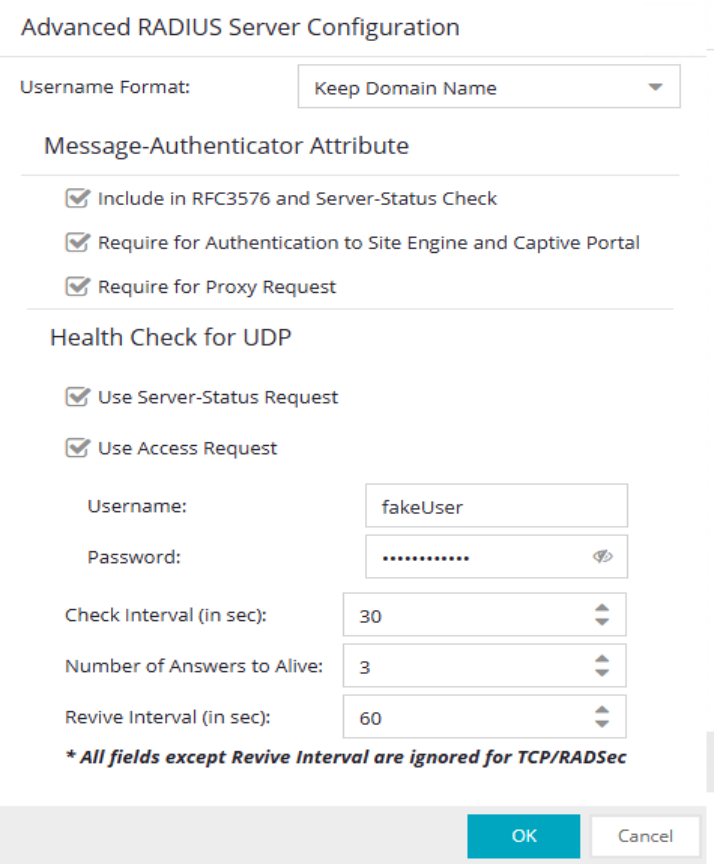
Select the **Edit** button to open the Edit RADIUS Attribute Settings window, which allows you to edit an existing attribute configuration.

Delete

Select an attribute and select the **Delete** button to remove an existing attribute configuration.

Advanced RADIUS Server Configuration

Use this window to configure advanced RADIUS settings used by ExtremeCloud IQ Site Engine when proxying authentication requests to a backend RADIUS server. You can access this window by selecting the **Advanced** button at the bottom of the Add/Edit RADIUS Server window.



Username Format

This field is used by ExtremeCloud IQ Site Engine to determine what format to use for the username when proxying a request to the backend RADIUS server. There are two options:

- **Strip Domain Name** *(default)* - This option removes a domain name from the username when proxying the request. Select this option unless the backend RADIUS server requires the domain name to be included.
- **Keep Domain Name** - This option keeps any domain names on the username when proxying the request to the backend RADIUS server. If the backend RADIUS server is a Microsoft IAS or NPS server, this option could cause the RADIUS server to time out if a guest comes onto the network with another domain. In that scenario, if the request is proxied to the backend RADIUS server with the domain name, the server does not respond to the request because it is from an unknown domain. Therefore, if you use this

option with a Microsoft IAS or NPS server, use an advanced AAA configuration so that only requests for the desired domain(s) are sent to the backend RADIUS server, and all unknown domains are processed locally so they are rejected.

Include in RFC3576 and Server-Status Check

Enable this checkbox if the backend RADIUS server requires a Message-Authenticator attribute to be part of the request. If enabled, ExtremeCloud IQ Site Engine adds the Message-Authenticator attribute when proxying the request.

Require for Authentication to Site Engine and Captive Portal

Enable this checkbox to include the Message-Authenticator attribute in the RADIUS request and require the Message-Authenticator attribute in the RADIUS response when RADIUS is used for authenticating to the ExtremeCloud IQ Site Engine or through the Captive Portal. If enabled, the RADIUS packets without the Message-Authenticator attribute are dropped.

Require for Proxy Request

Enable this checkbox to require that all RADIUS packets to and from the upstream RADIUS server must contain the Message-Authenticator attribute. If you enable Require for Proxy Request, and the Message-Authenticator attribute is not present then the packet is dropped. Not every RADIUS server supports the Message-Authenticator attribute, but the security best practice is to enable Require for Proxy Request. You can verify the context of the Message-Authenticator attribute in the Access Control > Switch settings.

Health Check for UDP

ExtremeCloud IQ Site Engine uses the options in this section to determine how to check the health of a backend RADIUS server, if that server stops responding to requests.

NOTE: For backend RADIUS server options other than UDP (for example, TCP or RADSec), all fields except Revive Interval in the Health Check for UDP are not available.

Use Server-Status Request

When selected, ExtremeCloud IQ Site Engine attempts to use Server-Status RADIUS packets as defined by RFC 5997, to determine if the backend RADIUS server is up.

Use Access Request

When selected, ExtremeCloud IQ Site Engine attempts to use an access request message to determine if the RADIUS server is up. The request is made using the username and password specified below. The username and password do not need to be valid, as ExtremeCloud IQ Site Engine is looking for a response and a reject also works. The username/password fields are provided in case you want to prevent rejects from being logged in the backend RADIUS server.

Check Interval

The interval to wait between checks to see if the RADIUS server is up. This is only applicable if the Server-Status request or Access request methods are used.

Number of Answers to Alive

The number of times the RADIUS server must respond before it is marked as alive. This is only applicable if the Server-Status request or Access request methods are used.

Revive Interval

If Server-Status requests and Access requests are not allowed or supported by the RADIUS server, then ExtremeCloud IQ Site Engine waits the amount of time specified here before allowing requests to go to a backend RADIUS server, if it stops responding. Only use this if there is no other way to detect the health of the backend RADIUS server.

Manage RADSec Certificates

This panel lets you view and define the CA certificates and certificates that the Access Control engine pushes to switches to configure RadSec, and the mappings that determine which CA certificates and certificate each switch receives. RadSec is RADIUS over TCP (secured by TLS). In RadSec, the switch is the RadSec client and the Access Control engine is the RadSec server.

To configure RadSec on a switch, you create a mapping for the switch. A mapping identifies the CA certificates and the certificate that the Access Control engine pushes to the switch. The Access Control engine installs the CA certificates as the trusted CA certificates on the switch and installs the certificate as the SSL/TLS certificate of the switch. The switch uses the certificates to establish the RadSec connection to the Access Control engine. You can create one mapping for many switches, so that all of the switches receive the same CA certificates and certificate.

NOTE: The Access Control engine installs the CA certificates in the RADSec Certificates panel on the switch as its trusted CA certificates. The Access Control engine uses the Trusted Authorities in your AAA configuration to validate the certificate of the switch. Add the CA that issued the certificate of the switch to the Trusted Authorities in your AAA configuration.

You can access this panel by selecting RADSec Certificates from the **Control** > **Access Control** > **Configuration** > **AAA** tree in the left panel.

RADSec Client CA Certificate

This table lists the CA certificates that you can assign to RadSec clients (switches).

Summary
A summary of the CA certificate, including the name of the CA and the date until which the certificate is valid.

Add Button
Opens a window where you can add a CA certificate that you can assign to RadSec clients.

Delete Button
Deletes the selected CA certificate.

RADSec Client Certificate

This table lists the certificates that you can assign to RadSec clients (switches).

Summary
A summary of the certificate, including the name, the CA that issued the certificate, and the date until which the certificate is valid.

Issued To
The name of the entity to which the certificate was issued.

Issued By
The CA that issued the certificate.

Valid From
The date and time from which the certificate is valid.

Valid To
The date and time until which the certificate is valid.

Serial Number
The serial number of the certificate.

Add Button
Opens a window where you can add a certificate.

Delete Button
Deletes the selected certificate.

Assign Certificate to RADSec Clients

This table lists the RadSec clients (switches) and the CA certificates and certificate assigned to each of them. The assignments determine which CA certificates and certificate are pushed to each switch.

Switch IP
The IP address of the switch.

CA Certificates
The CA certificates that are pushed to the switch as its trusted CA certificates.

Certificate Issued To
The name of the entity to which the certificate pushed to the switch was issued.

Certificate Serial Number
The serial number of the certificate pushed to the switch.

Add Button
Opens the Assign Certificate to RADSec Clients window where you can create a mapping that determines which CA certificates and certificate are pushed to one or more switches.

Edit Button
Opens a window where you can edit the selected mapping.

Delete Button
Deletes the selected mapping.

Assign Certificate to RADSec Clients

Use the Assign Certificate to RADSec Clients window to create a mapping for one or more RADSec Clients. A mapping identifies the trusted CA certificates and the SSL/TLS certificate that the Access Control engine pushes to the RADSec Clients during the next enforce. If you change the assigned certificate later, enforce again to apply the update.

When you select more than one RADSec Client, all of the selected RADSec Clients are mapped to the same CA certificates and certificate.

You can access this window from the Manage RADSec Certificates window.

Filter
Filters the list of switches. Enter an IP address, nickname, or engine to display only the matching switches.

Switch List
Lists the switches by engine group and engine. Select the check box next to an engine group, engine, or switch to create the mapping for the engine group, engine, or switch. Selecting an engine group or engine selects all switches that belong to the engine group or engine.

CA Certificates
Use the drop-down list to select the CA certificates to push to the selected switches. The switches use the CA certificates that you select as their trusted CA certificates.

Certificate
Use the drop-down list to select the certificate to push to the selected switches. The switches use the certificate that you select as their SSL/TLS certificate.

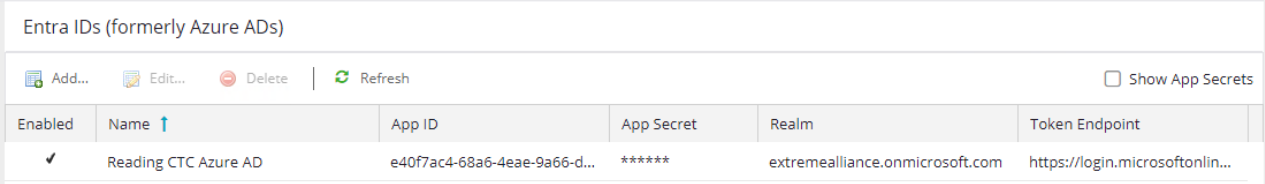
Save Button
Saves the mapping and closes the window.

Apply Button
Saves the mapping and keeps the window open.

Cancel Button
Closes the window without saving the mapping.

Manage Entra ID (formerly Azure AD) Configurations

This panel lets you view and define the Microsoft Entra IDs used in ExtremeCloud IQ Site Engine. You can use Entra IDs in ExtremeControl AAA configurations. You can access this panel by selecting Entra IDs from the left-panel in the Access Control Configurations > AAA Configurations tree. Any changes made are saved to the ExtremeCloud IQ Site Engine database and must be enforced to Access Control Engines.



Enabled

If checked, the enabled Entra IDs are pushed to the configuration of Access Control Engine. If unchecked, the not enabled Entra IDs are not used.

Name

The user-defined name of the Entra ID. The name provides local meaning only.

App ID

The application identifier of the registered application in Entra ID. In Entra ID the App ID is the "Application (client) ID".

App Secret

The client secret defined of the registered application in Entra ID.

Realm

The Realm defines what Entra ID configuration to use based on username. Realm is usually the part after the @ in the login username. All enabled Entra IDs are used once the Entra ID is referenced in AAA rules.

Token Endpoint

The OAuth 2.0 token endpoint (v2) provided by Entra ID in App registrations.

Show App Secrets

If checked, the shared secrets are shown in clear text form. If unchecked, the shared secrets are shown as a string of asterisks.

Add Button 

Select the **Add** button to open the Add Entra ID window where you can define a new Entra ID.

Edit Button  Edit...

Select an entry in the Entra IDs section of the window and select the **Edit** button to open the Edit Entry window where you can edit an existing entry.

Delete Button  Delete

Select an entry in the Entra IDs section of the window and select the **Delete** button to delete an existing entry. You cannot delete the last Entra ID configuration currently in use. You can remove the AAA rule if you do want to delete all Entra IDs.

Policy Mapping Configuration

In your ExtremeControl profiles, each access policy (Accept, Quarantine, Failsafe, and Assessment) is associated to a *policy mapping* that defines exactly how end-system traffic is handled on the network. Each mapping specifies a policy role (created in the **Policy** tab) and/or any additional RADIUS attributes included as part of a RADIUS response to a switch.

The RADIUS attributes required by a switch are specified in the RADIUS Attributes to Send field configured in the Edit Switch window. The actual switch RADIUS attribute values (Login-LAT-Port, Custom 1, etc.) are defined within each policy mapping configured in this window. Each policy mapping is associated with the access policy selected in your Access Control profiles.

When an end-system authenticates to the network, the Access Control profile is applied and the appropriate RADIUS response attributes are extracted from the mapping based on the switch the authentication request originated from. The attributes are returned to the switch in the RADIUS Access-Accept response.

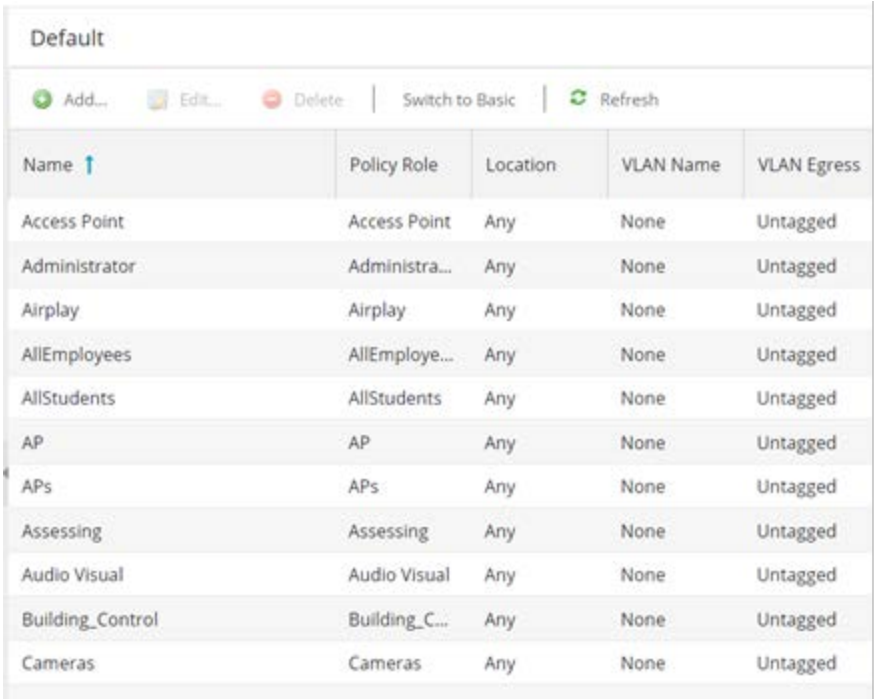
For more information on configuring policy mappings, see How to Set Up Access Policies and Policy Mappings. For a description of each Access Control access policy, and some guidelines for creating corresponding policy roles in the **Policy** tab, see the section on Access Policies in the Concepts file.

To access this window, select the **Policy Mappings** left-panel option in the **Access Control Configurations** > **Access Control** left-panel menu.

The columns displayed in this window vary depending on whether you are using a Basic or Advanced policy mapping configuration. For a definition of each column, see below.

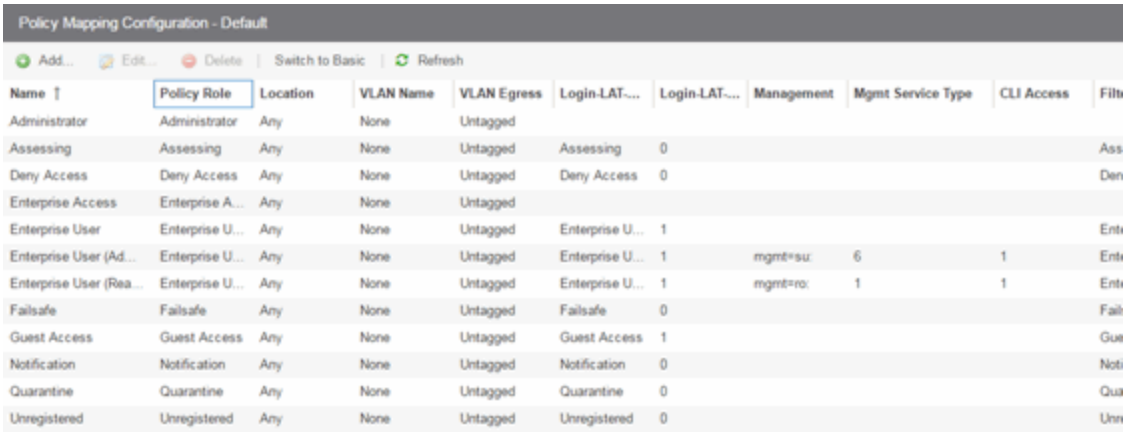
Basic AAA Configuration

Basic AAA Configurations define the RADIUS and LDAP configurations for all end-systems connecting to your Access Control engines.



Name	Policy Role	Location	VLAN Name	VLAN Egress
Access Point	Access Point	Any	None	Untagged
Administrator	Administra...	Any	None	Untagged
Airplay	Airplay	Any	None	Untagged
AllEmployees	AllEmploye...	Any	None	Untagged
AllStudents	AllStudents	Any	None	Untagged
AP	AP	Any	None	Untagged
APs	APs	Any	None	Untagged
Assessing	Assessing	Any	None	Untagged
Audio Visual	Audio Visual	Any	None	Untagged
Building_Control	Building_C...	Any	None	Untagged
Cameras	Cameras	Any	None	Untagged

Advanced Policy Mapping Configuration



Name	Policy Role	Location	VLAN Name	VLAN Egress	Login-LAT-...	Login-LAT-...	Management	Mgmt Service Type	CLI Access	Filt
Administrator	Administrator	Any	None	Untagged						
Assessing	Assessing	Any	None	Untagged	Assessing	0				Ass
Deny Access	Deny Access	Any	None	Untagged	Deny Access	0				Den
Enterprise Access	Enterprise A...	Any	None	Untagged						
Enterprise User	Enterprise U...	Any	None	Untagged	Enterprise U...	1				Ent
Enterprise User (Ad...	Enterprise U...	Any	None	Untagged	Enterprise U...	1	mgmt=su:	6	1	Ent
Enterprise User (Rea...	Enterprise U...	Any	None	Untagged	Enterprise U...	1	mgmt=ro:	1	1	Ent
Failsafe	Failsafe	Any	None	Untagged	Failsafe	0				Fail
Guest Access	Guest Access	Any	None	Untagged	Guest Access	1				Gue
Notification	Notification	Any	None	Untagged	Notification	0				Noti
Quarantine	Quarantine	Any	None	Untagged	Quarantine	0				Qua
Unregistered	Unregistered	Any	None	Untagged	Unregistered	0				Unr

Column Definitions

Name

The policy mapping name.

Policy Role

The policy role assigned to this mapping. All policy roles used in your mappings must be part of your ExtremeControl (Access Control) Controller policy configuration and/or defined in the **Policy** tab and enforced to the policy-enabled switches in your network.

Location

Policy mapping locations permit authentication requests that match the same Access Control rule and corresponding Access Control profile to be authorized to different accept attributes (policy/VLAN/Custom Attribute) based on the location the request originated from. For example, in the Policy Mapping Configuration screenshot above, the Administration policy mapping has five entries, with each entry assigning a different VLAN (for RFC 3580-enabled switches) for authentication requests matching the specified location. Requests originating from the 1st floor South location will be authorized to VLAN 100, and requests originating from the 2nd floor North location (matching the same Access Control rule) is authorized to VLAN 220. Using locations in this manner lets you authorize end-systems to different access criteria using a single Access Control rule, whereas the alternative would be to create multiple location-based Access Control rules each with an Access Control Profile that corresponds with the desired access value.

When policy mapping locations are used in this manner, it is important to include a catch-all policy mapping (the fifth Administration mapping in the example above) that has a location of "any" and sets the access behavior for an authorization originating from any other location. The access behavior could be a policy/VLAN/Custom Attribute that grants some form of restricted access, or denies access altogether. If a catch-all mapping is not included, a warning message appears on enforce indicating that there is no catch-all mapping configured, and authorizations that match the policy but do not originate from a defined location, can result in errors or unpredictable behavior.

VLAN Name

If you have RFC 3580-enabled switches in your network, this column displays the VLAN name assigned to this mapping.

VLAN Egress

If you have RFC 3580-enabled switches in your network, this column displays the VLAN ID assigned to this mapping.

Filter

This value is only displayed in Basic mode if ExtremeWireless Controllers have been added to ExtremeCloud IQ Site Engine. The Filter column typically maps to the Filter-Id RADIUS attribute. This value applies to ExtremeWireless Controllers and other switches that support the Filter-Id attribute.

Login-LAT-Group

If your network devices require a Login-LAT-Group, it displays here.

Login-LAT-Port

If you have ExtremeWireless Controllers on your network, the Login-LAT-Port is an attribute returned in the default RADIUS response. The Login-LAT-Port value is used by the controller to determine whether the authentication is fully authorized. A value of "1" indicates the authentication is authorized, where a value of "0" indicates that authorization is not complete. The value of "0" is used by the controller to determine that additional authentication is

required and is a signal for the controller to engage its external captive portal and use HTTP redirection to force HTTP traffic from the end-system to the defined Access Control engine. This is used in conjunction with the Registration and Assessment features of Access Control.

Management

The authorization attribute returned for successful administrative access authentication requests that originate from network equipment configured to use RADIUS as the authentication mechanism for remote management of switches, routers, VPN concentrators, etc. Examples of management values for EOS devices are: "mgmt=su:", "mgmt=rw:", or "mgmt=ro:". The management attribute determines the level of access the administrator will have when authorized to access the device: superuser, read/write, or read-only.

Custom

Some network devices require additional RADIUS response attributes in order to provide authorization or define additional parameters for the authenticated session. These additional attributes can be defined in the five available Custom option fields.

Attribute List 1-3

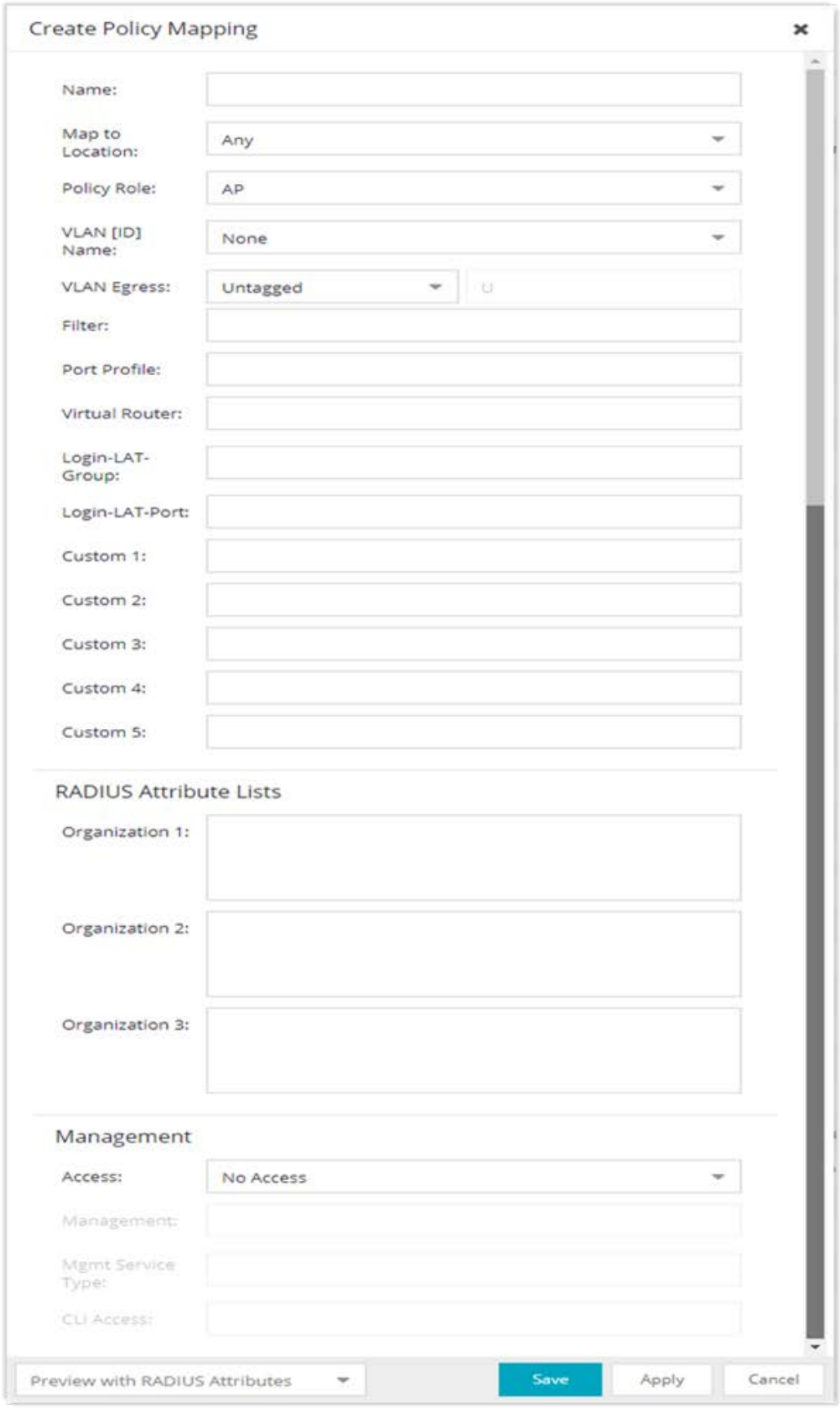
The **Attribute List** fields display additional RADIUS response attributes in a single mapping. For example, you can use each field to provide a complete ACL for a different third-party vendor.

Add/Edit Policy Mapping

Use this window to add a new policy mapping or edit an existing policy mapping. A policy mapping specifies a policy role (created on the **Policy** tab) and/or any additional RADIUS attributes included as part of a RADIUS response to a switch (as defined in the RADIUS Attributes to Send field configured in the Edit Switch window). For additional information about configuring policy mappings, see How to Set Up Access Policies and Policy Mappings.

Access this window by selecting the **Add** or **Edit** toolbar buttons in the Edit Policy Mapping Configuration window.

The fields in this window vary depending on whether you are using a basic or advanced policy mapping configuration. For a definition of each field, see below.


Create Policy Mapping
Name:
Map to Location:
Any
Policy Role:
AP
VLAN [ID] Name:
None
VLAN Egress:
Untagged
Filter:
Port Profile:
Virtual Router:
Login-LAT-Group:
Login-LAT-Port:
Custom 1:
Custom 2:
Custom 3:
Custom 4:
Custom 5:
RADIUS Attribute Lists
Organization 1:
Organization 2:
Organization 3:
Management
Access:
No Access
Management:
Mgmt Service Type:
CLI Access:
Preview with RADIUS Attributes
Save
Apply
Cancel

Name

Enter a name for the policy mapping.

Map to Location

Allows you to specify a certain location for the mapping. You should first configure your locations using the Location Group (**Control** tab > **Access Control** > Access Control Configurations > Group Editor > Location Groups) or you can select the **Edit** button to the right of the field to add a location group to the list. For more information on using the Location option in Policy Mappings, see the Edit Policy Mapping Configuration Window Help topic.

Policy Role

Use the drop-down list to select a policy role, or enter a policy role in the field. The drop-down list displays any policy roles you have created and saved in the **Policy** tab and/or all the policy roles contained in the Access Control Controller policy configuration. Roles from all your policy domains are listed; if there are duplicate names, only one is listed. The list is not case sensitive, so "Enterprise User" and "enterprise user" are considered duplicate policy names. All policy roles used in your mappings must be part of your Access Control) Controller policy configuration and/or defined in **Policy** tab and enforced to the EOS policy-enabled switches in your network.

NOTE: Entering a new policy role does **not** create a new role in the **Policy** tab.

VLAN [ID] Name

Use the drop-down list to select the appropriate VLAN associated with the policy. This list displays any VLANs defined in ExtremeCloud IQ Site Engine. Select the configuration menu button to the right of the field to add a VLAN to the list. VLANs you add remain in the list only as long as they are used in a mapping and they are **not** added to the ExtremeCloud IQ Site Engine database.

VLAN Egress

Use the drop-down list to select the appropriate VLAN the egress forwarding state: Tagged (frames are forwarded as tagged), Untagged (frames are forwarded as untagged), Same as Ingress (frames are forwarded as specified by the VLAN Ingress), or User Defined (you define how frames are forwarded).

Filter

If your network devices require a custom Filter-Id, enter it here. The Filter column typically maps to the Filter-Id RADIUS attribute. This value applies to ExtremeWireless Controllers and other switches that support the Filter-Id attribute.

Port Profile

For ExtremeXOS/Switch Engine devices on which legacy firmware is installed, this field indicates the profile used by Extreme Policy.

Login-LAT-Group

If your network devices require a Login-LAT-Group, enter it here.

Login-LAT-Port

If you have ExtremeWireless Controllers on your network, the Login-LAT-Port is an attribute returned in the default RADIUS response. The Login-LAT-Port value is used by the controller to determine whether the authentication is fully authorized. A value of "1" indicates the authentication is authorized, where a value of "0" indicates that authorization is not complete. The value of "0" is used by the controller to determine that additional authentication is required and is a signal for the controller to engage its external captive portal and use HTTP redirection to force HTTP traffic from the end-system to the defined Access Control engine. This is used in conjunction with the Registration and Assessment features of Access Control.

Custom

If your network devices require additional RADIUS response attributes in order to provide authorization or define additional parameters for the authenticated session, you can define them in the five available Custom option fields.

Organization 1-3

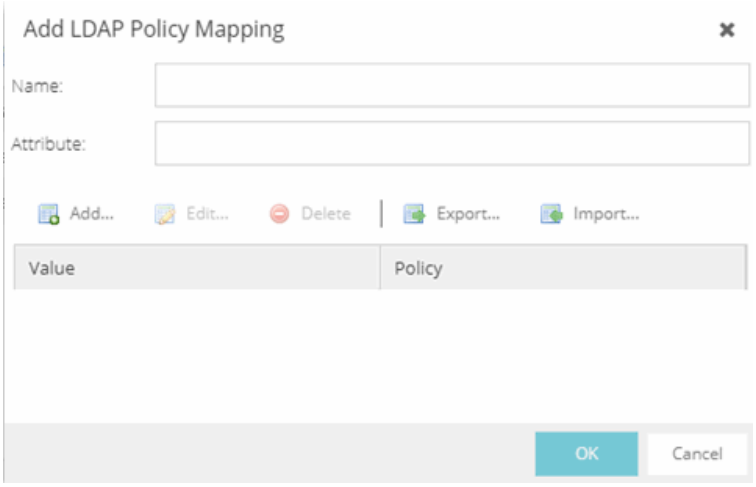
Enter additional RADIUS response attributes in a single mapping in the **Organization** fields. For example, you can use each field to provide a complete ACL for a different third-party vendor.

Management

Enter a management attribute used to authenticate requests for administrative access to the selected switches, for example, "mgmt=su:", "mgmt=rw:", or "mgmt=ro:". The management attribute determines the level of access the administrator will have to the switch: superuser, read/write, or read-only. Be sure to include the final colon (":") in the attribute, or the management access will not work.

Add LDAP Policy Mappings

Use the Add LDAP Policy Mapping window to add LDAP Policy authentication mappings that define what policy will be assigned to an end-system, based on LDAP information.



The Add LDAP Policy Mapping window includes the following information:

Name
A unique name used to identify the LDAP Policy Mapping.

Attribute
The LDAP attribute for which the value to policy mappings are defined. This is the attribute that will be queried in the LDAP database to determine which policy to assign to a given end-system.

Value - Policy Table
Lists mappings between the LDAP database attribute value and authentication policies.

Use the buttons in the Add LDAP Policy Mappings window to perform the following functions:

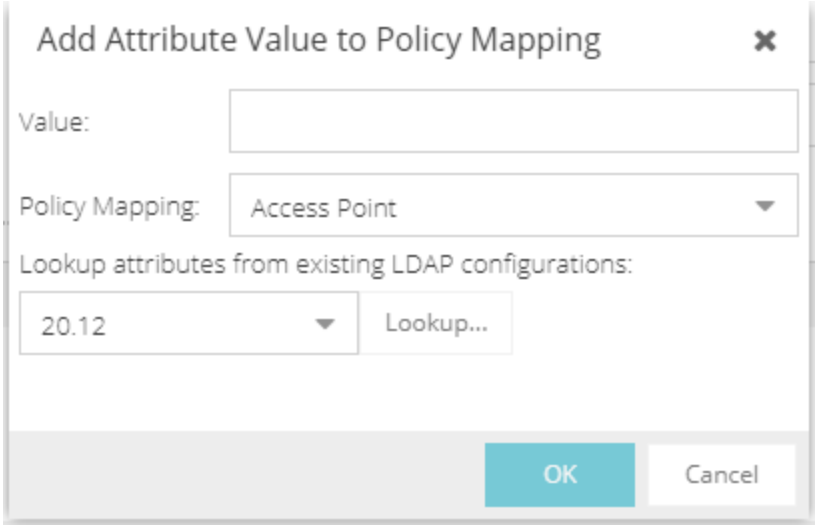
Add
Opens the Add Attribute Value to Policy Mapping window, where you can define a new entry.

Edit
Opens the Edit Attribute Value to Policy Mapping window, where you can edit the selected entry.

Delete
Enables you to delete a selected entry.

Add Attribute Value to Policy Mapping

Use the Add Attribute Value to Policy Mapping window to edit the values and attributes to an end-system.



The Add Attribute Value to Policy Mapping window includes the following information:

Value
The specific value that the Attribute of the LDAP Policy Mapping must match in order to assign a given end-system a policy mapping.

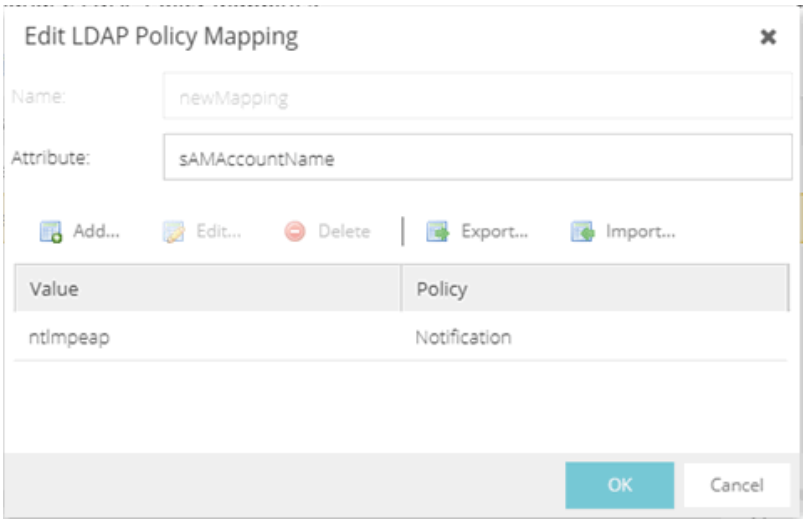
Policy Mapping
The policy mapping, and by extension, the policy, which is assigned to an end-system that matches the Attribute-Value.

Lookup Attributes from Existing LDAP Configurations
Use this field to query an LDAP database of an existing LDAP configuration, which can help you determine what attributes and values to use for a given policy mapping. This field has no impact on the configuration; it is only meant to aid the user in the configuration.

Edit LDAP Policy Mappings

Edit LDAP Policy Mappings

Use the Edit LDAP Policy Mapping window to add or edit LDAP Policy authentication mappings that define what policy will be assigned to an end-system, based on LDAP information.



The Edit LDAP Policy Mapping window includes the following information:

Name
A unique name used to identify the LDAP Policy Mapping.

Attribute
The LDAP attribute for which the value to policy mappings are defined. This is the attribute that will be queried in the LDAP database to determine which policy to assign to a given end-system.

Value - Policy Table
Lists mappings between the LDAP database attribute value and authentication policies.

Use the buttons in the Edit LDAP Policy Mappings window to perform the following functions:

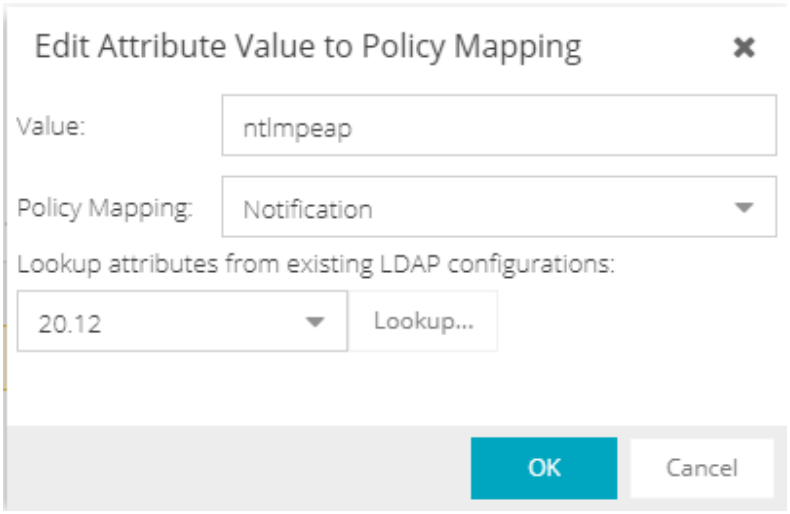
Add
Opens the Add Attribute Value to Policy Mapping window, where you can define a new entry.

Edit
Opens the Edit Attribute Value to Policy Mapping window, where you can edit the selected entry.

Delete
Enables you to delete a selected entry.

Edit Attribute Value to Policy Mapping Window

Use the Edit Attribute Value to Policy Mapping window to edit the values and attributes to an end-system.



The Edit Attribute Value to Policy Mapping window includes the following information:

Value
The specific value that the Attribute of the LDAP Policy Mapping must match in order to assign a given end-system a policy mapping.

Policy Mapping
The policy mapping, and by extension, the policy, which is assigned to an end-system that matches the Attribute-Value.

Lookup Attributes from Existing LDAP Configurations
Use this field to query an LDAP database of an existing LDAP configuration, which can help you determine what attributes and values to use for a given policy mapping. This field has no impact on the configuration; it is only meant to aid the user in the configuration.

Access Control Profiles

ExtremeCloud IQ Site Engine includes ten system-defined ExtremeControl profiles that define the authorization and assessment requirements for the end-systems connecting to the network.

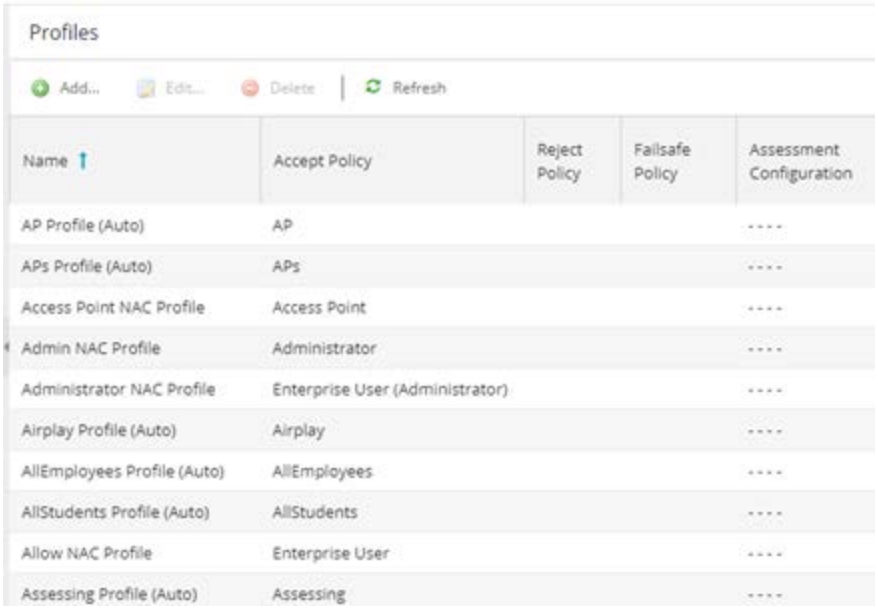
The system-defined profiles are:

- Administrator
- Allow
- Default

- Guest Access
- Notification
- Pass Through
- Quarantine
- Registration Denied Access
- Secure Guest Access
- Unregistered

Use the Access Control Profiles window to view and edit these profiles, and define new profiles if desired. Any changes made in this window are written immediately to the ExtremeCloud IQ Site Engine database.

To open the Access Control Profiles window, navigate to the **Access Control** tab and select the Access Control Profiles tab in the left-panel.



The window includes the following buttons and functionality:

Add Button Add...

Use this button to open the New ExtremeControl Profile window, where you can add an Access Control profile.

Edit Button Edit...

Use this button to open the Edit ExtremeControl Profile window, where you can edit an existing Access Control profile.

Delete Button Delete

Use this button to add an Access Control profile.

The Access Control Profiles table includes the following columns:

Name
The name of the Access Control profile.

Accept Policy
The Accept policy defined for this profile. An Accept policy is applied to an end-system when

- an end-system has been authorized locally by the Access Control engine and has passed an assessment (if assessment in enabled).
- authentication is configured to replace the attributes returned from the RADIUS server with the Accept policy.

NOTES:

- If your Accept policy is "Use User/Host LDAP Policy Mappings," an Accept Policy will be assigned, based on the end-system information in the LDAP database and the LDAP Policy Mappings configured in the Authentication Mapping.
- Authenticated Guest and IoT Management provisioners cannot match a rule associated with an **Accept Policy =** `-- No Policy --`. Guest and IoT Management authenticated provisioners must match a rule in Control, mapped to an Accept Policy that is not mapped to "`-- No Policy --`".

Reject Policy
Indicates whether all authentication requests are rejected.

Failsafe Policy
The Failsafe policy defined for this profile. A Failsafe policy is applied to an end-system if the end-system's IP address cannot be determined from its MAC address, or if there has been a scanning error and a scan of the end-system could not take place.

Assessment Configuration
The assessment configuration defined for this profile. The configuration define the assessment requirements for end-systems

Assessment Interval
If assessment is required, this defines the interval between required assessments for an end-system.

Quarantine Policy
The Quarantine policy defined for this profile. A Quarantine policy is applied to an end-system if the end-system fails an assessment.

Assessment Policy

The Assessment policy defined for this profile. An Assessment policy is applied to an end-system while it is being assessed.

Hide Assessment/Remediation Details

Denotes whether the option to hide assessment or remediation information on the Remediation Web Page has been selected.

New/Edit ExtremeControl Profile

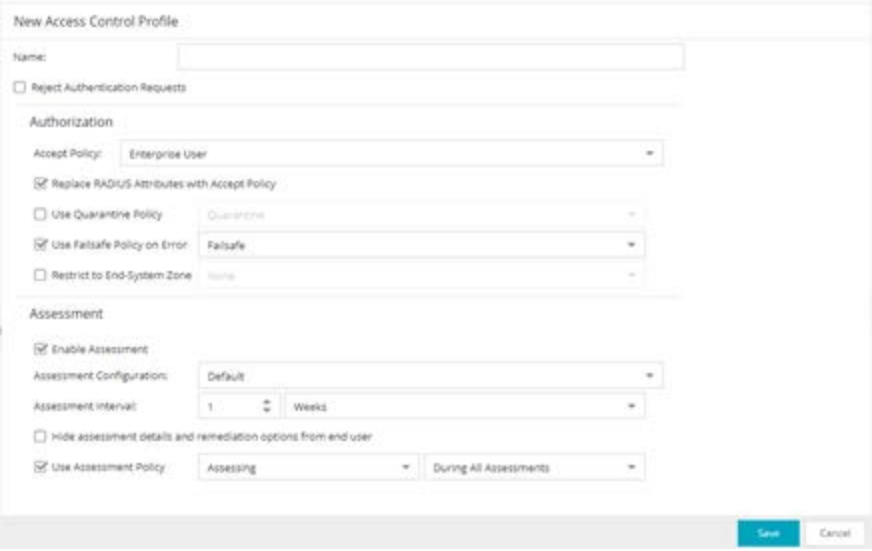
ExtremeControl Profiles specify the authorization and assessment requirements for the end-systems connecting to the network. Profiles also specify the security policies that will be applied to end-systems for network authorization, depending on authentication and assessment results.

ExtremeCloud IQ Site Engine comes with ten system-defined Access Control profiles:

- Administrator
- Allow
- Default
- Guest Access
- Notification
- Pass Through
- Quarantine
- Registration Denied Access
- Secure Guest Access
- Unregistered

You can edit these profiles or you can define your own profiles to use for your Access Control configurations. Use this window to create a new profile, or edit an existing profile. When you create a new profile, it is added to the Manage ExtremeControl Profiles window. When you edit a profile, it changes the profile wherever it is used, so you don't have to do individual edits for each profile.

To create a new profile, select the **Add** button in the Manage ExtremeControl Profiles window. To edit an existing profile, select a profile in the Manage Access Control Profiles window and select the **Edit** button or select it from the left-panel.



Name

Enter a name for a new profile. If you are editing a profile, the name of the profile is displayed and cannot be edited. To change the name of a profile, right-click on the profile name in the Access Control Profiles left-hand panel navigation tree and select **Rename** from the menu.

Reject Authentication Requests

If you select this checkbox, all authentication requests are rejected.

Authorization

Accept Policy

Use the drop-down list to select the Accept policy you want to use in this ExtremeControl profile. An Accept policy is applied to an end-system when:

- an end-system has been authorized locally (MAC authentication) by the Access Control engine and has passed an assessment (if assessment in enabled).
- you have selected the **Replace RADIUS Attributes with Accept Policy** option.

If you select "No Policy," then the Access Control engine does not include a Filter ID or VLAN Tunnel Attribute in the RADIUS attributes returned to the switch, and the default role configured on the port is assigned to the end-system. This option is necessary when configuring single user plus IP phone authentication supported on C2/C3 and B2/B3 devices.

If you select "Use User/Host LDAP Policy Mappings," an Accept Policy will be assigned, based on the end-system information in the LDAP database and the LDAP Policy Mappings configured in the Authentication Mapping.

Replace RADIUS Attributes with Accept Policy

When this option is checked, the attributes returned from the RADIUS server are replaced by the policy designated as the Accept policy. If the RADIUS server does not return a Filter ID or

VLAN Tunnel attribute, the Accept policy is inserted. When this option is unchecked, the attributes returned from the RADIUS server are forwarded back "as is" and the Accept Policy would only be used to locally authorize MAC authentication requests. If the RADIUS server does not return a Filter ID or VLAN Tunnel attribute, no attributes are returned to the switch.

Use Quarantine Policy

Select this checkbox if you want to specify a Quarantine policy. The Quarantine policy is used to restrict network access for end-systems that have failed the assessment. You must have the **Enable Assessment** checkbox selected to activate this checkbox.

If a Quarantine policy is not specified and you have configured RADIUS in your AAA configuration, then the policy from the RADIUS attributes would be applied (unless **Replace RADIUS Attributes with Accept Policy** has been selected, in which case the Accept policy would be used.) If **Authorize Authentication Requests Locally** has been selected in your AAA configuration, then the Accept policy would be applied to those end-systems that are authorized locally. This allows an end-system onto the network with its usual network access even though the end-system failed the assessment.

Use Failsafe Policy on Error

Select this checkbox if you want to specify a Failsafe policy to be applied to an end-system when it is in an Error connection state. An Error state results if the end-system's IP address could not be determined from its MAC address, or if there was a scanning error and a scan of the end-system could not take place. A Failsafe policy should allocate a nonrestrictive set of network resources to the connecting end-system so it can continue its work, even though an error occurred in Access Control operation.

If a Failsafe policy is not specified and you have configured RADIUS in your AAA configuration, then the policy from the RADIUS attributes would be applied (unless **Replace RADIUS Attributes with Accept Policy** has been selected, in which case the Accept policy would be used.) If **Authorize Authentication Requests Locally** has been selected in your AAA configuration, then the Accept policy would be applied to those end-systems that are authorized locally. This allows end-systems onto the network with their usual network access when an error occurs in Access Control operation.

Assessment

Enable Assessment

Select the **Enable Assessment** checkbox if you want to require that end-systems are scanned by an assessment server.

NOTES: If you require end-systems to be scanned by an assessment server, you need to configure the assessment servers performing the scans. The Manage Assessment Settings window is the main window used to manage and configure assessment servers. To access this window, select **Assessment** from the Access Control Configurations > Access Control Profiles left-hand panel navigation tree.

The ExtremeControl engine restarts when you enforce if **Enable Assessment** is selected the first time in an ExtremeControl profile. The ExtremeControl engine also restarts when you enforce when **Enable Assessment** is deselected for all ExtremeControl profiles.

Assessment Configuration

Use the drop-down list to select the assessment configuration you would like to use in this ExtremeControl Profile. Use the **Edit** button to add a new assessment configuration or edit a configuration, if needed. After you create an assessment configuration, it becomes available for selection in the list.

Assessment Interval

Enter an assessment interval that defines the interval between required assessments:

- Minutes - 30 to 120
- Hours - 1 to 48
- Days - 1 to 31
- Weeks - 1 to 52
- None

Hide Assessment Details and Remediation Options from User

If you select this option, the end user does not see assessment or remediation information on the Remediation Web Page. They are informed that they are quarantined, and told to contact the Help Desk for assistance.

Use Assessment Policy

Select this checkbox if you want to specify a certain policy to be applied to an end-system while it is being assessed. Use the drop-down list to select the desired policy.
Select when to apply the policy:

- During Initial Assessment Only - Only initial assessments receive the assessment policy. If the end-system is being re-assessed, it remains in its current policy.
- During All Assessments - All end-systems being assessed receive the specified assessment policy.

If an assessment policy is not specified and you have configured RADIUS in your AAA configuration, then the policy from the RADIUS attributes are applied (unless "Replace RADIUS Attributes with Accept Policy" is selected, in which case the Accept policy is used.) If "Authorize Authentication Requests Locally" is selected in your AAA configuration, then the

Accept policy is applied to those end-systems authorized locally. This allows the end-system immediate network access without having to wait for assessment to be complete.

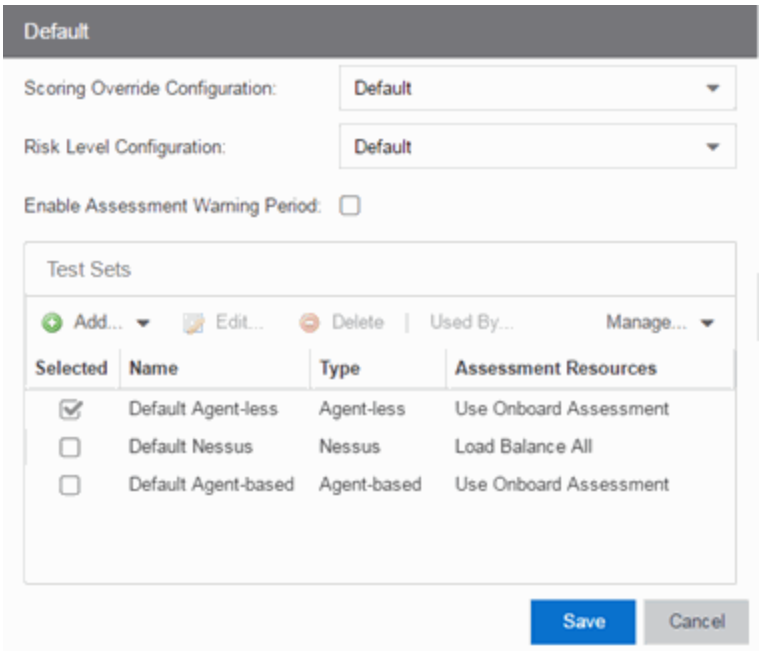
Edit Assessment Configuration

Use the Assessment Configuration window to view and configure the assessment configurations that define the assessment requirements for end-systems. Assessment configurations define the following information:

- How to score assessment results (determined by the selected Risk Level and Scoring Override configurations).
- What assessment tests to run (determined by the selected test sets).

After you have defined your assessment configurations, they are available for selection when creating your ExtremeControl configurations.

To access this window, select **Access Control Configurations > Access Control Profiles > Assessment** in the left-hand menu to open the Manage Assessment Settings window. Select an existing configuration and select **Edit** to open the Edit Assessment Configuration window, or you can select **Add** to add a new assessment configuration, and then open the Edit Assessment Configuration window.



Scoring Override Configuration

Use the drop-down list to select the scoring override configuration for this assessment configuration. Scoring overrides let you override the scoring mode and test result scores for a particular assessment test. The default scoring override configuration provided by ExtremeCloud IQ Site Engine specifies no overrides, but can be edited to contain overrides, if desired.

Risk Level Configuration

Use the drop-down list to select the risk level configuration for this assessment configuration. The risk level configuration determines what risk level is assigned to an end-system (high, medium, or low) based on the end-system's health result details score.

Enable Assessment Warning Period

This section allows you to enable assessment warning periods. Warning periods let you specify a grace period and probation period used for assessment warnings.

Grace Period

Specify the number of days the end user has to resolve the warning issues before the end-system is quarantined.

Probation Period

The number of days after an end user is quarantined that additional warnings results in immediate quarantine. This allows administrators to block repeat offenders by limiting their access to the network. When the probation period has passed, the end user can again receive assessment warnings. Setting the probation period to 0 is the same as having no probation period.

Test Sets

Select one or more test sets to run for this assessment configuration. Test sets define which type of assessment to launch against the end-system, what parameters to pass to the assessment server, and what assessment server resources to use.

For networks that use on-board agent-less assessment, you can create a custom Saint scan and add it to your agent-less test set configuration and use it for your end-system assessment.

If you select multiple agent-based test sets, the first test set you select is called the Controller test set. A Controller test set includes the Agent Configuration settings, the Advanced Settings, and all the specified test cases. Each subsequent agent-based test set that you select for the configuration is a "supporting" test set. For supporting test sets, only the "Application" test cases are used; all other configuration values are ignored. In the list of Test Sets, Controller test sets have a "(Master)" designation after them.

For example, you might want to use multiple agent-based test sets if you are managing multiple networks, and you have a unique agent-based test set for each network as well as secondary test sets for specific application tests that all the networks would use. In the assessment configuration for each network, select the unique test set as the Controller test set and then select any number of secondary test sets to be included in the configuration as well.

If the Controller test set is deselected, then a new controller is automatically selected. To specify a different test set as Controller, deselect all test sets, select the desired Controller test set first, and select the additional supporting test sets.

Name

The name of the test set.

Type
: The type of assessment server used in the test set.

Assessment Resources
: Specifies the network assessment servers that perform the assessments for the test set:

- Load Balance All - The assessment load is balanced across all the servers of the specified type on the network.
- Use Assessment Server Pool - As a more granular approach, you can specify an assessment server pool. For example, if you have four agent-less assessment servers, you can put server A and server B in server pool 1, and server C and server D in server pool 2. Then, you can specify which server pool the configuration should use.
- Use Onboard Assessment - The onboard assessment server is used to perform the assessments.

Buttons

Use the configuration menu buttons to perform the following functions:

Used By
: Opens a window that lists all assessment configurations currently using the selected test sets.

Add
: Select to add a new test set.

Edit
: Select to edit the selected test set.

Delete
: Select to delete the selected test set(s).

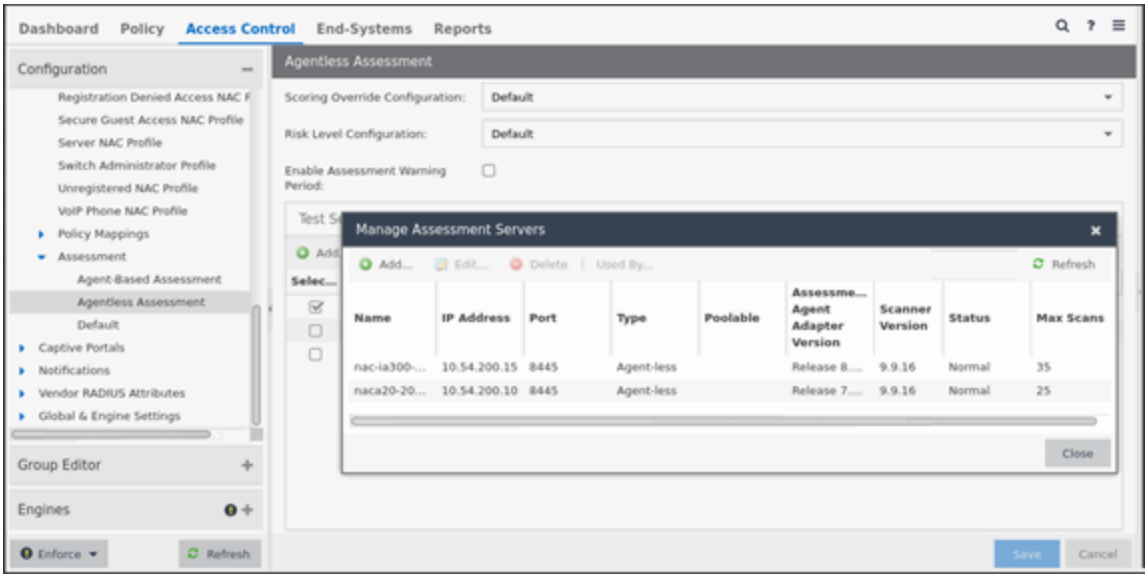
Manage
: Select to open the Manage Assessment Servers window, where you can view and define the assessment servers that are used in your assessment configurations.

- Manage Assessment Servers
- Manage Assessment Settings

Manage Assessment Servers

Use the Manage Assessment Servers window to view and configure the assessment servers that perform the end-system assessments in your network. After you have configured your assessment servers, they can be added to an assessment server pool and participate in assessment server load-balancing, if desired.

Agent-less Assessment Servers are automatically displayed in this window and cannot be edited or deleted. In order to enable your Agent-less Assessment Servers to participate in assessment server load-balancing and server-pools, you must add them manually to this window.



The following columns are included in the Manage Assessment Servers table:

Name

The name of the assessment server. This is the name that is entered when you add an assessment server. For on-board assessment servers, the name is determined by the name of the ExtremeControl engine. For example, if you create an Access Control engine and name it MyAccess Control engine, then the on-board assessment server name is listed as MyAccess Control engine as well.

IP Address

The IP address of the assessment server. This is the IP address entered when you add an assessment server. For on-board assessment servers, the IP address is determined by the address of the Access Control engine. For example, if you create an Access Control engine with an IP address of 10.20.80.8, then the on-board assessment server IP address is listed as 10.20.80.8 as well.

Port

The port number on the assessment server to which the Access Control engine sends assessment requests.

Type

The assessment server type: Agent-less, Nessus, or a FusionAssessmentAgent.

Poolable

A check mark in this column indicates that the assessment server can be part of an assessment server pool. If you have multiple assessment servers on your network, creating assessment server pools enables you to control which assessment server resources are used

for each assessment configuration. External assessment servers are "poolable," however, in order to enable your agent-less on-board assessment servers to participate in server-pools, you must add them manually to this window.

Assessment Agent Adapter Version
The version of assessment agent adapter software that is installed on the assessment server.

Scanner Version
The version of scanner software installed on the assessment server.

Status
When the assessment server is operational, then the status is Normal. Otherwise, this column provides status information regarding an upgrade procedure: Downloading, Download failed, Updating..., Update complete, or Update failed.

Used By Button
Opens a window that lists the assessment server pools currently using the selected assessment servers.

Add Button
Opens the **Add Assessment Serve**r window, where you can define a new assessment server.

Edit Button
Opens the **Edit Assessment Server** window, where you can edit the settings for the selected assessment server. You cannot edit on-board assessment server settings.

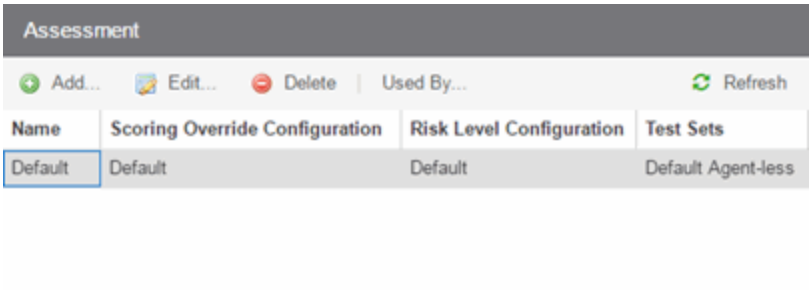
Delete Button
Deletes the selected assessment server. You cannot delete on-board assessment servers or servers that are currently in use.

Refresh Button
Reloads the latest assessment server information in the table. You can also refresh just the version information by right-clicking on a row in the table and selecting **Refresh Version Info**.

Manage Assessment Settings

The Manage Assessment Settings panel is the main panel used to manage and configure the assessment servers performing the end-system assessments in your network. To access this window, select **Access Control Configurations > Access Control Profiles > Assessment** from the menu bar.

Assessment configurations define the different assessment requirements for end-systems connecting to your network. When you create an ExtremeControl profile, you select an assessment configuration that defines the assessment requirements for the end-systems using that profile. You can also select the **Used By** button to view a list of all assessment configurations currently being used by Access Control configurations.



Name

The name of the assessment configuration. This is the name that is entered when you add an assessment configuration in the Edit Assessment Configuration window.

Scoring Override Config

The scoring override configuration for this assessment configuration. The scoring override configuration lets you override the default scoring assigned by the assessment server to a particular assessment test ID.

Risk Level Config

The risk level configuration for this assessment configuration. The risk level configuration determines what risk level is assigned to an end-system (high, medium, or low) based on the end-system's health result details score.

Test Sets

The test sets that runs for this assessment configuration. Test sets define which type of assessment to launch against the end-system, what parameters to pass to the assessment server, and what assessment server resources to use.

Create a Custom Scan for Agent-less Assessment

You can create a custom Saint scan for networks that use on-board agent-less assessment.

The custom scan feature is useful if you are already using Saint assessment and want to integrate existing custom scans into Access Control. It also allows you to create a custom scan with assessment criteria that requires only a limited number of port scans and tests.

To create a custom scan, you must connect to the Saint web service and use the Saint web interface to configure the scan. After you have created the scan, you will be able to add it to your agent-less test set configuration and use it for your end-system assessment.

Use the following steps to create a custom scan:

1. Connect a monitor and keyboard to your ExtremeControl engine, or connect via SSH.
2. From the CLI, "cd" to the directory /opt/nac/saint/saint.

   NOTE: On some ExtremeControl engines, the second Saint directory includes a version number. For example, `/opt/nac/saint/saint-8.5.11`.

3. Start the Saint web service by entering the following command line argument: `./custom_policy_editor.pl -r -h <ip>` where `<ip>` is the IP address of the system that is going to connect to the Saint web service and configure the custom scan (for example, your laptop system).

   NOTE: You cannot run `custom_policy_editor.pl` from any directory. You must "cd" to the directory `/opt/nac/saint/saint`.

4. During the web service start-up, you are asked to create login user names and passwords for two accounts: saint and admin. The accounts are disabled by default, but they become enabled when you provide a password for them. After you complete the start-up by providing the user names and passwords, you are ready to connect to the web service and configure your custom scan.
5. From the connecting system, connect to the Saint web service by entering the following URL in a web browser window: `http://ip of Extreme Access Control engine>:1414`
6. Login using the admin user name and password that you created during the web service startup. (The Welcome screen automatically displays the Saint username and password; you need to change it to the admin username and password.)
7. Select the **Create** option in the Custom Scan Level Selection screen after you have logged in.
8. Create a new scan by entering a name, choosing a template, and selecting the **Add** button.
9. Configure your custom scan by selecting the Vulnerability Checks, Port Scans, and other desired options in the Custom Scan Setup screen. Select **Save** at the bottom of the web page to save your scan. (You might need to scroll down to see this button).
10. The custom scan is created. Close your web browser window.

11. Enter the name of the scan in your agent-less test set in Access Control:
    a. From the Extreme Access Control engine command line, cd to the `/opt/nac/saint/saint/config/policy` directory to determine the name of the scan.

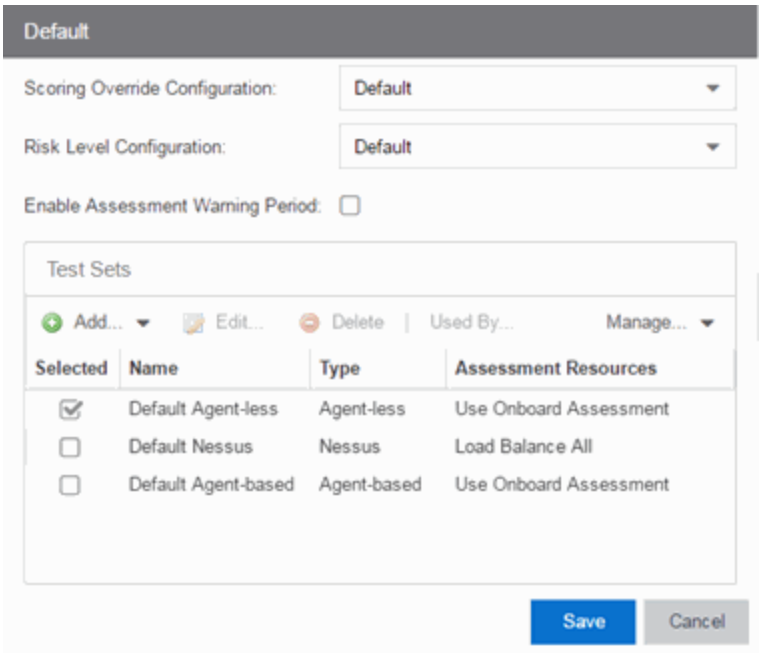
    NOTE: On some ExtremeControl engines, the second Saint directory will include a version number. For example, `/opt/nac/saint/saint-8.5.11/config/policy`.

    b. In the policy directory, there are two files that contain the name of the scan as you entered it in the Saint web interface. For example, if you named the scan "MyCustom," you'll see the following two files in the directory:
    `saint_data_MyCustom.probe`
    and
    `saint_data_MyCustom.conf`.

    In this example, the scan name that you enter into ExtremeControl is saint_data_ MyCustom. You can rename the scan if desired, as long as you rename both the .probe and .conf files. If you rename the scan, enter the new name into Access Control.

    c. Select **Access Control Configurations > Access Control Profiles > Assessment** in the left-hand menu to open the Manage Assessment Settings window.

    d. In the **Assessment Configurations** tab, select any configuration and select **Edit**. The Edit Assessment Configuration window opens. You can also select **Add** to add a new assessment configuration, and then open the Edit Assessment Configuration window.



e. The Test Sets section of the window includes a list of all the test sets available for your assessment configurations. Select the agent-less test set that will be configured to use the custom scan, select the test set you want to configure, and select **Edit**. (Select **Add Agent-less** if you need to create a new test set.)

f. In the Scanning Level section of the Edit Agent-less Test Set window, select **Custom** from the drop-down list and enter the scan name as determined in step b. Select **OK**.

g. The agent-less test set with the custom scan can now be used in your assessment configurations.

- How to Set Up Assessments
- Edit Assessment Configuration

Portal Configuration Overview

If your network is implementing registration or assessment / remediation, you define the branding and behavior of the portal website used by the end user during the registration or assessment/remediation process using a Portal Configuration. ExtremeCloud IQ Site Engine allows you to create two types of portal configurations.

ExtremeControl engines ship with a default Portal Configuration. You can use this default configuration as is, or make changes to the default configuration using this window, if desired.

If you network is using an external captive portal service (for example, ExtremeGuest), use the External configuration type when creating a new portal configuration.

Accessing the Portal Configuration

Use the following steps to access the Portal Configuration:

1. Open the **Control** > **Access Control** tab.
2. In the left-panel, expand **Configuration**.
3. Expand **Captive Portals**.
4. Expand a Portal Configuration.

Default Portal Configuration

The following settings relate to the default type portal configuration:

Network Settings

Use this panel to configure common network web page settings that are shared by both the Assessment / Remediation and the Registration portal web pages.

Administration

Use this panel to configure settings for the Registration Administration web page and grant access to the page for administrators and sponsors.

The Registration Administration web page allows Helpdesk and IT administrators to track the status of registered end-systems, as well as add, modify, and delete registered end-systems on the network.

Website Configuration

Use this tab to configure the common settings used by the different registration web pages, including selecting guest access, authentication settings, and whether assessment and remediation is supported.

Look and Feel

Use the Look and Feel panel to configure common web page settings shared by both the Assessment / Remediation and the Registration portal web pages.

Guest Access and Registration

Guest Web Access provides a way for you to inform guests that they are connecting to your network and lets you display an Acceptable Use Policy (AUP).

Guest Registration forces any new end-system connecting on the network to provide the user's identity in the registration web page before being allowed access to the network.

Secure Guest Access provides secure network access for wireless guests via 802.1x PEAP by sending a unique username, password, and access instructions for the secure SSID to guests via an email address or mobile phone (via SMS text). Secure Guest Access supports both pre-registered guests and guests self-registering through the captive portal. No agent is required.

Authenticated Web Access

Authenticated Web Access provides a way to inform end users that they are connecting to your network and lets you display an Acceptable Use Policy. End users are required to authenticate to the network using the Authenticated Web Access login page. However, end users are only granted one-time network access for a single session, and no permanent end user registration records are stored. Authentication is required each time a user logs into the network, which can be particularly useful for shared computers located in labs and libraries.

Authenticated Registration

Authenticated Registration provides a way for existing corporate end users to access the network on end-systems that don't run 802.1X (such as Linux systems) by requiring them to authenticate to the network using the registration web page. After successful registration, the end-system is permitted access until the registration expires or is administratively revoked.

Assessment / Remediation

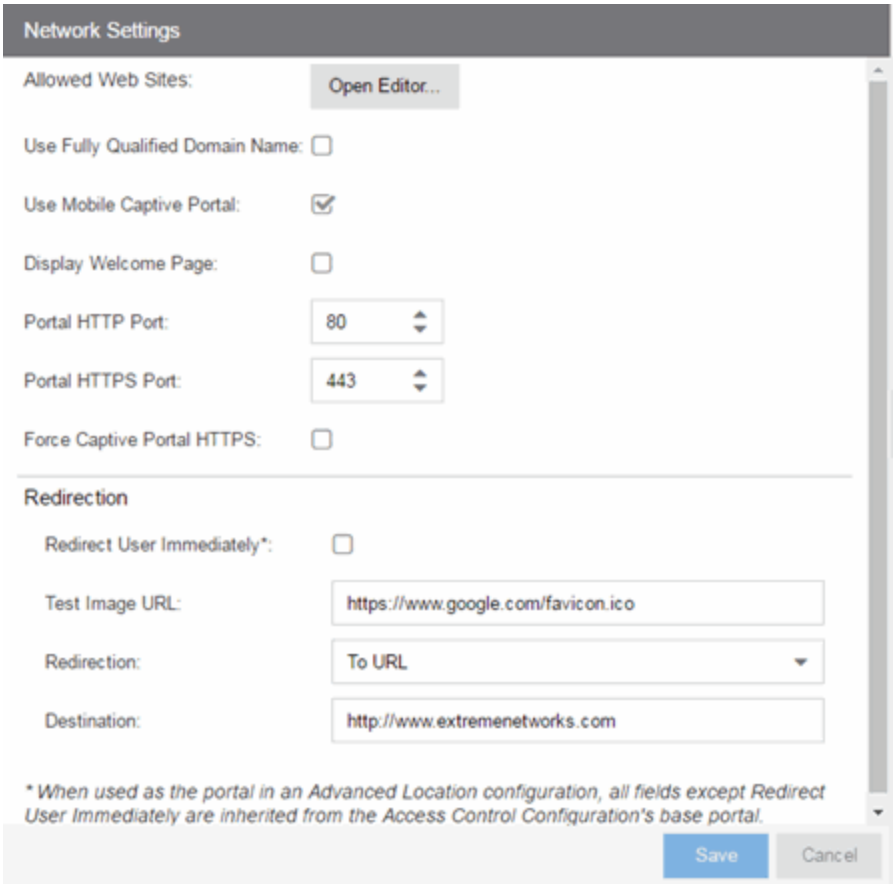
Use this panel to configure settings for the Assessment / Remediation portal web page.

External Captive Portal

Use this tab to configure an external captive portal, outside of ExtremeCloud IQ Site Engine.

Portal Configuration Network Settings

Use this panel to configure common network web page settings that are shared by both the Assessment / Remediation and the Registration portal web pages.



Allowed Web Sites

Select the **Open Editor** button to open the Allowed Web Sites window, where you can configure the web sites that end users are allowed to access during the assessment/remediation and registration process.

Use Fully Qualified Domain Name

Select this checkbox if you would like the URLs in the portal web pages to display the engine's hostname instead of IP address. When this is enabled, the user's browser does a DNS lookup to find the IP address for the fully qualified hostname of the ExtremeControlengine. Enable this option only if all Access Control engines have their hostname defined in DNS.

Portal Redirect to Engine's FQDN

Select this checkbox to redirect web request to the captive portal to the FQDN of the particular engine. Portal redirect allows you to implement a generic captive portal URL with multiple DNS entries, and to use DNS-based high availability and load balancing together with the Open ID based integration. When the user authenticates or registers with Open ID the user must be redirected back to the FQDN of the particular engine.

Use Mobile Captive Portal

Select this checkbox to allow end users using mobile devices to access the network with captive portal registration and remediation. In addition, it allows Helpdesk and IT administrators to track the status of registered end-systems, as well as add, modify, and delete registered end-systems on the network using a mobile device. This feature is supported on the following mobile devices: IPod Touch, IPad, IPhone, Android Phone/Tablet/NetBook, and Windows phones.

Display Welcome Page

Select this checkbox to display the welcome page. If the checkbox is not selected, users bypass the welcome page and access the portal directly.

Portal HTTP Port

Specify which port the ExtremeCloud IQ Site Engine server and Access Control engine use for HTTP web server traffic. Any change does not take effect on the Access Control engine until an Enforce is performed.

Portal HTTPS Port

Specify which port the ExtremeCloud IQ Site Engine server and Access Control engine use for HTTPS web server traffic. Any change does not take effect on the Access Control engine until an Enforce is performed.

Force Captive Portal HTTPS

Select this checkbox to force captive portal web pages to be served securely over HTTPS (instead of HTTP) to end users on the network. It is recommended this checkbox is enabled if Authenticated Registration is configured for the registration process. The default setting is unchecked, specifying to serve the captive portal web pages over HTTP.

Redirect User Immediately

This option redirects end users to the specified test image URL as soon as they have network access. The redirect happens regardless of where the end user is in the connection process. If the end-system's browser can reach the test image URL, then it assumes the end user has network access and redirects the end user out of the captive portal. The test image URL should be an internal image on your own website that end users don't have access to until they're accepted. It is recommended that the test image URL is a link to an SSL site because if the Access Control captive portal is configured for Force Captive Portal HTTPS, the browser does not allow the attempt to an HTTP test image site. It is also recommended that the captive portal policies, (typically the Unregistered, Assessing, and Quarantine policies), are configured to deny HTTPS traffic. This prevents the test image connection attempt from successfully completing and moving the end-system out of the captive portal prematurely. In the event

access to the test image is available, the user may experience the captive portal reverting to the "click here to access the network page", and then upon selecting the link, returning to the previous page based on their state. This behavior continues until the user is finally accepted on the network.

NOTE: If using the portal for an Access Control Advanced Location, all portal configurations are inherited from the Access Control base portal.

Redirection

There are three Redirection options that specify where the end user is redirected following successful registration or remediation, when the end user is allowed on the network:

- **To URL** — This option lets you specify the URL for the web page where the end user is redirected. When selected, the **Destination** field displays, allowing you to indicate the URL of the web page.
- **Disabled** — This option disables redirection. The end user stays on the same web page where they were accepted onto the network.
- **To User's Requested URL** — This option redirects the end user to the web page they originally requested when they connected to the network.

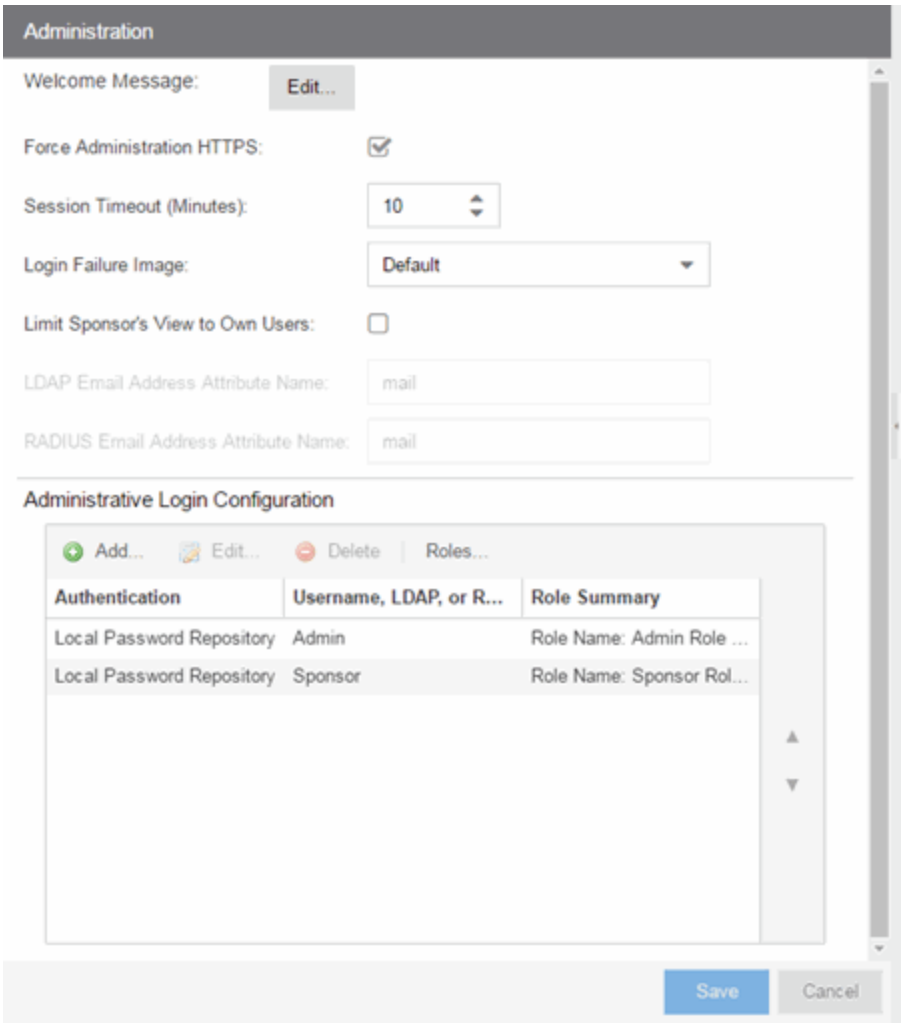
- Portal Configuration Overview

Portal Registration Administration

The Registration Administration web page allows Helpdesk and IT administrators to track the status of registered end-systems, as well as add, modify, and delete registered end-systems on the network.

Administration

Use this panel to configure settings for the Registration Administration web page and grant access to the page for administrators and sponsors.



Administration Web Page Settings

Welcome Message

Select the **Edit** button to open a window where you can modify the message displayed to users when they log into the administration or sponsor portal. The default welcome message is *Registration System Administration*.

Force Administration HTTPS

Select this checkbox to force the administration web page to be served securely over HTTPS (instead of HTTP) to administrators and sponsors on the network. It is recommended this is enabled for additional security.

Session Timeout (Minutes)

This field specifies the length of time an administrator can be inactive on the administration web page before automatically being logged out. The default value is 10 minutes.

Login Failure Image

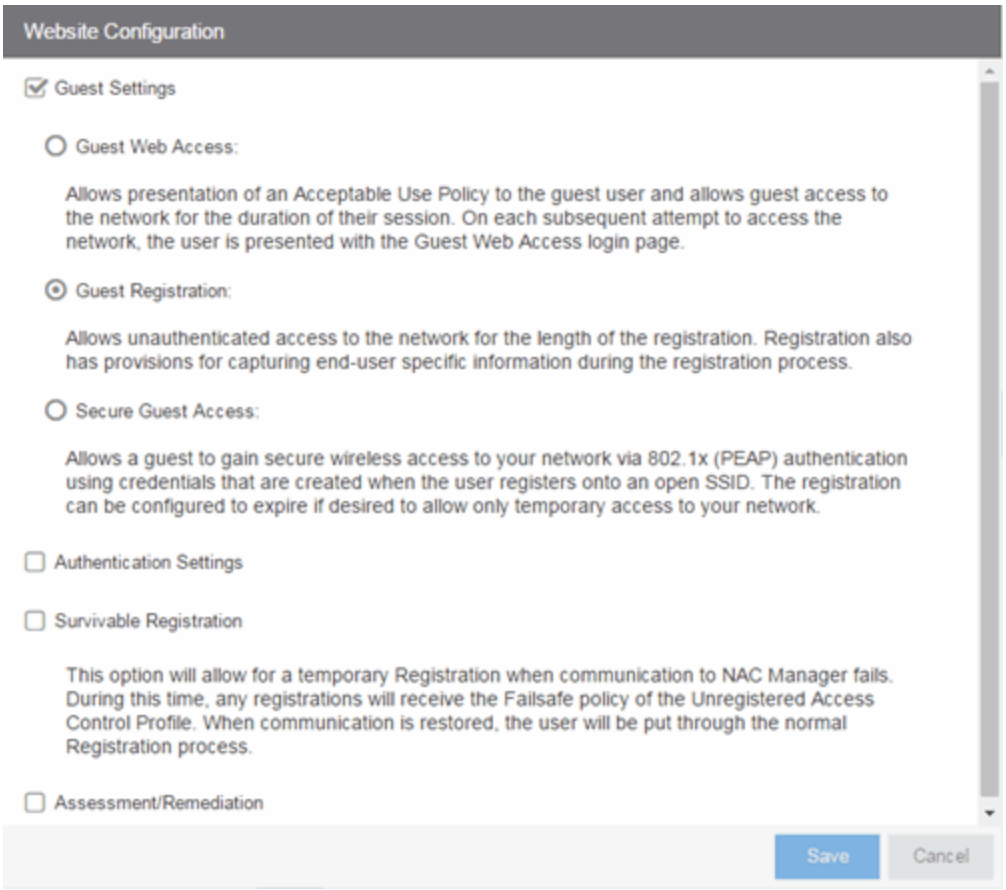
Select an image to display when the end user fails to correctly log in to the web page. The drop-down selection menu displays all the images defined in the Images window for your selection. To add a new image, access the Look & Feel panel.

Limit Sponsor's View to Own Users

Select this checkbox if you want to limit a sponsor's view to only the users they have sponsored. This option is valid only if you configure LDAP or RADIUS authentication of your sponsors. If you select this checkbox, you must enter the **LDAP Email Address Attribute Name** or **RADIUS Email Address Attribute Name** so a sponsor's login name can be matched to their email address, and only the registered users for that sponsor are displayed.

Portal Configuration Website Configuration

Use this tab to configure the common settings used by the different registration web pages, including selecting guest access, authentication settings, and whether assessment and remediation is supported. The options selected in this panel change the panels displayed in the left-panel Website Configuration tree.



Guest Settings

Select the behavior of the web site for users with guest access and the level of access to your network. For additional information, see the Guest Web Access, Guest Registration, and Secure Guest Access sections.

Authentication Settings

Select the behavior of the web site for users with authentication credentials and their level of access to your network. For additional information, see the Authenticated Web Access and Authenticated Registration sections.

Enable Survivable Registration

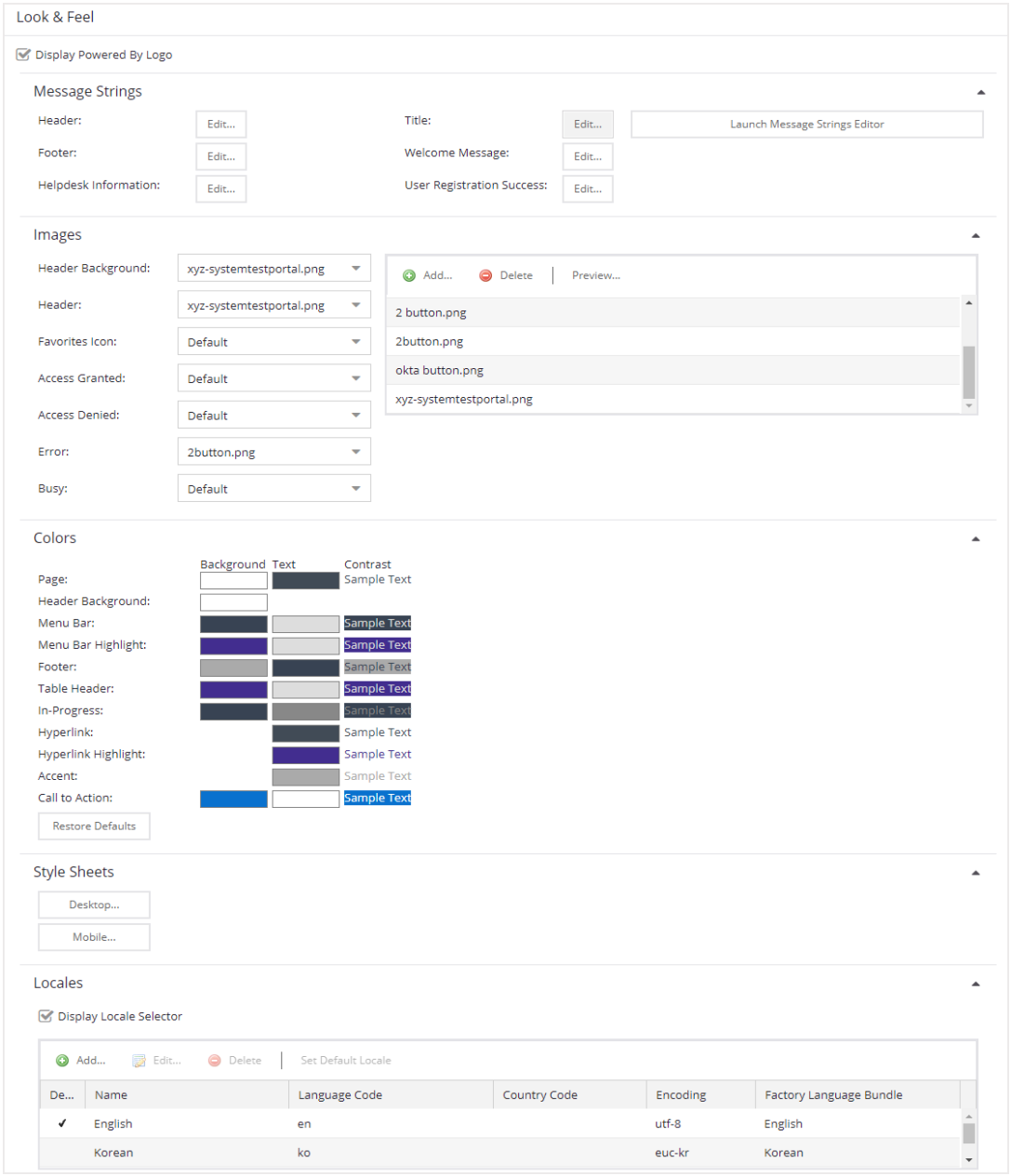
This feature provides temporary Registration for unregistered end-systems when the ExtremeCloud IQ Site Engine server is unreachable. If you select this checkbox, unregistered users that try to register while the ExtremeCloud IQ Site Engine server is unreachable are redirected to the Registration web page. After entering the required information, users are assigned the Failsafe policy and allowed on the network. When the connection to the ExtremeCloud IQ Site Engine server is reestablished, the users are reassigned the Unregistered policy and forced to re-register. If you enable Survivable Registration, make sure that the Failsafe policy provides the appropriate network services for unregistered users.

Assessment/Remediation

Allows you to configure the behavior of the Assessment/Remediation web portal.

Portal Configuration Look & Feel

Use this panel to configure common web page settings shared by both the Assessment and Remediation, as well as the Registration portal web pages.



Display Powered by Logo

Select this check box to display the Extreme Networks logo at the bottom of all of your portal web pages.

Message Strings

Select the **Editor** button to configure each of the fields:

Header

Use to configure the link for the header image displayed at the top of all portal web pages. By default, the header image is configured as the Extreme Networks logo acting as a link to the Extreme Networks website. Text entered in this window can be formatted in HTML.

Footer

Use to configure the footer displayed at the bottom of all portal web pages. By default, the footer is configured with generalized information concerning an organization. Change the *example* text in this section to customize the footer to your own organization. Text entered in this window can be formatted in HTML.

Helpdesk Information

Use to configure the Helpdesk contact information provided to end users in various scenarios during the assessment/remediation and registration process (e.g. an end-system exceeded the maximum number of remediation attempts).

By default, this section is configured with generalized Helpdesk information, such as contact URL, email address, and phone number. Change the *example* text to customize the Helpdesk information for your own organization.

Text entered in this window can be formatted in HTML. In addition, the entire contents of the Helpdesk Information section are stored in the variable "HELPDESK_INFO". By entering "HELPDESK_INFO" (without the quotation marks) in any section that accepts HTML in the Common Page Settings (or any other settings), all information configured in this section will be displayed in place of "HELPDESK_INFO".

Title

Use to modify the text that appears in the title bar of the registration and web access page browser tabs. The default page title is "Enterprise Registration."

Welcome Message

Use to modify the message displayed to users on the menu bar of any registration or web access page. The default welcome message is "Welcome to the Enterprise Network's Registration Center."

User Registration Success

Use to edit the message displayed to users after successfully registering their end-system to the network.

Launch Message Strings Editor

Select to open the Message Strings Editor, where you can modify the message strings that display on any registration or web access page.

Images

Using the drop-down menus, you can specify the image files used in the portal web pages. All image files used for Assessment and Remediation and Registration portal web pages must be defined in this list. The image files defined here are sent to the ExtremeControlengine along with the web page configuration. Use the **Add** button (in the field to the right) to select an image file to add to the list. You can select an image in the list and use the **Preview** button (in the field to the right) to preview the image.

Once an image file is defined, it is available for selection from the configuration drop-down lists (for example, when you configure the Access Granted), and may be referenced in the sections supporting HTML. Available drop-down lists include:

Header Background
Select the background image displayed behind the header image at the top of all portal web pages. The drop-down list displays all the images defined in the Images window for your selection. To add a new image, select **Add** to open the Images window.

Header
Select the image displayed at the top of all portal web pages. The drop-down list displays all the images defined in the Images window for your selection. To add a new image, select **Add** to open the Images window.

Favorites Icon
Select the image displayed as the Favorites icon in the web browser tabs. The drop-down list displays all the images defined in the Images window for your selection. To add a new image, select **Add** to open the Images window.

Access Granted
Select the image displayed when the end user is granted access to the network either based on compliance with the network security policy or upon successful registration to the network. The drop-down list displays all the images defined in the Images window for your selection. To add a new image, select **Add** to open the Images window.

Access Denied
Select the image you would like displayed when the end user has been denied access to the network. The drop-down selection list displays all the images defined in the Images window for your selection. To add a new image, select Manage Images to open the Images window.

Error
Select the image displayed when there is a communication error with the ExtremeCloud IQ Site Engine Server. The drop-down list displays all the images defined in the Images window for your selection. To add a new image, select **Add** to open the Images window.

Busy

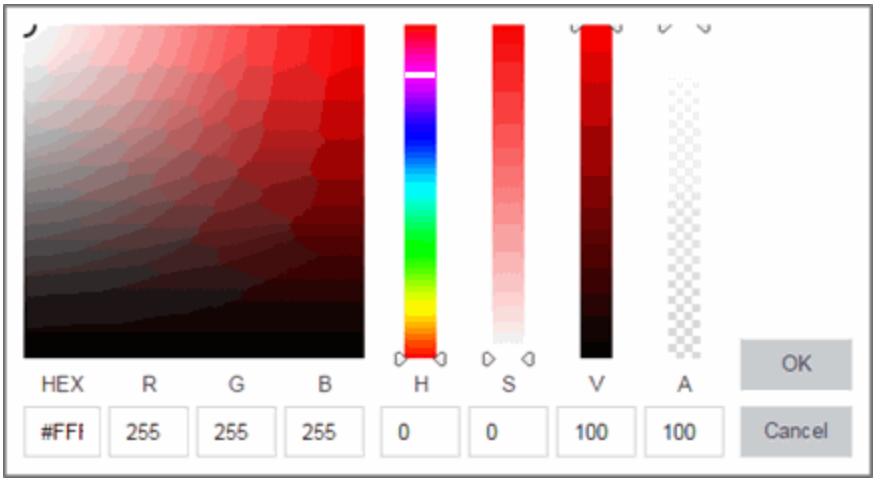
Select the progress bar image displayed to the end user when the web page is busy processing a request. The drop-down list displays all the images defined in the Images window for your selection. To add a new image, select **Add** to open the Images window.

Colors

Select the Background or Text color box corresponding to each item to open the Choose Color window, displayed below, where you can define the colors used in the portal web pages:

- Page — Define the background color and the color of all primary text on the web pages.
- Header Background Color — Define the background color displayed behind the header image.
- Menu Bar — Define the background color and text color for the menu bar.
- Menu Bar Highlight — Define the background color and text color used for the menu bar highlights in the Administration pages.
- Footer — Define the background color and text color for the footer.
- Table Header — Define the background color and text color for the table column headers in the Administrative web pages.
- In-Progress — Define the background color and text color for task in-progress images.
- Hyperlink — Define the color used for hyperlinks on the web pages.
- Hyperlink Highlight — Define the color of a hyperlink when it is highlighted.
- Accent — Define the color used for accents on various parts of the web pages.

Select **OK** to save the changes.



Style Sheets

Select the **Desktop** or **Mobile** buttons to open the Edit Style Sheet window where you can create a style sheet that adds to or overwrites the formatting styles for the portal, or mobile version of the portal web pages, respectively.

Locales

This field lists the locales (languages) presented as options to the user in the captive portal, in addition to the default locale.

Display Locale Selector
Select this check box if you want a locale (language) selector to display as a drop-down list in the menu bar on the captive portal welcome and login pages. This is useful for a shared machine where the users of the machine may speak different languages. (On the mobile captive portal, the selector is displayed as a list of links at the bottom of the welcome screen.)

Default
Indicates the locale is the default language.

Name
The name of the language.

Language Code
The language code associated with the locale.

Country Code
The country code assigned to the locale.

Encoding
The encoding assigned to the locale.

Factory Language Bundle
The language that is assigned to the locale.

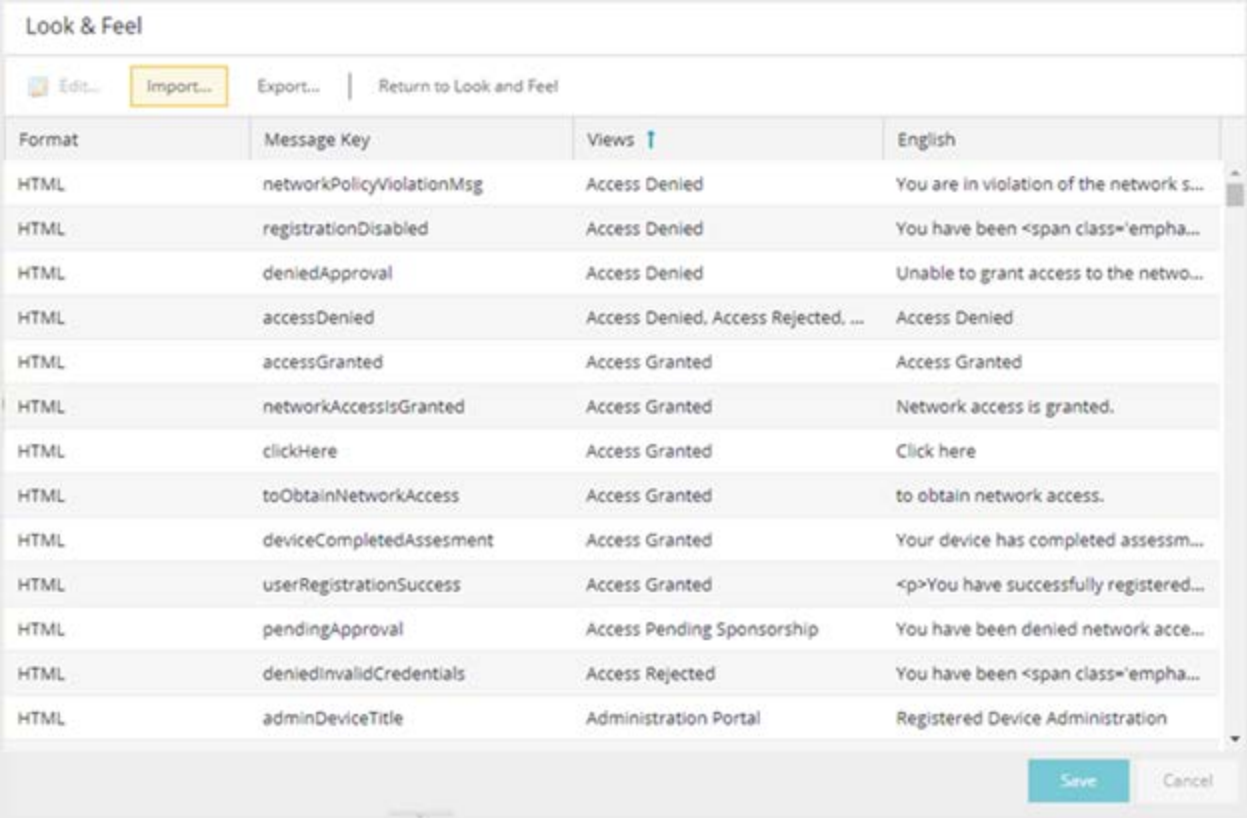
- Portal Configuration Overview

Message String Editor

Use the Message Strings Editor to edit the text and formatting of the various system-defined messages used on the portal web pages or add a custom message string. You can also import a file of message strings or export message strings to a file.

To configure message strings:

1. Select **Control > Access Control**
2. Expand **Configuration**
3. Select **Captive Portals > [portal name] > Website Configuration > Look & Feel**
4. Select **Launch Message Strings Editor**



The Message Strings table displays all the message strings used in ExtremeControl. It includes the following columns:

Format
Displays the supported format for the message text: HTML or Text.

Message Key
The message identifier.

Views
The ExtremeControl portal views where this message is used.

Description
Describes the reason the message is used. Hidden by default.

Variables
Lists variables you can use for the message. Hidden by default.

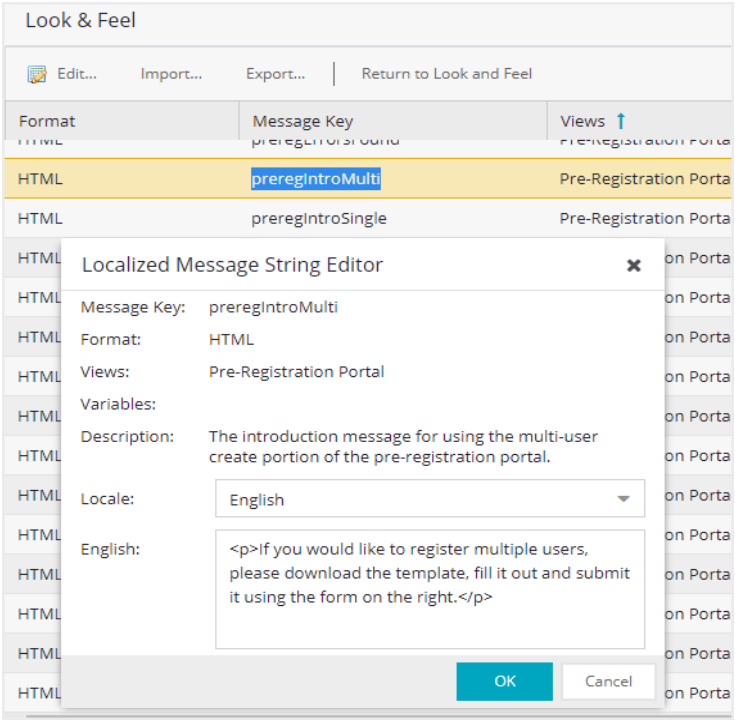
English

The text of the message.

Use the toolbar to add or change message strings, import a file of message strings. or export the message strings to a file. The toolbar functions are:

Edit

Select the key you want to edit. Next, select **Edit** from the toolbar or double-click the key to open the **Localized Message String Editor**.



NOTE: To change the **Message Key** for a user-defined message, you must delete and recreate the message using the new key.

Import

Select to open a window where you can select a file of message strings to import for a selected locale. The list of locales includes the default locale and any locales defined in the portal configuration. Message strings in the file must be in the following format:

`messageKey=messageValue`

with `messageKey` being the message identifier and `messageValue` being the message text.

CAUTION:	Importing message strings from a file overwrites the corresponding default message strings for the selected locale. For example, if you import a file with 15 message entries, only the default messages for those 15 entries are overwritten. The other default messages for that locale remain.

Export

Select to open a window where you can export messages for a selected locale to a file. In the **Export** window, select the locale to export. The list of locales includes the default locale and any locales defined in the portal configuration. Specify the encoding to use:

- Native — Use this encoding if you want to read the file in the native language.
- UTF-8 — Use this encoding to export a file in a readable format that you can share. For example, if you export a French locale file and send it to someone in Japan, the characters display correctly (providing the Japanese system can display French characters).
- UTF-8 with Unicode — Use this encoding to export the file in order to use it (import it) on another ExtremeCloud IQ Site Engine server or client.

NOTE:	Non-ASCII characters are not readable, and it displays as \u####.

Select **Include System-Defined Messages** to include in the export file all the system-defined messages provide by ExtremeControl.

Return to Look and Feel

Select the **Return to Look and Feel** button to redirect back to the **Look & Feel** screen.

Portal Configuration Authenticated Access and Registration

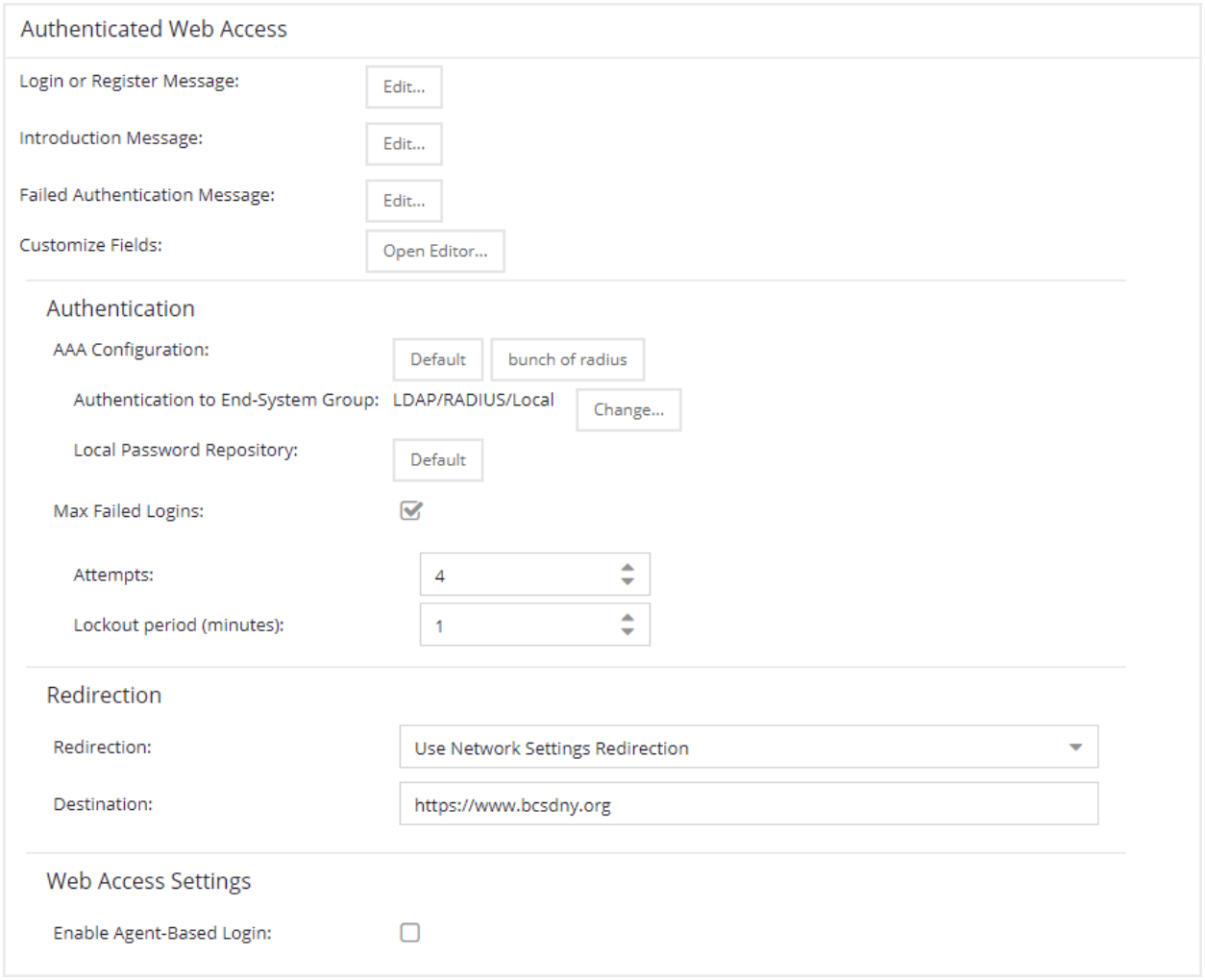
Authenticated web access provides a way to inform end users that they are connecting to your network and lets you display an Acceptable Use Policy. Authenticated registration provides a way for existing corporate end users to access the network on end-systems that don't run 802.1X (such as Linux systems) by requiring them to authenticate to the network using the registration web page.

NOTE: The Authentication and Redirection settings are shared by the Authenticated Web Access and Authenticated Registration access types. Changing them for one type also changes them for the other.

Authenticated Web Access

End users are required to authenticate to the network using the Authenticated Web Access login page. However, end users are only granted one-time network access for a single session, and no permanent end user registration records are stored. Authentication is required each time a user logs into the network, which can be particularly useful for shared computers located in labs and libraries.

Implementing authenticated web access requires web redirection or DNS proxy.



Login or Register Message

Select the **Edit** button to open a window where you can edit the message displayed to the end user when they are registering. By default, the message states that the end user is required to register before being allowed on the network.

Introduction Message

Select the **Edit** button to open a window where you can edit the introductory message displayed to the end user when they are registering. By default, the message states that the end user is agreeing to the terms and conditions in the Acceptable Use Policy.

Failed Authentication Message

Select the **Edit** button to open a window where you can edit the message displayed to the end user if the end user fails authentication. By default, this message advises the end user to contact their network administrator for assistance. Note that the default configuration of the message references the "HELPDESK_INFO" variable which represents the Helpdesk Information that is defined in the Look and Feel Settings.

Customize Fields (Shared)

Select the **Open Editor** button to open the Manage Custom Fields window where you can manage the fields displayed in the Registration web page.

Authentication

AAA Configuration

This section displays the name of the AAA configuration being used by the Access Control configuration and provides a link to open the AAA Configuration window where you can make changes to the AAA Configuration, if desired. If the portal configuration is shared between multiple Access Control Configurations using different AAA configurations, the different AAA configurations are listed here (maximum of 3), allowing you to open the appropriate AAA configuration.

The section also displays the method(s) utilized for validating the credentials entered during registration (LDAP, RADIUS, and/or a Local Password Repository) as specified in the AAA configuration(s).

- **Authentication to End-System Group** — Select the **Change** button to open the User Group to End-System Group Map window where you can map the LDAP/RADIUS/Local User Group to the appropriate end-system group to specify end user access levels. When an end-system group has been mapped to a user group, the icon for the end-system group changes to display a key indicating that it is no longer available for general use. You can use the Move Up/Move Down arrows to set the precedence order for the mappings, allowing you to change the authentication order that takes place during the user authenticated registration.
- **Local Password Repository** — If you are using a local repository, authenticated end users are assigned to the Web Authenticated Users group. Select the **Default** button to open a window where you can edit the Local Password Repository. Multiple links may be listed if there are different repositories associated with different AAA configurations.

Max Failed Logins

Select this checkbox to specify the maximum consecutive number of times an end user can attempt to authenticate on an end-system and fail. You can specify a lockout period that must elapse before the user can attempt to log in again on that end-system.

Redirection

Redirection

There are four Redirection options that specify where the end user is redirected following successful registration, when the end user is allowed on the network. The option selected here overrides the Redirection option specified on the Network Settings.

- **Use Network Settings Redirection** — Use the Redirection option specified on the Network Settings panel.
- **Disabled** — This option disables redirection. The end user stays on the same web page where they were accepted onto the network.
- **To User's Requested URL** — This option redirects the end user to the web page they originally requested when they connected to the network.
- **To URL** — This option lets you specify the URL of the web page to which the end user is redirected. This is typically the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Web Access Settings

Enable Agent-Based Login

If this option is enabled, when the end user connects to the network with an agent installed, the login dialog is displayed in an agent window instead forcing the user to go to the captive portal via a web browser. This allows you to provide authenticated web access without having to set up the captive portal. Agent-based login is useful for shared access end-systems running an agent because it prompts for a login dialog and also provides a logout option. Login credentials are limited to username/password and an Acceptable Use Policy is not displayed.

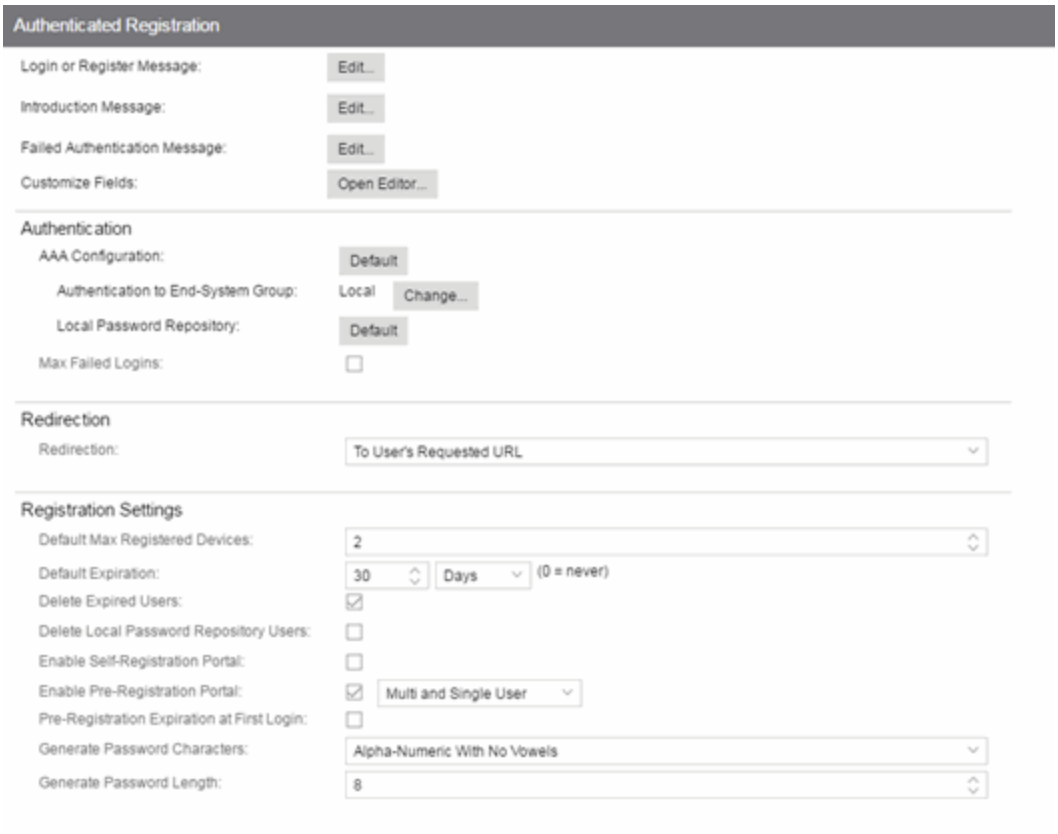
You can customize the messages in the Agent Login window using the Message Strings Editor available in the Look and Feel Settings. Use the agentLoginMessage string to change the message. Any changes you make in the Message Strings Editor override the internationalized messages used in the Agent Login window.

Authenticated Registration

Authenticated registration provides a way for existing corporate end users to access the network on end-systems that don't run 802.1X (such as Linux systems) by requiring them to authenticate to the network using the registration web page. After successful registration, the end-system is permitted access until the registration expires or is administratively revoked.

It is recommended that the Force Captive Portal HTTPS option is enabled if authenticated registration is required for security reasons.

NOTE: If you configure both guest registration and authenticated registration for an area on your network, the end user is presented with a choice on the registration web page whether or not to authenticate.



Login or Register Message

Select the **Edit** button to open a window where you can edit the message displayed to the end user when they are registering. By default, the message states that the end user is required to register before being allowed on the network.

Introduction Message

Select the **Edit** button to open a window where you can edit the introductory message displayed to the end user when they are registering. By default, the message states that the end user is agreeing to the terms and conditions in the Acceptable Use Policy.

Failed Authentication Message

Select the **Edit** button to open a window where you can edit the message displayed to the end user if the end user fails authentication. By default, this message advises the end user to contact their network administrator for assistance. Note that the default configuration of the message references the "HELPDESK_INFO" variable which represents the Helpdesk Information that is defined in the Look and Feel Settings.

Customize Fields (Shared)

Select the **Open Editor** button to open the Manage Custom Fields window where you can manage the fields displayed in the Registration web page.

Authentication

These settings are shared by the Authenticated Web Access and Authenticated Registration access types. Changing them for one type also changes them for the other.

AAA Configuration

This section displays the name of the AAA configuration being used by the Access Control configuration and provides a link to open the AAA Configuration window where you can make changes to the AAA Configuration, if desired. If the portal configuration is shared between multiple Access Control Configurations using different AAA configurations, the different AAA configurations are listed here (maximum of 3), allowing you to open the appropriate AAA configuration.

The section also displays the method(s) utilized for validating the credentials entered during registration (LDAP, RADIUS, and/or a Local Password Repository) as specified in the AAA configuration(s).

- **Authentication to End-System Group** — Select the **Change** button to open the User Group to End-System Group Map window where you can map the LDAP/RADIUS/Local User Group to the appropriate end-system group to specify end user access levels. When an end-system group has been mapped to a user group, the icon for the end-system group changes to display a key indicating that it is no longer available for general use. You can use the Move Up/Move Down arrows to set the precedence order for the mappings, allowing you to change the authentication order that takes place during the user authenticated registration.
- **Local Password Repository** — If you are using a local repository, authenticated end users are assigned to the Web Authenticated Users group. Select the **Default** button to open a window where you can edit the Local Password Repository. Multiple links may be listed if there are different repositories associated with different AAA configurations.

Max Failed Logins

Select this checkbox to specify the maximum consecutive number of times an end user can attempt to authenticate on an end-system and fail. You can specify a lockout period that must elapse before the user can attempt to log in again on that end-system.

OpenID Registration

Select this checkbox to enable OpenID. Edit the OpenID Registration configuration to support Entra ID or Keycloak authentication registration.

Redirection

These settings are shared by the Authenticated Web Access and Authenticated Registration access types. Changing them for one type also changes them for the other.

Redirection

There are four Redirection options that specify where the end user is redirected following successful registration, when the end user is allowed on the network. The option selected here overrides the Redirection option specified on the Network Settings.

- **Use Network Settings Redirection** — Use the Redirection option specified on the Network Settings.
- **Disabled** — This option disables redirection. The end user stays on the same web page where they were accepted onto the network.
- **To User's Requested URL** — This option redirects the end user to the web page they originally requested when they connected to the network.
- **To URL** — This option lets you specify the URL of the web page to which the end user is redirected. This is typically the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Registration Settings

The Generate Password Character and Generate Password Length settings are shared by Authenticated Registration and Secure Guest Access.

Default Maximum Registered Devices

Specify the maximum number of MAC addresses each authenticated end user is allowed to register on the network. If a user attempts to register an additional MAC address that exceeds this count, an error message is displayed in the Registration web page stating that the maximum number of MAC addresses is registered to the network and to call the Helpdesk for further assistance. The default value for this field is 2.

Default Expiration

Enter a value and select a unit of time to configure the amount of time before an end user's registration automatically expires. When the registration expires, the end user is either suspended (registration must be manually approved by administrator/sponsor) or permanently deleted from the registration list. If a registration is deleted, the end-user must re-enter all their required personal information the next time they attempt to access the network. Individual registration expiration time can also be set by the administrator/sponsor through the Registration Administration web page.

Delete Expired Users

Select this checkbox to delete a user from the Registered users list in the Registration Administration web page when their registration expires. If a registration is deleted, the end-user must re-enter all their required personal information the next time they attempt to access the network.

Check Session Validity in Entra ID

Select this checkbox to enable Entra ID Registered User Status Monitor for this captive portal. This option only applies if OpenID Registration is used. This feature needs to be configured in

Administration > Options > Access Control > Entra ID Registered User Status Monitor. For more information, see Entra ID Registered User Status Monitor

Delete Local Password Repository Users

If you select **Delete Expired Users**, then selecting this checkbox also deletes the expired user from the local password repository.

Enable Self-Registration Portal

This checkbox allows an authenticated and registered user to be directed to a URL (provided by an administrator) to self-register additional devices that may not support authentication (such as Linux machines) or may not have a web browser (such as game systems). For example, a student may register to the network using their PC. Then, using a self-registration URL provided by the system administrator, they can register their additional devices. When the additional devices have been registered, the student can access the network using those devices. The URL for the Self Registration web page is `https://<Access ControlEngineIP>/self_registration`. You can change the instructions displayed on this web page using the Message Strings Editor on the Look and Feel Settings; select the selfRegIntro message string.

Enable Pre-Registration Portal

Select this checkbox to enable pre-registration functionality. With pre-registration, guest users can be registered in advance, allowing for a more streamlined and simple registration process when the guest user connects to the network. This is useful in scenarios where guest users are attending a company presentation, sales seminar, or a training session. From the drop-down list, select whether you want to pre-register a single user (when you want to pre-register one user at time) or multiple users (when you have a larger group of users to pre-register) or both. For more information, see How to Configure Pre-Registration.

Pre-Registration Expiration at First Login

Select this checkbox to set the **Default Expiration** of a pre-registered user to begin when the user first registers a device, instead of setting it the moment the pre-registered user is created (added via the pre-registration administration process). Select **Enable Pre-Registration Portal** to enable this option. For more information, see How to Configure Pre-Registration.

NOTE: This option is only valid when importing a CSV file to pre-register multiple users in the Pre-Registration Portal and not when entering information for a single user.

Generate Password Characters

This option is available if you select **Enable Pre-Registration Portal**. During the pre-registration process, ExtremeCloud IQ Site Engine can automatically generate the password that the guest user uses when connecting to the network. The password is generated according to the specification selected here. This setting is shared by Authenticated Registration and Secure Guest Access. Changing it for one access type also changes it for the other.

Generate Password Length

This option is available if you select **Enable Pre-Registration Portal**. During the pre-registration process, ExtremeCloud IQ Site Engine can automatically generate the password that the guest user uses when connecting to the network. The password length is generated according to the number of characters specified here.

- Portal Configuration Overview

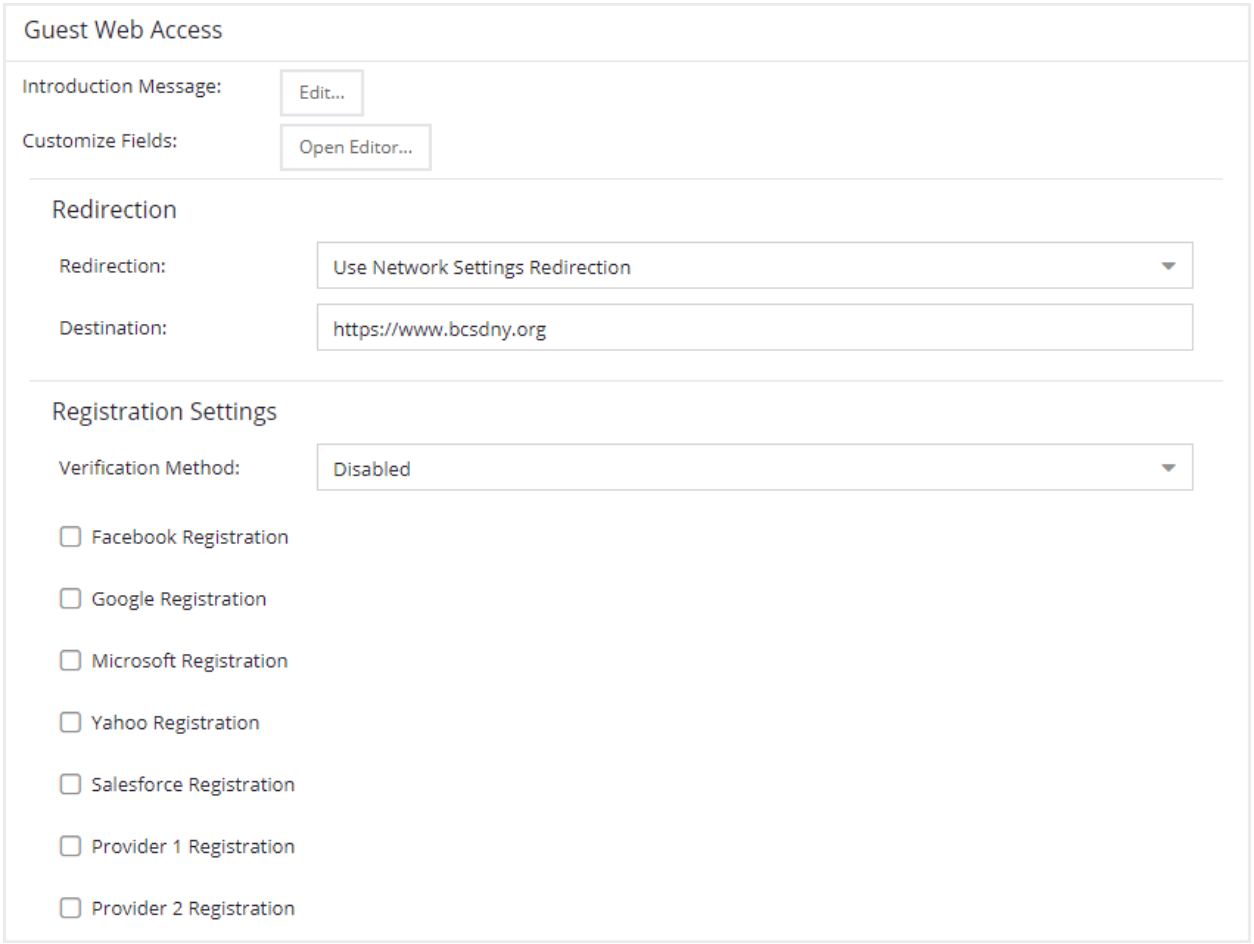
Portal Configuration Guest Access

Guest Web Access provides a way for you to inform guests that they are connecting to your network and lets you display an Acceptable Use Policy (AUP).

End users are initially redirected to the captive portal when they first connect to the network. After the user enters the required information on the Guest Web Access login page (typically, their name and email address), they are allowed access on the network according to the assessment and authorization defined in the Guest Access profile.

Guest web access provides a single session, and no permanent end user records are stored. This provides increased network security, and also allows you to minimize the number of registration records stored in the ExtremeCloud IQ Site Engine database.

Implementing guest web access requires web redirection or DNS proxy.



Introduction Message

Select the **Edit** button to open a window where you can edit the introductory message displayed to end users when gaining web access as guests. It may include an introduction to the network and information stating that the end user is agreeing to the Acceptable Use Policy (AUP) for the network upon registering their device. A link to the URL that contains the full terms and conditions of the network's AUP can be provided from this introductory message. Note that the URL for this link must be added as an Allowed URL in the Allowed Web Sites window accessed from the Network Settings. By configuring the introductory message with this information, end users can be held accountable for their actions on the network in accordance with the terms and conditions set forth by the network's AUP. This message is shared by Guest Web Access and Guest Registration. Changing it for one access type also changes it for the other.

Customize Fields

Select the **Open Editor** button to open the Manage Custom Fields window where you can manage the fields displayed in the Guest Web Access login page. These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing them for one access type also changes them for the others.

Redirection (Shared)

There are four Redirection options that specify where the end user is redirected following successful access, when the end user is allowed on the network. The option selected here overrides the Redirection option specified on the Network Settings. This setting is shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing it for one access type also changes it for the others.

- **Use Network Settings Redirection** — Use the Redirection option specified on the Network Settings.
- **Disabled** — This option disables redirection. The end user stays on the same web page where they were accepted onto the network.
- **To User's Requested URL** — This option redirects the end user to the web page they originally requested when they connected to the network.
- **To URL** — This option lets you specify the URL for the web page where the end user will be redirected. This would most likely be the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Registration Settings

Verification Method

User verification requires that guest end users registering to the network enter a verification code that is sent to their email address or mobile phone (via SMS text) before gaining network access. This ensures that network administrators have at least one way to contact the end user. For more information and complete instructions, see How to Configure Verification for Guest Registration.

Select from the following verification methods:

- **Email** — The end user must enter an email address in the Guest Web Access login page. The Email Address field must be set to **Required** in the Manage Custom Fields window.
- **SMS Gateway** — The end user must enter a mobile phone number in the Guest Web Access login page. The Phone Number field must be set to **Required** in the Manage Custom Fields window.
- **SMS Gateway or Email** — The end user must enter a mobile phone number or email address in the Guest Web Access login page. The Phone Number and Email Address fields must be set to **Visible** in the Manage Custom Fields window.
- **SMS Text Message** — The end user must enter a mobile phone number in the Guest Web Access login page. The Phone Number field must be set to **Required** in the Manage Custom Fields window.
- **SMS Text or Email** — The end user must enter either a mobile phone number or email address in the Guest Web Access login page. The Phone Number and Email Address fields must be set to **Visible** in the Manage Custom Fields window.

If you have selected the "SMS Text Message" or the "SMS Text or Email" Verification method: select the Service Providers **Edit** button (below the verification method) to configure the list of mobile service providers from which end users can select the Registration web page. This setting allows ExtremeControl to correctly format the email address to which to send an email. This email is then received by the service provider and converted to an SMS text which is sent the user. The default configuration provides lists of the major US cellular service providers.

NOTE: Not all cellular service providers provide a way to send SMS text messages via email.

If you have selected the "SMS Gateway" or "SMS Gateway or Email" method: enter the SMS Gateway Email address provided by the SMS Gateway provider.

For all methods: use the Message Strings **Edit** button (below the verification method) to open the Message Strings Editor and modify the registration verification messages displayed to the user during the verification process. For example, if you have selected **Email**, you need to modify the "registrationVerificationEmailSentFromAddress" message string to be the appropriate email address for your company.

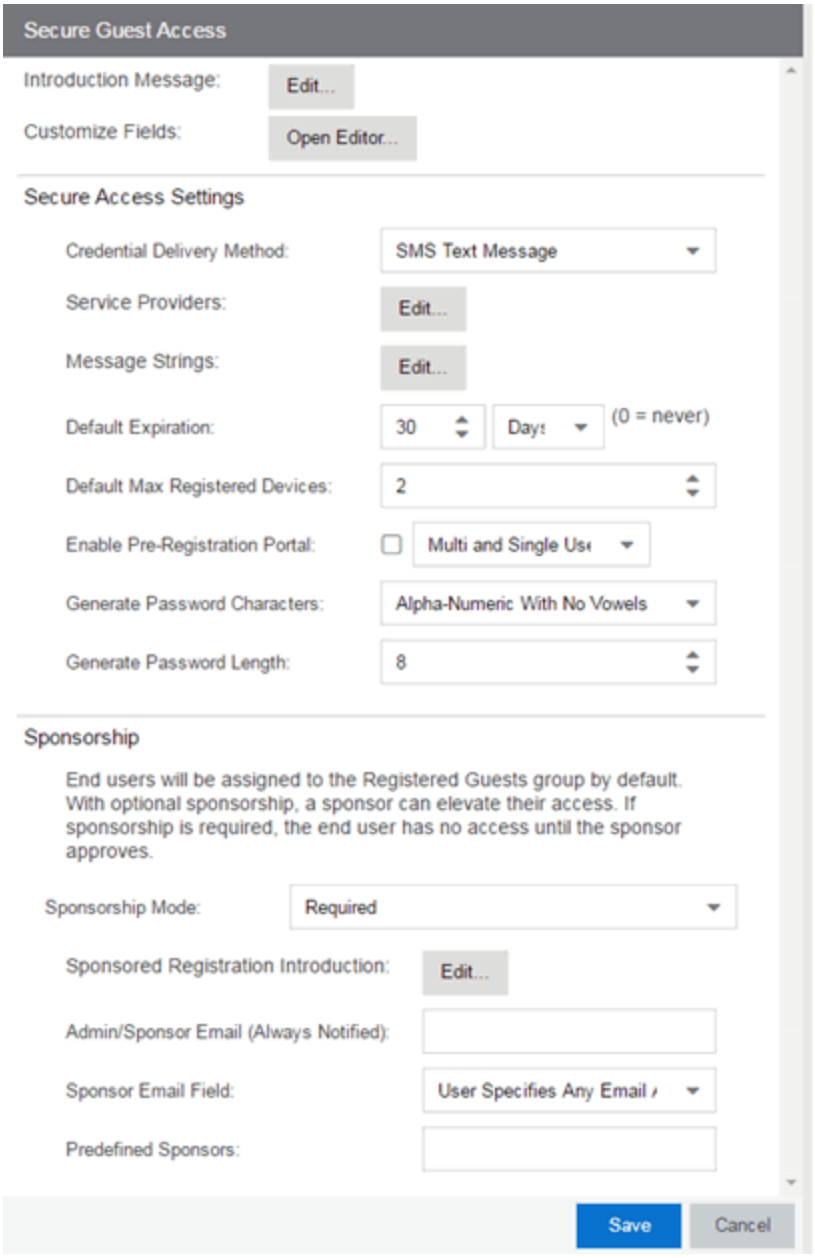
For all methods: set the Verify Pin Characters and Verify Pin Length options to define the characteristics and length of the verification code that is sent to the guest end user. This setting is shared by Guest Registration and Guest Web Access. Changing it for one access type also changes it for the other.

Secure Guest Access

Secure Guest Access provides secure network access for wireless guests via 802.1x PEAP by sending a unique username, password, and access instructions for the secure SSID to guests via an email address or mobile phone (via SMS text). Secure Guest Access supports both pre-registered guests and guests self-registering through the captive portal. No agent is required.

Here are three scenarios where Secure Guest Access provides increased network security:

- An enterprise provides secure guest access for visitors. Guests self-register through the captive portal and receive connection credentials and instructions for the secure SSID via a text message on their mobile phone.
- A hospitality company provides guests with secure Internet access using pre-registration. A receptionist generates a voucher using the ExtremeControl pre-registration portal. The voucher is handed to the guest, providing them with instructions and credentials for connecting directly to the secure SSID.
- An enterprise provides secure guest access with the option of elevated access through employee sponsors. Guests self-register through the captive portal and receive connection credentials and instructions via a text message. Sponsors approve guests for secure guest access. Later, sponsors can elevate guest access using the sponsorship portal.



Introduction Message

Select the **Edit** button to open a window where you can edit the introductory message displayed to end users when registering as guests. It may include an introduction to the network and information stating that the end user is agreeing to the Acceptable Use Policy (AUP) for the network upon registering their device. A link to the URL that contains the full terms and conditions of the network's AUP can be provided from this introductory message. Note that the URL for this link must be added as an Allowed URL in the Allowed Web Sites window accessed from the Network Settings. By configuring the introductory message with this information, end users can be held accountable for their actions on the network in accordance with the terms and conditions set forth by the network's AUP. This message is

shared by Guest Web Access and Guest Registration. Changing it for one access type also changes it for the other.

Customize Fields

Select the **Open Editor** button to open the Manage Custom Fields window where you can manage the fields displayed in the Registration web page. These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing them for one access type also changes them for the others.

Secure Access Settings

Credential Delivery Method

Select the method that will be used to send guests their credentials and access instructions for the secure SSID. For more information and complete instructions, see How to Configure Credential Delivery for Secure Guest Access.

- **Captive Portal** — The credential information displays on the Registration web page.
- **Email** — The end user must enter an email address in the Registration web page. The Email Address field must be set to **Required** in the Manage Custom Fields window.
- **SMS Gateway** — The end user must enter a mobile phone number in the Registration web page. The Phone Number field must be set to **Required** in the Manage Custom Fields window.
- **SMS Gateway or Email** — The end user must enter a mobile phone number or email address in the Registration web page. The Phone Number and Email Address fields must be set to **Visible** in the Manage Custom Fields window.
- **SMS Text Message** — The end user must enter a mobile phone number in the Registration web page. The Phone Number field must be set to **Required** in the Manage Custom Fields window.
- **SMS Text or Email** — The end user must enter either a mobile phone number or email address in the Registration web page. The Phone Number and Email Address fields must be set to **Visible** in the Manage Custom Fields window.

If you have selected the "SMS Text Message" or the "SMS Text or Email" Verification method: select the Service Providers **Edit** button (below the verification method) to configure the list of mobile service providers from which end users can select the Registration web page. This setting allows ExtremeControl to correctly format the email address to which to send an email. This email is then received by the service provider and converted to an SMS text which is sent the user. The default configuration provides lists of the major US cellular service providers.

NOTE: Not all cellular service providers provide a way to send SMS text messages via email.

If you have selected the "SMS Gateway" or "SMS Gateway or Email" method: enter the

SMS Gateway Email address provided by the SMS Gateway provider.

For all methods: use the Message Strings **Edit** button (below the verification method) to open the Message Strings Editor and modify the registration verification messages displayed to the user during the verification process. For example, if you have selected "Email", you need to modify the "secureGuestAccessEmailSentFromAddress" message string to be the appropriate email address for your company.

Default Expiration

Enter a value and select a unit of time to configure the amount of time before an end user's registration automatically expires. When the registration expires, the end user is either suspended (registration must be manually approved by administrator/sponsor) or permanently deleted from the guest registration list. If a registration is deleted, the end-user must re-enter all their personal information the next time they attempt to access the network. Individual expiration time can also be set by the sponsor.

Default Max Registered Devices

Specify the maximum number of MAC addresses each authenticated end user is allowed to register on the network. If a user attempts to register an additional MAC address that exceeds this count, an error message is displayed in the Registration web page stating that the maximum number of MAC addresses has already been registered to the network and to call the Helpdesk for further assistance. The default value for this field is 2.

Enable Pre-Registration Portal

Use this checkbox to enable Pre-Registration functionality. With pre-registration, guest users can be registered in advance, allowing for a more streamlined and simple registration process when the guest user connects to the network. This can be particularly useful in scenarios where guest users will be attending a company presentation, sales seminar, or a training session. From the drop-down list, select whether you want to pre-register a single user (when you want to pre-register one user at time) or multiple users (when you have a larger group of users to pre-register) or both. For more information, see How to Configure Pre-Registration.

Generate Password Characters (Shared)

ExtremeControl uses this option when generating passwords for guest users who are either self-registering or are pre-registered, to use when connecting to the network. This setting is shared by Authenticated Registration and Secure Guest Access. Changing it for one access type also changes it for the other.

Generate Password Length (Shared)

NAC Manager will use this option when generating passwords for guest users who are either self-registering or are pre-registered, to use when connecting to the network. The password length is generated according to the number of characters specified here. This setting is shared by Authenticated Registration and Secure Guest Access. Changing it for one access type also changes it for the other.

Sponsorship

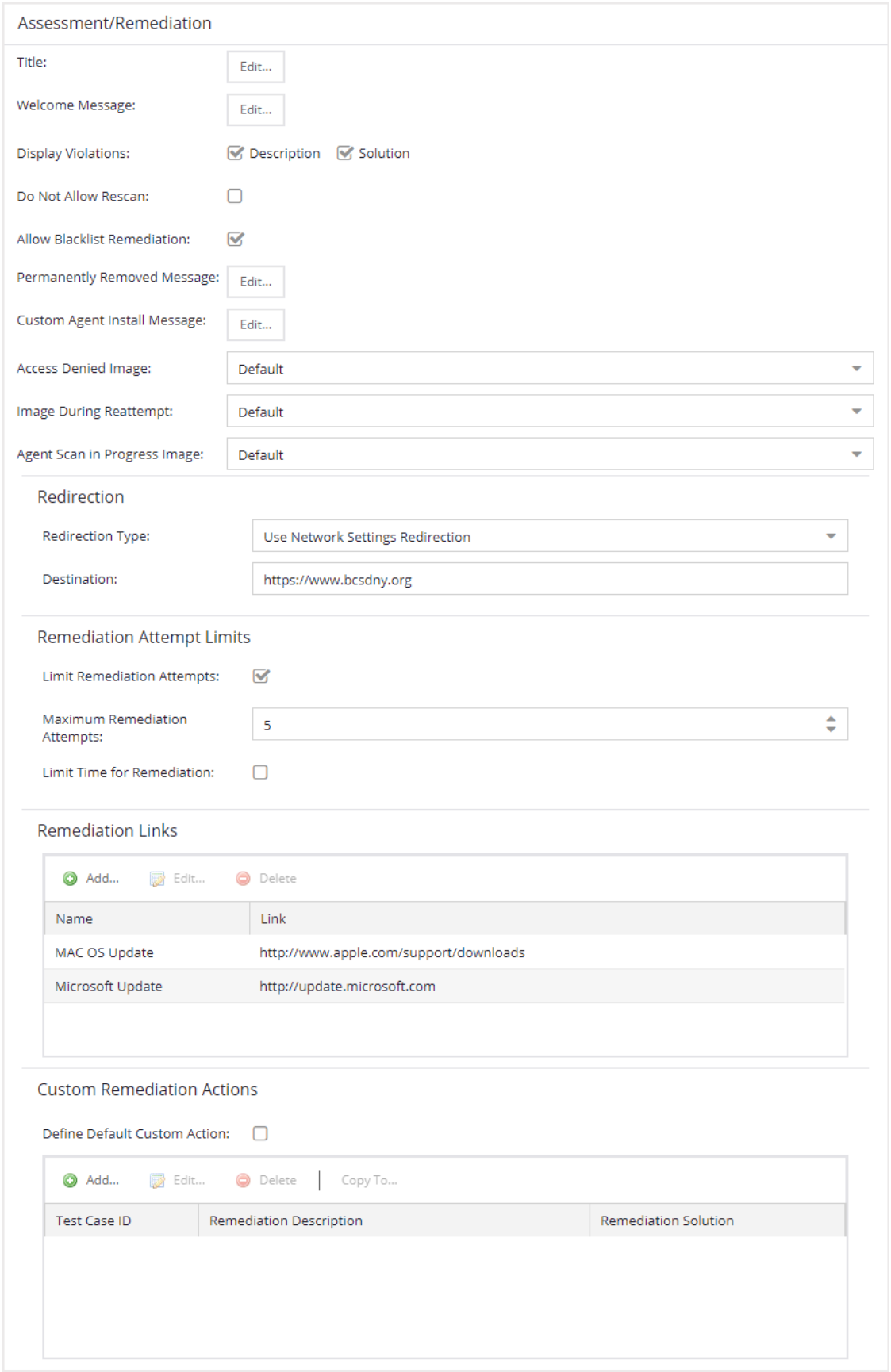
Use this section to configure sponsorship for Secure Guest Access registration. Select the Sponsorship Mode required. Additional settings are displayed if you select optional or required sponsorship. For information on each option, see How to Configure Sponsorship for Guest Registration.

With sponsored registration, end users are only allowed to register to the network when approved by a "sponsor," an internal trusted user to the organization. Sponsorship can provide the end user with a higher level of access than just guest access and allows the sponsor to fine-tune the level of access for individual end users. The end user registers and declares a sponsor's email address. The sponsor is notified and approves the registration, and can assign an elevated level of access, if desired.

- Portal Configuration Overview

Portal Configuration Assessment / Remediation

Use this panel to configure settings for the Assessment/Remediation portal web page. Also, the Network Settings and Look and Feel panels provide you access to common settings that are shared by the Assessment/Remediation portal web page.


Assessment/Remediation
Title:
Edit...
Welcome Message:
Edit...
Display Violations:
Description
Solution
Do Not Allow Rescan:
Allow Blacklist Remediation:
Permanently Removed Message:
Edit...
Custom Agent Install Message:
Edit...
Access Denied Image:
Default
Image During Reattempt:
Default
Agent Scan in Progress Image:
Default
Redirection
Redirection Type:
Use Network Settings Redirection
Destination:
https://www.bcsdny.org
Remediation Attempt Limits
Limit Remediation Attempts:
Maximum Remediation Attempts:
5
Limit Time for Remediation:
Remediation Links
Add...
Edit...
Delete
Name
Link
MAC OS Update
http://www.apple.com/support/downloads
Microsoft Update
http://update.microsoft.com
Custom Remediation Actions
Define Default Custom Action:
Add...
Edit...
Delete
Copy To...
Test Case ID
Remediation Description
Remediation Solution

Web Page Settings

Title

Select the **Edit** button to open a window where you can modify the message displayed in the title bar of the Assessment/Remediation web pages. The default page title is "Enterprise Remediation."

Welcome Message

Select the **Edit** button to open a window where you can modify the message displayed in the banner at the top of the Assessment/Remediation web page. The default welcome message is "Welcome to the Enterprise Remediation Center."

Display Violations

Use the checkboxes to select the assessment violation information that displays to the end user:

- **None** — No violations are displayed to the web page. This option might be used for an Access Controlengine that is serving web pages to guest users, when you do not want the guest users to attempt to remediate their end-system.
- **Description** — Only the description is displayed for violations. This provides the end user with information concerning what violation was found, but no information concerning how it can be fixed. Use this configuration in scenarios where the user population of the network does not possess technical IT knowledge and is not expected to self-remediate. It provides the Helpdesk personnel with technical information about the violation when the end user places a call to the Helpdesk.
- **Solution** — Only the solution is displayed for violations, enabling the end user to perform self-service remediation without knowing what the violation is. Use this configuration in scenarios where the user population on the network does not possess technical IT knowledge but is expected to self-remediate.
- **Description and Solution** — Both the description and solution are displayed for violations. This provides the end user with information concerning what violation was found and how to fix it. Providing complete information concerning the violation gives the end user the best chance of self-remediation, however, the technical details of the violation can result in end user confusion. Therefore, use this configuration in scenarios where the user population of the network possesses more technical IT knowledge.

Do Not Allow Rescan

Select this checkbox if you do not want the end-user to have the ability to initiate a rescan of their end-system when quarantined. When selected, the **Reattempt Network Access** button is removed from the Assessment/Remediation web page, and the user is not provided with any way to initiate a rescan on-demand for network access. The end user is forced to contact the Help Desk for assistance. You can edit the "Permanently Removed Message" which, by default, advises the end user to contact the Helpdesk to obtain access to the network. Note that the default configuration of the "Permanently Removed Message" references the "HELPDESK_INFO"

variable which represents the Helpdesk Information that is defined in the Look and Feel Settings.

Allow Blacklist Remediation

Select this checkbox if you want black-listed end users to have the ability to remediate their problem and attempt to reconnect to the network. When selected, a "Reattempt Network Access" button is added to the blocked list web page, enabling end users to remove themselves from the blocked list and reauthenticate to the network.

Permanently Removed Message

Select the **Edit** button to open a window where you can modify the message displayed when users can no longer self-remediate and must contact the Help Desk for assistance. Note that the default message references the "HELPDESK_INFO" variable which represents the Helpdesk Information that is defined in the Look and Feel Settings.

Custom Agent Install Message

Select the **Edit** button to open a window where you can create a message containing additional agent install information to add to the default text on the Install Agent portal web page.

Access Denied Image

Select the image you want displayed when the end user is quarantined and denied access to the network. The drop-down list displays all the images defined in the Images window for your selection.

Image During Reattempt

Select the image you want displayed when the end-user is reattempting network access after they repair their system. The drop-down list displays all the images defined in the Images window for your selection.

Agent Scan in Progress Image

Select the progress bar image you want displayed while the end-user is being scanned. The drop-down list displays all the images defined in the Images window for your selection.

Redirection

There are four Redirection options that specify where the end-user is redirected following successful remediation, when the end-user is allowed on the network. The option selected here overrides the Redirection option specified in the Network Settings for Remediation only.

- **Use Network Settings Redirection** — Use the Redirection option specified in the Network Settings.
- **Disabled** — This option disables redirection. The end-user stays on the same web page where they were accepted onto the network.
- **To User's Requested URL** — This option redirects the end user to the web page they originally requested when they connected to the network.

- **To URL** — This option lets you specify the URL of the web page to which the end-user is redirected. This is typically the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Remediation Attempt Limits

Limit Remediation Attempts

Select this checkbox to limit the maximum number of times an end-user is allowed to initiate a rescan of their end-system after initially being quarantined, in an attempt to remediate their violations. If selected, enter the number of attempts allowed.

Limit Time for Remediation

Select this checkbox to limit the total interval of time an end user is allowed to initiate a rescan of their end-system after initially being quarantined, in an attempt to remediate their violations. If selected, enter the amount of time in minutes.

Remediation Links

This table lists the links displayed on the Assessment/Remediation web page for the end users to use to remediate their end-system violations. There are two default remediation links: Microsoft Support and MAC OS Support. Use this tab to add additional links such as an internal website for patches. Links must contain a valid protocol prefix (http://, https://, ftp://).

Select **Add** to open a window where you can define a new link's name and URL. Select a link and select **Edit** to edit the link's information. Select **Delete** to remove a URL from the table.

Custom Remediation Actions

Use this table to create your own custom remediation action for a particular violation to use in place of the remediation action provided by the assessment server.

Use the following steps to add a custom remediation action:

1. Select the **Add** button to open the Add Custom Remediation Action window.
2. Enter the Test Case ID for the particular violation being remediated by the custom action. Test Case ID is found in the Health Results Details subtab in the End-Systems tab.
3. Add a custom description of the violation (required) and an optional custom solution.
4. If you have multiple portal configurations and you want to use this custom remediation action in all of your configurations, select the **Add to All Portal Configurations** option. This option overwrites any existing custom actions defined for the test case ID.
5. Select **OK**. Whenever the test case ID is listed as a violation on the web page, the custom violation description and solution you define is displayed instead of the remediation actions provided by the assessment server.

Select the **Define Default Custom Action** checkbox to advise end-users to contact the Helpdesk regarding additional security violations not explicitly listed with custom remediation actions. If this checkbox is selected, only the violations and associated custom remediation actions listed in the table would be presented to the user, along with a message advising them to contact the Helpdesk for any other security violations not explicitly configured with a custom remediation action. Select the **Edit** button to edit this message.

To copy a custom action to another portal configuration, select the action in the table and select the **Copy To** button. A window opens where you can select the portal configurations where you want to copy the action, and whether you want it to overwrite any existing custom remediation actions already defined for that test case ID.

Portal Web Page URLs

The following table provides a list of URLs for accessing commonly used portal web pages. You can also access these web pages using the **Engine Portal Pages** button at the bottom of the Portal Configuration window.

Web Page	URL
Preview Web Page Enables you to preview the web pages an end-user can access during the assessment/remediation and registration process.	https://*Access ControlengineIP*/screen_preview
Registration Administration Page Lets administrators view registered devices and users, and manually add, delete, and modify users.	https://*Access ControlengineIP*/administration
Registration Sponsor Page Lets sponsors view registered devices and users, and manually add, delete, and modify users.	https://*Access ControlengineIP*/sponsor
Pre-Registration Page The pre-registration web page lets selected personnel easily register guest users in advance of an event, and print out a registration voucher that provides the guest user with their appropriate registration credentials.	https://*Access ControlengineIP*/pre_registration
Self-Registration Page Enables an authenticated and registered user to self-register additional devices that might not have a web browser (for example, game systems).	https://*Access ControlengineIP*/self_registration

Portal Configuration Guest Registration

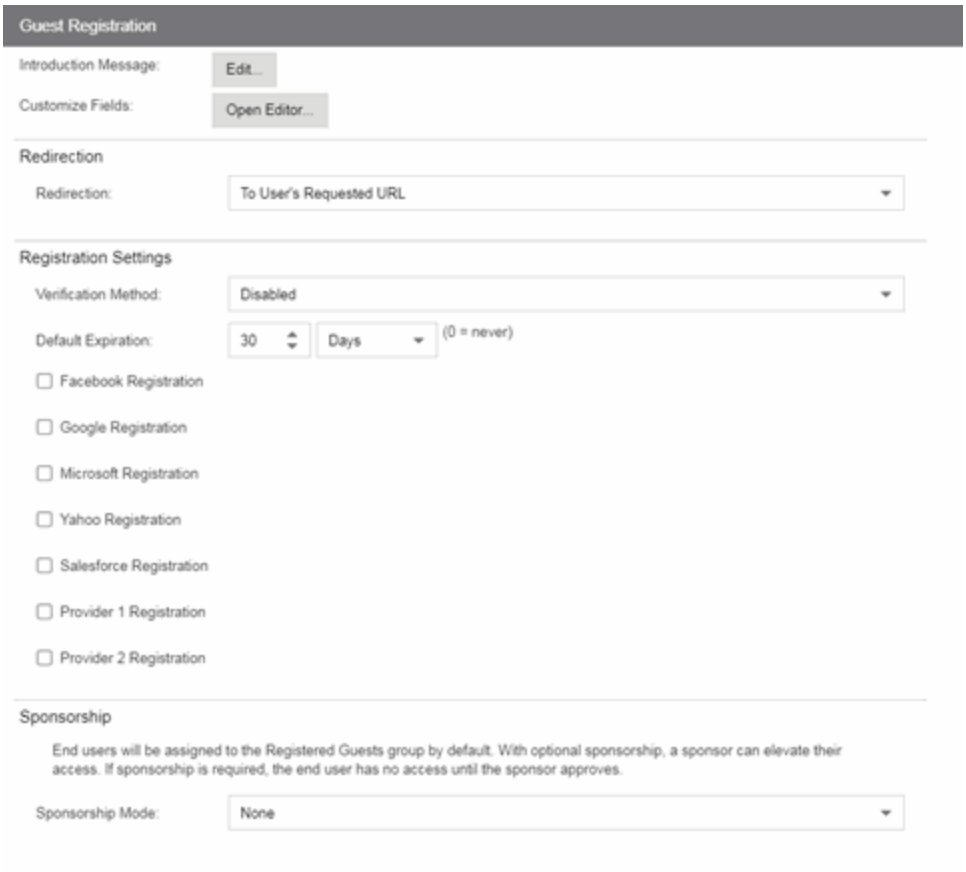
Guest registration forces any new end-system connecting on the network to provide the user's identity in the registration web page before being allowed access to the network. Guests are initially redirected to a web page for registering their end-system when it is first connected to the network. After successful registration, the end-system is permitted access until the registration expires or is administratively revoked.

The end user's level of network access is determined by the settings specified here, and whether they are required to have a sponsor. With sponsored registration, end users are only allowed to register to the network when approved by a "sponsor," an internal trusted user to the organization. Sponsorship can provide the end user with a higher level of access than just guest registration and allows the sponsor to fine-tune the level of access for individual end users. The end user registers and declares a sponsor's email address. The sponsor is notified and approves the registration, and can assign an elevated level of access, if desired.

NOTES:

If you configure both Guest Registration and Authenticated Registration for an area on your network, the end user is presented with a choice on the registration web page whether or not to authenticate.

The Network Settings and Look and Feel panels provide you access to common settings that are shared by the Registration portal web page.



Introduction Message

Select the **Edit** button to open a window where you can edit the introductory message displayed to end users when registering as guests. It may include an introduction to the network and information stating that the end user is agreeing to the Acceptable Use Policy (AUP) for the network upon registering their device. A link to the URL that contains the full terms and conditions of the network's AUP can be provided from this introductory message. Note that the URL for this link must be added as an Allowed URL in the Allowed Web Sites window accessed from the Network Settings. By configuring the introductory message with this information, end users can be held accountable for their actions on the network in accordance with the terms and conditions set forth by the network's AUP. This message is shared by Guest Web Access and Guest Registration. Changing it for one access type also changes it for the other.

Customize Fields

Select the **Open Editor** button to open the Manage Custom Fields window, where you can manage the fields displayed in the Registration web page. These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing them for one access type also changes them for the others.

Redirection

There are four Redirection options that specify where the end user is redirected following successful registration, when the end user is allowed on the network. The option selected here overrides the Redirection option specified on the Network Settings. This setting is shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing it for one access type also changes it for the others.

- **Use Network Settings Redirection** — Use the Redirection option specified on the Network Settings.
- **Disabled** — This option disables redirection. The end user stays on the same web page where they were accepted onto the network.
- **To User's Requested URL** — This option redirects the end user to the web page they originally requested when they connected to the network.
- **To URL** — This option lets you specify the URL for the web page where the end user is redirected. This would most likely be the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Registration Settings

Verification Method

User Verification requires that guest end users registering to the network enter a verification code sent to their email address or mobile phone (via SMS text) before gaining network access. This ensures that network administrators have at least one way to contact the end user.

Select from the following verification methods:

- **Email** — The end user must enter an email address in the Registration web page. The Email Address field must be set to **Required** in the Manage Custom Fields window.
- **SMS Gateway** — The end user must enter a mobile phone number in the Registration web page. The Phone Number field must be set to **Required** in the Manage Custom Fields window.
- **SMS Gateway or Email** — The end user must enter a mobile phone number or email address in the Registration web page. The Phone Number and Email Address fields must be set to **Visible** in the Manage Custom Fields window.
- **SMS Text Message** — The end user must enter a mobile phone number in the Registration web page. The Phone Number field must be set to **Required** in the Manage Custom Fields window.
- **SMS Text or Email** — The end user must enter either a mobile phone number or email address in the Registration web page. The Phone Number and Email Address fields must be set to **Visible** in the Manage Custom Fields window.

If you have selected the "SMS Text Message" or the "SMS Text or Email" Verification method: select the Service Providers link (below the verification method) to configure the list of mobile service providers from which end users can select the Registration web page. This setting allows ExtremeCloud IQ Site Engine to correctly format the email address to which to send an email. This email is then received by the service provider and converted to an SMS text which is sent the user. The default configuration provides lists of the major US cellular service providers. NOTE: Not all cellular service providers provide a way to send SMS text messages via email.

If you have selected the "SMS Gateway" or "SMS Gateway or Email" method: enter the SMS Gateway Email address provided by the SMS Gateway provider.

For all methods: use the Message Strings link (below the verification method) to open the Message Strings Editor and modify the registration verification messages displayed to the user during the verification process. For example, if you have selected **Email**, you need to modify the "registrationVerificationEmailSentFromAddress" message string to be the appropriate email address for your company.

For all methods: set the Verify Pin Characters and Verify Pin Length options to define the characteristics and length of the verification code sent to the guest end user. This setting is shared by Guest Registration and Guest Web Access. Changing it for one access type also changes it for the other.

Default Expiration

Enter a value and select a unit of time to configure the amount of time before an end user's registration automatically expires. When the registration expires, the end user is either suspended (registration must be manually approved by administrator/sponsor) or permanently deleted from the guest registration list. If a registration is deleted, the end-user must re-enter all their personal information the next time they attempt to access the network. Individual expiration time can also be set by a sponsor.

Registration

The Registration checkboxes indicate the providers from which ExtremeControl can gather registration information: Facebook, Google, Microsoft, Yahoo, and Salesforce. You can configure these providers or configure additional OpenID Connect providers using the **Provider Registration** fields.

Sponsorship

Use this section to configure sponsorship for Guest Registration. Select the Sponsorship Mode required. Additional settings display if you select optional or required sponsorship.

With sponsored registration, end users are only allowed to register to the network when approved by a "sponsor," an internal trusted user to the organization. Sponsorship can provide the end user with a higher level of access than just guest registration and allows the sponsor to fine-tune the level of

access for individual end users. The end user registers and declares a sponsor's email address. The sponsor is notified and approves the registration, and can assign an elevated level of access, if desired.

Portal Web Page URLs

The following table provides a list of URLs for accessing commonly used portal web pages. You can also access these web pages using the **Engine Portal Pages** button at the bottom of the Portal Configuration window.

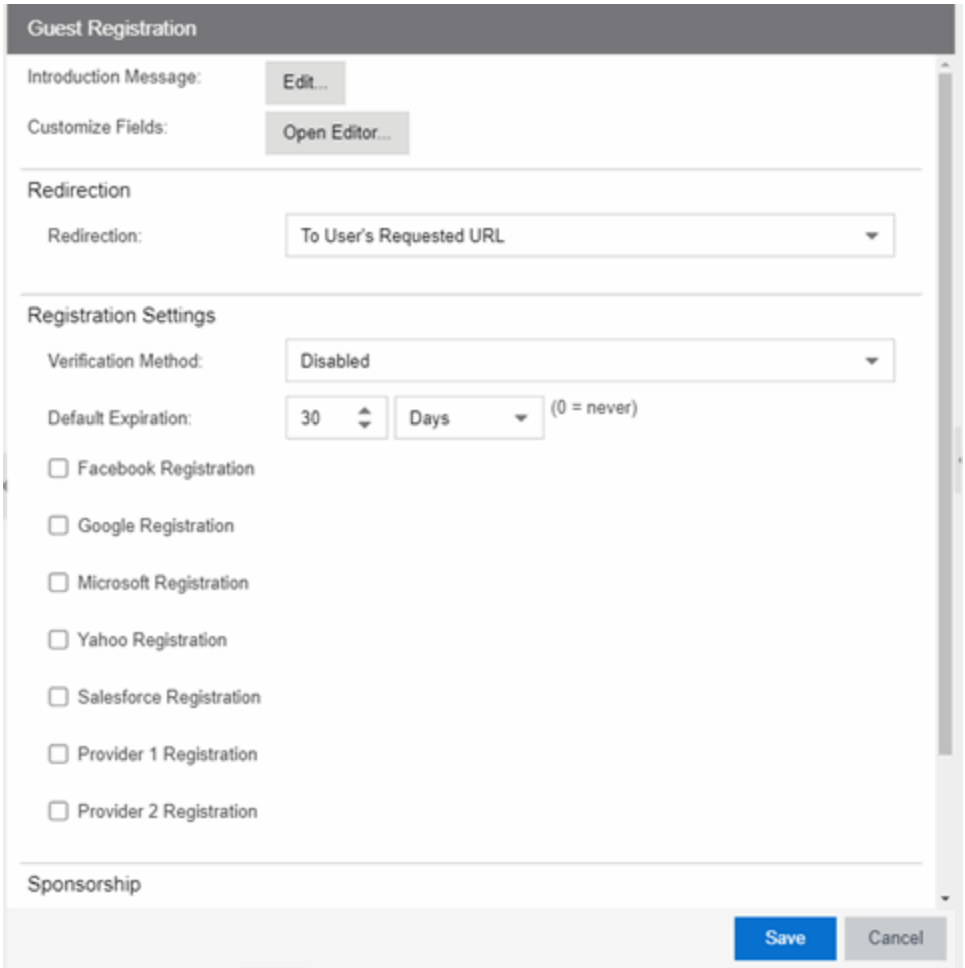
Web Page	URL
Preview Web Page Allows you to preview the web pages that may be accessed by the end user during the assessment/remediation and registration process.	https://*Access ControlengineIP* /screen_preview
Registration Administration Page Lets administrators view registered devices and users, and manually add, delete, and modify users.	https://*Access ControlengineIP* /administration
Registration Sponsor Page Lets sponsors view registered devices and users, and manually add, delete, and modify users.	https://*Access ControlengineIP* /sponsor
Pre-Registration Page The pre-registration web page lets selected personnel easily register guest users in advance of an event, and print out a registration voucher that provides the guest user with their appropriate registration credentials.	https://*Access ControlengineIP* /pre_registration
Self-Registration Page Allows an authenticated and registered user to self-register additional devices that may not have a web browser (for example, game systems).	https://*Access ControlengineIP* /self_registration

- Portal Configuration Overview

Portal Configuration Provider Registration

The Registration Section includes a list of providers from which ExtremeControl can gather registration information. Configure registration using these providers or configure other OpenID Connect providers using the **Provider 1 Registration** and **Provider 2 Registration** options.

NOTE: Guest OAuth (for example, Google, Yahoo) may not support native mobile browsers and display a “user agent” error. To access the network, use a standard browser application (e.g. Google Chrome).



Facebook Registration

1. Select the Facebook Registration checkbox if you are implementing guest registration using Facebook as a way to obtain end user information. In this scenario, the Guest Registration portal provides the end user with an option to log into Facebook in order to complete the registration process.
2. Enter the Facebook App ID – When you create an application you are given a Facebook App ID to enter here.
3. Enter the Facebook App Secret – When you create an application you are given a Facebook App Secret to enter here.
4. Enter the Facebook Redirect URI – This information allows you to configure the provider as `fb_oauth`.
5. Press OK to save your changes.

Google Registration

1. Select the Google Registration checkbox if you are implementing guest registration using Google as a way to obtain end user information. In this scenario, the Guest Registration portal provides the end user with an option to log into Google in order to complete the registration process.
2. Enter the Google Discovery URI – (a benefit of Open ID Connect) - This url gives you access to all the end-points you need to complete authorizations of user data.
3. Enter the Google App ID – When you create an application you are given a Google App ID to enter here.
4. Enter the Google App Secret – When you create an application you are given a Google App Secret to enter here.
5. Enter the Google Redirect URI – This information allows you to configure the provider as `google_oauth`.
6. Press OK to save your changes.

Microsoft Registration

1. Select the Microsoft Registration checkbox if you are implementing guest registration using Microsoft as a way to obtain end user information. In this scenario, the Guest Registration portal provides the end user with an option to log into Microsoft in order to complete the registration process.
2. Enter the Microsoft Discovery URI – (a benefit of Open ID Connect) - This url gives you access to all the end-points you need to complete authorizations of user data.
3. Enter the Microsoft App ID – When you create an application you are given a Microsoft App ID to enter here.
4. Enter the Microsoft App Secret – When you create an application you are given a Microsoft App Secret to enter here.
5. Enter the Microsoft Redirect URI – This information allows you to configure the provider as ms_oauth.
6. Press OK to save your changes.

Yahoo Registration

1. Select the Yahoo Registration checkbox if you are implementing guest registration using Yahoo as a way to obtain end user information. In this scenario, the Guest Registration portal provides the end user with an option to log into Yahoo in order to complete the registration process.

2. Enter the Yahoo Discovery URI – (a benefit of Open ID Connect) - This url gives you access to all the end-points you need to complete authorizations of user data.
3. Enter the Yahoo App ID – When you create an application you are given a Yahoo App ID to enter here.
4. Enter the Yahoo App Secret – When you create an application you are given a Yahoo App Secret to enter here.
5. Enter the Yahoo Redirect URI – This information allows you to configure the provider as `yahoo_oauth`.
6. Press OK to save your changes.

Salesforce Registration

1. Select the Salesforce Registration checkbox if you are implementing guest registration using Salesforce as a way to obtain end user information. In this scenario, the Guest Registration portal provides the end user with an option to log into Salesforce in order to complete the registration process.
2. Enter the Salesforce Discovery URI – (a benefit of Open ID Connect) - This url gives you access to all the end-points you need to complete authorizations of user data.
3. Enter the Salesforce App ID – When you create an application you are given a Salesforce App ID to enter here.
4. Enter the Salesforce App Secret – When you create an application you are given a Salesforce App Secret to enter here.
5. Enter the Salesforce Redirect URI – This information allows you to configure the provider as `salesforce_oauth`.
6. Press OK to save your changes.

Provider Registration (Generic)

1. To add a provider not already considered by Access Control, but uses Open ID Connect, select the box near Provider 1 (generic).
2. Provider 1 Discovery URI – (a benefit of Open ID Connect) – You can use the company's own discovery URI. This feature gives you access to all the end-points that you need to complete authorizations of user data
3. Provider 1 App ID – This information is given by the provider.
4. Provider 1 App Secret – This information is given by the provider.
5. Provider 1 Image – You can add an image or a logo by selecting New from the drop-down list. Drag and drop a file or select a file using the browser to add an image for this provider.

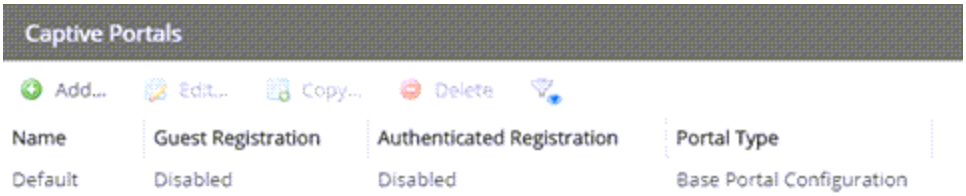
6. Provider 1 Text – Press the Text button to open the Localized Message String Editor window. Use the box to add text. Press OK to save your changes.
7. Provider 1 Redirect URI - This information allows you to configure the provider as `genprovider_oauth`.

The Enterprise Registration Center will include logos buttons for providers in Register as Guest panel. Select each logo to be redirected to the provider's website for user authentication. You will then be redirected back to complete Open ID access authorization.

Portal Configurations

The Portal Configurations panel in the **Control** > **Access Control** tab lets you view and edit all the portal configurations defined in ExtremeCloud IQ Site Engine.

To access the Portal Configurations panel, select **Access Control Configurations > Portal** from the left-menu tree. If you expand the Portal tree, the Default portal configuration plus any other configurations you have defined are displayed.

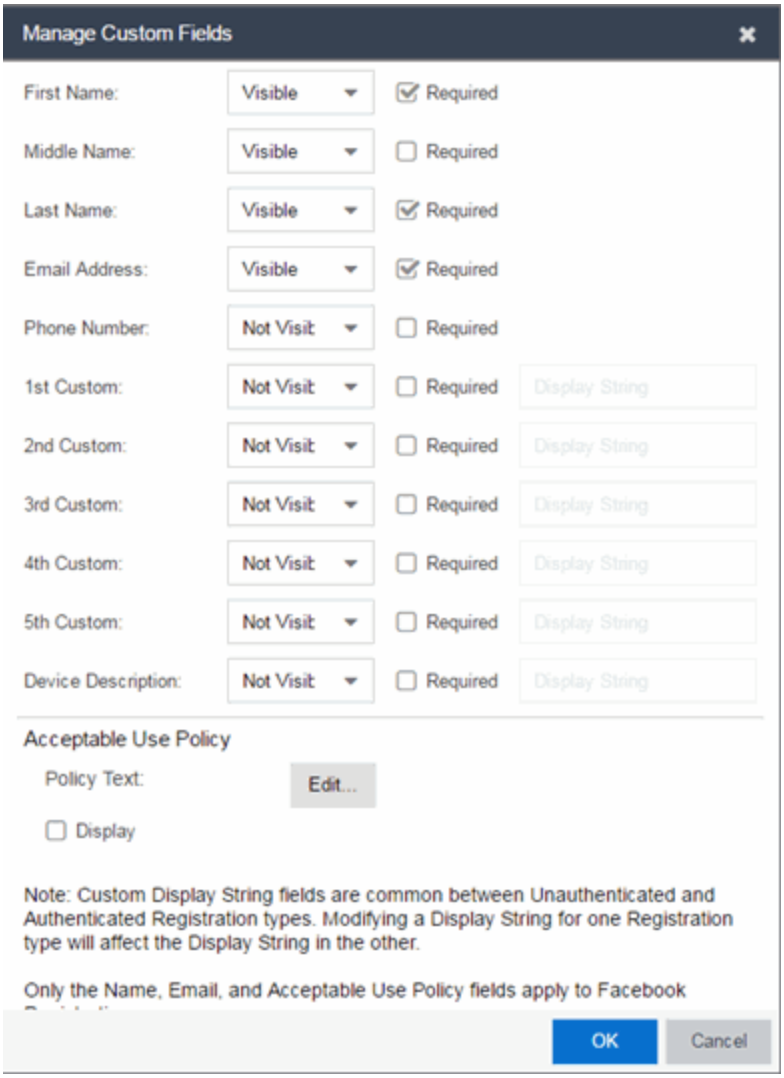


Manage Custom Fields

This window lets you manage the fields displayed in the web pages presented to the end user when they access the network. It is configured as part of your portal configuration, and is accessed from the Customize Fields **Open Fields** button in Edit Portal Configuration. You can manage custom fields for both guest and authenticated access types:

- **Guest Access Types** — By default, the guest login/registration web page displays the First Name, Last Name, and Email Address fields. You can use this window to specify other fields you would like to be displayed (visible) and required. These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Modifying settings for one access type also changes them for the others.
- **Authenticated Access Types** — By default, the authenticated login/registration web page displays only the Acceptable Use Policy. You can use this window to specify other fields you would like to be displayed (visible) and required. These settings are shared by the Authenticated Web Access and Authenticated Registration access types. Modifying settings for one access type also changes them for the other.

Sample Manage Custom Fields Window



For each field, use the drop-down list to select whether the field is:

- **Visible** - the field is displayed in the login/registration web page for the end user. If you want the field information to be required (the end user must enter the information), select the "Required" checkbox.
- **Not Visible** - the field is not displayed in the login/registration web page for the end user.
- **Admin Only** - the field is visible to network administrators only, in the Add/Edit User web page accessed from the Registration System Administration web page. The end user is not able to see or edit the field.

NOTES: For Guest Registration and Guest Web Access: If you are configuring a Verification Method, the Email Address field and/or the Phone Number field are required (depending on the verification method you have selected) and must be set to **Visible/Required**. For more information, see How to Configure Verification for Guest Access Registration.

For Secure Guest Access: The Credential Delivery method requires the Email Address field and/or the Phone Number field (depending on the delivery method you have selected) to be set to **Visible/Required**. For more information, see Credential Delivery Method in the Edit Portal Configuration panel.

For Facebook Registration: Only the First Name, Last Name, and Email Address fields are filled using Facebook data. These fields and the Acceptable Use Policy (AUP) option are the only fields that apply to Facebook registration. If the display AUP option is selected, the captive portal verifies that the AUP is acknowledged before redirecting the user to Facebook.

Use the **Custom fields** to add additional fields to the login/registration web page. Set the field to **Visible**, and then add the text to display by adding a display string. Here are some examples of how to use custom fields:

- In a higher education environment, you can set a custom field display string to "Student ID Number" or "Dorm Room Number" to record additional information about students registering to the network.
- In a corporate environment, you can set a custom field display string to "Company Name" to obtain information about organization to which a partner or guest belongs. Or, you might want the end user to enter a device description, such as an asset tag number.
- In a convention deployment, you can set a custom field display string to "Booth Number" to record the booth to which a registering end-system is associated.

Select the **Acceptable Use Policy** checkbox if you would like the web page to display your organization's Acceptable Use Policy (AUP) and select the **Edit** button to open a window where you can add the AUP text.

NOTE: The Pre-Registration web page always displays the First Name and Last Name fields even if they are not selected as visible/required in the Manage Custom Fields window. If they are selected as required, they are displayed as required on the Pre-Registration web page, otherwise they are displayed as optional. This is because it is important to prompt for a first and last name to be included on the pre-registration voucher printed out.

Keywords

The Custom Arguments field is used to specify the arguments passed to a program. Each argument is delimited by spaces. An argument can be a literal, passed to the program exactly as typed, or a variable, specified as $keyword. A group of literals and variables can be combined into a single argument by using double quotes. The value "all" is a special value that tells ExtremeCloud IQ Site Engine to pass all variable values to the program as individual arguments. See below for a list of available keywords, along with their definitions.

Keyword Definitions

There are certain "keywords" that you can use in your email, syslog, and trap messages to provide specific information. These $keywords are replaced with information from the notification when the notification action is executed.

Following is a list of available keywords for ExtremeControl notifications, along with the value the keyword return. The keywords are organized according to the notification type they pertain to (End-System, Registration, Health Result, User Group, or End-System Group), and can only be used when that specific type of notification action is being edited. The Default keywords can be used with any notification type.

Keyword	Returned Value
Default Keywords	
$type	The notification type.
$trigger	The notification trigger.
$conditions	A list of the conditions specified in the notification action.
$server	The ExtremeCloud IQ Site Engine server IP address.
End-System Keywords	
$macAddress	The end-system's current MAC address.
$oldmacAddress	The end-system's previous MAC address.
$macOUIVendor	The Vendor name for the end-system MAC Address.
$ipAddress	The end-system's current IP address.
$oldipAddress	The end-system's previous IP address.
$username	The current username used to authenticate the end-system.
$oldusername	The previous username used to authenticate the end-system.
$hostname	The end-system's hostname.

Keyword	Returned Value
$oldhostName	The end-system's previous hostname.
$operatingSystemName	The full operating system running on the end-system.
$oldoperatingSystemName	The previous full operating system the end-system was running.
$ESType	The end-system's current operating system family (for example, Windows, Mac, or Linux).
$oldESType	The end-system's previous operating system family (for example, Windows, Mac, or Linux).
$state	The end-system's current state: ACCEPT, REJECT, SCAN, QUARANTINE, DISCONNECTED, or ERROR.
$oldstate	The end-system's previous state: ACCEPT, REJECT, SCAN, QUARANTINE, DISCONNECTED, or ERROR.
$stateDescr	A description of the end-system's current state.
$oldstateDescr	A description of the end-system's previous state.
$extendedState	An extended description of the end-system's current state.
$oldextendedState	An extended description of the end-system's previous state.
$switchSysName	The sysName of the switch to which the end-system is currently connected.
$switchNickName	The nickName of the switch to which the end-system is currently connected.
$switchIP	The IP address of the switch to which the end-system is currently connected.
$oldswitchIP	The IP address of the switch to which the end-system was previously connected.
$oldswitchSysName	The sysName of the switch to which the end-system was previously connected.
$oldswitchNickName	The nickName of the switch to which the end-system was previously connected.
$switchLocation	The physical location of the switch the end-system is currently connected to (for example, the building/floor location).
$oldswitchLocation	The physical location of the switch the end-system was previously connected to (for example, the building/floor location).

Keyword	Returned Value
$switchPort	The ifIndex of the switch port the end-system is currently connected to.
$oldswitchPort	The ifIndex of the switch port the end-system was previously connected to.
$switchPortId	The name of the switch port the end-system is currently connected to (for example, ge.1.1).
$oldswitchPortId	The name of the switch port the end-system was previously connected (for example, ge.1.1).
$authType	The latest authentication method used by the end-system to connect to the network.
$oldauthType	The previous authentication method used by the end-system to connect to the network.
$allAuthTypes	A comma-separated list of authentication types currently used for this end-system in its current location. The list is only provided if there is more than one authentication type.
$oldallauthTypes	A comma-separated list of authentication types previously used for this end-system in its current location. The list is only provided if there is more than one authentication type.
$nacProfileName	The Access Control profile currently assigned to the end-system.
$oldnacProfileName	The Access Control profile previously assigned to the end-system.
$reason	The reasons why the end-system is assigned its current Access Control profile or is in a particular state.
$oldreason	The reasons why the end-system was assigned its previous Access Control profile or is in a particular state.
$policy	The access policy currently assigned to the end-system, if on a policy-based switch.
$oldpolicy	The access policy previously assigned to the end-system, if on a policy-based switch.
$firstSeentime	The first time the end-system was seen by the Access Control engine.
$lastSeenTime	The last time the end-system was seen by the Access Control engine.

Keyword	Returned Value
$oldlastSeenTime	The previous last time the end-system was seen by the Access Control engine.
$nacApplianceIp	The IP address of the Access Control engine on which the end-system authenticated.
$oldnacApplianceIp	The IP address of the previous Access Control engine on which the end-system authenticated.
$nacapplianceGroupName	The engine group for the Access Control engine where the end-system was last heard.
$oldnacApplianceGroupName	The previous engine group for the Access Control engine where the end-system was last heard.
$lastScanTime	The last time a scan was performed on the end-system.
$lastScanResultState	The resulting state of the last scan: ACCEPT, QUARANTINE, or empty.
$ssid	The Service Set Identifier (SSID) of the wireless network to which the end-system is connected.
$oldssid	The Service Set Identifier (SSID) of the wireless network to which the end-system was previously connected.
$wirelessAp	The name of the Wireless Access Point (AP) to which the end-system is connected. If the AP's name is unavailable, then the AP's MAC address is reported. If the MAC address is unavailable, then the AP's serial number is reported.
$oldwirelessAp	The name of the Wireless Access Point (AP) to which the end-system was previously connected. If the AP's name is unavailable, then the AP's MAC address is reported. If the MAC address is unavailable, then the AP's serial number is reported.
$ifAlias	The ifAlias of the switch port to which the end-system is currently connected.
$oldifAlias	The ifAlias of the switch port to which the end-system was previously connected.
$ifDescription	The ifDescription of the switch port to which the end-system is currently connected.
$oldifDescription	The ifDescription of the switch port to which the end-system was previously connected.
$ifName	The ifName of the switch port to which the end-system is currently connected.

Keyword	Returned Value
$oldifName	The ifName of the switch port to which the end-system was previously connected.
$custom1	The text from the Custom 1 end-system information column.
$custom2	The text from the Custom 2 end-system information column.
$custom3	The text from the Custom 3 end-system information column.
$custom4	The text from the Custom 4 end-system information column.
$regName	The registered username supplied by the end user during the registration process.
$regEmail	The email address supplied by the end user during the registration process.
$regPhone	The phone number supplied by the end user during the registration process.
$regData1	The text from the Custom 1 registration field supplied by the end user during the registration process.
$regData2	The text from the Custom 2 registration field supplied by the end user during the registration process.
$regData3	The text from the Custom 3 registration field supplied by the end user during the registration process.
$regData4	The text from the Custom 4 registration field supplied by the end user during the registration process.
$regData5	The text from the Custom 5 registration field supplied by the end user during the registration process.
$regDeviceDescr	The device description supplied by the end user during the registration process.
$regSponsor	The registered device's sponsor.
$memberOfGroups	The current list of MAC end-system groups listed in the Groups end-system information column.
$oldmemberOfGroups	The previous list of MAC end-system groups listed in the Groups end-system information column.
$groupDescr1	The entry description that was entered when the end-system was added to a MAC-based end-system group.
$groupDescr2	The entry description that was entered when the end-system was added to a MAC-based end-system group.

Keyword	Returned Value
$groupDescr3	The entry description that was entered when the end-system was added to a MAC-based end-system group.
Registration Keywords	
$category	The type of action that was performed, for example: Registered Device Added, Registered Device Updated, Registered User Added; Registered Device Removed, Registered User Removed.
$time	The time the end-system registered to the network.
$source	The MAC address of the registered device or the name of the registered user.
$message	A message describing the action that was performed (for example, Added Registered Device for User: <username> - MacAddress: <MAC address>).
Health Result Keywords	
$macAddress	The end-system's MAC address.
$ipAddress	The end-system's IP address.
$startScanDate	The date and time the scan started.
$endScanDate	The date and time the scan ended.
$hostUnreachable	Whether the host was unreachable before or after the scan was run: true or false.
$testSets	A list of test sets that were run during assessment.
$totalScore	The total sum of the scores for all the health details for the health result.
$topScore	The highest score received for a health detail in the health result.
$riskLevel	The risk level assigned to the end-system based on the health result.
$riskLevelReason	The reason the health result was placed into the specified risk level.
$assessmentSummary	A list of all the test cases that were run against the device during assessment.
$statusDetail	A list of the vulnerabilities that were found during assessment.

Keyword	Returned Value
$assessmentServerIpAddress	The IP address of the assessment server that performed the scan.
$assessmentServerName	The name of the assessment server that performed the scan.
User Group Keywords	
$name	The name of the user group.
$createdBy	The name of the user that created the user group.
$creationTime	The time and date the user group was created.
$description	A description of the user group (if one was defined when the group was created).
$added	A comma-separated list of user entries that were added to the group during the change.
$removed	A comma-separated list of user entries that were removed from the group during the change.
$lastModifiedTime	The last time the user group was modified.
$oldlastModifiedTime	The previous last time the user group was modified.
$lastModifiedBy	The name of the user who most recently edited the user group.
$oldlastModifiedBy	The name of the user who had previously edited the user group.
$revisionCounter	The current revision count (the number of changes that have been made) for the user group.
$oldrevisionCounter	The previous revision count (the number of changes that have been made) for the user group.
$listtype	One of the following types: Username, LDAP User Group, RADIUS User Group.
End-System Group Keywords	
$name	The name of the end-system group.
$createdBy	The name of the user that created the end-system group.
$creationTime	The time and date the end-system group was created.
$description	A description of the end-system group (if one was defined when the group was created).
$added	A comma-separated list of end-system entries that were added to the group during the change.

Keyword	Returned Value
$removed	A comma-separated list of end-system entries that were removed from the group during the change.
$lastModifiedTime	The last time the end-system group was modified.
$oldlastModifiedTime	The previous last time the end-system group was modified.
$lastModifiedBy	The name of the user who most recently edited the end-system group.
$oldlastModifiedBy	The name of the user who had previously edited the end-system group.
$revisionCounter	The current revision count (the number of changes that have been made) for the end-system group.
$oldrevisionCounter	The previous revision count (the number of changes that have been made) for the end-system group.
$listtype	One of the following types: MAC, IP, Hostname.
Guest and IoT Manager Keywords	
$category	The type of action that was performed, for example: GIM Device Added, GIM Device Updated, GIM User Added; GIM Device Removed, GIM User Removed.
$devicetype	This notification is for a GIM device, not a GIM user.
$domain	The Guest and IoT Manager Domain.
$message	A message describing the action that was performed (for example, Added GIM device).
$source	The MAC address of the GIM device or the name of the GIM user.
$template	The Guest and IoT Manager Onboarding Template.
$time	The time when the GIM device or user event occurred.

Allowed Web Sites

Use this window to configure the web sites end users are allowed to access during the ExtremeControl Assisted Remediation and Registration process. This window is configured as part of your portal configuration, and is accessed by selecting the **Open Editor** button in the Network Settings panel of the Portal Configuration tree.

There are three subtabs in the window: Allowed URLS, Allowed Domains, and Web Proxy Servers.

Allowed URLs

This tab lists the URLs that end-systems can access while the end-system is being assessed, when the end-system is quarantined, or when the end-system is not registered on the network. The ExtremeControl engine proxies these HTTP connections to the allowed URLs as long as the engine is configured with an appropriate DNS server.

Any URLs that you have referenced in the captive portal configuration must be entered into this tab so an end-system with restricted access to the network is permitted to communicate to the URL. For example, a URL entered in the Helpdesk Information section should be entered here so a quarantined end-system can access the Helpdesk web site while quarantined.

Enter the URL you want to add to the list and select **Add**. URLs must be entered without "http://www". For example, if "http://www.apple.com" is an allowed website, then enter "apple.com" as the allowed URL.

You can use the **Import** button to import a file of URLs to the list. Files must be formatted to contain one URL per line. Lines starting with "#" or "//" are ignored.

NOTE: It is not necessary to enter URLs that are accessed over secure HTTP (HTTPS). To restrict access to these URLs, you must configure network policy to allow or disable HTTPS traffic all together or restrict it to specific IP ranges.

When an allowed URL is added, all web pages located within the directory are also allowed. For example, if apple.com is configured as an allowed URL, then HTTP connections for the following URLs are also permitted:

```
www.apple.com/downloads
www.apple.com/downloads/macosx
```

HTTP connections to URLs located on different hosts than that of the allowed URL entry are not permitted. These HTTP connections are redirected to the Assisted Remediation or MAC Registration web page. Using the same example, if apple.com is configured as an allowed URL, HTTP connections for the following URLs are not allowed:

```
store.apple.com
store.apple.com/download
```

Images on the web page are displayed properly if the images are served on a separate HTTP connection at a different URL. For example, the web page `http://www.apple.com/support/downloads/` contains images downloaded from `http://images.apple.com`. Therefore, if `apple.com/support/downloads/` is configured as an allowed URL, all of the text on the web page would be displayed properly, but the images would not be displayed on the web page unless `images.apple.com` is also entered as an Allowed URL.

Allowed Domains

This tab lists the domains to which end users can browse while the end-system is being assessed, the end-system is quarantined, or when the end-system is not registered on the network. The ExtremeControl engine proxies these HTTP connections to the allowed domains as long as the engine is configured with an appropriate DNS server.

The higher-level domain information not explicitly specified in an allowed domain entry are also permitted for an end-system as well as any web pages served from within the domain. For example, if apple.com is configured as an allowed domain, then HTTP connections for the following URLs are also permitted:

```
www.apple.com
www.info.apple.com
store.apple.com
store.apple.com/info
images.apple.com
www.apple.com/software
apple.com/software
```

HTTP connections not matching the specified domain level information in an allowed domain entry are not permitted. These HTTP connections are redirected to the Assisted Remediation or Registration web page. Using the same example, if apple.com is configured as an allowed domain, HTTP connections for the following URLs are not allowed:

```
www.apple2.com
store.apple-chat.com
www.msn.com
```

If multiple allowed domain entries are configured with overlapping first-level and second-level domain information, then the allowed domain entry that is more specific takes precedence. For example, if `apple.com` and `store.apple.com` are configured as allowed domain entries, then the `apple.com` entry is effectively disabled. Therefore, HTTP connections for the following URLs are allowed:

```
store.apple.com
store.apple.com/info
www.store.apple.com/info
```

The following HTTP connections are not allowed:

```
www.apple.com
www.apple.com/support
images.apple.com
```

The following is a list of default allowed domains that are pre-configured for ExtremeControl remediation. These allowed domains are provided as part of the assisted remediation assessment functionality, which allows end-users limited Internet access to update patches, antivirus definitions, and to upgrade vulnerable software in order to comply with the network security policy. The ExtremeControl engine proxies traffic to these allowed domains when an end user selects a remediation link presented on the violations page.

A default allowed domain should only be deleted if it is determined that a quarantined user should not be able to access it. In some cases, you need to add additional URLs or domains. If a quarantined user selects a remediation link to resolve an issue and is redirected back to the remediation web page, the domain or URL needs to be added to provide access to that site.

adobe.com	akadns.net	akamai.com
akamai.net	altn.com	apache.org
apple.com	archives.neohapsis.com	asp.net
aws.amazon.com	bitdefender.com	bugzilla.org
ca.com	cdnetworks.com	cert.org
cisco.com	clamav.net	cve.mitre.org
debian.org	drupal.org	eset.com
eu.ntt.com	f-secure.com	gnu.org
godaddy.com	ibm.com	ipswitch.com
isc.org	kaspersky.com	lac.co.jp
level3.com	localmirror.com	kaspersky-labs.com
macromedia.com	mandriva.com	mcafee.com
microsoft.com	mozilla.org	mysql.com
netwinsite.com	norton.com	novell.com
nsatc.net	openssl.org	oracle.com
osvdb.org	pandasecurityusa.com	php.net
phpnuke.org	redhat.com	samba.org
secunia.com	securiteam.com	securityfocus.com
securitytracker.com	sendmail.org	sophos.com
sourceforge.net	squid-cache.org	sun.com
support.citrix.com	suse.com	suse.de
symantec.com	symantecliveupdate.com	techtarget.com
trendmicro.com	ubuntu.com	us-cert.gov
verisign.com	verisigninc.com	vmware.com

vupen.com	web.mit.edu	webroot.com
windows.com	windowsupdate.com	wireshark.org
xforce.iss.net	zerodayinitiative.com	zope.org

Web Proxy Servers

This tab is used to specify the web proxy server(s) deployed on the network. The ExtremeControl engine proxies end-system Allowed URL and Allowed Domain HTTP traffic to the defined web proxy servers if the network utilizes proxy servers to access the Internet.

If multiple web proxy servers are configured, the ExtremeControl engine round robins HTTP connections to the configured proxy servers. If the allowed web site is located with the ExtremeControl engine's configured domain, the ExtremeControl engine directly contacts the web site and does not go through the configured web proxy servers.

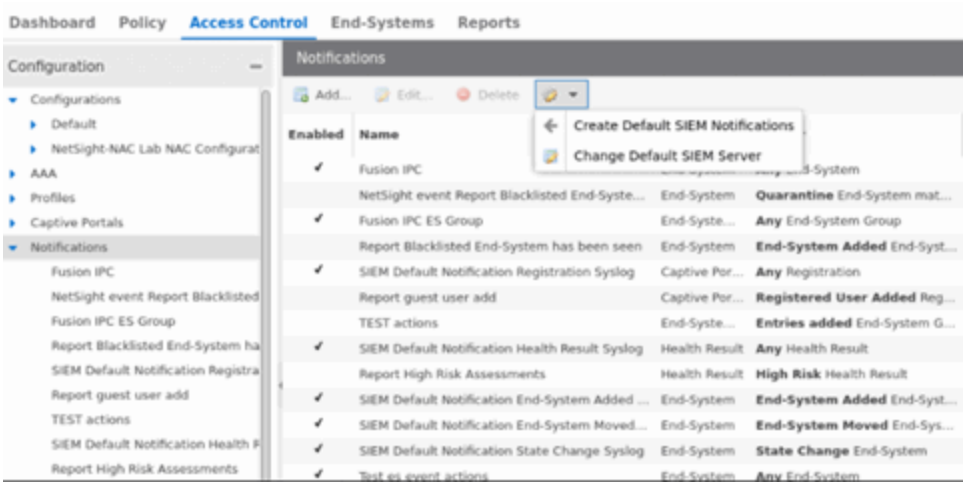
For information on related help topics:

- Edit Portal Configuration Panel

Manage Notifications

Use the **Notifications** tab to review all the notifications you create, and to add, edit, and test specific notification rules. Notifications enable you to create alert actions performed when specific events or triggers take place in ExtremeCloud IQ Site Engine. Notification actions include sending an email, creating a syslog entry, sending an SNMP trap, and launching a custom program or script.

To access this window, expand **Access Control> Configuration** in the left-panel and select **Notifications**.



Notifications Table Buttons

Use these buttons to add, edit, delete, or test a notification.

Add

Select to open the Add Notification window, where you can define a new notification rule.

Edit

Select to open the Edit Notification window, where you can edit notification rule actions for selected notification(s).

Delete

Select to delete notification(s) you select in the table.

Configuration

Use the configuration menu button to create default SIEM Notifications or change the default SIEM server:

Create Default SIEM Notifications - Creates five default notifications that enable the notification feature to integrate with SIEM (Security Information and Event Manager) by sending syslog messages to your SIEM server. The notifications are based on the following conditions and triggers:

- Any Registration event
- Any Health Result
- End-System events:
    - End-system added
    - End-system moved
    - End-system state changed

The generated syslog messages include the following information:

- IP address
- MAC address
- Username
- Switch IP address
- Switch port
- Hostname
- Operating system
- State
- Extended State

- Reason
- NAC Appliance

Change Default SIEM Server - Use this option to change the default SIEM server IP address used when you generate new default SIEM notifications. The specified default SIEM server only applies to newly generated notifications; manually edit previously generated notifications to change the server.

Notifications Table

The following columns are included in the Notifications Table:

Enabled
The checkbox indicates whether the notification is enabled. When a notification is enabled, the defined action takes place when the trigger occurs and the conditions are met.

Name
The name of the notification.

Type
The notification type defines the source of the event triggering the notification: End-System Group, End-System, User Group, Health Result, or Registration.

Trigger
The trigger determines when a notification action occurs, based on filtering for a specific event.

Action
The actions that take place when a notification is triggered.

NOTE:	Actions cannot be defined for default notification rules starting with the name "Connect ES".

Override Content
Specifies whether Override Content is enabled or disabled for the notification.

Notes
A short description of the notification rule. This description is created when a new notification is added.

Enable Default Notifications

ExtremeControl includes four default notifications you can enable and edit. To enable a default notification, perform the following steps:

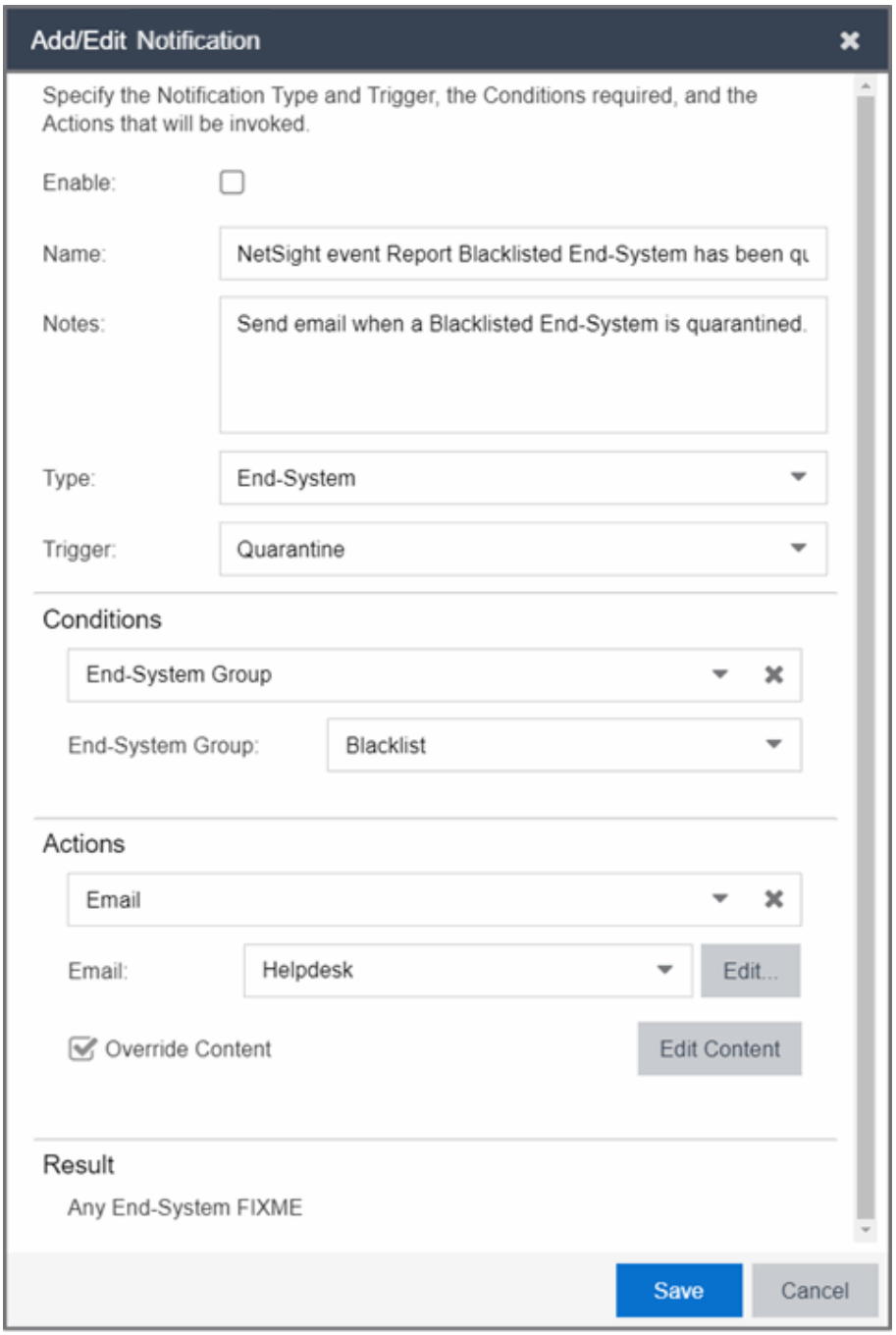
1. Select the notification in the table and select the **Edit** button to open the **Edit Notification** window.
2. Use the **Edit Email Lists** button and change the default address to an address specific to your network.
   Default notifications are configured to send an email to this address.
3. Configure the **SMTP E-Mail Server** option in the SMTP Email Options to identify the SMTP email server used for outgoing messages generated by the Notification feature.
4. Select the **Enable Notification** check box and then select **OK** in the Edit Notification Action window.
   The default notification is now enabled in the Manage Notifications window.

The following examples show how notifications can be used to alert you of changes or events in your network:

- Send an email to the Helpdesk when an end-system changes location, for example if it moves from a wired connection in a building to a wireless connection outside.
- Send a trap if an end-system fails registration.
- Send a syslog message if an end-system reports a high risk assessment result.
- Send an email if an end-system that is reported as a stolen laptop authenticates on the network.
- Send an email if someone logs into the network after normal work hours.
- Send an email when an end-system is added or removed from an end-system group, such as the blocked list end-system group or other defined end-system group.
- Send an email when a user is added or removed from a user group, such as an Administrator or Help Desk user group.

Add/Edit Notification

The Add/Edit Notification window lets you edit an existing notification or create a new one. In the window, you can enable or disable the notification, specify the notification type and trigger, define the required conditions, and configure the actions that occur when the notification is activated. At the bottom of the window, provide a summary description of the notification's properties.



To create a new notification, select the **Add** button on the **Notifications** tab. To edit a notification, select a notification on the **Notifications** tab and select the **Edit** button.

Enable

Select the checkbox to enable the notification. When a notification is enabled, then the defined action takes place when the trigger occurs and the conditions are met.

Name

Enter a name for the notification.

Notes

Enter notes for the notification that describe the notification action or other notification details. This information is displayed on the **Notifications** tab.

Type

The notification type defines the source of the event that activates the notification. Use the drop-down list to select one of the following notification types:

- End-System
- Captive Portal Registration
- Guest and IoT Manager Provisioning
- End-System Group
- User Group
- Health Result

Trigger

Triggers allow you to determine when a notification action occurs based on filtering for a specific event. Use the drop-down list to select the event for which you want to filter. The list of triggers changes according to the notification type you have selected. Selecting "Any" or "Any Change" means that no filtering occurs.

- End-System - the actions are performed based on:
  - an end-system being added, deleted, or moved
  - an end-system state or a state change
  - an authentication type or device type change
  - a custom field change
  - whether the end-system is registered
  - an end-system IP address change. An event is generated when an end-system is added with a static IP, the end-system IP changes after IP resolution, or the end-system IP changes due to DHCP rediscover.
  - when an end-system is added to a MAC-based end-system group. Note that a notification is not generated if the end-system is already a member of three end-

system groups and is added to an additional group, unless the option "Remove from Current Group Assignments" is enabled when the end-system is added to the group.

    - certain errors occurring

- Captive Portal Registration - the actions occur when a registered user or device is added, removed, or updated.
- Guest and IoT Manager Provisioning - the actions occur when a user or device is added, removed, or updated via Guest and IoT Manager.
- End-System Group - the actions are performed when entries in the group are added or removed. "Any Change" would include added, removed, and modified.
- User Group - the actions occur when entries in the group are added or removed. "Any Change" would include added, removed, and modified.
- Health Result - the actions occur based on the risk level of a health result.

Conditions

This section lets you define additional conditions that, in addition to the trigger, determines when actions occur. Conditions can be used to limit the scope of events that trigger a notification action. The list of conditions changes according to the notification type you have selected.

Access Control Engines
Filter end-system notifications based on the engines you select here. Only end-systems being managed by the selected engines trigger the notification actions.

Profile
End-System events are filtered based on the ExtremeControl profile assigned to the end-system. Use the drop-down list to select the desired profile.

Device Type Group
Specify a device type group to use as a filter for the End-System, Health Result, and Registration notification types. When the end-system's device type matches the device type group, then the notification actions are performed.

End-System Group
Select an end-system group to use as a filter for the End-System Group notification type. When the end-system is a member of this end-system group, then the notification actions are performed. If you don't select this checkbox and specify a group, then the notification is sent if any end-system group is matched.

Location Group
Specify a location group to use as a filter for the End-System, Health Result, and Registration notification types. When the location where the end-system (the source of the event) connects to the network matches the location group, then the notification actions are performed.

Time Group

Specify a time group to use as a filter for the End-System, Health Result, and Registration notification types. When the day and time that the end-system (the source of the event) connects to the network matches the time group, then the notification actions are performed.

User Group

Select a user group to use as a filter for the User Group notification type. When the end-system is a member of this user group, then the notification actions are performed. If you don't select this checkbox and specify a group, then the notification is sent if any user group is matched.

Guest and IoT Manager Domain

Select the GIM Domain or Domains in which the **Trigger** must occur for the **Actions** to be invoked.

Guest and IoT Manager Onboarding Templates

After you select a **Guest and IoT Domain**, select the GIM Onboarding Template or Templates to which the Provisioner performing the event defined in the **Trigger** must be assigned for the **Actions** to be invoked.

Actions

Use the checkboxes to specify the actions you want to take place when a notification is triggered and the conditions are met. You can test a notification by selecting the **Test** button. (A notification must be saved before it can be tested.)

If an action depends on details from the triggered notification, the **Test** button triggers the notification, but the action might not complete successfully.

For example, if the action is to execute a Script or Workflow, selecting the Test button will not successfully complete the action if the script or workflow is using variables from the notification itself because the notification does not contain the details of the variables.

Default notification rules that begin with the name "Connect ES" cannot have an action defined.

Email

Select this checkbox if you want an email sent when the notification is triggered. Use the drop-down list to select one of your pre-defined email lists. If no lists have been defined, the menu is empty and you can select the **Edit Email Lists** button to define a list.

Syslog to Server(s)

Select this checkbox if you want to create a syslog message when the notification is triggered. Enter the IP address or hostname for each syslog server where the message is sent. Multiple syslog servers can be listed, separated by either a comma or a space.

Trap Server

Select this checkbox if you want to send an SNMP trap when the notification is triggered. Enter the IP address for a trap receiver where the trap is sent. Valid trap receivers are systems

running an SNMP Trap Service. From the Credential drop-down list, select the appropriate SNMP credential used when sending the trap to the trap receiver. Credentials are defined in the **Profiles/Credentials** tab in the Authorization/Device Access window (Tools > Authorization/Device Access).

Execute Program
Select this checkbox to specify a custom program or script run on the ExtremeCloud IQ Site Engine Server when the notification is triggered. In the **Workflow** field, select the workflow from the drop-down list. Select the **Test** button to run the workflow.

Access Control Events Workflow
Select this checkbox if you want an Access Control event workflow run when the notification is triggered. To configure Access Control event workflows, create a workflow on the **Workflows** tab and select **Access Control Events** in the **Menus** drop-down list on the **Menus** tab of the Workflow Details section.

Override Content
Select this checkbox if you want to override the default content contained in the action message. Use the **Edit Content** button to open the **Edit Action Overrides** window, where you can change the defaults for this specific notification only. Additionally, select the **Show Keywords** button in the **Edit Action Overrides** window to view the keywords available for the overrides.

Result

This section summarizes the notification type, trigger, conditions, and specified actions.

MAC Locking

This tab displays the settings for locked MAC address. MAC Locking lets you lock a MAC address to a specific switch or port on a switch so that the end-system can only access the network from that port or switch. If the end-system tries to authenticate on a different switch/port, it is rejected or assigned a specific policy. You can add or edit MAC locks from the End-Systems tab.

NOTE: MAC Locking to a specific port on a switch is based on the port interface name (e.g. fe.5.1). If a switch board is moved to a different slot in a chassis, or if a stack reorders itself, this name changes and breaks the MAC Locking settings.

MAC Address
The locked MAC address.

Switch IP
The IP address of the switch on which the MAC address is locked.

Port

The port on the switch for which the MAC address is locked.

Lock to Switch and Port

Indicates whether the MAC address is locked to a specific port on the switch, and enter the port interface name.

Failed Action

The action ExtremeCloud IQ Site Engine takes when this MAC address tries to authenticate on a different port and/or switch:

- Reject - The authentication request is rejected.
- Use Policy - Use the drop-down list to select the policy that you want applied. This policy must exist in the **Policy** tab and be enforced to the switches in your network.

MAC to IP Mappings

Use the **MAC to IP Mappings** tab to view MAC to IP address mappings for devices with statically assigned IP addresses. You can also import a file of MAC to IP mappings to the list.

The MAC to IP mappings are sent to the ExtremeControl engines in the configuration enforce. The ExtremeControl engines use this table to resolve IP addresses.

MAC Address
The MAC address mapped to the static IP address.

IP Address
The statically assigned IP address.

Description
A description of the mapping; for example, a description of the device with the statically assigned IP address.

Add Button
Opens the Add MAC to IP Mapping window where you can add a new mapping and description to the table.

Edit Button
Opens the Edit MAC to IP Mapping window where you can edit the IP address and description for a mapping.

Delete Button
Deletes the selected MAC to IP mapping.

Import Button
Use the **Import** button to import a file of MAC to IP mappings to the list. In the file, MAC to IP mappings must be listed in CSV format, with one mapping for each line. All three columns are required even if the description is empty. For example:

```
macAddress,ipAddress,description
02:0A:40:0B:01:44,122.111.45.66,description of mapping
34:34:34:44:44:48,122.111.45.48,description of mapping
```

MAC addresses can be delimited with colons (:), periods (.), or dashes (-), but they display in the table with colons. Lines starting with "#" or "//" are ignored.

Export Button
Use the **Export** button to export the MAC to IP Mappings to CSV file. The following columns are part of the exported file: "macAddress,ipAddress,description".

Access Control Engine Settings

Engine settings provide advanced configuration options for Access Control engines. ExtremeCloud IQ Site Engine comes with a default engine settings configuration. If desired, you can edit these default settings or you can define your own settings to use for your Access Control engines.

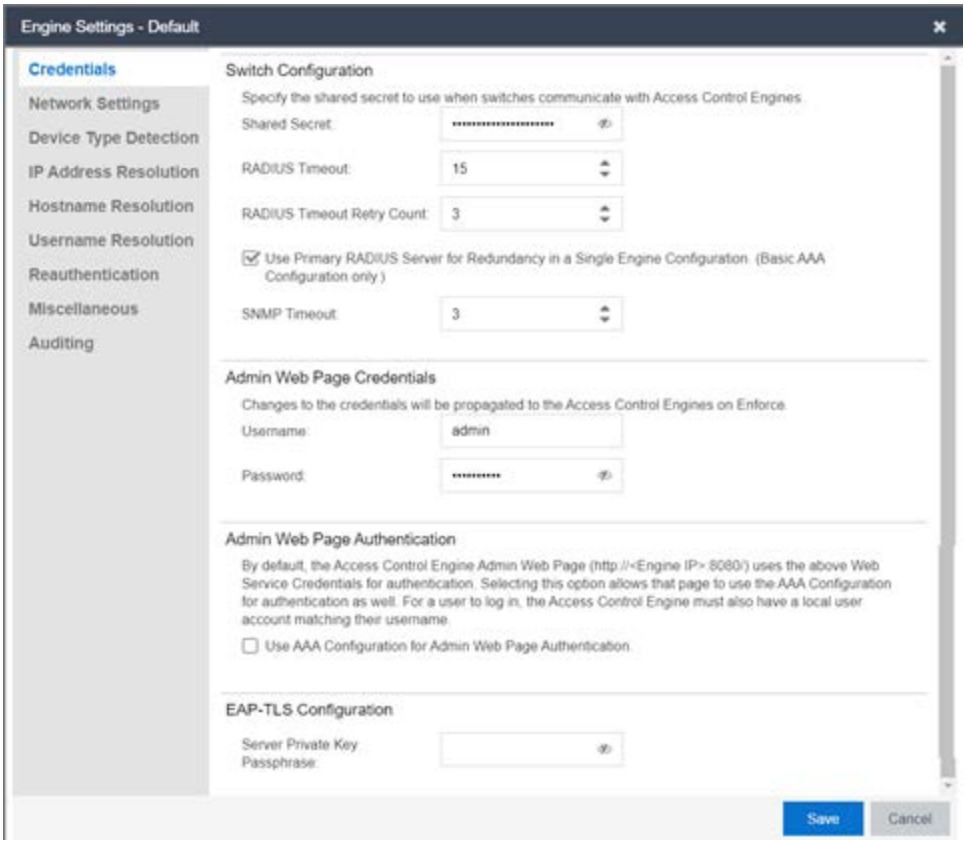
Launch the **Engine Settings** window by selecting the Control > Access Control tab, expanding the Engines left-panel menu, selecting an Access Control engine, and selecting the **Engine Settings** button. The **Engine Settings** window contains the following tabs available for configuration:

- Credentials
- Network Settings
- Device Type Detection
- IP Address Resolution
- Hostname Resolution
- Username Resolution
- Reauthentication
- Miscellaneous
- Auditing
- Advanced Settings

NOTE: To access status and diagnostic information for an Access Control engine, launch the Access Control Engine administration web page by right-clicking on the Access Control engine in the left-panel tree and selecting WebView. You can also access the administration web page using the following URL: https://<AccessControlEngineIP>:8444/Admin. The default user name and password for access to this web page is "admin/Extreme@pp." The username and password can be changed in the Web Service Credentials field on the Credentials Tab in the Engine Setting window.

Credentials

Use this tab to configure various parameters for your network engines including switch configuration, web service credentials, and EAP-TLS configuration.



Switch Configuration

Enter the shared secret that switches uses when communicating with Access Control engines.

Shared Secret

A string of alpha-numeric characters used to encrypt and decrypt communications between the switch and the Access Control engine. The shared secret is shown as a string of asterisks. Select the **Eye** icon to reveal the **Shared Secret**.

RADIUS Timeout

The amount of time (in seconds) that a switch waits before re-sending a RADIUS request to the Access Control engine. The default is 15 seconds and the maximum is 60 seconds. Note that the time specified should be long enough to allow the Access Control engine to receive a response from the RADIUS server.

NOTE: Although this option allows a maximum of 60 seconds, the actual maximum time allowed varies depending on the switch model. If a switch does not support the timeout value specified here, then the value is not set on the switch and an error message displays in the Access Control engine log. Check your switch documentation to verify supported values.

RADIUS Timeout Retry Count

The number of times the switch attempts to contact an Access Control engine with a RADIUS request, when an attempted contact fails. The default setting is 3 retries, which means that the switch retries a timed-out request three times, making a total of four attempts to contact the engine.

Use Primary RADIUS Server for Redundancy in Single Engine Configuration

If your Access Control deployment has only one Access Control engine, this option allows you to configure redundancy by using the primary RADIUS server as a backup when configuring the switches. This option would not apply to Access Control deployments using advanced AAA configurations with more than one set of RADIUS servers, or if you have configured primary and secondary Access Control engines.

SNMP Timeout

The amount of time (in seconds) that ExtremeCloud IQ Site Engine waits before re-trying to contact the Access Control engine. The value for this setting must be between 1 and 60.

NOTE: When SNMP requests are redirected through the server, all SNMP timeouts are extended by a factor of four (timeout X 4) to allow for the delays incurred by redirecting requests through the server.

Admin Web Page Credentials

Access Control Engine Web Service Credentials

The credentials specified here provide access to the Access Control engine administration web page and the web services interface between the ExtremeCloud IQ Site Engine server and the Access Control engine. ExtremeCloud IQ Site Engine provides default credentials that can be changed, if desired. Changes to the credentials are propagated to the Access Control engines on Enforce.

NOTE: The Web service credentials are used to communicate between ExtremeCloud IQ Site Engine and Access Control Engine. If you use non-default credentials and add a new Access Control Engine, then you must pre-provision the new Access Control Engine with the new credentials manually by running `/opt/nac/configWebCredentials <username> <password>`.

Admin Web Page Authentication

By default, the Access Control engine administration web page (`https://<AccessControlEngineIP>:8444/Admin/`) uses the above Web Service Credentials for authentication. However, you can configure the web page to use the AAA Configuration assigned to

that engine for authentication as well. This allows you to use LDAP or RADIUS authentication for the web page.

There are three steps for setting up the web page to use LDAP or RADIUS authentication:

1. Verify that the Access Control Configuration assigned to the engine has LDAP or RADIUS authentication configured in its AAA Configuration.
2. Create a local user account on the Access Control engine that matches the user name of the user logging in. Use the `useradd` command on the Access Control engine CLI to create the local user account.
3. Select the **Use Access Control AAA Configuration for Admin Web Page authentication** option here on the Credentials tab. Select **OK**. Enforce the change to the engine.

The Access Control engine begins using the AAA configuration for the administration web page authentication. Note that it may take the Linux operating system on the Access Control engine up to two minutes to recognize that the new user is valid.

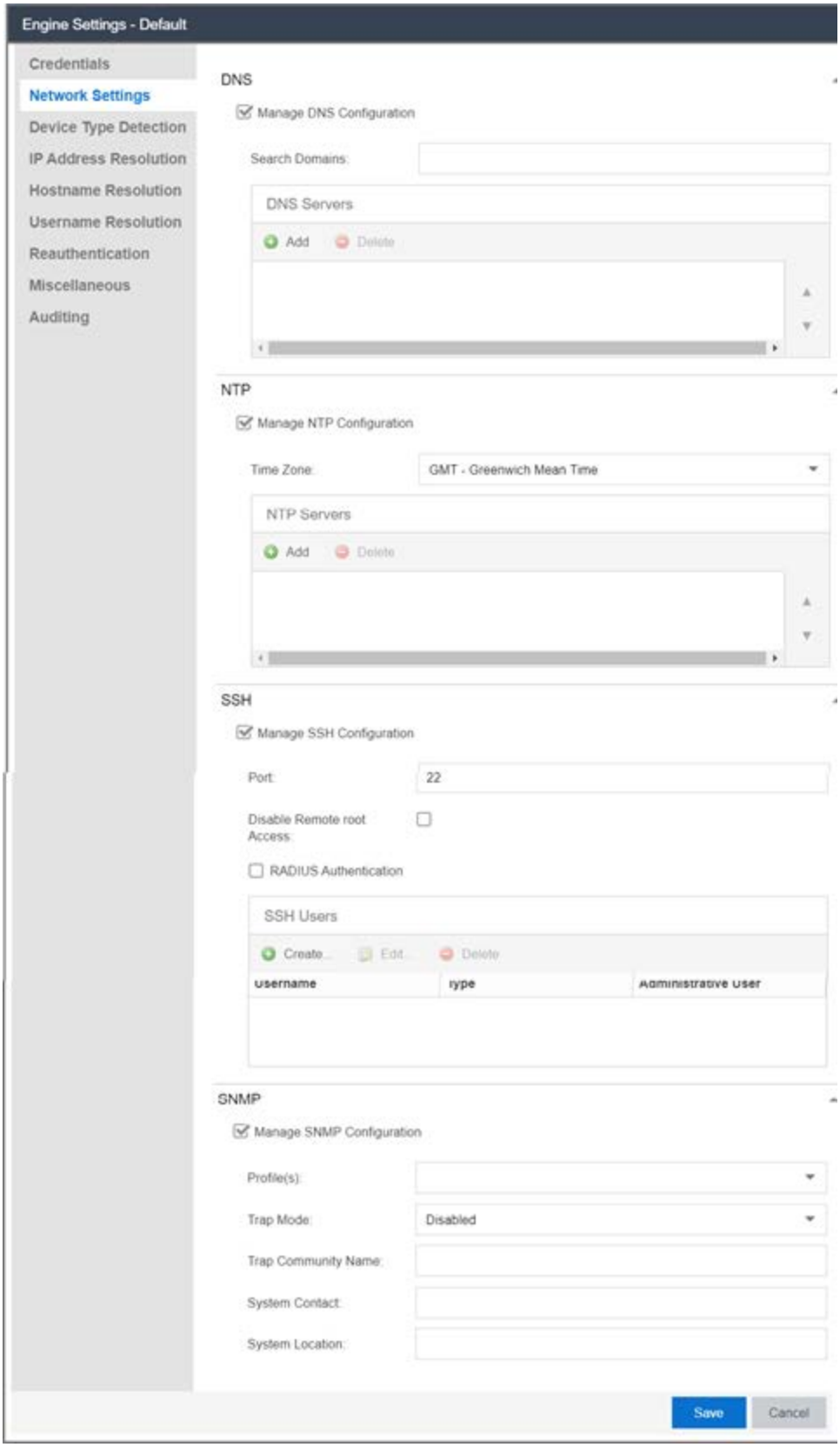
EAP-TLS Configuration

Server Private Key Passphrase

The Server Private Key Passphrase is used to encrypt the private key created during certificate request generation of server certificates for use by Access Control engines during Local EAP-TLS Authentication. The passphrase must be identical for all Access Control engines, and must be configured properly, or Local EAP-TLS Authentication does not operate successfully.

Network Settings

Use this tab to configure the following network services for the Access Control engine: DNS, NTP, SSH, and SNMP.


Engine Settings - Default
Credentials
Network Settings
Device Type Detection
IP Address Resolution
Hostname Resolution
Username Resolution
Reauthentication
Miscellaneous
Auditing
DNS
Manage DNS Configuration
Search Domains:
DNS Servers
Add
Delete
NTP
Manage NTP Configuration
Time Zone:
GMT - Greenwich Mean Time
NTP Servers
Add
Delete
SSH
Manage SSH Configuration
Port:
22
Disable Remote root Access:
RADIUS Authentication
SSH Users
Create...
Edit...
Delete
Username
Type
Administrative User
SNMP
Manage SNMP Configuration
Profile(s):
Trap Mode:
Disabled
Trap Community Name:
System Contact:
System Location:
Save
Cancel

Manage DNS Configuration

Select the Manage DNS Configuration checkbox and enter a list of search domains and DNS servers.

Search Domains

A list of search domains used by the Access Control engine when doing lookups by hostname. When an attempt to resolve a hostname is made, these domain suffixes are appended to the hostname of the device. For example, if someone does a ping to server1, ExtremeControl appends the search domains in an attempt to resolve the name: server1.domain1 server1.domain2, and so on.

DNS Servers

A list of DNS servers the Access Control engine sends DNS lookups to for name resolution. The list is used by both hostname resolution and by the DNS proxy. You can enter multiple servers for redundancy. Use the Up and Down arrows to list the servers in the order they should be used.

Manage NTP Configuration

NTP (Network Time Protocol) configuration is important for protocols such as SNMPv3 and RFC3576 which incorporate playback protection. In addition, having accurate time configured on the Access Control engine is essential for event logging and troubleshooting. Select the Manage NTP Configuration checkbox, specify the appropriate time zone, and create a list of NTP servers.

Time Zone

Select the appropriate time zone. This allows ExtremeControl to manage all date/time settings.

NTP Servers

A list of NTP servers. You can enter multiple servers for redundancy. Use the Up and Down arrows to list the servers in the order they should be used.

Manage SSH Configuration

SSH configuration provides additional security features for the Access Control engine. Select the Manage SSH Configuration checkbox and provide the following SSH information.

Port

The port field allows you to configure a custom port to be used when launching SSH to the engine. The standard default port number is 22.

Disable Remote root Access

Select this option to disable remote root access via SSH to the engine and force a user to first log in with a real user account and then su to root (or use sudo) to perform an action. When remote root access is allowed, there is no way to determine who is accessing the engine. With remote root access disabled, the /var/log/message file displays users who log in and su to root. The log messages looks like these two examples:

```
sshd[19735]: Accepted password for <username> from 10.20.30.40 port 36777
ssh2
su[19762]: + pts/2 <username>-root
```

Enabling this option does not disable root access via the console. Do not disable root access unless you have configured RADIUS authentication or this disables remote access to the Access Control engine.

RADIUS Authentication

This option lets you specify a centralized RADIUS server to manage user login credentials for users that are authorized to log into the engine using SSH. Select a primary and backup RADIUS server to use, and use the table below to create a list of authorized RADIUS users.

Authorized Users Table

Use the toolbar buttons to create a list of users allowed to log in to the Access Control engine using SSH. You can add Local and RADIUS users and grant the user Administrative privileges, if appropriate. A user that is granted administrative rights can run sudo commands and commands that only a root user would be able to run. For example, some commands that require administrative rights to run would be:

sudo nacctl restart
sudo reboot
sudo nacdb

If a user is not granted administrative rights, they can log in, view files, and run some commands such a ping and ls.

SNMP Configuration

The SNMP configuration section allows you to deploy SNMP credentials for the Access Control engine. The credentials can include different read/write credentials, for example, the read credential can be "public" and the write credential can be "private". In addition, basic host traps can be enabled from the Access Control engine. Select the Manage SNMP Configuration checkbox and provide the following SNMP information.

Profile

Use the drop-down list to select a device access profile (or multiple profiles) to use for the Access Control engine.

Trap Mode

Set the trap mode.

Trap Community Name

Supply the trap community name.

System Contact

Allows you to specify contact information for the person maintaining the device. Additionally, enter a backslash "\" between contacts to create a device group in a tiered tree structure. For example, to move the device into a device group called "John's Devices" within a device group

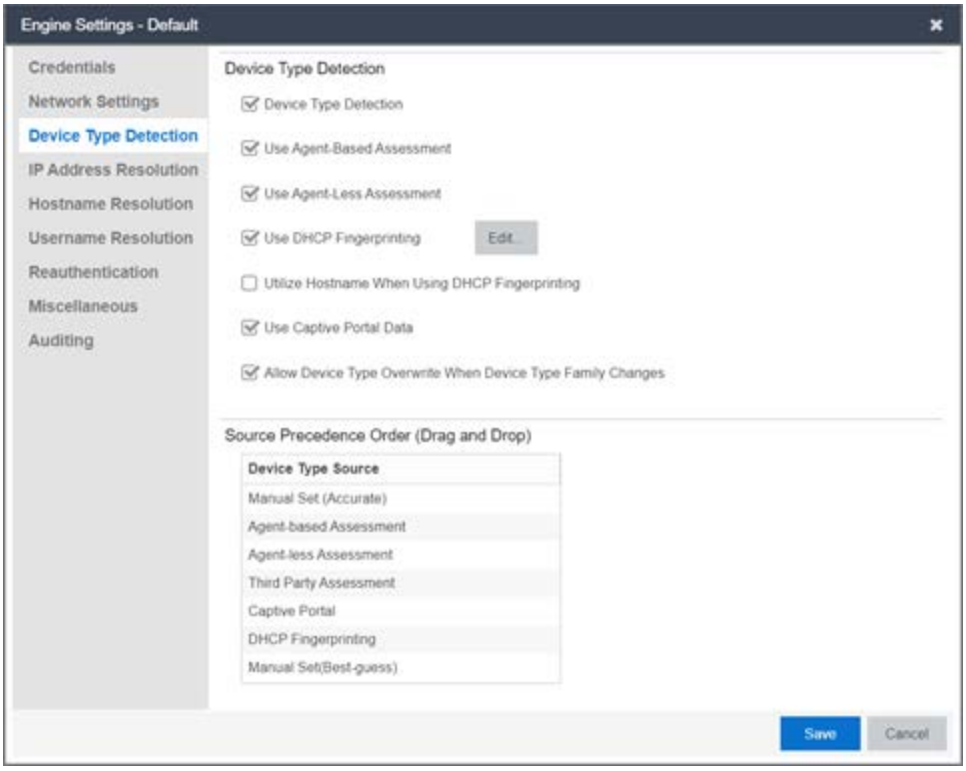
called "Quality Assurance Testing", enter **Quality Assurance Testing\John's Devices** in this field.

System Location

The physical location of the device. Additionally, enter a backslash "\" between locations to create a device group in a tiered tree structure. For example, to move the device into a device group called "London" within a device group called "Europe", enter **Europe\London** in this field.

Device Type Detection

The device type detection settings are advanced settings with complex requirements. Before editing these mappings, contact your Extreme Networks representative or Extreme Networks Support for information and assistance.



Device Type Detection

When the device type detection option is selected, ExtremeControl determines the end-system's device type using the selected detection methods below. Device type can be an operating system family, an operating system, or a hardware type, such as a printer or a smartphone. ExtremeControl uses the selected methods in the order configured in the detection source precedence. When this option is deselected, all device type detection functionality on the Access Control engine is disabled.

Use Agent-Based Assessment

This option causes the Access Control engine to query connected agents for the end-system device type. This is the most accurate method of device type detection.

Use Agent-less Assessment

This option allows the Access Control engine to use the results of an agent-less scan to determine the end-system's device type.

Use DHCP Fingerprinting

This option enables passive device type detection by fingerprinting DHCP packets snooped from an end-system. Select the **Edit** button to change the mapping of the DHCP packet properties to map to a different operating system or physical hardware type.

Utilize Hostname When Using DHCP Fingerprinting

This option allows the end-system hostname to be used to fine-tune device type detection results using DHCP fingerprinting. With certain device types, if DHCP fingerprinting does not result in a unique device type match, the hostname can be used as one possible tie-breaker. For example, with Apple iOS devices, the hostname can be a good indicator of the device type.

Use Captive Portal Data

This option allows the Access Control engine to detect the end-system's device type by using the agent string returned from the end-system's browser. This is the least secure method for device type detection, since it can be faked by the end-system. However, this option should be enabled if you have configured agent-based assessment with the "Allow Agent Unreachable for Unsupported Operating Systems" option enabled, so that the operating system can be detected when the end-system gets the Remediation web page when it is quarantined.

Allow Device Type Overwrite When Device Type Family Changes

This option allows the device type to be changed by a lower precedence detection method, if the device type family has changed. This option is required if you are supporting dual boot systems and have configured agent-based assessment with the "Allow Agent Unreachable for Unsupported Operating Systems" option enabled. For example, let's say Microsoft Windows XP SP3 was detected by an agent running on a dual boot end-system. If the system is rebooted and switched to Red Hat Linux 4.4, and the end-system is quarantined for not running the agent, the device type detection using captive portal data (a lower precedence method) would yield the device type family of Linux instead of Windows. The device type would be updated and would now pass the unsupported operating system test, and be allowed onto the network.

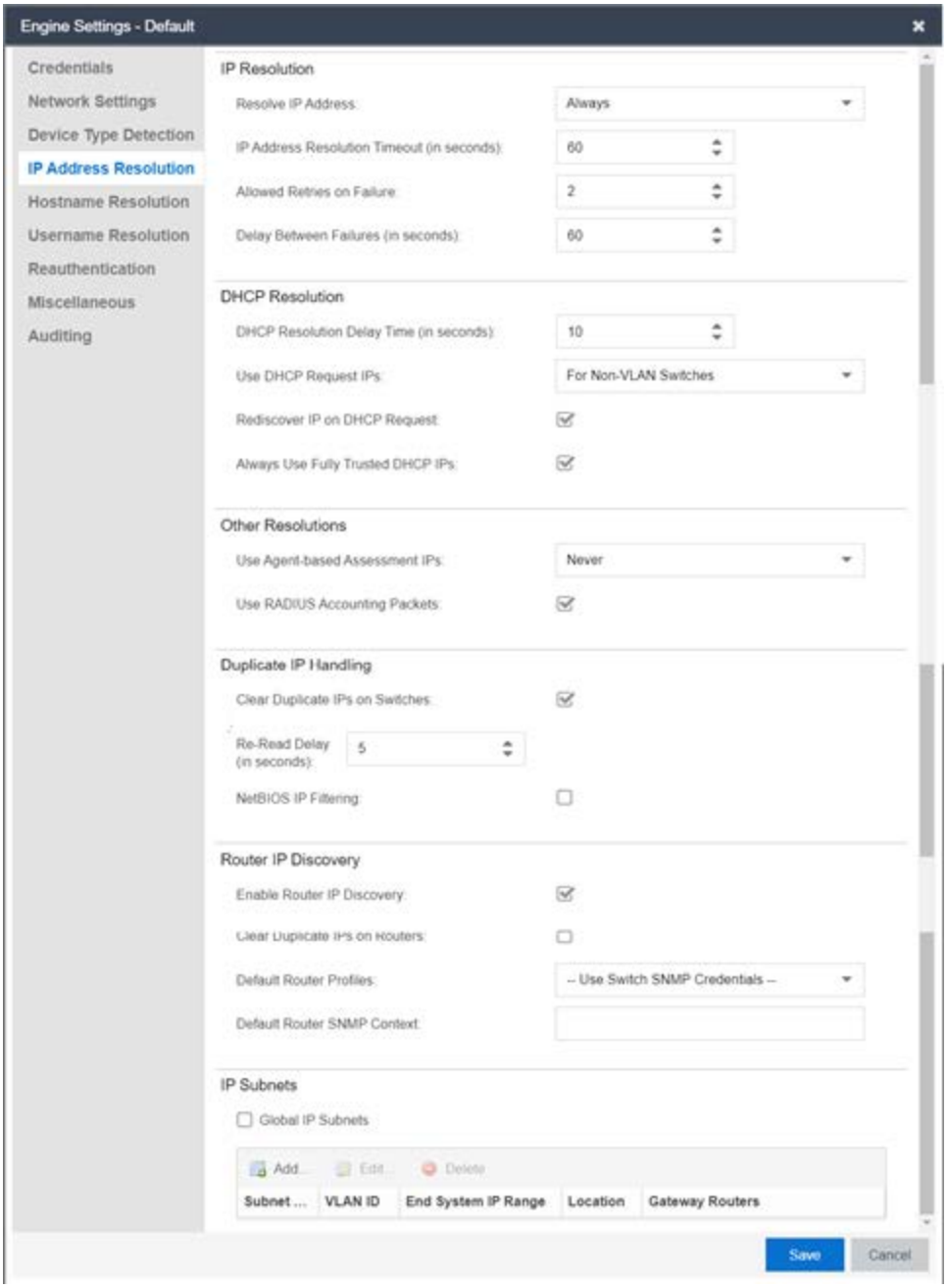
Source Precedence Order

This list specifies the precedence for the source of information used to determine end-system device type, with the highest precedence listed first. Select an item in the list and use the Move Up and Move Down arrows to change its position in the list. Manual Set refers to device type information that has been hard-coded via ExtremeCloud IQ Site Engine Web Services. Typically, Manual Set (Accurate) has the highest precedence because the exact device type is known and the remaining sources of detection aren't needed, while Manual Set (Best-Guess)

has the lowest precedence because it is a best-guess of the device type and should be used only when the other detection methods cannot provide a device type.

IP Address Resolution

The IP Address Resolution tab is used to define how and when ExtremeControl resolves an end-system's MAC address to an IP address for the end-system. These parameters are applicable for Access Control engines and L2 Access Control Controllers, but not L3 Access Control Controllers.



Resolve IP Address

Specify when an Access Control engine resolves the IP address for end-systems:

- Always - (Default) Resolve the IP address for every end-system that ExtremeControl sees.
- Only for Assessment - Resolve the IP address for end-systems that need to be assessed (scanned).

IP Address Resolution Timeout

Enter the maximum time an Access Control engine waits trying to resolve an IP address from an end-system's MAC address before giving up and returning the Error state (MAC to IP Resolution Timed Out) for that end-system.

Allowed Retries on Failure

The number of attempts made to resolve the IP address after the first attempt fails. The default setting is 2 retries, which means that ExtremeControl retries a timed-out request two times, making a total of three attempts to resolve the IP address. Enter the amount of delay time in seconds that ExtremeControl waits before retrying to resolve the IP address.

Delay Between Failures

Enter the amount of time an Access Control engine waits after failing to resolve an IP address before attempting again.

DHCP Resolution Delay Time

The number of seconds an Access Control engine should wait after learning about an end-system before attempting to resolve the end-system's IP address. This delay is used to allow the end-system to negotiate its DHCP IP address. If Port Link Control is enabled, this delay is used after the Access Control engine links down/up the port to force the end-system to request a new IP address on the new VLAN.

NOTE: If the delay time specified here is less than the amount of time the end-system needs to renew its IP address, then the Access Control engine may resolve the end-system's IP address incorrectly. This is a problem when assessment is enabled and may cause the engine to scan the incorrect IP address. Be sure to take into account the amount of time required for an end-system to get a new IP address when setting the delay time value.

Use DHCP Request IPs

Specify when, if ever, an IP address learned from a DHCP request packet could be used when resolving an end-system's IP address. This option is applicable only for Access Control engines, since an inline Access Control Controller should always hear the DHCP response as well.

- Always - Always consider the IP address learned from a DHCP request for an end-system's IP, after all more reliable methods have been exhausted.
- Never - Never consider an IP address learned from a DHCP request when resolving an end-system's IP address. In a situation where the Access Control engine receives DHCP

packets from both the client and server, the gateway uses this IP when these packets are received during the IP resolution process. With subsequent authentications for which there is no additional DHCP exchange, Access Control uses the enabled resolution options to resolve the IP address but does not use any previously learned DHCP information to resolve the IP.

- For Non-VLAN Switches Only - (Default) Only consider IP addresses learned from DHCP request packets when the NAS switch the end-system was authenticated for does not use VLANs for access control. The IP addresses from request packets in a VLAN environment is always incorrect, because as an end-system transitions through VLANs, it always requests the IP from the previous VLAN.

Rediscover IP on DHCP Request

When this option is selected, ExtremeControl re-runs IP resolution on an authenticated end-system if a DHCP request causes its IP address to change. In this instance, the Access Control policy applies to the new IP address and removed from the old IP address, and assessment scans and port resolution are not performed.

Always Use Fully Trusted DCHP IPs

When this options is selected, the Access Control engine runs a DHCP table lookup to see if DHCP IP address is fully trusted for the end-system. If the address is fully trusted in the table, ExtremeControl resolves the IP address for the end-system without attempting additional resolution processes. If the address is not fully trusted or not found, the Access Control engine attempts to resolve the IP address as normal. When this option is not selected, there is no fast IP resolution using DHCP IP packets.

Use Agent-based Assessment IPs

Specify when, if ever, an IP address reported by a connected agent could be used when resolving an end-system's IP address. This process looks for the end-system's MAC address in the list of MAC addresses from known connected agents. If an agent is connected and heartbeats during the IP Resolution process, then ExtremeControl uses the IP address of that agent.

- Always - Always consider the IP address reported by a connected agent for an end-system's IP, after all more reliable methods have been exhausted.
- Never - (Default) Never consider an IP address reported by a connected agent when resolving an end-system's IP address.
- For Non-VLAN Switches Only - Only consider IP addresses reported by a connected agent when the NAS switch the end-system was authenticated for does not use VLANs for access control.

Use RADIUS Accounting Packets (IPv4 address)

When this option is selected, if the Access Control engine receives a RADIUS accounting packet with a Framed-IP-Address in it, the engine skips IP resolution and uses the IP address in the RADIUS accounting packet.

Use RADIUS Accounting Packets (IPv6 address)

When this option is selected (Access Control engine enforce required), the Framed-IPv6-Address attributes learned from the RADIUS accounting packet are shown in the IPv6 Address column.

NOTE: IPv6 address resolution by SNMP is not used if enabled, (even when the 'Enable IPv6 Addresses for End-Systems' is enabled in **Options> Access Control> Advanced**).

Clear Duplicate IPs on Switches

Select this option to have an Access Control engine clear out duplicate entries in the node alias and ARP tables of the NAS switch the end-system was authenticated for, if duplicates are found while trying to resolve the IP address of an end-system. The Access Control engine then tries to re-read the IP address from the table to find the most recent entry.

Re-Read Delay

Specify the amount of time in seconds that an Access Control engine waits after clearing duplicate IPs on a switch or a router before re-reading the node alias or ARP tables.

NetBIOS IP Filtering

This option causes the Access Control engine to make NetBIOS requests to a list of IP addresses, if multiple IP addresses are found when trying to resolve the IP address of an end-system. See NetBIOS Timeout and NetBIOS Timeout Retry Count on the Miscellaneous tab.

Enable Router IP Discovery

This option causes ExtremeControl to make requests to an end-system's gateway router ARP table to try to resolve the IP address for an end-system, if the Access Control engine was unable to resolve the IP address by querying the NAS switch. The gateway router for an end-system can be discovered by the relay router field of a DHCP packet or by using the gateway router defined for an IP subnet for the VLAN an end-system is put into by ExtremeControl. See IP Subnets.

Clear Duplicate IPs on Routers

This option causes an Access Control engine to clear out duplicate entries in the ARP tables of an end-system's gateway router, if duplicates are found while trying to resolve the IP address of an end-system. The Access Control engine then tries to re-read the IP address from the table to find the most recent entry. See Clear Duplicate IP Re-Read Delay.

Default Router Profile

The profile used to make SNMP requests to the gateway router for an end-system, if one is not defined for a specific router's interface IP address as part of an IP subnet. Use the **Edit** button to open the Profiles/Credentials tab in the Authorization/Device Access window where you can define authentication credentials and create the profiles that use those credentials.

Default Router SNMP Context

The SNMP context used when making requests to the router, if the credentials used for the router are SNMP v3 and the specific router's interface IP address has not been defined as part of an IP subnet.

IP Subnets

IP subnets are used to assist in IP resolution in the following three scenarios:

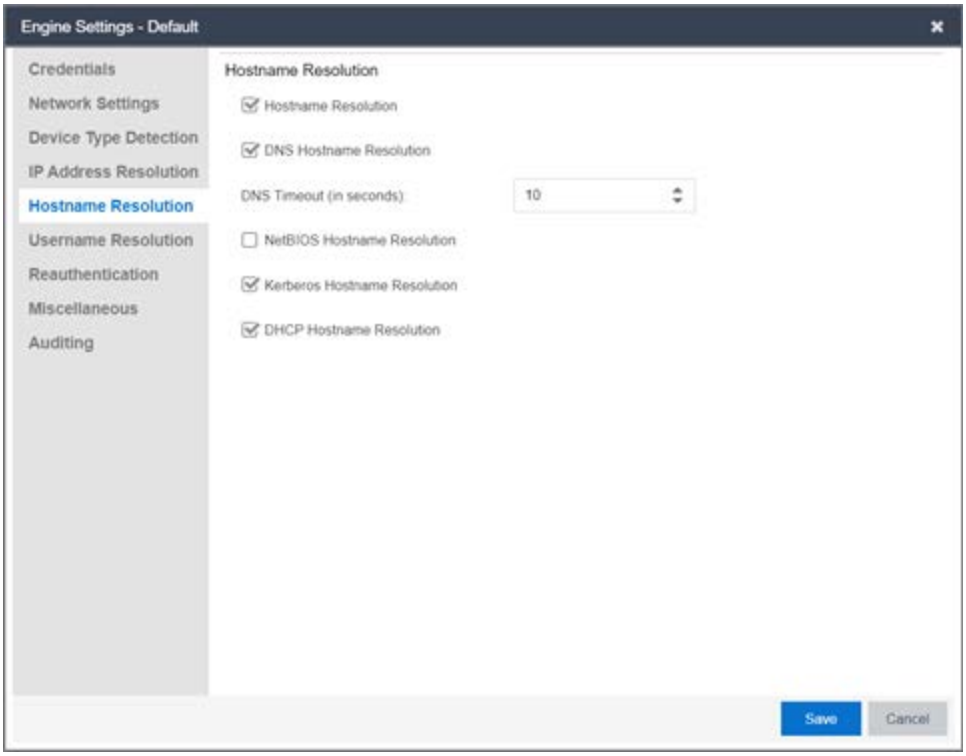
- If a switch is using RFC3580 (VLAN enforcement of access control), the process for determining an IP address is much more difficult. In this scenario, IP subnets can be defined for each VLAN to provide an IP range filter, which can be used to filter the list of IPs discovered on the switch. IP subnets also provide a way to specify a gateway router for the VLAN's subnet, which can be used for doing SNMP reads on a router if DHCP snooping did not capture the relay router.
- When VRRP or HSRP is used, and you want ExtremeControl to query the router if needed, ExtremeControl needs to know the primary/secondary router relationship. This order of precedence can be defined in the IP subnet and ensures that ExtremeControl queries the primary router first to get the most accurate data. This is needed in a VRRP or HSRP environment, because both routers send out a DHCP inform message, and it is most likely that the Access Control engine gets the secondary router's message last causing it to query the incorrect router.
- When DHCP snooping is used, the router SNMP credentials are not the same for all routers. In this scenario, if you want ExtremeControl to query the router for IP resolution, the IP subnets can be used to define the mapping between the relay router IPs and the correct SNMP credentials to use for them.

You can add, edit, or delete IP subnets using the toolbar buttons at the top of the table. There is also a File Import button that lets you import a file of IP subnets; see the File Import window for the file format that must be used.

The **Global IP subnets** option is used to create a global list of IP ranges used for the purpose of IP Resolution. The IP Resolution process ignores any IP address outside the configured ranges. The checkbox is disabled unless there is at least one subnet configured.

Hostname Resolution

The tab is used to define how and when ExtremeControl resolves an end-system's hostname and an end-system's username. These parameters are engine for Access Control engines, L2 Access Control Controllers, and L3 Access Control Controllers.



Hostname Resolution

Use this checkbox to enable or disable hostname resolution for Access Control engines. Hostname resolution is only performed for end-systems for which ExtremeControl has an IP address.

DNS Hostname Resolution

This option allows the use of reverse DNS lookup on the Access Control engine to resolve an end-system's hostname. In order for this option to work, a valid DNS server IP address must have been specified when the Access Control engine was installed. Use the **DNS Timeout** field to specify the amount of time in seconds that the Access Control engine waits after making a reverse DNS lookup prior to giving up and moving on to the next hostname resolution mechanism.

NetBIOS Hostname Resolution

This option allows the Access Control engine to make a NetBIOS request to the end-system to query the end-system for its hostname. See NetBIOS Timeout and NetBIOS Timeout Retry Count on the Miscellaneous tab.

Kerberos Hostname Resolution

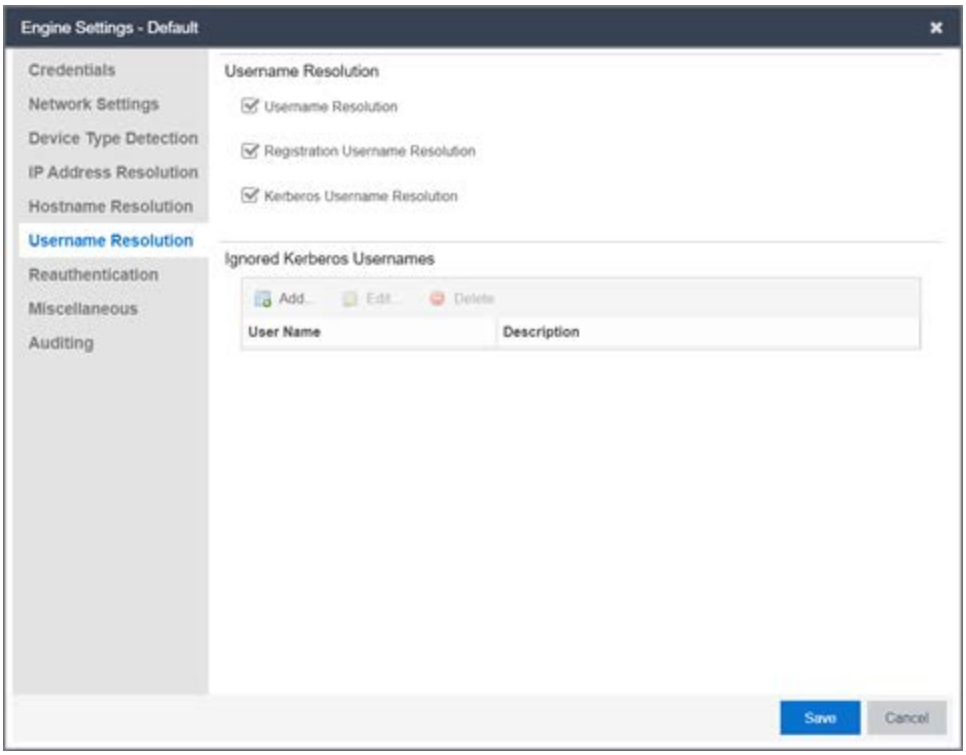
This options allows the Access Control engine to do a lookup in the table of data learned from Kerberos snooping, to resolve the end-system's host name.

DHCP Hostname Resolution

This options allows the Access Control engine to do a lookup in the table of data learned from DHCP snooping, to resolve the end-system's host name.

Username Resolution

The tab is used to define how and when ExtremeControl resolves an end-system's hostname and an end-system's username. These parameters are engine for Access Control engines, L2 Access Control Controllers, and L3 Access Control Controllers.



Username Resolution

Use this checkbox to enable or disable username resolution, which allows the Access Control engine to try resolve the name of a user currently on an end-system when the username was not part of the authentication request. MAC authentication and L3 Access Control Controller authentication are the two cases where username resolution can currently be used.

Registration Username Resolution

This options causes ExtremeControl to use the username used for authenticated registration or the user's full name for unauthenticated registration in the format: Last Name, First Name.

Always Override Username by Registered User

Use this checkbox to enable or disable an override value in the User Name field with the value in the Registered User column:

- If enabled, the value from Registered User is copied to the User Name field even when 802.1X authentication is used.

- If disabled, and the user or computer authenticates through 802.1X authentication, then the User Name field contains the username from the 802.1X authentication.
- If disabled, and the user is registered with Authenticated Registration or Guest Registration, the Registered User field contains the name used during registration. If the User Name is empty, then the Registered User is copied to the User Name field.
- The User Group conditions in NAC rules are using the value in the User Name field.

Kerberos Username Resolution

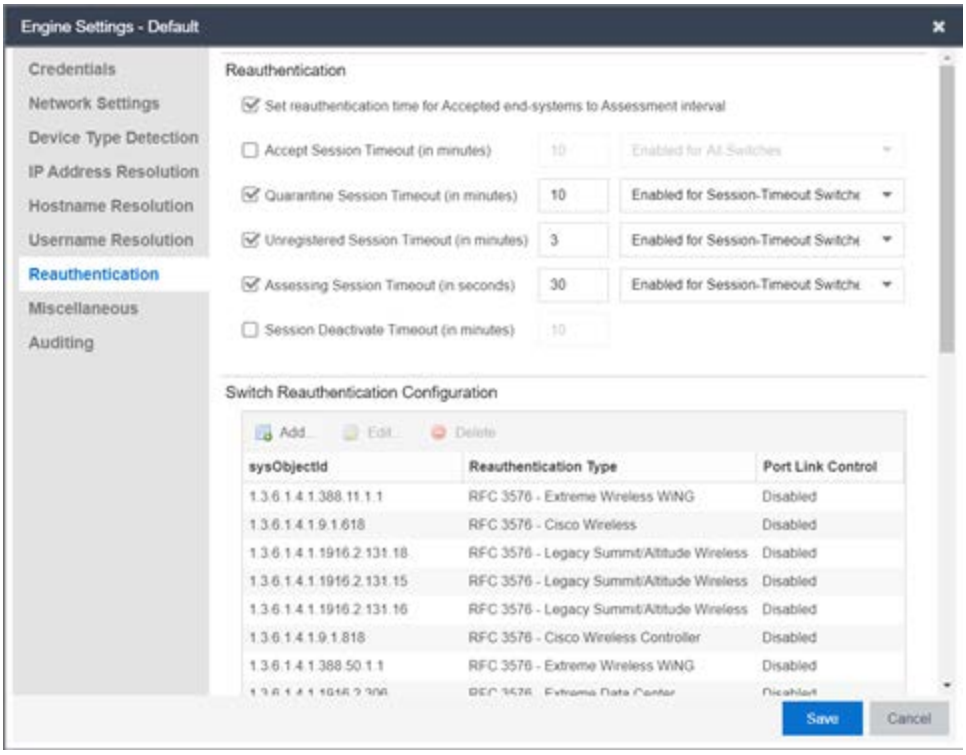
This options allows the Access Control engine to do a lookup in the table of data learned from Kerberos snooping, to resolve the name of the user currently logged into the end-system.

Ignored Kerberos Usernames

The table is used to define usernames for which Kerberos data is ignored. This is useful when applications running on an end-system use a global user over the Kerberos protocol to pass information for a program. Two known cases of this would be Sophos Anti-Virus software and the IBM Rational ClearCase source control system. You can add, edit, or delete entries using the toolbar buttons at the top of the table.

Reauthentication

This tab is used to define global session-timeout behavior for L2 Access Control Controllers and Access Control engines, and how Access Control engines reauthenticates end-systems on various NAS switches. This tab is not applicable for L3 Access Control Controllers.



Set Reauthentication Time for Accepted End-Systems to Assessment Interval

This option allows the Access Control engine to set session-timeouts for accepted end-systems, causing the end-system to be reauthenticated the next time a scan needs to be performed. This option is required for networks using 802.1X authentication on wireless switches that do not support the IEEE 802.1X Port Reauthenticate MIB. It is also required for networks using MAC or Web-Based authentication on third-party switches. These switches do not have a mechanism to force re-authentication on end-systems when assessment is complete. This checkbox does not apply for Layer 3 Access Control Controller engines.

Accept Session Timeout

If enabled, this timeout applies to all end-systems that are accepted, but not considered by ExtremeControl to be unregistered end-systems. If both this option and the "Set Reauthentication Time For Accepted End-Systems to Assessment Interval" option are enabled, Access Control uses the lower value. The timeout can be either:

- Enabled For Session-Timeout Switches - (Default) The timeout only applies to accepted end-systems authenticated for a NAS switch where ExtremeControl cannot reauthenticate sessions on demand via SNMP or RFC3576.
- Enabled for All Switches - The timeout is applied to any accepted end-system (not considered by ExtremeControl to be unregistered) on any switch.

Quarantine Session Timeout

If enabled, this timeout applies to all end-systems quarantined by ExtremeControl. The timeout can be either:

- Enabled For Session-Timeout Switches - (Default) The timeout is only applied to quarantined end-systems that were authenticated for a NAS switch where ExtremeControl cannot reauthenticate sessions on demand via SNMP or RFC3576.
- Enabled for All Switches - The timeout is applied to any quarantined end-system on any switch.

Unregistered Session Timeout

If enabled, this timeout applies to all end-systems determined to be unregistered by ExtremeControl. The timeout can be either:

- Enabled For Session-Timeout Switches - (Default) The timeout only applies to unregistered end-systems authenticated for a NAS switch where ExtremeControl cannot reauthenticate sessions on demand via SNMP or RFC3576.
- Enabled for All Switches - The timeout is applied to any unregistered end-system on any switch.

Assessing Session Timeout

If enabled, this timeout applies to all end-systems being scanned by ExtremeControl. The timeout can be either:

- Enabled For Session-Timeout Switches - (Default) The timeout applies to end-systems being assessed authenticated for a NAS switch where ExtremeControl cannot

reauthenticate sessions on demand via SNMP or RFC3576.

- Enabled for All Switches - This option tells ExtremeControl to apply the session timeout for end-systems being assessed on any switch.

Session Deactivate Timeout

This option can be used to provide more up-to-date information about which end-systems are still active on the network. When it is enabled, ExtremeControl checks periodically to determine if an authentication request is received from an end-system within the specified time. If a user is still on the network, then the user is reauthenticated and a new event is generated stating the user is still active on the network. If the user is no longer on the network, the session is removed on the switch and the end-system is displayed in ExtremeControl with the **Disconnected** state. (Note that when a user leaves the network within the period of time specified, ExtremeControl does not display them as "**Disconnected** until the specified time has passed.) While this option does provide a more up-to-date list of active end-systems, RADIUS accounting should be used to provide real-time connection status. This option is useful when RADIUS accounting is not desired or is not supported on certain network devices.

NOTE:	The timeout process could be off by approximately 60 seconds from the specified time, depending on when ExtremeControl runs the check for authentication requests.

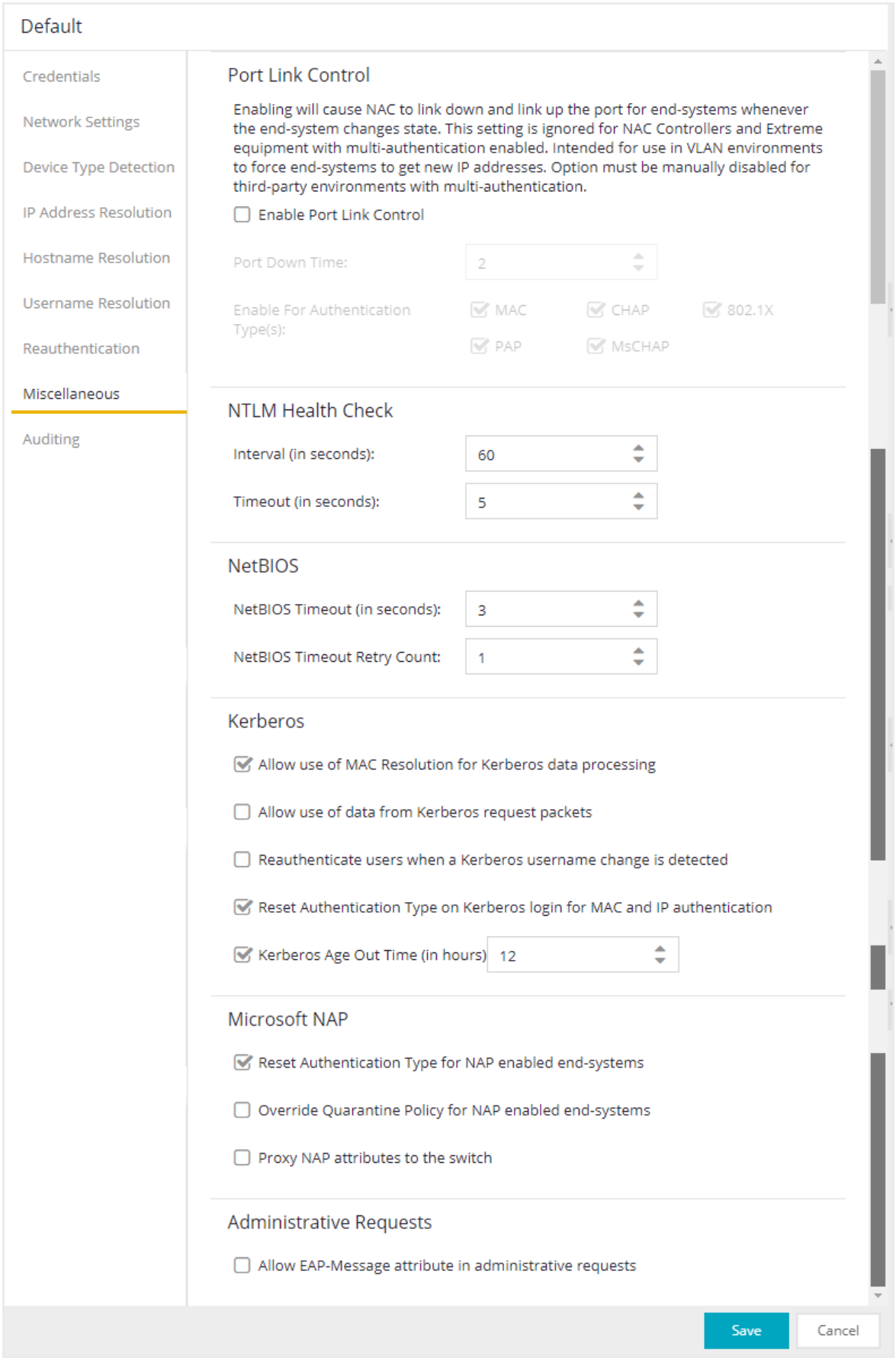
Switch Reauthentication Configuration

This table is used to configure the reauthentication method an Access Control engine uses on a switch. For example, you may want to add support for another wireless switch. In this case, you would add an entry for the new switch by selecting the Add button, entering the sysObjectId of the switch, and setting the Reauthentication Type to either RFC3576 (if the switch supports it) or Session Timeout. This table is also where you can disable port link control for switches by selecting the switch, selecting the Edit button, and setting the Port Link Control option to disabled.

If you've deleted or edited any of the default configurations, the **Restore Defaults** button restores them to their original state and add back any that are missing. Any custom entries you added are retained unless they have the same sysObjectId as a default configuration. Following a restore, you need to save the configurations.

Miscellaneous

Use this tab to configure various parameters for your network engines including port link control, NetBIOS, Kerberos, and Microsoft NAP.


Default
Credentials
Network Settings
Device Type Detection
IP Address Resolution
Hostname Resolution
Username Resolution
Reauthentication
Miscellaneous
Auditing
Port Link Control
Enabling will cause NAC to link down and link up the port for end-systems whenever the end-system changes state. This setting is ignored for NAC Controllers and Extreme equipment with multi-authentication enabled. Intended for use in VLAN environments to force end-systems to get new IP addresses. Option must be manually disabled for third-party environments with multi-authentication.
Enable Port Link Control
Port Down Time:
2
Enable For Authentication Type(s):
MAC
CHAP
802.1X
PAP
MsCHAP
NTLM Health Check
Interval (in seconds):
60
Timeout (in seconds):
5
NetBIOS
NetBIOS Timeout (in seconds):
3
NetBIOS Timeout Retry Count:
1
Kerberos
Allow use of MAC Resolution for Kerberos data processing
Allow use of data from Kerberos request packets
Reauthenticate users when a Kerberos username change is detected
Reset Authentication Type on Kerberos login for MAC and IP authentication
Kerberos Age Out Time (in hours)
12
Microsoft NAP
Reset Authentication Type for NAP enabled end-systems
Override Quarantine Policy for NAP enabled end-systems
Proxy NAP attributes to the switch
Administrative Requests
Allow EAP-Message attribute in administrative requests
Save
Cancel

Port Link Control

Enable Port Link Control

Use this checkbox to enable or disable port link control. Port link control is required if you are using VLAN only (RFC 3580) switches or if you are using policy with VLANs on EOS policy-enabled switches. When a VLAN is assigned to a switch port, the end-system needs to get a new IP address for the assigned VLAN. To do this, the Access Control engine links down the port, waits the configured amount of time, and then links up the port, causing the end-system to make a new DHCP request and get a new IP address.

Be aware that when multiple devices are connected to a switch port where authentication is enabled (such as an IP phone cascaded with a PC on a single port), port link down disconnects all devices. In this scenario, you may want to disable port link control, set the Access Control profile to "Use Assessment Policy During Initial Assessment Only," and set the DHCP lease time for the IP address pools that correspond to the VLAN(s) associated to the Quarantine and Assessment access policies to a low value (e.g. 1 minute).

This setting is ignored for Access Control Controllers and EOS equipment with multi-authentication enabled. The option must be manually disabled for third-party environments with multi-authentication.

In the **Port Down Time** field, enter the amount of time in seconds that the engine waits before linking up the port. The time must be sufficient to cause the end-system to make the DHCP request.

In the **Enable for Authentication Types** field, you can enable port link control for only specific authentication types, depending on the checkboxes you select. For example, you can disable port link control for 802.1x, but have it enabled for MAC authentication so that a port is only linked down when a MAC authentication session changes VLANs.

NTLM Health Check

Windows provides an authentication protocol called New Technology LAN Manager (Windows NTLM). NTLM is a challenge-response authentication protocol used to authenticate a client to a remote on an Active Directory. NTLM Health Check is an Access Control test that can be enabled in LDAP configurations using NTLM Authentication, and actively used in Access Control AAA configuration rules.

When enabled, the health check runs at regular intervals and test the current domain controller for the specified domain. The test domain is specified in the LDAP configuration. The interval and a timeout can be configured in the **Miscellaneous** section of ExtremeControl settings (**Control > Access Control > Configuration > Global Engine Settings > Engine Settings > Default > Miscellaneous**).

Interval (in seconds)

This value tells Access Control how often to run the health check.

Timeout (in seconds)

This value tells Access Control how long to wait for an authentication response from the Active Directory. If the timeout threshold is exceeded, the failover occurs and the `Access Control Lost Partial Contact with LDAP Service` alarm is generated.

To complete the health check setup, refer to the documentation sections on NTLM Authentication and Advanced. To configure these additional settings in Access Control, go to **Control > Access Control > Configuration > AAA > LDAP Configuration**.

OCSP Responder Health Check

OCSP is a protocol to send a request to the OCSP responder to validate the client certificate during the authentication. If both the Default Responder URL and the Secondary Responder URL are defined, then the Access Control Engine monitors the reachability of the Default Responder and can failover to the Secondary Responder if the Default Responder is not reachable.

Interval (in seconds)

This value tells Access Control Engine how often to check the reachability of the Default Responder URL.

Timeout (in seconds)

This value tells Access Control Engine how long to wait for a response from the Default Responder URL.

Timeout Retry Count

This value tells Access Control Engine how many times to re-check for reachability of the Default Responder URL, before performing a failover to the Secondary Responder URL.

Entra ID Attributes

The User Group type **User: OpenID User Group** by default provides the option to check if the user is a member of the Security Group in Entra ID.

Resolve Extension Attributes from EntraID

If enabled the values of extensionAttribute1 through extensionAttribute15 are requested through an API from Entra ID.

Resolve Custom Security Attribute from EntraID

If enabled the values of Custom Security Attributes are requested through an API from Entra ID.

Enter the name of the custom security attribute as the **Attribute Name** in the user group definition. Enter the expected value as the **Attribute Value**.

NetBIOS

This section controls the timeout and retries that an Access Control engine uses when making NetBIOS requests for IP resolution, MAC resolution, or hostname resolution.

NetBIOS Timeout

The amount of time in seconds that an Access Control engine waits for a response to a NetBIOS request to an end-system, before giving up on that request and retrying.

NetBIOS Timeout Retry Count

The number of times an Access Control engine retries making a NetBIOS request to an end-system, if the end-system does not respond.

Kerberos

Controls how an Access Control engine deals with data it receives from Kerberos snooping.

Allow Use of MAC Resolution for Kerberos Data Processing

When end-systems are behind a router, the Access Control engine uses MAC resolution to resolve an end-system's MAC address from its IP address. This is because when end-systems are behind a router (not in the local network), the Kerberos packets carry the MAC address of the router instead of the end-system. This option allows you to turn off the use of MAC resolution for Kerberos processing, if desired.

Allow Use of Data from Kerberos Request Packets

This option allows the use of data such as username and hostname, from Kerberos request packets. The data in the request packet is provided by the user, and is not guaranteed to be accurate, since it is not authenticated.

Reauthenticate Users on Kerberos Username Change Detected

This option causes the Access Control engine to reauthenticate a user if the username in the Kerberos packet changes.

Reset Authentication Type on Kerberos Login for MAC and IP Authentication

This option is supported for Access Control deployments with inline Access Control Controllers that can capture the end user login. When a user logs in via Kerberos, (for example, a user logs into a Windows domain,) the Access Control Controller resets the authentication type from MAC (for an L2 Access Control Controller) or IP (for an L3 Access Control Controller) to Kerberos. The Kerberos authentication type can then be used by rules to give elevated access to users that have successfully logged into a Windows domain.

Kerberos Age Out Time

This option provides a way to disable the aging out of Kerberos authentication data. This authentication data is used by ExtremeControl to provide elevated access to end-systems. By default, the authentication data is automatically aged out every 12 hours. During that 12-hour period, any time the end-system reauthenticates with ExtremeControl, the user would receive

their elevated access privileges. After the 12 hours is exceeded and the authentication data is aged out, the end-system must log in again to get their elevated access. You can use this option to change the age out time or disable the aging altogether. For example, you might want to change the 12 hours to 8 hours, based on a shorter 8-hour workday.

WARNING:	Keep in mind that disabling the age out would create a potential security hole. Elevated access is tied to the end-system, so if it isn't aged out, the elevated access is always available. For example, if a user leaves their laptop and someone logs them out and then logs in as a local user, that person continues to have the elevated access privileges of the original user. Also, a person could spoof someone else's MAC address and receive their elevated access, if the access isn't aged out.

Microsoft NAP

This section provides options related to Microsoft NAP for Windows.

Reset Authentication Type for NAP Enabled End-Systems

When this option is enabled, the Access Control engine resets the authentication type from 802.1x to MS NAP (Microsoft NAP), if the end-system authenticating is NAP-enabled (Windows XP SP2 or higher) and the 802.1x authentication request was proxied to a NAP-enabled server. The MS NAP (Microsoft NAP) authentication type can then be used by rules to assign a different Access Control profile. To configure ExtremeControl to perform as it did in ExtremeControl version 3.1.x, you can create a rule that maps the MS NAP (Microsoft NAP) authentication type to the Pass Through Access Control Profile. With this profile, ExtremeControl does not assess the end-system, and uses the NAP determination of whether or not to quarantine a user.

Override Quarantine Policy for NAP Enabled End-Systems

This option allows ExtremeControl to replace the quarantine policy for NAP-enabled end-systems, using the quarantine policy defined in the profile's Use Quarantine Policy field. Be aware that when this NAP option is enabled, the Use Quarantine Policy checkbox becomes active for all Access Control profiles, even if assessment is disabled. However, you can deselect the checkbox for an individual profile, in which case the policy from the RADIUS attributes is applied.

Proxy NAP Attributes to Switch

This option is disabled by default. When disabled, the following attributes are **not** proxied to the switch if they are present in the response from the backend RADIUS server:

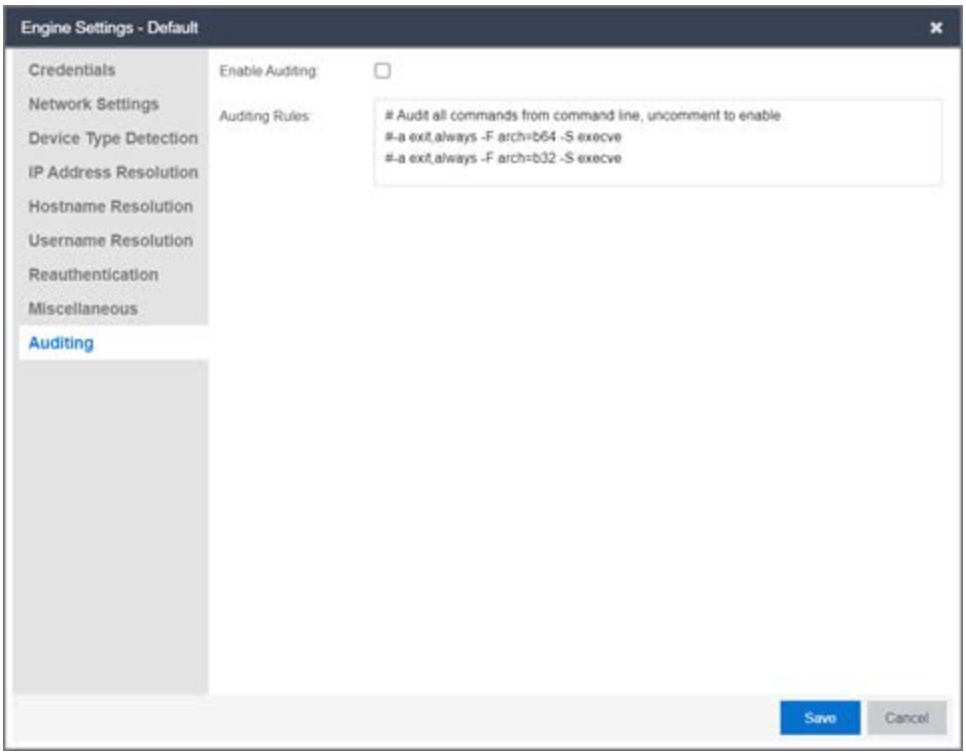
- MS-Machine-Name
- MS-Extended-Quarantine-State

- MS-RNAP-Not-Quarantine-Capable
- MS-Quarantine-State

If the option is enabled, the attributes are proxied to the switch.

Auditing

Use this tab to enable auditing of users connected to the Access Control engine CLI via SSH.



Enable Auditing

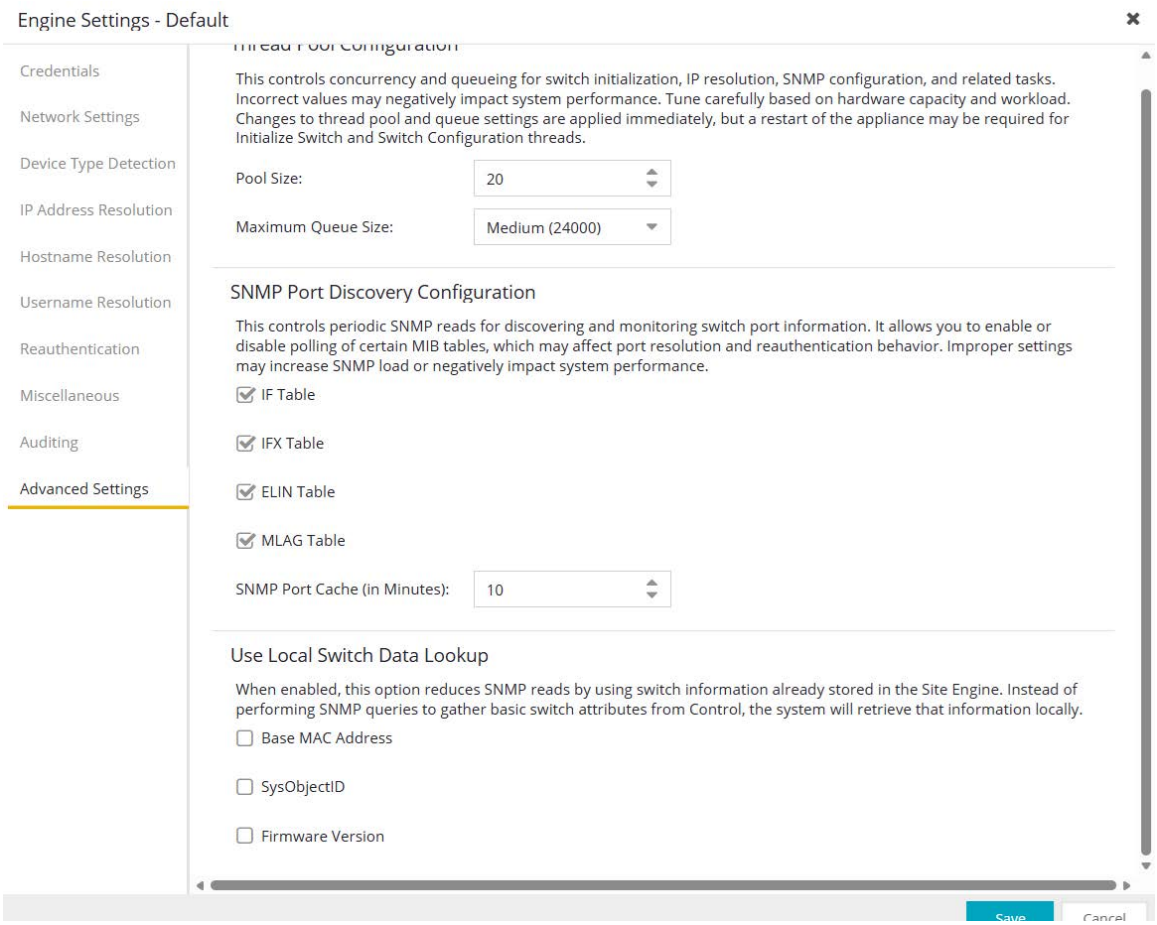
Selecting the **Enable Auditing** option enables the **Auditing Rules** field, where you can configure ExtremeCloud IQ Site Engine to store all commands entered by a user connected to the Access Control engine CLI via SSH in the engine's local syslog file.

Auditing Rules

Remove the # symbol from the beginning of a command line to enable the command and store user commands entered using the Access Control engine CLI.

Advanced Settings

Use this tab to configure advanced settings for your Access Control engine, such as Thread Pool and SNMP Port Discovery.



Thread Pool Configuration

This option controls the concurrency and queuing of switch initialization, IP resolution, SNMP configuration, and related tasks. Incorrect values may negatively impact system performance. Tune carefully based on hardware capacity and workload. Changes to thread pool and queue settings apply immediately, but a restart of the appliance may be required to Initialize Switch and Switch Configuration threads.

Pool Size

You can increase the Pool Size value if the Access Control Engine takes an excessive amount of time to start or does not start because of too many switches. For 1000 switches, you can increase the Pool Size to 50. The default value is 20.

Maximum Queue Size

Do not change the Maximum Queue Size value unless instructed to by GTAC. The default value is Medium (24000).

SNMP Port Discovery Configuration

This option controls the periodic SNMP reads for discovering and monitoring switch port information. SNMP Port Discovery Configuration allows you to enable or disable the polling of certain MIB tables, which may affect port resolution and reauthentication behavior. Improper settings may increase SNMP load or negatively impact system performance.

IF Table
The standard classic interface table in MIB. The default is enabled (checked).

IFX Table
The newer enhanced interface table in MIB. Supports 64 bit counters, usually supported in platforms with 10G+ interfaces. The default is enabled (checked).

ELIN Table
The Emergency Location Identification Number table in MIB. The default is disabled (unchecked).

MLAG Table
The Multi-Chassis Link Aggregation table in MIB. The default is disabled (unchecked).

SNMP Port Cache (in Minutes)
The time until SNMP Port Cache is refreshed in minutes. The default is 15 minutes.

Use Local Switch Data Lookup

When enabled and enforced, the Use Local Switch Data Lookup option reduces SNMP reads by using switch information already stored in the ExtremeCloud IQ Site Engine. The system retrieves the information locally stored instead of performing SNMP queries to gather basic switch attributes from the Access Control Engine.

Base MAC Address
Select to Use Local Switch Data Lookup to retrieve the Base MAC Address.

SysObjectID
Select to Use Local Switch Data Lookup to retrieve the SysObjectID.

Firmware Version
Select to Use Local Switch Data Lookup to retrieve the Firmware Version.

Verbosity Level Persistence

The configured verbosity (diagnostic) level for Access Control Engines. You can view and modify the verbosity level for each Access Control Engine. When you change the verbosity level, the new setting is saved and restored automatically after a reboot or upgrade.

The following behaviors apply to Verbosity Level Persistence:

- When you adjust the verbosity level to a value other than the default, the configured level is preserved across engine reboots and software upgrades.
- If a high verbosity level remains active for an extended period (approximately 30 days), a warning notification is displayed. The warning communicates the potential performance impact of elevated logging. You can acknowledge or dismiss the warning. A warning remains visible as long as the high verbosity level is active to ensure you are aware of the current state.

Verbosity Level
Specifies the diagnostic logging level for an Access Control Engine. The configured level persists engine reboots and upgrades.

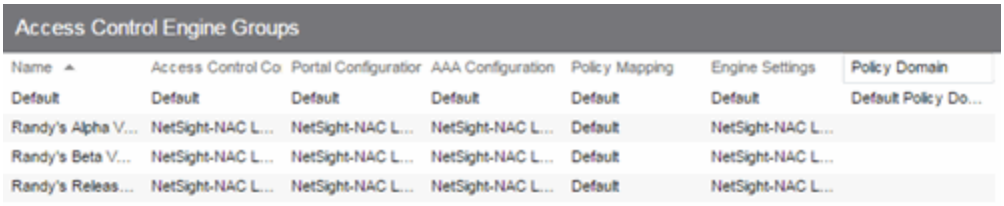
Important: Higher than default verbosity levels increase resource usage and file I/O on the Access Control Engine, which can impact engine performance. The best practice is to use high verbosity levels only for active troubleshooting sessions, and restore the default level when the troubleshooting session is complete.

NOTE: The verbosity level is configured for each engine. If you manage multiple Access Control Engines, you must configure the Verbosity Level for each engine individually.

Access Control Engine Groups

The Access Control Engine Groups panel is displayed in the right panel when you select the Access Control Engine Groups folder in the left panel. (The Access Control Engine Groups folder is only displayed if you have created engine groups.) The tab displays a table of information about the engine groups in the folder.

Use the table options and tools to filter, sort, and customize table settings. You can access the options by selecting the down arrow in the right corner of any column header.



Name
The name of the engine group.

Access Control Configuration
The Access Control Configuration currently selected for this engine group.

Portal Configuration

If your network is implementing Registration or Assisted Remediation, the Portal Configuration that defines the branding and behavior of the website used by the end user during the registration or remediation process.

AAA Configuration

The AAA Configuration used by this engine group.

Policy Mapping

The Default policy mapping can be viewed in the Access Control Configurations tree (under Access Control Profiles) or accessed from the Edit ExtremeControl Profile window.

Engine Settings

The Engine Settings configured for the group. Use the Edit Engine Settings window to specify and configure engine settings.

ExtremeControl Access Control Group Editor

This panel lists the various rule groups used to define the criteria for the rules used in your ExtremeControl configuration. You can use this window to view and edit the defined rule groups and also to add new rule groups for use in your Access Control configuration. Any changes made in this window are written immediately to the ExtremeCloud IQ Site Engine database.

ExtremeCloud IQ Site Engine comes with system-defined rule groups. ExtremeCloud IQ Site Engine also contains system-defined end-system groups that automatically populate. The Assessment Warning end-system group includes end-systems that have assessment warnings and must acknowledge them before being granted access to the network. The blocked list end-system group includes end-systems denied access to the network. The other system-defined groups are populated as the end-systems register through the Registration portal.

Select from the following rule group categories when you create a new rule group:

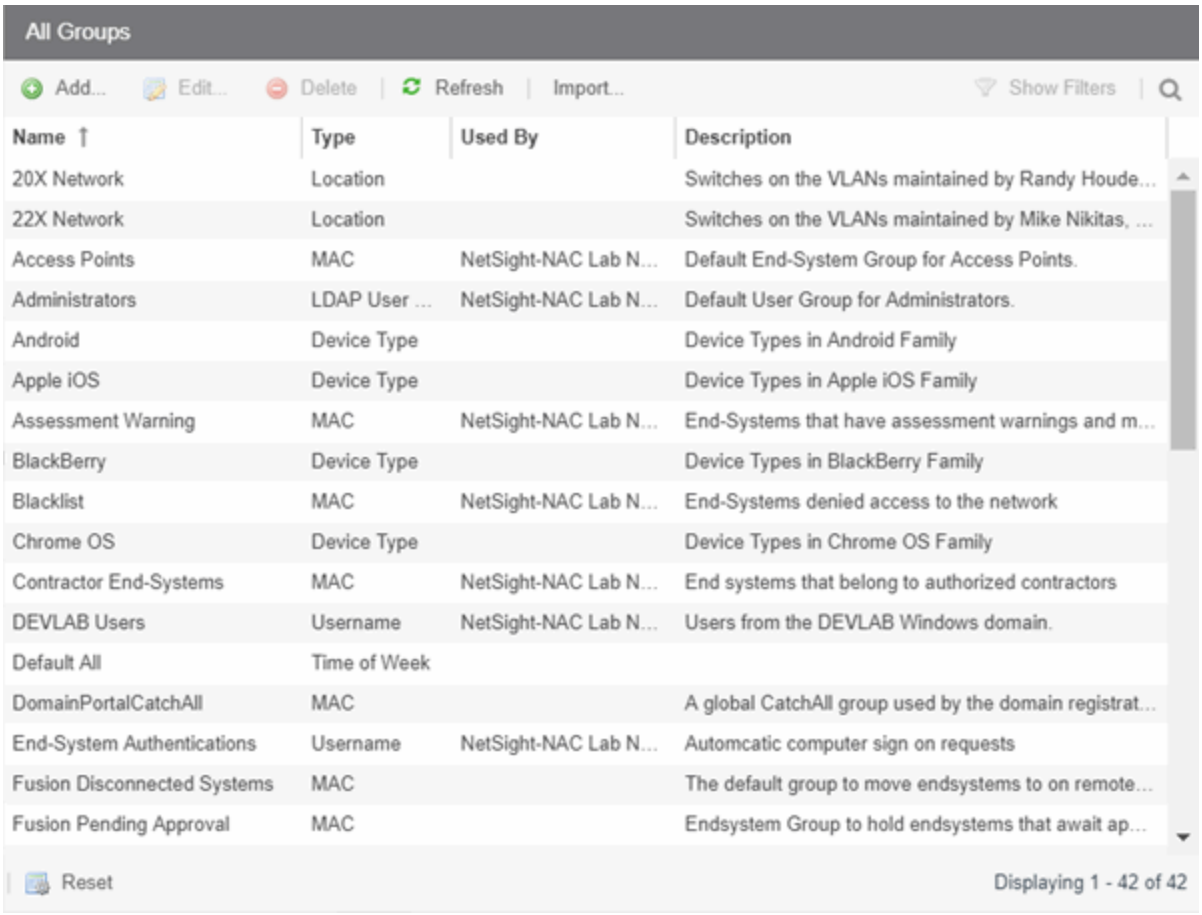
Category	Group Types	Value Types
All Groups	All Types	A list of all group types.
Device Type Groups	Device Type	A list of device types.
End-System Groups	Hostname	A list of hostnames, which can be an exact match or wild card (for example, *.extremenetworks.com).
	IP	A list of IP addresses or subnets.
	LDAP Host Group	A way to group hosts by doing an LDAP lookup on the resolved hostname of the end-system detected on the network, which can be an exact match or wild card.
	MAC	A list of MAC addresses, MAC OUI, or MAC masks.

Category	Group Types	Value Types
Location Groups	Location	A list of switches, switches and ports, or switches and SSIDs.
Time Groups	Time of Week	A list of the times of the week when the end user is accessing the network.
User Groups	LDAP User Group	A list imported from an LDAP Server, organized by Organization Unit (OU), which can be an exact match or wild card.
	RADIUS User Group	A list of attributes returned by the RADIUS server, which can be an exact match or wild card.
	Username	A list of usernames, which can be based on an exact match or a wild card.

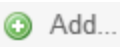
To access this window:

- Access the **ExtremeCloud IQ Site Engine > Access Control** tab.
- Select the **Access Control** tab.
- Expand the **Group Editor** tab in the left-panel.

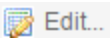
The right-panel rule group detail table opens.



The following buttons are included in the rule group detail table:

Add 

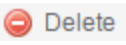
Use this button to add rule groups or to import MAC entries from a file for viewing and assigning to various end-system groups.

Edit 

Use this button to edit existing rule groups.

Copy 

Use this button to copy a selected rule group.

Delete 

Use this button to delete existing rule groups.

Refresh 

Use this button to reload group entries in the table.

Import

Use this button to import MAC entries into groups.

Reset 

Use this button to clear the search field and any filters, and to update the data in the table.

The following columns display in the rule group detail table:

Name

The name of the rule group.

Type

The type selected for the specific rule group; for example, an end-system group could have a type of MAC.

Used By

The name of the Identity and Access configuration using this rule group.

Description

A description of the rule group.

Add/Edit Device Type Group

There are nine system-defined operating system family device type groups that are automatically populated by ExtremeCloud IQ Site Engine: Android, Apple iOS, Blackberry, Chrome OS, Game Console, Linux, Mac, Windows, and Windows Mobile. You can view these system-defined groups and your other device type groups by expanding the Access Control Configurations > Group Editor > Device Type Groups left-panel tree.

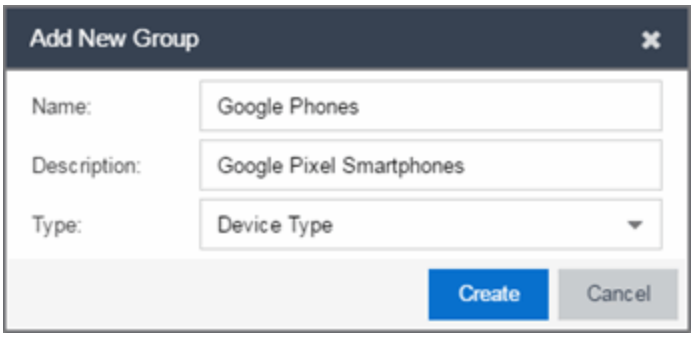
Device type groups are comprised of entries that ExtremeControl uses to determine if an end-system's device type matches the group. Entries can be a specific device type or a wildcard, such as Windows 7 or win*. If an entry does not already contain a wildcard, ExtremeCloud IQ Site Engine creates a wildcard by adding an asterisk (*) to the beginning and end of the entry. For example, if the entry is **Gentoo**, the match pattern is ***Gentoo*** allowing a match for any end-system device type that contains Gentoo. This allows you to restrict the match to a very specific value that might include a version number or model number, or expand the match to include all versions and model numbers of a certain operating system or hardware family.

For additional information about how to use device type groups, see How to Use Device Type Profiling.

NOTE: Changes to rule groups do not require an enforce. Changes are automatically synchronized with engines on the next status update. Changes do not affect end-systems until the next authentication and/or assessment occurs.

To access the Add New Group window, select **Add** (Add...) in the Device Type Groups right panel.

The Add New Group window opens.



Name

Enter a new name for the device type group. After a group is created, you cannot edit the name of the group.

Description

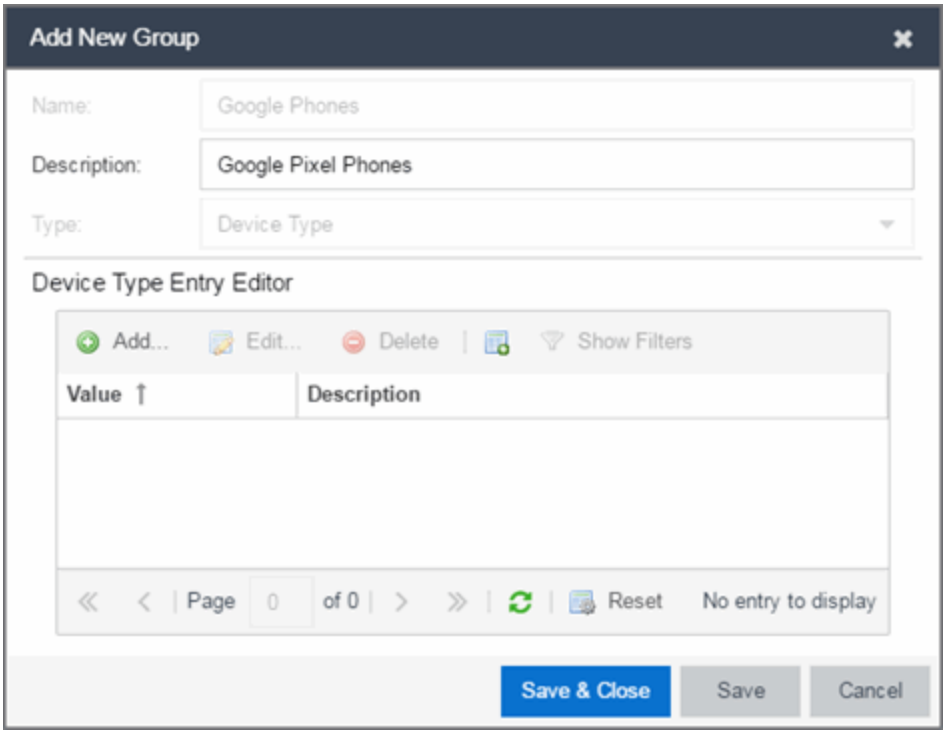
Enter a description of the device type group.

Type

To create a new device type group, select **Device Type** from the drop-down list.

Select the **Create** button to open the Device Type Entry Editor section of the window.

Select the **Select from Existing Types** button ( ) to open the Select Device Types window from which you can choose a list of predefined entries. Select the **Add** button in the Device Type Entry Editor section of the window to open the Add Entry window.



Use this window to add a new entry by entering a device type or a wildcard, such as Google Pixel or *pixel. Alternately, you can select a type from a list of entries that already appear in existing device type groups from the Select Device Types window. This window can be accessed by selecting the **Select from Existing Types** button. This list allows you to multi-select entries, and each entry appears as a separate row in the table. The list also allows you to select **Unknown** that matches against any device that does not have an operating system name, either due to failed detection or because detection hasn't happened yet.

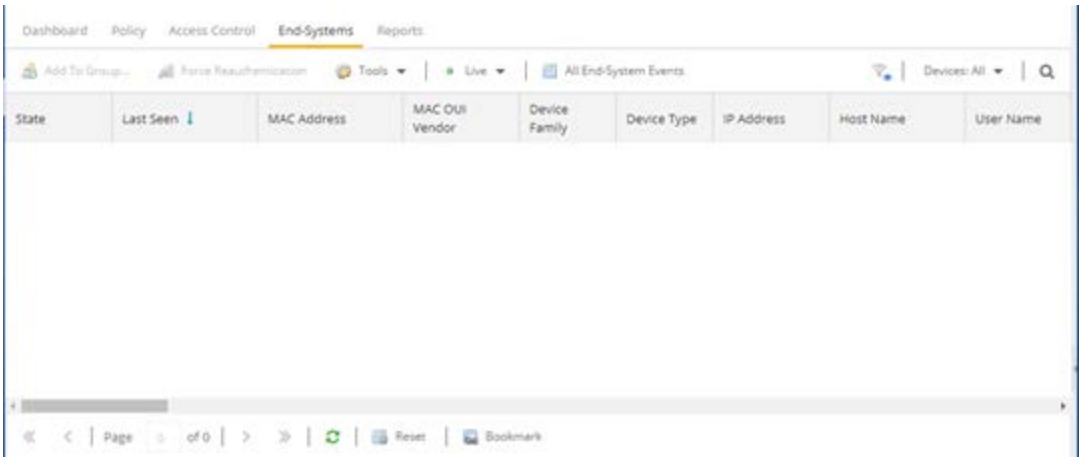
All entries selected from the list are assigned the same description. If you would like a separate description for each type, you need to add each entry individually.

End-Systems

Use the **End-Systems** tab to view end-system connection information for a single Access Control engine, all Access Control engines, or all the engines in an engine group, depending on what you select in the left-panel tree. You can also monitor end-system events and view the health results from an end-system's assessment.

The **End-Systems** tab is available from the **Control** tab. You can also access the tab by selecting a single Access Control engine, the All Engines folder, or an engine group in the left-panel tree, then selecting the **End-Systems** tab in the right panel. Selecting a single engine or engine group displays only the end-systems accessing the network via the selected engines.

Use the table options and tools to filter, sort, and customize table settings. Access the options by selecting the down arrow in the right corner of any column header.



End-Systems

This table displays the last known connection state for each end-system that has attempted connection.

State

The end-system's connection state:

- Scan — The end-system is currently being scanned.
- Accept — The end-system is granted access with either the Accept policy or the attributes returned from the RADIUS server.
- Quarantine — The end-system is quarantined because the assessment failed.
- Reject — The end-system was rejected because the assigned Access Control profile was set to Reject, the MAC Locking test failed, or the RADIUS server was reachable but rejected the authentication request.

- Disconnected — All sessions for the end-system are disconnected. This state is only applicable for end-systems connected to switches that have RADIUS accounting enabled.
- Error — Indicates one of nine problems:
  - the MAC to IP resolution failed, if assessment is enabled
  - the MAC to IP resolution timed out, if assessment is enabled
  - all RADIUS servers are unreachable
  - the RADIUS request was non-compliant
  - all assessment servers are unavailable
  - the assessment server can't reach the end-system
  - no assessment servers are configured
  - the assessment server is not compatible with the current version of Access Control
  - the username and password configured in the Assessment Server panel of the Access Control options (Administration > Options > Access Control > Assessment Server) are incorrect for the assessment server.

ID

The device identification number.

Last Seen

The last time the end-system was seen by the Access Control engine.

Note: The End-Systems table is sorted by the Last Seen Time by default. Sorting using any other column will automatically pause the table to allow sorting on those columns (except the OUI Vendor and Switch Nickname columns - these columns cannot be sorted). Reverting to a Live view will revert back to the "Last Seen Time" sort, in descending order.

IP Address

The end-system's IPv4 address.

IPv6 Address

The end-system's IPv6 address or addresses.

OV MAC Address

The end-system's OV MAC address.

MAC Address

The end-system's MAC address. MAC addresses can be displayed as a full MAC address or with a MAC OUI (Organizational Unique Identifier) prefix. If the MAC address of the end system belongs to an administratively assigned range (randomized MAC), then the MAC is displayed in italic font.

MAC OUI Vendor
The vendor associated with the MAC OUI.

Host Name
The end-system's hostname.

Device Family
The hardware family or the operating system family for the end-system.

Device Type
The hardware type or the operating system type for the end-system.

User Name
The user name used to connect.

Site
The site of the switch to which the end-system is connected.

Switch IP
The IP address of the switch to which the end-system is connected. If the end-system is connected to an Access Control Controller engine, this is the Access Control Controller PEP (Policy Enforcement Point) IP address.

Switch Nickname
An alternate name for the switch.

NOTE: Configure the nickname on the **Device Annotation** tab in the **Configure Device** window.

Switch Port
The port alias (if defined) followed by the switch port number to which the end-system connected. If the end-system is connected to a Layer 2 Access Control Controller engine, this is the Access Control Controller PEP (Policy Enforcement Point) port. However, for Layer 3 Access Control Controller engines, this column is blank.

- If you add or update the port alias on the switch, you must enforce the Access Control engine in order for the new information to be displayed in the End-Systems table.
- If you don't want the port alias displayed, remove the PORT_DESCRIPTION_FORMAT variable from the /opt/nac/server/config/config.properties file. If this variable is removed, only the switch port number is displayed.

Policy
The name of the ExtremeControl policy role assigned to the end-system when it connected to the network.

Authorization
The attributes returned by the RADIUS server for this end-system. If the end-system is connected to a switch that supports multi-authentication, then this column may not reflect

the actual active policy for the authenticated user. For Layer 3 Access Control Controller engines, this column displays the policy assigned to the end-system for its authorization.

Risk

The overall risk level assigned to the end-system based on the health result of the scan:

- Red — High Risk
- Orange — Medium Risk
- Yellow — Low Risk
- Green — No Risk
- Gray — Unknown

Profile

The name of the Access Control profile assigned to the end-system when it connected to the network.

Reason

Provides information about the reason the ExtremeControl profile is assigned to the end-system.

Authentication Type

Identifies the latest authentication method used by the end-system to connect to the network. (For Layer 3 Access Control Controller engines, this column displays "IP.")

State Description

This column provides more details about the end-system state. For example, if the end-system's connection state is Reject, this column might list the RADIUS server (primary or secondary) that rejected the authentication request.

Extended State

Provides the reasons why the end-system is in its particular connection state. It gives you an idea as to why a certain policy was applied to the end-system or why the end-system was rejected.

Access Control Engines/Source IP

The Access Control engine to which the end-system is connecting.

Engine Group

This column is only displayed if you have multiple engine groups. It displays what engine group the Access Control engine was in when the end-system event was generated. For example, if the engine was in Engine Group A when an end-system connected, but then later the engine was moved to Engine Group B, this column would still list Engine Group A for that end-system's entry.

RFC3580 VLAN

For end-systems connected to RFC 3580-enabled switches, this is the RFC3580 VLAN ID assigned to the end-system.

Warning Time
Shows the time for warning. This column is hidden by default.

Last Quarantined
The last time the end-system was quarantined.

Score
The total sum of the scores for all the health details that were included as part of the quarantine decision.

Top Score
The highest score received for a health detail in the health result.

Actual Score
The actual score is what the total score would be if all the health details including those marked Informational and Warning were included in the score.

Switch Port Index
The SNMP index (ifIndex) of the port to which the end-system connected.

Switch Location
The physical location of the switch to which the end-system connected. If the end-system is connected to an Access Control Controller engine, this is the Access Control Controller PEP (Policy Enforcement Point) location.

ELIN
An extended set of data for an end-system based on a MAC address.

Port Info Raw
Displays unformatted information as it is received from the port.

All Authentication Types
This column displays all the authentication methods the end-system has used to authenticate. The authentication types are listed in order of precedence from highest to lowest: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking. View details about each authentication session (such as the Access Control profile that was assigned to the end-system for each authentication type) in the End-System Events tab.

Last Scan Result
The last scan result assigned to the end-system: Scan, Accept, Quarantine, Reject, Error. This is the state assigned to the end-system as a result of the last completed scan. This typically matches the end-system State if scanning is currently enabled and has been performed recently.

Last Scanned
The last time an assessment (scan) was performed on the end-system.

First Seen
The first time the end-system was seen by the Access Control engine.

NAP Capable
Indicates whether the end-system is Microsoft NAP (Network Access Protection) capable: **Yes** or **No**

Custom
Use this column to add additional information about the end-system. To add or edit custom information, right-click on the table and select **Edit Custom Information**. You can add information for up to four Custom columns. The columns for Custom 2, Custom 3, and Custom 4 are hidden by default. To display these columns, select the down arrow to the right of the table header and select Columns > Column 2, Column 3, or Column 4.

NOTE: Change the name of the Custom columns in the ExtremeControl options.

Registered User
The registered username supplied by the end-user during the registration process.

Registered Email
The registered email address supplied by the end-user during the registration process.

Registered Phone
The registered phone number supplied by the end-user during the registration process.

Sponsor
The registered user's sponsor, if sponsorship is enabled.

Registration
Custom information supplied by the end-user during the registration process.

Registration Description
The device description supplied by the end user during the registration process.

Groups
Displays any end-system and/or user groups to which the end-system belongs.

Group 1-3
Displays the names of up to three end-system and/or user groups to which the end-system belongs.

Zone
Displays the end-system zone to which the end-system is assigned.

Request Attributes
Indicates if RADIUS attributes are requested.

Registration Type
Shows the type of end-system connection (for example, **Transient**).

RADIUS Server IP
The IP address of the RADIUS server to which the end-system authenticated.

Source

Displays the origin of the end-system in the network:

- Access Controlengine — An Access Control engine.
- Wireless Manager — An ExtremeWireless Controller or AP.
- ExtremeXOS/Switch Engine ID Manager — An Extreme switch running ExtremeXOS/Switch Engine with the Identify Manager feature configured to send events to ExtremeCloud IQ Site Engine.
- OneFabric Connect — An ExtremeConnect module (e.g. Solutions Architecture and Innovation (SAI) integration)
- One Controller — The Extreme SDN Controller.

DCM

Data Center Manager. This column is hidden by default.

Certificate Expiration

Expiration date of the certificate issued for 802.1x authentication.

Certificate Issuer

Name of the issuer of the certificate issued for 802.1x authentication.

Certificate Fingerprint

The attributes in an SSL handshake used for identifying the end-system.

Certificate URI

The URL portion of the Subject Alternative Name when 802.1X EAP-TLS is used. This field is hidden by default.

Actions

TIP: These actions are also available from the right-click menu off an end-system entry in the table.

Force Reauthentication

Forces the selected end-system to re-authenticate. End-systems authenticated to a VPN device are disconnected from the VPN.

Force Reauth and Scan

Forces the selected end-system to re-authenticate and undergo an assessment (scan). (End-systems authenticated to a VPN device are disconnected from the VPN.) The assessment only takes place if scanning is enabled in the Access Control profile assigned to the end-system.

Add to Group

Lets you add the selected end-system to a specific end-system or user group. If the end-system is a registered device, it can be added to a registration group. After adding an end-system to a group, any rules created that involved that group apply to the end-system as well. Changes to end-system group membership do not require an enforce and are synchronized

with engines immediately. Changes do not affect the end-system until the next authentication or assessment occurs.

NOTE: Entries in the Blacklist are not moved or removed using this function. You must manually remove entries from the Blacklist End-System group.

Lock MAC

Opens the Add MAC Lock window where you can lock the MAC address of the selected end-system to a switch or switch and port.

Show Details

Opens the End-System Details tab where you can view summary information for the end-system selected in the table.

Delete

Deletes the selected end-system entries from the table and also deletes the associated end-system events. You are given the option to delete any custom information, group assignment, MAC locks, and registration and web authentication associated with the end-systems.

The Force Delete of End-System option completely deletes the end-system from ExtremeCloud IQ Site Engine, regardless of whether the end-system reauthentication is successful when the delete is executed. The option is deselected by default. When deselected, it prevents possible synchronization conditions where the authentication session remains active on the switch even though the end-system has been deleted from ExtremeCloud IQ Site Engine. These conditions can occur when there are underlying issues that prevent the end-system reauthentication from completing properly.

NOTES: The Delete operation does not remove an end-system from the blocked list group. Blocked list is a special group that requires end-systems to be manually removed using the Edit End-System Group window.

Deleting an end-system from the table also deletes the user's current authentication. If the user is connected to the network at the time of the delete, they are forced to re-authenticate.

Menu Buttons

The menu at the top of the window contains most of the options available via a right-click previously mentioned in the Actions section above, as well as the End-System Events button, described below.

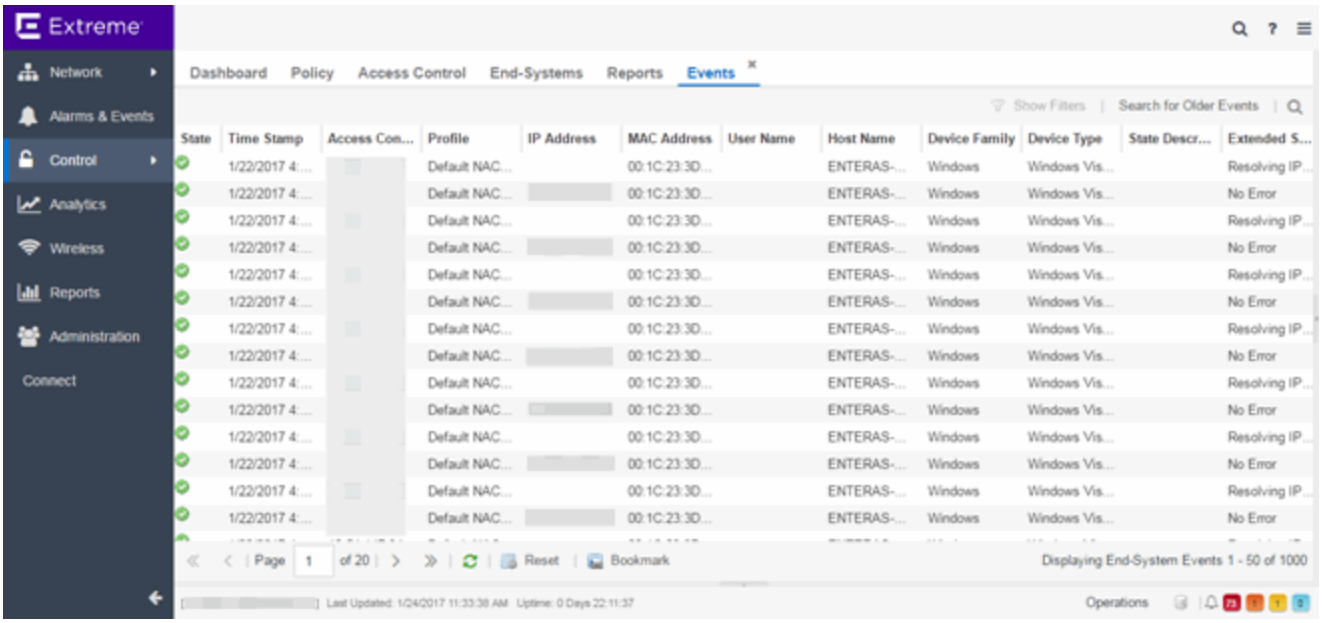
All End-System Events

Opens the End-System Events tab where you can view information about events for all end-systems accessing your network.

End-System Events Tab

This tab displays historical connection information for all end-systems accessing your network. End-system events are stored daily in the database. In addition, the end-system event cache stores in memory the most recent end-system events and displays them here in this tab. This cache allows ExtremeCloud IQ Site Engine to quickly retrieve and display end-system events without having to search through the database. You can configure parameters for the event cache (such as the number of events to display) using the End-System Event Cache options in the Access Control Options view (Administration > Options > Access Control > End-Systems Event Cache).

NOTE: The **End-System Events** tab displays events up to the most recent delete event for the end-system, if one exists. If you want to see events that happened prior to the most recent delete event, use the **Search for Older Events** button.



State

The end-system's connection state:

- Scan — The end-system was scanned.
- Accept — The end-system was granted access with either the Accept policy or the attributes returned from the RADIUS server.
- Quarantine —The end-system was quarantined because the assessment failed.
- Reject — The end-system was rejected because the assigned Access Control profile was set to Reject, the MAC Locking test failed, or the RADIUS server was reachable but rejected the authentication request.
- Disconnected — This end-system session was disconnected, however other sessions for the end-system may still be active. For example, the end-system may have a

disconnected session with an authentication type of 802.1X, but still have an active MAC authentication session. This state is only applicable for end-systems connected to switches that have RADIUS accounting enabled.

- Error — Indicates one of nine problems:
  - the MAC to IP resolution failed
  - the MAC to IP resolution timed out
  - all RADIUS servers are unreachable
  - the RADIUS request was non-compliant
  - all assessment servers are unavailable
  - the assessment server can't reach the end-system
  - no assessment servers are configured
  - the assessment server is not compatible with the current version of ExtremeCloud IQ Site Engine
  - the username and password configured in the Assessment Server panel of the Access Control options (Administration > Options > Access Control > Assessment Server) are incorrect for the assessment server

Time Stamp
The date and time the end-system connected. When a millisecond precision time format is configured (for example, HH:mm:ss.SSS), the Time Stamp column displays sub-second accuracy for precise event sequencing.

ExtremeControl Engine/Source IP
The IP address of the Access Control engine on which the event occurred.

Profile
The name of the Access Control profile assigned to the end-system when it connected to the network.

IP Address
The end-system's IP address.

MAC Address
The MAC address of the end-system on which the event occurred. MAC addresses can be displayed as a full MAC address or with a MAC OUI (Organizational Unique Identifier) prefix.

User Name
The username used to connect.

Host Name
The end-system's host name.

Device Family
The hardware family or the operating system family for the end-system.

Device Type
The hardware type or the operating system type for the end-system.

State Description
This column provides more details about the end-system state. For example, if the end-system's connection state is Reject, this column might list the RADIUS server (primary or secondary) that rejected the authentication request.

Extended State
Provides additional information about the end-system's connection state.

Reason
Provides additional information about the reasons why the end-system is in its particular connection state. It provides information as to the reason a policy is applied to the end-system or the reason the end-system is rejected.

Authorization
The attributes returned by the RADIUS server. If the end-system is connected to a switch that supports multi-authentication, then this column may not reflect the actual active policy for the authenticated user. For Layer 3 Access Control Controller engines, this column displays the policy assigned to the end-system for its authorization.

Auth Type
Identifies the authentication method used by the end-system to connect to the network. For Layer 3 Access Control Controller engines, this column shows **IP**.

Switch IP
The IP address of the switch to which the end-system connected. If the end-system is connected to an Access Control Controller engine, this is the Access Control Controller PEP (Policy Enforcement Point) IP address.

Switch Nickname
The nickname defined for the switch to which the end-system is connected.

Switch Port
The switch port number to which the end-system is connected. If the end-system is connected to a Layer 2 Access Control Controller engine, this is the Access Control Controller PEP (Policy Enforcement Point) port. However, for Layer 3 Access Control Controller engines this column is blank.

Switch Location
The physical location of the switch to which the end-system is connected. If the end-system is connected to an Access Control Controller engine, this is the Access Control Controller PEP (Policy Enforcement Point) location.

Last Scan Time
Displays the last time ExtremeCloud IQ Site Engine scanned the end-system on which the event occurred.

Zone

Displays the end-system zone to which the end-system is assigned. For additional information, see End-System Zones.

Registration Type

Shows the type of end-system connection (for example, **Transient**).

RADIUS Server IP

The IP address of the RADIUS server to which the end-system authenticated.

Event Source

Displays the origin of the end-system in the network:

- Access Control engine — An Access Control engine.
- Wireless Manager — An ExtremeWireless Controller or AP.
- ExtremeXOS/Switch Engine ID Manager — An Extreme switch running ExtremeXOS/Switch Engine with the Identify Manager feature configured to send events to ExtremeCloud IQ Site Engine.
- OneFabric Connect — An ExtremeConnect module (e.g. Solutions Architecture and Innovation (SAI) integration)
- One Controller — The Extreme SDN Controller.

Engine Group

This column is only displayed if you have multiple engine groups. It displays what engine group the Access Control engine is in when the end-system event was generated. For example, if the engine began in Engine Group A when an end-system connected, then the engine is moved to Engine Group B, this column still lists Engine Group A for that end-system's entry.

Search for Older Events

This button lets you search for older events stored in the database outside of the end-system events cache. The maximum search parameters for this extended search are configured in the End-System Event Cache options in the Access Control Options view (Administration > Options > Access Control > End-System Event Cache). The search is ended when any one of the parameters is reached.

- Maximum number of results to return from search
- Maximum time to spend searching for events (in seconds)
- Maximum number of days to go back when searching

For information on related topics:

- Add MAC Lock Window
- End-System Details Tab

Add/Edit End-System Group

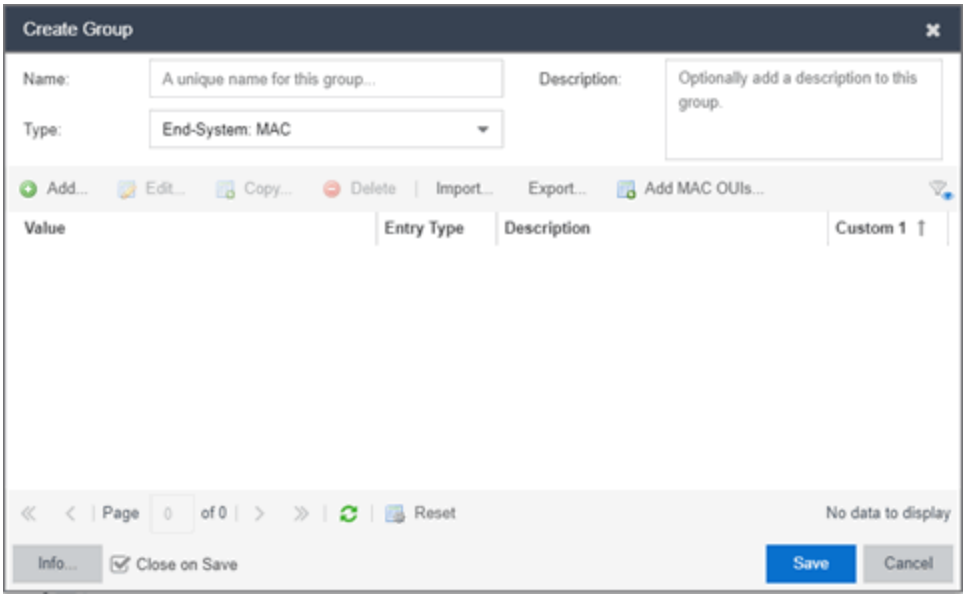
Use this window to add a new end-system group or edit an existing end-system group. End-system groups are rule components that enable you to group together devices having similar network access requirements or restrictions. You can access the Add/Edit End-System Group window from the Manage Rule Groups window or from the end-system group field in the Create Rule window.

There are six system-defined end-system groups automatically populated by ExtremeCloud IQ Site Engine. The first is the Assessment Warning end-system group that includes end-systems that have assessment warnings and must acknowledge them before being granted access to the network. The second is the blocked list end-system group that includes end-systems denied access to the network. The other four system-defined groups are populated as end-systems register through the Registration portal.

You can access the Create Group window by accessing the **Access Control** tab and selecting Access Control Configurations > Group Editor > End-System Groups in the left-panel menu and selecting the **Add** button in the right panel.

NOTE: Changes to rule components do not require an enforce. Changes are automatically synchronized with engines on the next status update. Changes do not affect end-systems until the next authentication and/or assessment occurs.

NOTE: The best practice is to not add or delete entries from the group used for the registration portal, such as Web Authenticated Users, Registered Users, Registration Denied Access, or Registration Pending Access. Manual changes can prevent the end-system from successfully registering again.



Name

Enter a new name for the end-system group. You cannot edit the name of a group.

Description

Enter a description of the end-system group. If you are using Data Center Manager (DCM), the end-system group description contains the DCM specific settings as key/value pairs.

Type

Specify whether the end-system group be based on:

- MAC - a list of MAC addresses, MAC OUI, or MAC Masks.
- IP - a list of IP addresses or subnets.
- Hostname - a list of hostnames: exact match or wild card (for example, *.extremenetworks.com).
- LDAP Host Group - a way to group hosts by doing an LDAP lookup on the resolved hostname of the end-system detected on the network. Note for the standard use with Active Directory, the Engine Settings > Hostname Resolution must be configured to use DNS Hostname Resolution so ExtremeCloud IQ Site Engine can resolve the Fully Qualified Domain Name. In the LDAP configuration, you must also have the "Use Fully Qualified Domain Name" checkbox selected.

Value

The MAC address, IP address, Hostname, or Attribute value of the end-system.

Description

The description of the end-system group.

Mode

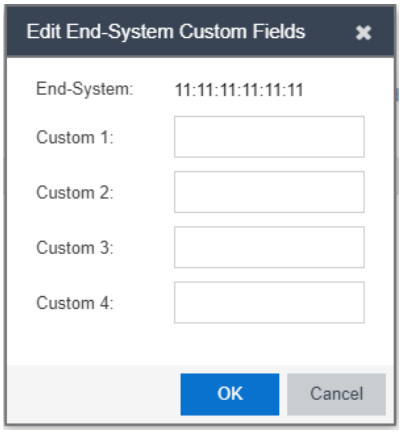
For LDAP Host Groups, the mode option lets you specify whether to match any or match all of the LDAP attributes listed below. You can also use "Exists" to just check to see if a host is present in LDAP.

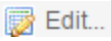
Custom 1

Displays additional information about the end-system. Up to four custom columns can be added to the table. The columns for Custom 2, Custom 3, and Custom 4 are hidden by default. To display these columns, select the down arrow next to the Custom 1 column header and select **Columns** > **Custom 2**, **Custom 3**, or **Custom 4**.

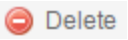
Add Button 

Select the **Add** button to open the Add Entry window, from which you can add an entry to the table. To add or edit custom information, right-click on the table entry and select Edit Custom Information. You can add information for up to four Custom columns.



Edit Button 

Select an entry in the Entry Editor section of the window and select the **Edit** button to open the Edit Entry window, from which you can edit an existing entry.

Delete Button 

Select an entry in the Entry Editor section of the window and select the **Delete** button to delete an existing entry.

Save Button

Select the **Save** button to save the location group.



Use the **Multiple MAC OUI Entries** button to open a window where you can select MAC OUI vendors.

Filter

Use the Filter functions to filter for a specific entry based on a numeric value or text.

End-System Details

The End-System Details window provides connection state and assessment information for a single end-system. It is launched from the End-Systems View in the **Control** tab, by double-clicking any end-system in the table or selecting an end-system and then selecting **Show Details** from the Tools menu.

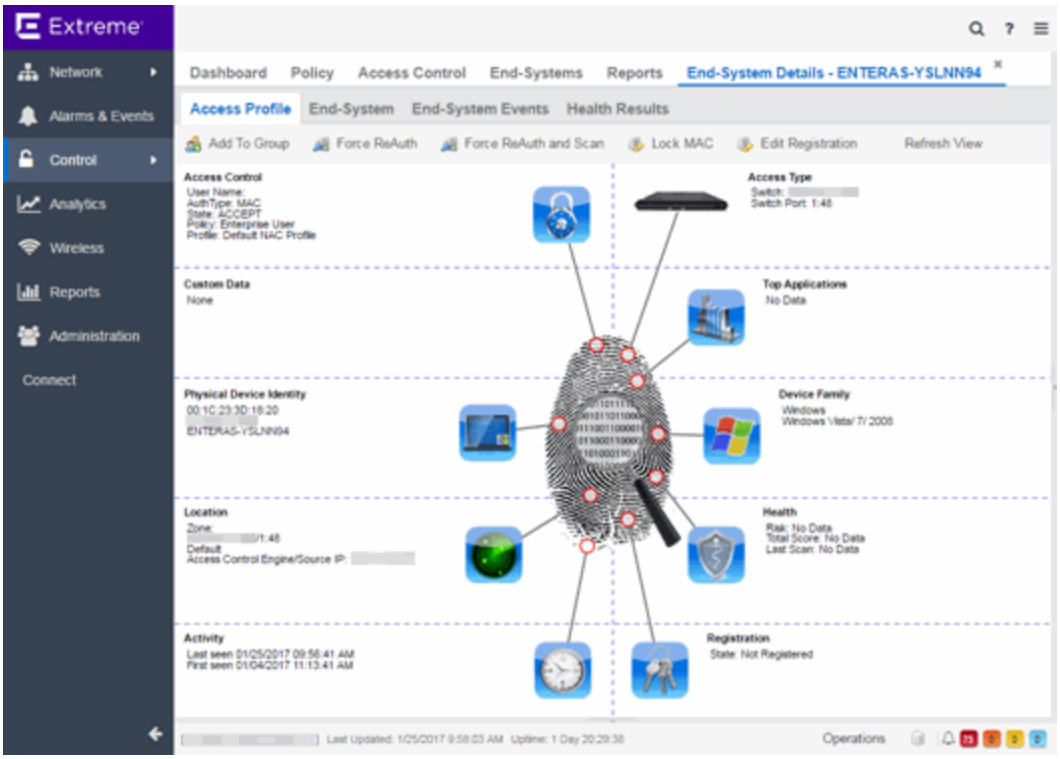
The End-System Details window has four tabs. The **Access Profile** tab provides end-system summary information. The End-System tab provides end-system connection state information. The **End-System Event** tab displays end-system event information. The **Health Results** tab displays end-system assessment result information.

This Help topic provides information on the four tabs:

- Access Profile Tab
- End-System Tab
- End-System Events Tab
- Health Results Tab

Access Profile Tab

The **Access Profile** tab presents a graphical view of end-system and health result information, providing an at-a-glance end-system summary. Select the information in each section to link to more detailed information.



Access Type
: Displays the switch IP address, port index, and port that the end-system is connected to. Select to open a PortView for the switch in a new tab.

Top Application Flows
: Lists the top five applications and flow counts for the end-system, listed in descending order by flow count. Select to open the Applications Dashboard in a new tab.

Device Family
: Displays the end-system's operating system (OS) family (for example: Windows, Linux, Android) and OS name. Use the device family icon to quickly determine the end-system type. Select to open the **End-System** tab where you can view additional end-system details.

Health
: Displays health data from the latest scan, including risk level, total score, and last scan time. Use the health icon to quickly determine risk level by color. Select to open the **Health Results** tab where you can view additional health result information and details.

Registration
: Displays the end-system's registration state, user name, and sponsor. Select to open the **End-System** tab where you can view additional registration information.

Activity
: Displays the last seen and first seen times for the end-system. Select to open the **End-System** tab where you can view additional end-system details.

NOTE: The Last Seen, First Seen, Last Scanned, and Last Quarantined fields show milliseconds when a millisecond-precision time format is configured in **Administration > Options > Site Engine – General > Date Time Format**.

Location
: Displays location summary information, including end-system zone membership, access point information, engine group, and engine IP address. Select to open the **End-System** tab where you can view additional location information.

Physical Device Identity
: Displays the end-system's MAC address, IP address, and host name. The device icon displays the end-system's physical device type with a small OS-based icon in the corner. Select to open the **End-System** tab where you can view additional end-system details.

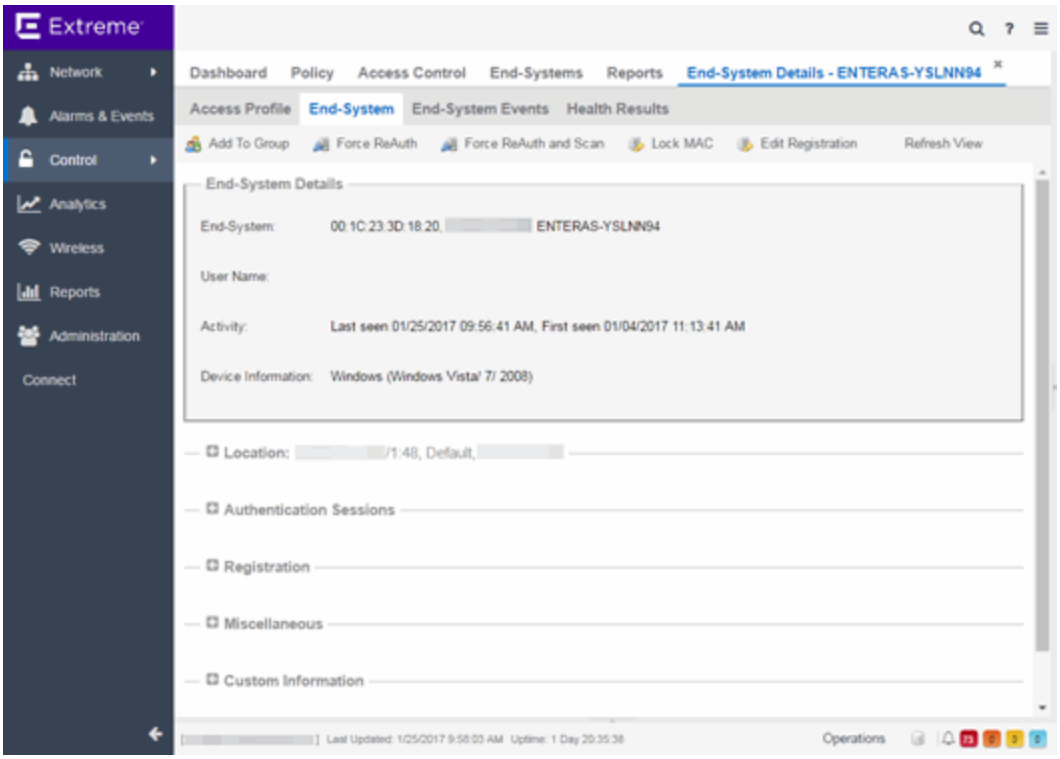
Virtual Device Identity
: If the end-system is a virtual machine, this section displays virtual device information, including VM name, ID, Guest Name, and manufacturer. Use the icon to quickly determine the virtual machine's operating system. If the end-system is not a virtual machine, this section is replaced by Custom Data.

Custom Data
: Displays any custom information associated with the end-system. Custom information for an end-system is added in the End-Systems tab or End-Systems View. If the end-system is a virtual machine, this section is replaced by Virtual Device Identity.

Access Control
: Displays the end-system's user name, authentication type, connection state, policy, and profile. Select to open the **End-System** tab where you can view additional end-system authentication session details.

End-System Tab

This tab presents detailed information on the selected end-system's connection, authentication, and registration. Expand the sections using the arrow buttons to see additional information.

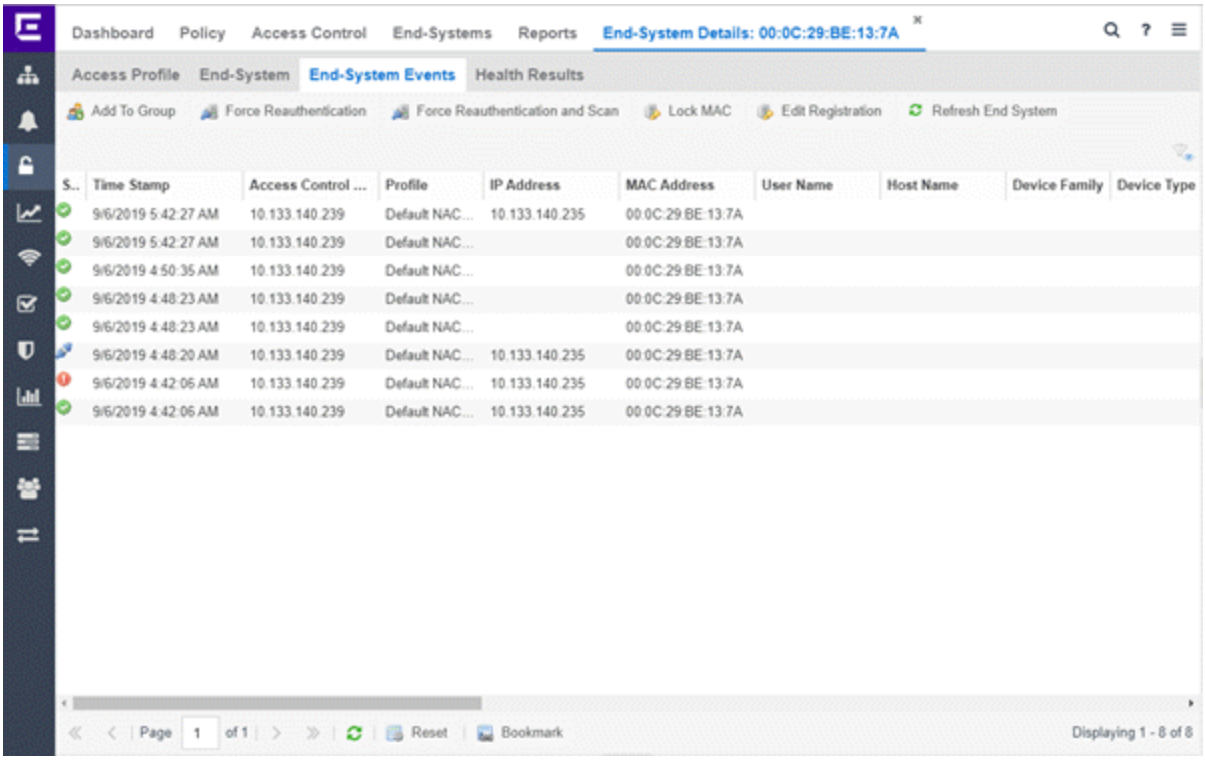


For a definition of various fields, see the column definitions included in the End-Systems topic.

Changes to group membership do not require an enforce and will be synchronized with engines immediately. Changes will not affect the end-system until the next authentication or assessment occurs.

End-System Events Tab

The **End-System Events** tab shows all the events for the selected end-system.

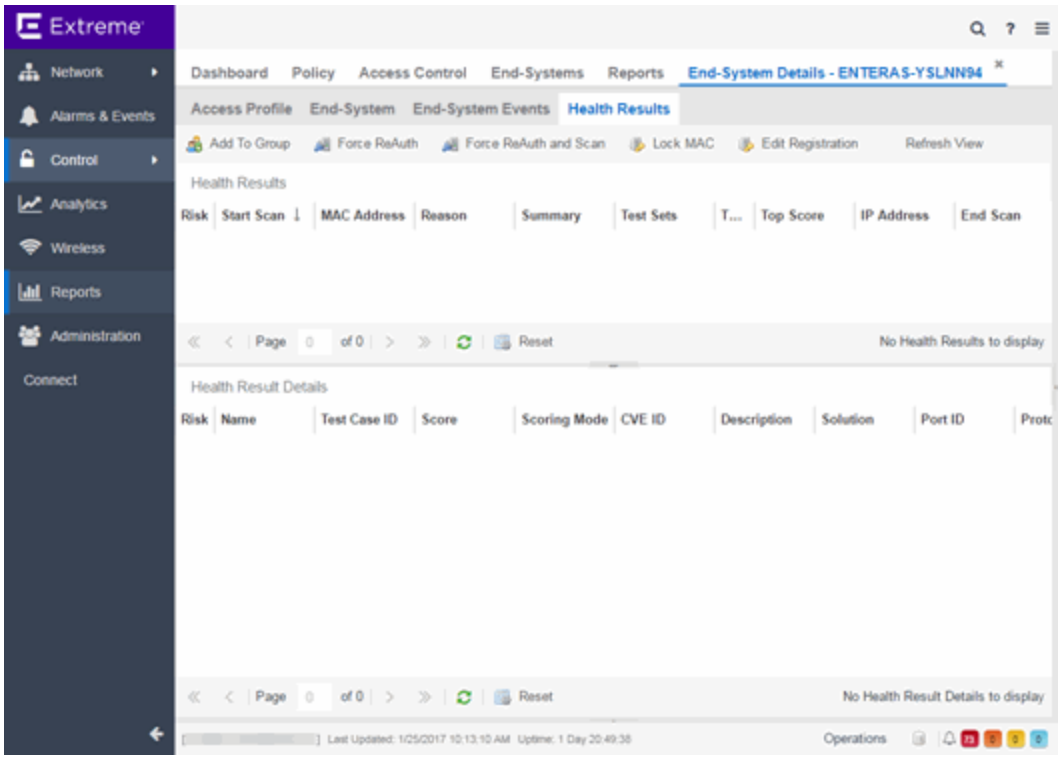


You can manipulate the table data in this window in several ways to customize the view for your own needs:

- Select the column headings to perform an ascending or descending sort on the column data.
- Hide or display different columns by selecting a column heading and selecting the column options from the menu.
- Rearrange columns by dragging a column heading to the desired position.
- Filter the data in each column in the table.

Health Results Tab

The top table in the **Health Results** tab provides summary information on scan results obtained for the selected end-system. The bottom table presents the individual health result details for the scan selected in the top table. Double-click any row in the bottom table to open the Health Result Details window and view a description, solution, and result for the health result. Information is displayed in this tab only if assessment is enabled on the network and there are health results in the database.



Health Results

This table presents health results for all the scans performed on the end-system.

Risk

The overall risk level assigned to the end-system based on the health result of the scan:

- Red - High Risk
- Orange - Medium Risk
- Yellow - Low Risk
- Green - No Risk
- Gray - Unknown

Start Scan

The date and time the scan started.

MAC Address

The end-system's MAC address.

Reason

The reason the health result was placed into the specified risk level. This is based on the risk level configuration that was used for the assessment, for example, if there was one or more

health result detail with a score greater than 7. If the end-system is NAP capable, then this is based on the values returned from NAP.

Summary

A list of all the test cases that were run against the device during assessment. The test case name will be listed, or if that is not available, the test case ID will be listed.

Test Sets

The list of test sets that were run during assessment, for example, Default Nessus, Default Agent-less, and Default Agent-based. Test sets are defined as part of the assessment configuration. If the end-system is NAP capable, then this column displays Microsoft NAP indicating that NAP performed the assessment.

Total Score

The total sum of the scores for all the health details that were included as part of the quarantine decision, followed by the actual score in parenthesis. The actual score is what the total score would be if all the health details were included as part of the quarantine decision. It includes all scores, including those marked Informational and Warning. If the total score and the actual score are the same, only one score is shown.

Top Score

The highest score received for a health detail that was included as part of the quarantine decision. Scores that are marked as Informational or Warning are not considered.

IP Address

The end-system's IP address.

End Scan

The date and time the scan ended.

Server Name

The name of the assessment server. For on-board assessment servers, the name is determined by the name of the ExtremeControl engine. For example, if you create an Access Control engine and name it MyAccessControlengine, then the on-board assessment server name will be listed as MyAccessControlengine as well.

Server IP

The IP address of the assessment server. For on-board assessment servers, the IP address is determined by the address of the Access Control engine. For example, if you create an Access Control engine with an IP address of 10.20.80.8, then the on-board assessment server IP address is listed as 10.20.80.8 as well.

Server Port

The port number on the assessment server to which the Access Control engine sends assessment requests.

Host Unreachable

Displays whether the end-system was unreachable and could not be scanned: Yes or No.

Warning Count
The total number of health result details that are marked as Warnings.

Health Result Details

This table displays the individual health result details for the scan selected in the top table. Double-click any health result detail to open the Health Result Details window that displays a description, solution, and result for the health result.

Risk
The risk level assigned to the problem found on the port:

- Red - High (corresponds to a Hole)
- Orange - Medium (corresponds to a Warning)
- Yellow - Low (corresponds to a Note)
- Black - No Result Available

Name
This column lists the name of the test that is reported by the health result detail.

Test Case ID
The unique number assigned to the test case.

Score
The score assigned to the test case. The score is a value between 0.0 and 10.0. In the case of agent-based test cases, the score will be either 0.0 for a passed test, or 10.0 for a failed test, unless specifically overwritten by the scoring override configuration.

Scoring Mode
The scoring mode that was used at the time the test was performed.

- Applied - The score returned by this test was included as part of the quarantine decision.
- Informational - The score returned by this test was reported, but did not apply toward a quarantine decision.
- Warning - The score returned by this test was only used to provide end user assessment warnings via the Notification portal web page.

CVE ID
The CVE (Common Vulnerability and Exposures) ID assigned to the security vulnerability or exposure. For more information on CVE IDs, refer to the following URL: https:/cve.mitre.org/.

Description
This column lists information about the health result detail.

Solution
A solution for the problem found in the health result detail.

Port ID
The port on the end-system that the security risk was detected on.

Protocol ID
The well-known number (ID) assigned to the IP Protocol Type.

Value
What this specific test case is testing or checking for on the end-system.

Assessment Type
The type of assessment server used in the test set.

Remediation Success
For agent-based assessment, this column lists the results of remediation attempts: Remediation Successful, Remediation Failed, or Not Applicable.

Type
A "type" is assigned to each security risk found on a port during an assessment, and is used to determine whether to Quarantine an end-system. Types are configurable on the assessment agent. There are three types:

- Hole - The port is vulnerable to attack.
- Warning - The port may be vulnerable to attack.
- Note - There may be a security risk on the port.

Buttons and Paging Toolbar

Add to Group
Lets you add the selected end-system to a specific end-system or user group. After adding an end-system to a group, any rules that have been created that involved that group will now apply to the end-system as well. Changes to end-system group membership do not require an enforce and will be synchronized with engines immediately. Changes will not affect the end-system until the next authentication or assessment occurs.

Force ReAuth
Forces the selected end-system to re-authenticate.

Lock MAC
Opens the Add MAC Lock window where you can lock the MAC address of the selected end-system to a switch or switch and port.

Edit Registration
Opens a window where you can edit the expiration time and maximum registered device count for the end user.

Refresh
Use the refresh button to update the data in the table.

Paging Toolbar

The paging toolbar provides four buttons that let you easily page through the table: first, previous, next, and last page.

Reset

The reset button clears the search field and search results, clears all filters, and refreshes the table.

Bookmark

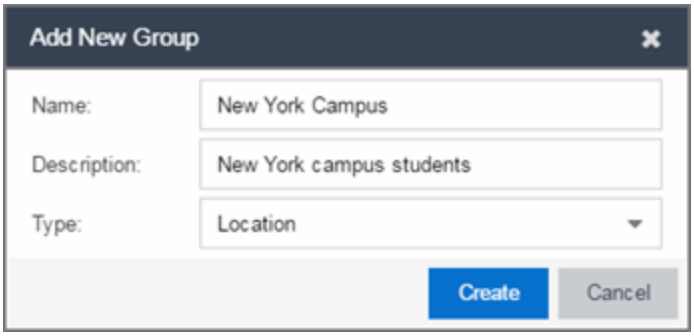
Use the bookmark button to save the search, sort, and filtering options you have currently set.

Add/Edit Location Group

Use this window to add a new location group or edit an existing location group. Location Groups are rule components that enable you to specify network access requirements or restrictions based on the network location where the end-user is connecting. For example, in an enterprise environment, an engineer logging on to the network from the corporate cafeteria could receive different network access than an engineer logging on from the engineering development area.

You can access the Add/Edit Location Group window by accessing the **Access Control** tab and selecting Access Control Configurations > Group Editor > Location Groups in the left-panel menu and selecting the **Add** button in the right panel.

NOTE: Changes to rule components do not require an enforce. Changes are automatically synchronized with engines on the next status update. Changes do not affect end-systems until the next authentication and/or assessment occurs.

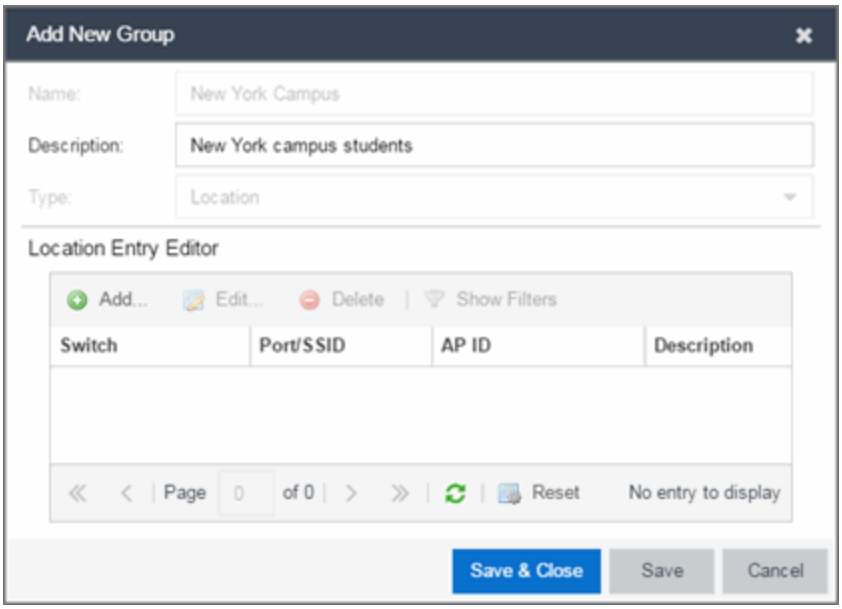


Name
Enter a name for a new location group. You cannot edit the name of a group.

Description
Enter a description of the location group.

Type
Select **Location** to create a Location group.

Select **Create** to display the Entry Editor section of the window. This section varies depending on the **Type** selected.



Switch

The IP address of the switches added to the location.

Port/SSID

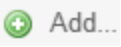
The port or port range for a wired switch or the SSIDs for a wireless switch.

AP ID

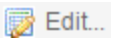
The access point identifiers for a wireless switch.

Description

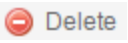
The description of the location group.

Add Button 

Select the **Add** button to open the Add Entry window, from which you can add an entry to the Entry Editor section.

Edit Button 

Select an entry in the Entry Editor section of the window and select the **Edit** button to open the Edit Entry window, from which you can edit an existing entry.

Delete Button 

Select an entry in the Entry Editor section of the window and select the **Delete** button to delete an existing entry.

Save Button

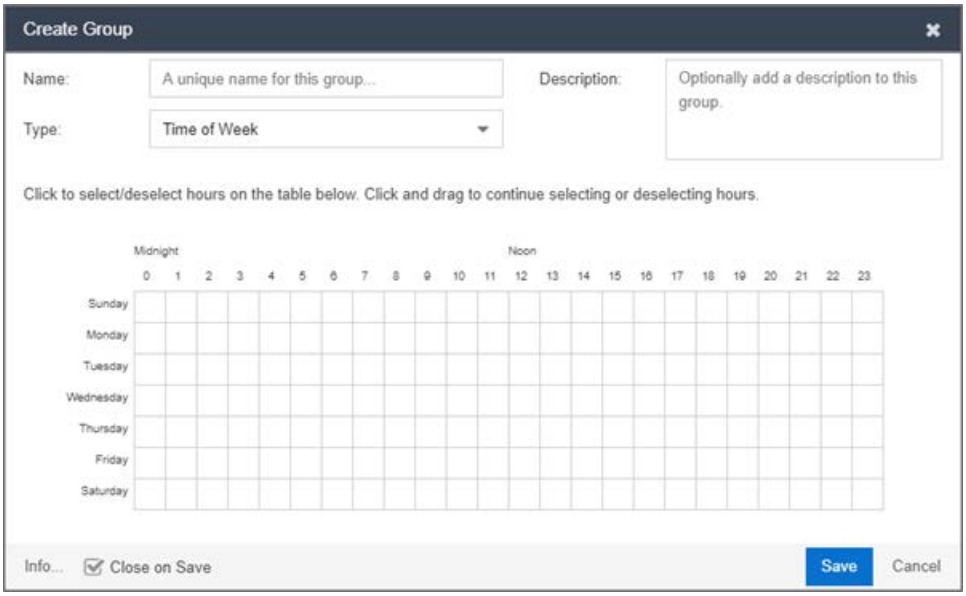
Select the **Save** button to save the location group.

Create Time Group Window

Use this window to add a new time group or edit an existing time group. Time groups are rule components that enable you to specify network access requirements or restrictions based on the day and time when the end user is accessing the network. For example, in an enterprise environment, an employee could be assigned different access privileges based on whether they log in during traditional work hours or after hours.

You can access the Add/Edit Time Group window from the Manage Rule Groups window or from the time group field in the Create Rule window.

NOTE: Changes to rule components do not require an enforce. Changes will be automatically synchronized with engines on the next status update. Changes will not affect end-systems until the next authentication and/or assessment occurs.



Name

Enter a name for a new time group. You cannot edit the name of an existing group. If you want to change the name, you must create a new time group with a new name and then delete the old time group.

Description

Enter a description of the time group. This description displays in the Manage Rule Groups window.

Calendar

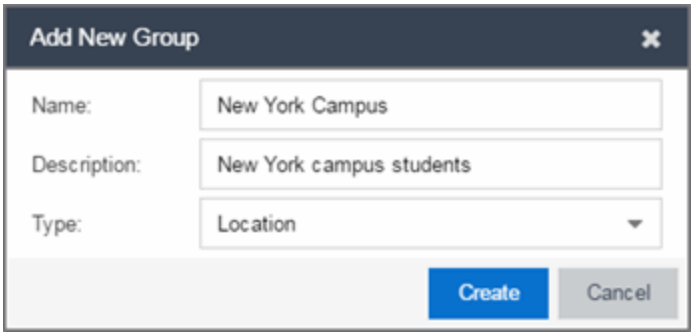
Use the calendar to select the desired weekly time periods. Select to choose a specific day and time, or select and drag to quickly select a time sequence or series of days. For example,

you can select Monday at 8 AM and drag down to select that hour for Monday through Friday. The select and drag feature makes it easy to select an entire week or chunk of time with just one action. Right-click on a selected square to access menu options that let you select all or clear all squares, and undo the last action. If a square is the first or last in a series, right-click to access the Refine Time Range Start/End options that let you specify hourly increments for the start and end times.

Add/Edit User Group

Use this window to add a new user group or edit an existing user group. User groups are rule components that allow you to group together end users having similar network access requirements or restrictions. You can access the Add/Edit User Group window from the Manage Rule Groups window or from the user group field in the Create Rule window.

NOTE: Changes to rule components do not require an enforce. Changes are automatically synchronized with engines on the next status update. Changes do not affect end-systems until the next authentication and/or assessment occurs.



Name
Enter a name for a new user group. You cannot edit the name of a group.

Description
Enter a description of the user group.

Type
Select **User** to create an end-system group. Specify whether the user group is based on:

- Username — a list of usernames which can be based on an exact match or a wild card.
- LDAP User Group — a list imported from an LDAP Server, organized by Organization Unit (OU), or a custom attribute lookup for any user or MAC address if they match a AAA configuration entry that assigns the request a valid LDAP Configuration.
- RADIUS User Group — a list of attributes the upstream RADIUS server returns or attributes the RADIUS client sends.
- OpenID User Group - a custom attribute lookup for the OpenID server. OpenID User Group can be combined with EAP-TTLS and Entra ID authentication, Captive Portal Registration with Entra ID, EAP-TLS with user authentication, and EAP-TLS with computer authentication.
    - memberOf can be used for group membership checks for both users and computers.

- extensionAttribute1 through extensionAttribute15 can be used for both users and computers.
- name of Custom Security Attribute can be used for user authentication.

Select **Create** to display the Entry Editor section of the window. This section varies depending on the group **Type** selected.

Mode

For LDAP, RADIUS, and OpenID user groups, select a mode option to **Match Any** or **Match All** of the LDAP or RADIUS or OpenID User Group entries (attribute names) listed below

For LDAP User Groups, you can also select **Exists**, as the username can be used to verify this criteria after the initial authentication (i.e., using Registration). The **Exists** mode is not available for RADIUS User Groups because they cannot be verified after an initial registration as the user credentials are not stored on the ExtremeControl engine for re-verification.

Attribute Lookup...

Select to search configured LDAP servers for matching attributes that can be added to the Attributes table. Searches can be performed against User or Host objects depending on the configured LDAP profile.

OU Import...

Select to Import all OUs from the LDAP server based on the selected LDAP configuration. Only available for group type "User: LDAP User Group".

Import...

Select to import a list of usernames to the user group. A newly created user group must be saved or exist first before import. Only available for group type "User: Username".

Export...

Select to export a list of usernames from the user group. A newly created user group must be saved or exist first before export. Only available for group type "User: Username".

Attribute Name

The name of the LDAP or RADIUS Attribute.

Value

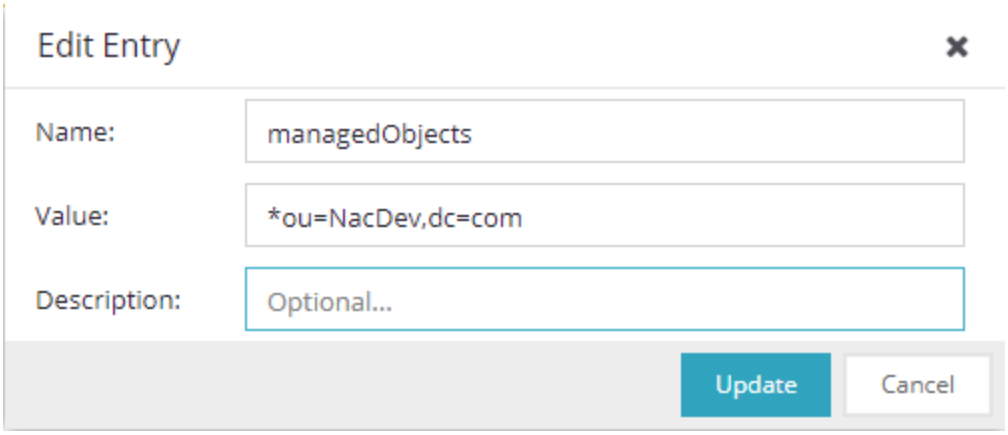
The Attribute value of the user group or username.

Add Button 

Select the **Add** button to open the Add Entry window, from which you can add an entry to the Entry Editor section.

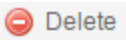
Edit Button 

Select an entry in the Entry Editor section of the window and select the **Edit** button to open the Edit Entry window, from which you can edit an existing entry.



IMPORTANT Commas are generally used to separate the attribute/value pairs in an entry to ensure they are evaluated separately. Adding a comma can impact how wildcards (*) are handled. To force the entry to be treated as a single value, do not use a comma before a second '='.

For Example: `ou=NacDev,DC=com` is evaluated as two separate entries; `ou=ou=NacDev,DC=com` is evaluated as a single entry.

Delete Button 

Select an entry in the Entry Editor section of the window and select the **Delete** button to delete an existing entry.

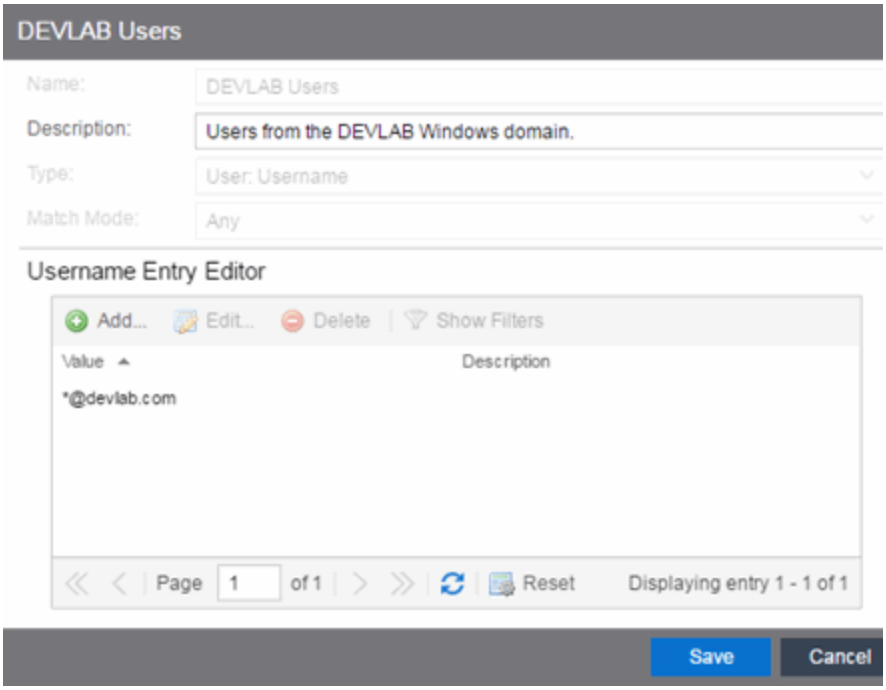
Filter 

Use the Filter functions to filter for a specific entry based on a numeric value or text.

Add/Edit User Group Window

Use this Access Control window to add a new user group or edit an existing user group. User groups are rule components that allow you to group together end-users having similar network access requirements or restrictions. You can access the Add/Edit User Group window from the Group Editor or from the user group field in the Add Rule window.

NOTE: Changes to rule components do not require an enforce. Changes automatically synchronize with the engines on the next status update. Changes do not affect end-systems until the next authentication and/or assessment occurs.



Name

Enter a name for a new user group. You cannot edit the name of a group.

Description

Enter a description of the user group.

Type

Specify the criteria on which the user group is based:

- Username - a list of usernames which can be based on an exact match or a wild card.
- LDAP User Group - a list imported from an LDAP Server, organized by Organization Unit (OU), or a custom attribute lookup for any user or MAC address if they match a AAA configuration entry that assigns the request a valid LDAP Configuration.

- RADIUS User Group - a list of attributes the upstream RADIUS server returns or attributes the RADIUS client sends.
- OpenID User Group - a custom attribute lookup for the OpenID server. OpenID User Group can be combined with EAP-TTLS and Entra ID authentication, Captive Portal Registration with Entra ID, EAP-TLS with user authentication, and EAP-TLS with computer authentication.
    - memberOf can be used for group membership checks for both users and computers.
    - extensionAttribute1 through extensionAttribute15 can be used for both users and computers.
    - name of Custom Security Attribute can be used for user authentication.

Match Mode

For LDAP, RADIUS, and OpenID user groups, the Match Mode option lets you select whether to match any or match all of the LDAP or RADIUS or OpenID User Group entries (attribute names) listed below.

For LDAP User Groups, you can also select "Exists", since the username can be used to verify this criteria after the initial authentication (i.e., using Registration). The "Exists" mode is not available for RADIUS User Groups because they cannot be verified after an initial registration as the user credentials are not stored on the ExtremeControl engine for re-verification.

Username Entry Editor

Use the buttons to add, edit, or delete entries in the group. Usernames can be an exact match or use wildcards.

Filter 

Use the Filter functions to filter for a specific entry based on a numeric value or text.

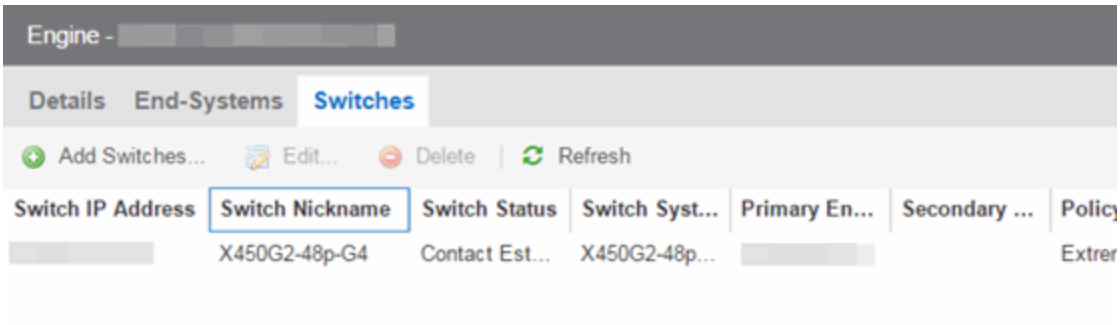
Switches

This tab provides information about the switches assigned to an ExtremeControl engine or Access Control Engine Group. To access this tab, select an engine or engine group in the left-panel tree, then select the **Switches** tab in the right panel.

You can right-click on one or more switch for a menu of options.

If you are using the **Policy** tab, you can also right-click on one or more switch and select from the options in the Policy menu.

Use the table options and tools to filter, sort, and customize table settings. You can access the options by selecting the down arrow in the right corner of any column header.



Switch IP Address
The switch's IP address.

Switch Nickname
The nickname assigned to the switch when it is added to the ExtremeCloud IQ Site Engine database.

Switch Status
The current operational status of the switch, based on the ExtremeCloud IQ Site Engine device poll. If the device poll did not update the status of a switch, and a Verify RADIUS Configuration operation is performed on that switch, the switch status in the **Switches** tab can differ from the switch status in the Verify RADIUS Configuration window.

Switch System Name
The assigned name of the device as stored in the device's sysName MIB object.

Primary Engine
The name and IP address of the switch's primary Access Control Engine. If load balancing has been configured for the engine group, the ExtremeCloud IQ Site Engine server determines the primary and secondary engines at Enforce, and this field displays "Determined by Load Balancer."

Secondary Engine
The name and IP address of the switch's secondary Access Control Engine. If load balancing has been configured for the engine group, the ExtremeCloud IQ Site Engine server determines the primary and secondary engines at Enforce, and this field displays "Determined by Load Balancer."

Policy/VLAN
The RADIUS attributes included as part of the RADIUS response.

Policy Domain
The Policy Manager domain the switch is assigned to (if any). You can populate this field by right-clicking on a switch and selecting Policy > Verify Domain. This information does not automatically update if there are domain assignment changes. You need to re-select the menu option to update the domain information.

Auth Access Type

The type of authentication access allowed for this switch:

- **Any access** — the switch can authenticate users originating from any access type.
- **Management access** — the switch can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- **Network access** — the switch can only authenticate users accessing the network via the following authentication types: MAC, PAP, CHAP, and 802.1X. If RADIUS accounting is enabled, then the switch also monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions.
- **Monitoring - RADIUS Accounting** — the switch monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. Access Control learns about these session via RADIUS accounting. This allows Access Control to be in a listen mode, and to display access control, location information, and identity information for end-systems without enabling authentication on the switch.
- **Manual RADIUS Configuration** — RADIUS configuration was performed manually on the switch using Policy Manager or CLI.

Switch Type

Specifies the switch type: a switch that authenticates layer 2 traffic via RADIUS to an out-of-band Access Control engine, or a VPN concentrator being used in an ExtremeControl VPN deployment.

Switch Location

The physical location of the switch.

Switch Contact

The person responsible for the switch.

Switch Description

A description of the switch, which can include its manufacturer, model number, and firmware revision number.

Management RADIUS Servers

RADIUS servers used to authenticate requests for administrative access to the switch.

RADIUS Accounting

Displays whether RADIUS accounting is enabled or disabled on the switch. RADIUS accounting can be used to determine the connection state of the end-system sessions on the Access Control engine, providing real-time connection status in ExtremeCloud IQ Site Engine. RADIUS accounting is also used to monitor switches for Auto Tracking, CEP (Convergence End Point), and Switch Quarantine authentication sessions, when used in conjunction with the Monitoring or Network Access switch authentication access types. For more information, see the Auth. Access Type section of the Add/Edit Switch Window Help topics.

Message-Authenticator Attribute

Defines if the Access-Request must contain the Message-Authenticator attribute in the RADIUS communication with this device. Not every RADIUS client supports this attribute, but the security best practice is to require the Message-Authenticator attribute. If set to "Required" the RADIUS packets without Message-Authenticator attribute are dropped.

IP Subnet for IP Resolution

Displays the IP subnet that the switch is using as an inclusive list for MAC to IP resolution. Specifying an IP subnet in a static IP network allows for a router to be used for IP resolution in cases where it would not be discovered via DHCP. IP Subnets also contain an IP range which can be used to filter out secondary IP addresses that are not valid for the network.

Policy Enforcement Points

If the switch is a VPN device (see Switch Type column), this column displays the Policy Enforcement Points that are being used to provide authorization for the connecting end-systems.

Add Switch

Opens the Add Switches to ExtremeControl Engine Group window where you can select switches to add to the engine or engine group.

Edit

Select a switch and select this button to open the Edit Switches in ExtremeControl Engine Group window where you can change the switch's primary and secondary Access Control Engine, and also edit other switch attributes, if desired.

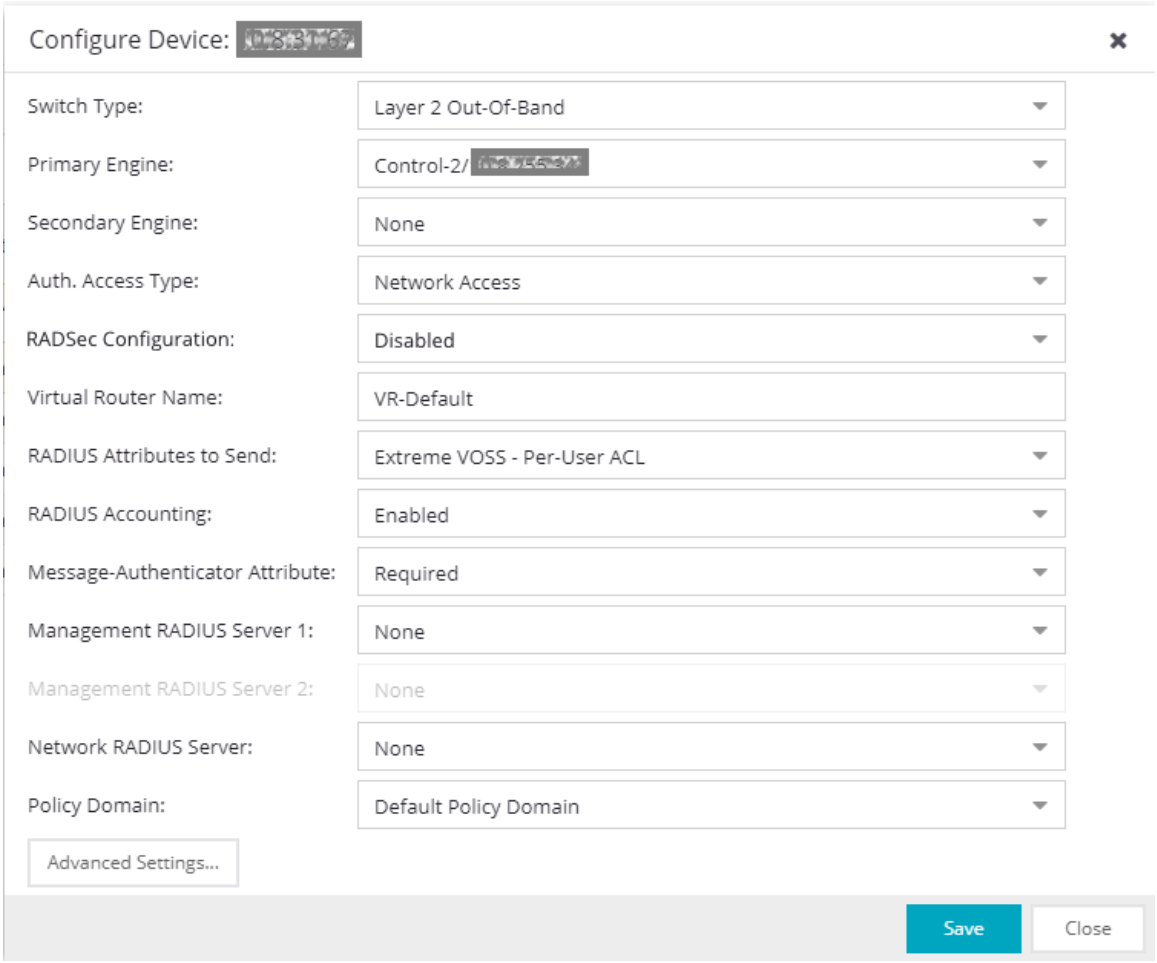
Delete

Select a switch and select this button to delete the switch from ExtremeCloud IQ Site Engine's device database. The switch's primary engine enforces its own primary RADIUS server as both the primary and secondary RADIUS servers on the switch.

Edit Switches in Access Control Engine Group

Use this window to change a switch's primary and secondary ExtremeControl engine, and also edit other switch parameters including the switch's authentication access type and the RADIUS attributes to send, if desired.

You can access this window by selecting an engine or engine group in the left-panel tree. Then, in the right-panel **Switches** tab, select the switches you wish to edit and select the **Edit** button.



Switch Type

Use the drop-down list to change the type of switch:

- **Layer 2 Out-Of-Band** — A switch that authenticates on layer 2 traffic via RADIUS to an out-of-band Access Control engine.
- **Layer 2 Out-Of-Band (No SNMP)** — A switch that authenticates on layer 2 traffic via RADIUS to an out-of-band Access Control engine, but does not use SNMP for communication between the Access Control engine and the switch. When you select this type, the Authentication Access Type automatically changes to Manual RADIUS Configuration, and you must perform the RADIUS configuration on the switch CLI. Select this type when SNMP communication between the Access Control engine and the switch is not permitted in your environment. SNMP-based features such as port discovery and port status monitoring are unavailable for this type. Use this option as a best practice for Cloud Native Access Points managed directly by ExtremeCloud IQ or Extreme Platform ONE Networking.
- **Layer 2 Out-Of-Band Data Center** — A switch within a data center where visualization and mobility are a factor. If an end-system changes location but does not move to a

different Access Control engine, Access Control removes the end-system authentication from their prior port/switch. This allows VMs that quickly move from one server to another and then back again to still have their location updated in ExtremeCloud IQ Site Engine, because only one authenticated session is allowed per end-system in ExtremeCloud IQ Site Engine.

- **Layer 2 RADIUS Only** — In this mode, ExtremeCloud IQ Site Engine does not require any information from the switch other than the end-system MAC address (from Calling-Station-Id or User-Name). The NAS-Port does not need to be specified. If the switch supports RFC 3576, you can set the Reauthentication Behavior in the Advanced Switch Settings window. IP resolution and reauthentication might not work in this mode.
- **VPN** - A VPN concentrator being used in an ExtremeControl VPN deployment. In this case, you should specify one or more Policy Enforcement Points below. If you do not specify a Policy Enforcement Point, then ExtremeCloud IQ Site Engine is unable to apply policies to restrict access after the user is granted access.

Primary Engine

Use the drop-down list to select the primary Access Control engine for the selected switches. If load balancing has been configured for the switch, this field is not displayed.

Secondary Engine

Use the drop-down list to select the secondary Access Control engine for the selected switches. If load balancing has been configured for the switch, this field is not displayed.

Auth Access Type

Use the drop-down list to select the type of authentication access allowed for these switches. This feature allows you to have one set of switches for authenticating management access requests and a different set for authenticating network access requests.

WARNING: Access Control uses CLI access to perform configuration operations on Fabric Engine devices. ExtremeControl uses SNMP and CLI access to perform configuration operations on Switch Engine devices based on the firmware version.

- Enabling an Auth type of "Any Access" or "Management Access" can restrict access to the switch after an enforce is performed. For management requests handled through Access Control, make sure that an appropriate administrative access configuration is in place by assigning a profile such as "Administrator Access Control Profile" to grant proper access to users. Also, verify that the current switch CLI credentials for the admin user are defined in the database against which Access Control authenticates management login attempts.
- Switching from an Auth type of "Any Access" or "Management Access" back to "Network Access" can restrict access to the switch after an enforce is performed. Verify that the current switch CLI credentials for the admin user are defined locally on the switch.

- **Any Access** — the switch can authenticate users originating from any access type.
- **Management Access** — the switch can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- **Network Access** - the switch can only authenticate users accessing the network via the following authentication types: MAC, PAP, CHAP, and 802.1X. If RADIUS accounting is enabled, then the switch also monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. If there are multiple sessions for a single end-system, the session with the highest precedence will be displayed to provide the most accurate access control information for the user. The Access Control authentication type precedence from highest to lowest is: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.
- **Monitoring - RADIUS Accounting** — the switch will monitor Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. ExtremeCloud IQ Site Engine learns about these session via RADIUS accounting. This allows ExtremeCloud IQ Site Engine to be in a listen mode, and to display access control, location information, and identity information for end-systems without enabling authentication on the switch. If there are multiple sessions for a single end-system, the session with the highest precedence displays to provide the most accurate access control information for the user. The Access Control authentication type precedence from highest to lowest is: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.
- **Manual RADIUS Configuration** — ExtremeCloud IQ Site Engine does not perform any RADIUS configurations on the switch. Select this option if you want to configure the switch manually using the **Policy** tab or CLI.

RADSec Configuration

Use the drop-down list to specify whether the Access Control engine configures RadSec on the selected switches. Select **Enabled** to configure the switches to send RADIUS requests to the Access Control engine over TCP (secured by TLS). Select **Disabled** to use RADIUS over UDP. To configure RadSec, you must also assign a certificate to the switches in the RADSec Certificates panel.

Virtual Router Name

Select the checkbox to enter the name of the Virtual Router. The default value for this field is **VR-Default**.

WARNING: For ExtremeXOS/Switch Engine devices only. If ExtremeCloud IQ Site Engine has not detected and populated this field, enter the Virtual Router Name carefully. Incorrectly entering a value in this field causes the RADIUS configuration to fail, which is not reported when enforcing the configuration to the switch.

RADIUS Attributes to Send

Use the drop-down list to select the RADIUS attributes settings included as part of the RADIUS response from the Access Control engine to the switch.

RADIUS Accounting

Use the drop-down list to enable RADIUS accounting on the switch. RADIUS accounting can be used to determine the connection state of the end-system sessions on the Access Control engine, providing real-time connection status in ExtremeCloud IQ Site Engine. It also allows Access Control to monitor Auto Tracking, CEP (Convergence End Point), and Quarantine (anti-spoofing) sessions.

Message-Authenticator Attribute

Defines if the Access-Request must contain the Message-Authenticator attribute in the RADIUS communication with this device. Not every RADIUS client supports this attribute, but the security best practice is to require the Message-Authenticator attribute. If set to "Required" the RADIUS packets without Message-Authenticator attribute are dropped.

Management RADIUS Server

Use the drop-down list to specify RADIUS servers used to authenticate requests for administrative access to the selected switches. Select from the RADIUS servers you have configured in ExtremeCloud IQ Site Engine, or select **New** or **Manage** to open the Add/Edit RADIUS Server or Manage RADIUS Servers windows.

Network RADIUS Server

This option lets you specify a backup RADIUS server to use for network authentication requests for the selected switches. This allows you to explicitly configure a network RADIUS server to use if there is only one Access Control engine. (This option is only available if a Secondary Engine is not specified.) Select from the RADIUS servers you have configured in Extreme Control, or select **New** or **Manage** to open the Add/Edit RADIUS Server or Manage RADIUS Servers windows.

Policy Domain

Use this option to assign the switch to a **Policy** tab domain and enforce the domain configuration to the switch. The switch must be an Extreme Networks switch.

NOTE: Selecting **-- Do Not Set --** for an Access Control engine on which a Policy Domain is configured does not unassign the Policy Domain. To unassign a Policy Domain, use the **Policy** tab.

Advanced Settings

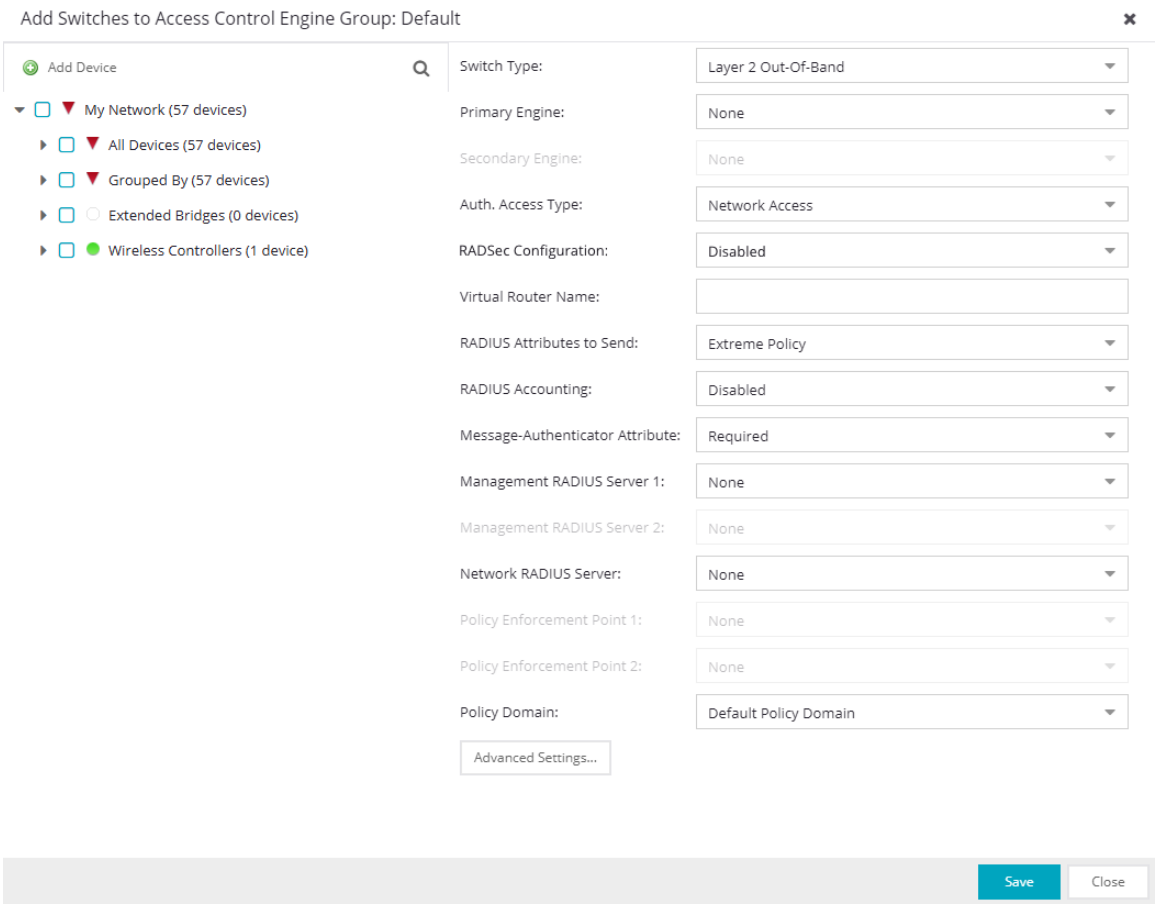
Select this button to open the Advanced Switch Settings window.

Add Switches to Access Control Engine Group

Use this window to add switches to an engine or engine group. The window allows you to select one or more switches from the device tree, and set the primary and secondary ExtremeControl Engines for the switches. It also lets you set other parameters including the authentication access type for the switches and the RADIUS attributes to send.

NOTE: If desired, you can set only the primary Access Control Engine for the switches; ExtremeCloud IQ Site Engine does not require the secondary Access Control Engine to be set. If only the primary Access Control Engine is set, then by default that engine uses its primary proxy RADIUS server as a secondary direct RADIUS server to the switch. This allows for redundancy without the requirement for a secondary Access Control Engine. In this scenario, if contact with the Access Control Engine fails, authentication traffic would bypass the Access Control Engine, but normal authentication would continue in the network, and still provide some security.

You can access this window by selecting an engine or engine group and selecting the **Add Switch** button in the right-panel **Switches** tab.



Device Tree

This area displays the device tree. Expand the tree and select the switches you want to add to the engine or engine group.

Add Device

Opens the Add Device window where you can add a device to the ExtremeCloud IQ Site Engine database. The device is displayed in the My Network folder in the device tree.

Switch Type

Use the drop-down list to select the type of switch you are adding:

- **Layer 2 Out-Of-Band** — A switch that authenticates on layer 2 traffic via RADIUS to an out-of-band Access Control engine.
- **Layer 2 Out-Of-Band (No SNMP)** — A switch that authenticates on layer 2 traffic via RADIUS to an out-of-band Access Control engine, but does not use SNMP for communication between the Access Control engine and the switch. When you select this type, the Authentication Access Type automatically changes to Manual RADIUS Configuration, and you must perform the RADIUS configuration on the switch CLI. Select this type when SNMP communication between the Access Control engine and the switch is not permitted in your environment. SNMP-based features such as port discovery and port status monitoring are unavailable for this type. Use this option as a best practice for Cloud Native Access Points managed directly by ExtremeCloud IQ or Extreme Platform ONE Networking.
- **Layer 2 Out-Of-Band Data Center** — A switch within a data center where visualization and mobility are a factor. If an end-system changes location but does not move to a different Access Control engine, Access Control removes the end-system authentication from their prior port/switch. This allows VMs that quickly move from one server to another and then back again to still have their location updated in ExtremeCloud IQ Site Engine, because only one authenticated session is allowed per end-system in ExtremeCloud IQ Site Engine.
- **Layer 2 RADIUS Only** — In this mode, ExtremeCloud IQ Site Engine does not require any information from the switch other than the end-system MAC address (from Calling-Station-Id or User-Name). The NAS-Port does not need to be specified. If the switch supports RFC 3576, you can set the Reauthentication Behavior in the Advanced Switch Settings window. IP resolution and reauthentication might not work in this mode.
- **VPN** - A VPN concentrator being used in an ExtremeControl VPN deployment. In this case, you should specify one or more Policy Enforcement Points below. If you do not specify a Policy Enforcement Point, then ExtremeCloud IQ Site Engine is unable to apply policies to restrict access after the user is granted access.

Primary Engine

Use the drop-down list to select the primary Access Control Engine for the selected switches. If load balancing has been configured for the engine group, the ExtremeCloud IQ Site Engine server determines the primary and secondary engines at Enforce, and this field displays **Determined by Load Balancer**.

Secondary Engine

Use the drop-down list to select the secondary Access Control Engine for the selected switches. If load balancing has been configured for the engine group, the ExtremeCloud IQ Site Engine server determines the primary and secondary engines at Enforce, and this field displays **Determined by Load Balancer**.

NOTE: To configure additional redundant Access Control engines for each switch (up to four), use the Display Counts option in the Display options panel (Administration > Options > Access Control).

Auth. Access Type

Use the drop-down list to select the type of authentication access allowed for these switches. This feature allows you to have one set of switches for authenticating management access requests and a different set for authenticating network access requests.

WARNING: Access Control uses CLI access to perform configuration operations on Fabric Engine devices. ExtremeControl uses SNMP and CLI access to perform configuration operations on Switch Engine devices based on the firmware version.

- Enabling an Auth type of "Any Access" or "Management Access" can restrict access to the switch after an enforce is performed. Make sure that an appropriate administrative access configuration is in place by assigning a profile such as "Administrator Access Control Profile" to grant proper access to users. Also, verify that the current switch CLI credentials for the admin user are defined in the database that ExtremeCloud IQ Site Engine authenticates management login attempts against.
- Switching from an Auth type of "Any Access" or "Management Access" back to "Network Access" can restrict access to the switch after an enforce is performed. Verify that the current switch CLI credentials for the admin user are defined locally on the switch.

- **Any Access** - the switch can authenticate users originating from any access type.
- **Management Access** - the switch can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- **Network Access** - the switch can only authenticate users that are accessing the network via the following authentication types: MAC, PAP, CHAP, and 802.1X. If RADIUS accounting is enabled, then the switch also monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. If there are multiple sessions for a single end-system, the session with the highest precedence displays to provide the most accurate access control information for the user. The Access Control authentication type precedence from highest to lowest is: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.
- **Monitoring - RADIUS Accounting** - the switch monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. ExtremeCloud IQ Site Engine learns about these session via RADIUS accounting. This allows ExtremeCloud IQ Site Engine to be in a listen mode, and to display access control, location information, and identity information for end-systems without enabling authentication on the switch. If there are multiple sessions for a single end-system, the session with the highest precedence displays to provide the most accurate access control information for the

user. The Access Control authentication type precedence from highest to lowest is: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.

- **Manual RADIUS Configuration** - ExtremeCloud IQ Site Engine does not perform any RADIUS configurations on the switch. Select this option if you want to configure the switch manually using the **Policy** tab or CLI. This access type is automatically selected when the **Switch Type** is configured as **Layer 2 Out-Of-Band (No SNMP)**.

RADSec Configuration

Use the drop-down list to specify whether the Access Control engine configures RadSec on the selected switches. Select **Enabled** to configure the switches to send RADIUS requests to the Access Control engine over TCP (secured by TLS). Select **Disabled** to use RADIUS over UDP. The default value is **Disabled**. To configure RadSec, you must also assign a certificate to the switches in the RADSec Certificates panel.

Virtual Router Name

Enter the name of the Virtual Router. The default value for this field is **VR-Default**.

WARNING: For ExtremeXOS/Switch Engine devices only. If ExtremeCloud IQ Site Engine has not detected and populated this field, enter the Virtual Router Name carefully. Incorrectly entering a value in this field causes the RADIUS configuration to fail, which is not reported when enforcing the configuration to the switch.

RADIUS Attributes to Send

Use the drop-down list to select the RADIUS attributes included as part of the RADIUS response from the Access Control engine to the switch. You can also select **New** or **Manage** from the menu to open the RADIUS Attribute Settings window where you can define, edit, or delete the available attributes.

RADIUS Accounting

Use the drop-down list to enable RADIUS accounting on the switch. RADIUS accounting can be used to determine the connection state of the end-system sessions on the Access Control engine, providing real-time connection status in ExtremeCloud IQ Site Engine.

Message-Authenticator Attribute

Defines if the Access-Request must contain the Message-Authenticator attribute in the RADIUS communication with this device. Not every RADIUS client supports this attribute, but the security best practice is to require the Message-Authenticator attribute. If set to "Required" the RADIUS packets without Message-Authenticator attribute are dropped.

Management RADIUS Server 1 and 2

Use the drop-down list to specify RADIUS servers used to authenticate requests for administrative access to the selected switches. Select from the RADIUS servers you have configured in ExtremeCloud IQ Site Engine, or select New or Manage RADIUS Servers to open the Add/Edit RADIUS Server or Manage RADIUS Servers windows.

Network RADIUS Server

This option lets you specify a backup RADIUS server to use for network authentication requests for the selected switches. This allows you to explicitly configure a network RADIUS server to use if there is only one Access Control engine. (This option is only available if a Secondary Engine is not specified.) Select from the RADIUS servers you have configured in ExtremeCloud IQ Site Engine, or select New or Manage RADIUS Servers to open the Add/Edit RADIUS Server or Manage RADIUS Servers windows.

Policy Enforcement Point 1 and 2

Select the Policy Enforcement Points used to provide authorization for the end-systems connecting to the VPN device you are adding. The list is populated from the N-Series, S-Series, and K-Series devices in your Console device tree. If you do not specify a Policy Enforcement Point, then Access Control is unable to apply policies to restrict end user access after the user is granted access.

Policy Domain

Use this option to assign the switch to a policy domain and enforce the domain configuration to the switch. The switch must be an Extreme Networks switch.

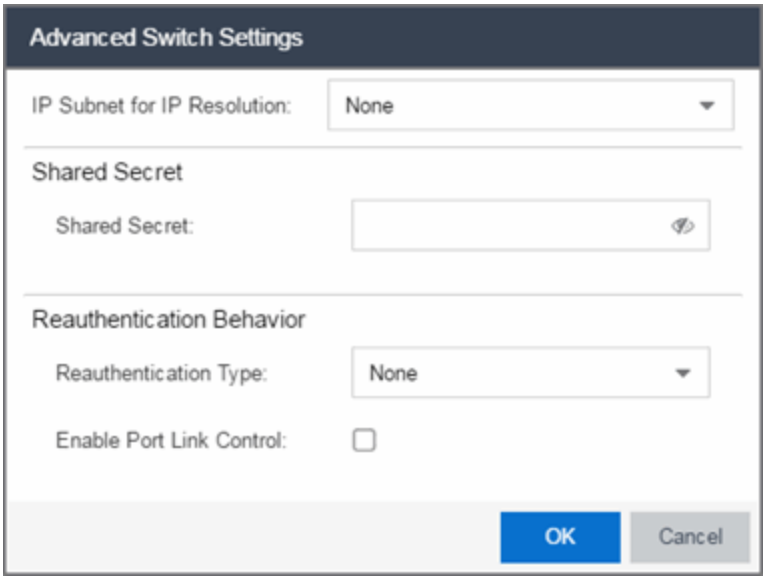
Advanced Settings

Select the Advanced Settings button to open the Advanced Switch Settings window.

Advanced Switch Settings

This window allows you to configure settings for switches that require a different configuration than your standard switch settings set in the Engine Settings window.

You can access the window from the Add Switch to ExtremeControl Engine Group window or from the Edit Switches in ExtremeControl Engine Group window.



IP Subnet for IP Resolution

Select the drop-down list to display a list of the IP subnets configured in the Engine Settings window. If you select a subnet, the switch uses it as an inclusive list for MAC to IP resolution. Specifying an IP subnet in a static IP network allows for a router to be used for IP resolution in cases where it would not be discovered via DHCP. IP subnets also contain an IP range which can be used to filter out secondary IP addresses that are not valid for the network.

Shared Secret

A string of alpha-numeric characters used to encrypt and decrypt communications between the switch and the ExtremeControl engine. The shared secret is shown as a string of asterisks. When the Show Password option is selected, the shared secret is shown in text.

Reauthentication Type

Select the reauthentication type for the switch:

- SNMP - uses SNMP to trigger reauthentication using various OIDs in different MIBs. The ExtremeControl engine checks a series of proprietary Enterasys MIBs, standardized MIBs, and proprietary third-party MIBs to determine availability, and forces reauthentication using any available SNMP method.
- Session Timeout - causes ExtremeControl to return a session timeout and terminate action to the end-system via RADIUS response attributes. The use of this mechanism causes the user to be automatically reauthenticated at a specified interval by the switch to which they are connected. Only use this option for wireless switches that do not have RFC 3576 support or wired switches that do not have SNMP support.
- RFC 3576 - a method of reauthenticating RADIUS sessions through the use of Disconnect-Request messages as defined by RFC 3576. (For more information, see http://www.ietf.org/rfc/rfc3576.txt). RFC 3576 configurations must be customized to work with the specific vendor implementation for each device type. To add, edit, or delete an RFC 3576 configuration, select the Manage RFC 3576 Configurations button.

Enable Port Link Control

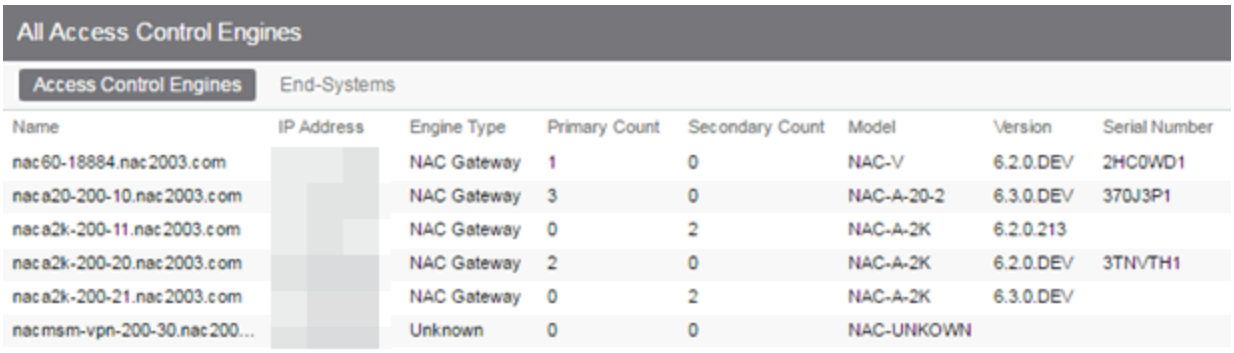
Port link control allows the toggle of the operational mode of a port. Select this option to enable port link control for specific switches.

All Access Control Engines

The **All Access Control Engines** tab is displayed in the right panel when you select the All Access Control Engine tree in the left panel or when you select the **Access Control Engines** tab when an Access Control Engine Group is selected. The panel displays a table of information about the engines in the folder or group. Right-click an engine for a menu of options.

Use the table options and tools to filter, sort, and customize table settings. You can access the options by selecting the down arrow in the right corner of any column header.

NOTE: The Access Control Engine administration web page allows you to access status and diagnostic information for an Access Control engine. Access the administration web page using the following URL: https://*Access ControlEngineIP*:8444/Admin. The default user name and password for access to this web page is "admin/Extreme@pp."



Name
The name of the Access Control engine (assigned when the engine is created).

IP Address
The Access Control engine's IP address.

Engine Type
The Access Control engine type: Access Control engine, ExtremeControl Layer 2 (L2) Controller, or Access Control Layer 3 (L3) Controller.

Primary Count
The number of switches for which the Access Control engine is the primary engine.

Secondary Count
The number of switches for which the Access Control engine is the secondary engine.

Model
The Access Control engine's model number.

Version
The Access Control engine's version number.

CPU Load (0–100%)
The percentage of the engine's CPU currently being used. This value gives you an indication of how busy the engine is and helps you determine if your network needs additional engines, or if you need to change your network configuration so that the load is more evenly distributed among your existing engines.

Memory Used
The amount of memory used by the engine.

Memory Available

The amount of memory available on the engine.

Connected Agents

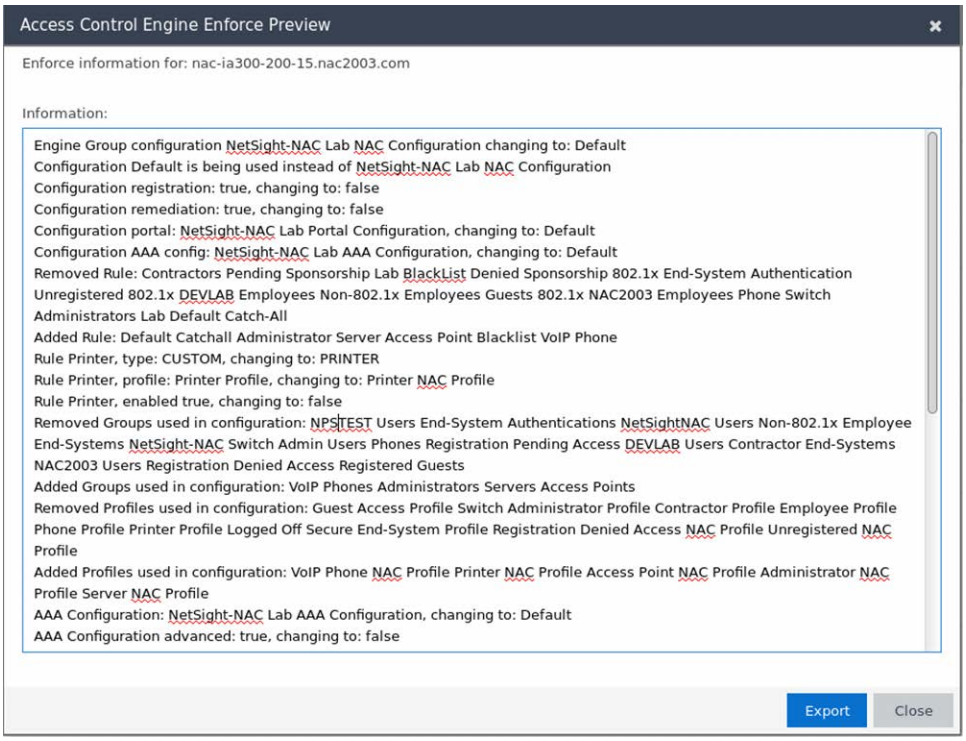
The number of assessment agents connected to the engine.

Capacity

The engine's current capacity, which is the number of end-systems that have authenticated within the last 24 hours out of the maximum number of authenticating end-systems supported for the engine.

Access Control Engine Enforce Preview

Use this window to preview what you are changing on an ExtremeControl engine by performing an enforce. You can access the Access Control Engine Enforce Preview window by right-clicking an engine in the Engines list on the Access Control tab and selecting **Enforce Preview** from the menu.



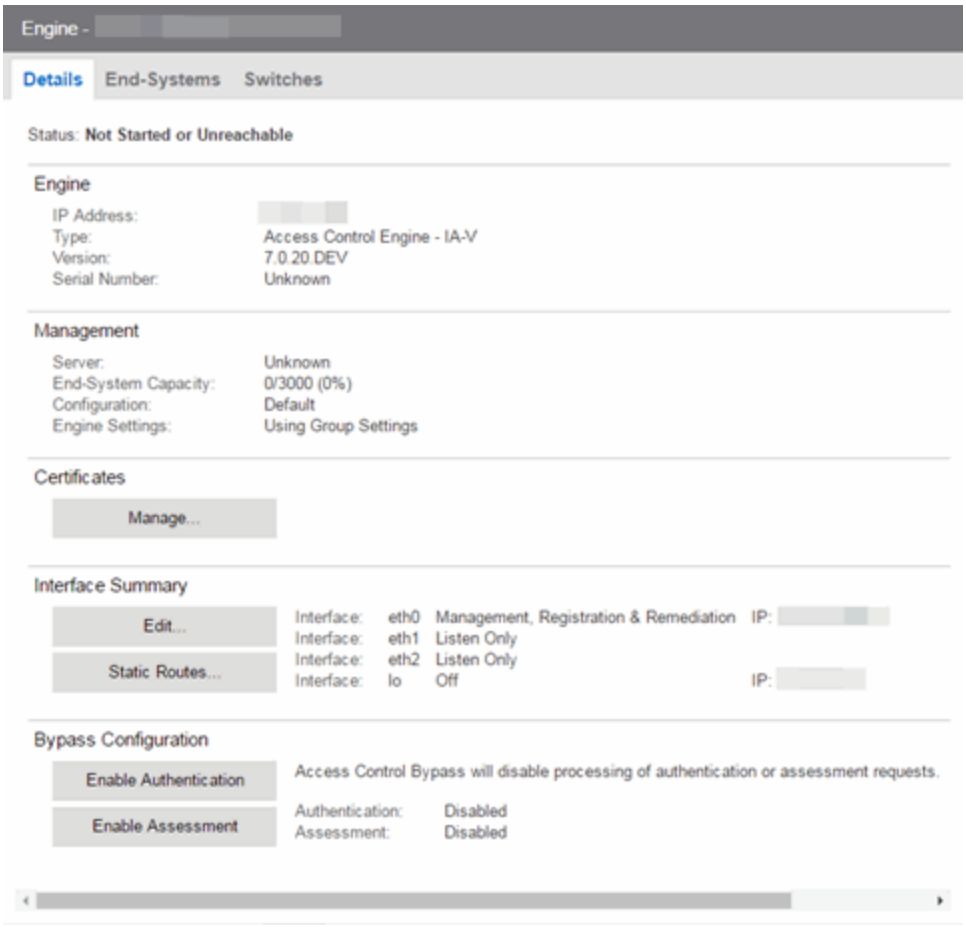
The window displays details of the changes you are making on the ExtremeControl engine.

Select the **Export** button to export the results to a text file.

Details (ExtremeControl Engine)

This tab provides information about an ExtremeControl engine's configuration. The information changes depending on the type of engine selected in the left-panel tree.

To access this tab, select an Access Control engine in the left-panel tree, then select the **Details** tab in the right panel.



General Information

This section displays general information about the Access Control engine, including its name, IP address, type (Access Control Engine or Layer 2/Layer 3 Access Control Controller), the engine version, the IP address of the ExtremeCloud IQ Site Engine Management server, and the Access Control engine status.

End-System Capacity

This field lists the engine's current capacity, which is the number of end-systems that authenticated within the last 24 hours out of the maximum number of authenticating end-systems supported for the engine.

Access Control Configuration

Displays the Access Control Configuration assigned to the engine. The Access Control Configuration determines the Access Control Profile assigned to an end-system connecting to the network.

Engine Settings

The engine settings configuration being used by your Access Control engine. Engine settings are configurable in the Engine Settings window by selecting the **Engine Settings** button.

Certificates

Select **Manage** to update the ExtremeControl certificates in the **Manage Certificates** window.

Interface Summary

Displays a summary of the current engine interface configuration.

Select **Edit** to open the **Interfaces** window, where you can change the engine Host Name and Gateway..

Select **Static Routes** to open the **Static Routes** window, where you can add or edit the static routes used for advanced routing configuration..

Access Control Bypass Configuration

The Access Control Bypass Configuration feature allows you to bypass Access Control processing of authentication requests from end-systems connecting to the network and also disable the Access Control assessment process. For Access Controlauthentication bypass, Access Control either configures the switch to authenticate directly to a RADIUS server to which Access Control is configured to proxy authentication requests, or it disables RADIUS authentication on the switch. This capability is useful for troubleshooting purposes. For example, if there is a problem with an Access Control Configuration, the **Disable** button lets you remotely disable Access Control functionality until the problem is resolved. You can then use the **Enable** button to re-enable Access Control functionality on the engines. When Access Control authentication or assessment is disabled, the Access Control engine name and IP address display in red text in the left-panel tree indicating the engine is in Bypass mode.

For Access Control engines, when you select the option to disable Access Control authentication processing, if proxy RADIUS servers are configured for authentication in a Basic AAA Configuration, the Access Control Engine configures the switches to send RADIUS packets directly to the primary and secondary RADIUS servers (from the Basic AAA Configuration), instead of talking to the RADIUS proxy through the Access Control. RADIUS authentication is not disabled on the switch, and end users still need to authenticate in order to connect to the network. The switches must be defined in the back-end proxy RADIUS server as RADIUS clients with the same shared secret used by the Access Control engines. If there are no proxy RADIUS servers configured in a Basic AAA Configuration, or if an Advanced AAA Configuration is used, RADIUS authentication on the switch is disabled when Access Control authentication processing is disabled.

NOTES: If you have disabled Access Control authentication processing and then enforce with new switches, the new switches are configured to send RADIUS packets directly to the primary and secondary RADIUS servers. These switches are reconfigured to talk to the RADIUS proxy when you enable Access Control; a second enforce is not necessary.

Bypass is not an option for switches set to Manual RADIUS Configuration or ExtremeWireless controllers not configured for RADIUS strict mode.

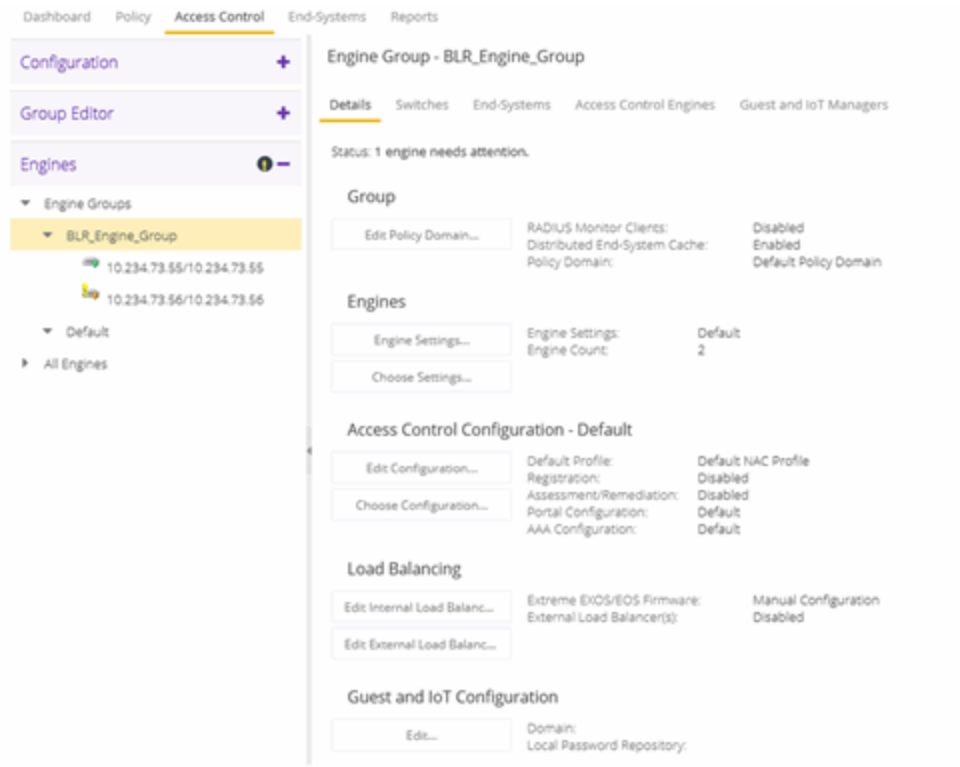
For Access Control Controller engines, when you disable Access Control authentication, then the Access Control Controller does **not** send RADIUS packets directly to the RADIUS servers. Authentication **is** disabled on the Access Control Controller and end-systems do not need to authenticate to the network. Traffic from the end-systems bypass the Access Control Controller and go directly onto the network.

The **Status** fields provide the current status of the Access Control authentication or assessment process. The authentication status field also includes a link to the Verify RADIUS Configuration on Switches feature. This feature is available for Access Control engines and Layer 2 Access Control Controllers, and can be used to alert you to any RADIUS configurations that are out of sync and could cause RADIUS authentication problems on the network.

Details (ExtremeControl Engine Groups)

This tab provides information about the ExtremeControl Details being used by your ExtremeControl engines.

To access this tab, select an engine group from within the Engine Group tree in the left-panel tree, then select the **Details** tab in the right panel.



Status

Status
Displays status of engines in the engine group.

Group

Policy Domain
Displays the policy domain for the Access Control engines in the folder. Select the **Edit Policy Domain** button to select a new policy domain for the engine group.

RADIUS Monitor Clients
Displays whether RADIUS Monitor Clients are enabled for the Access Control engines in the folder. RADIUS monitoring tools monitor ExtremeControl engine performance and availability.

Select the **Edit RADIUS Monitor Clients** button to open the **Configure RADIUS Monitor Clients** window, from which you can select a new client, change the monitoring client, and delete a client.

Engines

Engine Settings
The engine settings configuration being used by your Access Control engines. Engine settings are configurable in the Engine Settings window by selecting the **Engine Settings** button.

Engine Count
The number of engines in the engine group.

Access Control Configuration - Default

Access Control Configuration
The name of the Access Control Configuration being used by your Access Control engines. The Access Control Configuration determines the Access Control Profile assigned to an end-system connecting to the network.

Default Profile
The name of the Default Profile specified in the Access Control Configuration. The Default Profile serves as a "catch-all" profile for any end-system that doesn't match one of the rules listed in the Access Control Configuration.

Registration
Whether a registration/web access feature is enabled or disabled for the Access Control Configuration.

Assessment/Remediation
Whether the assessment/remediation feature is enabled or disabled for the Access Control Configuration.

Portal Configuration

The name of the Portal Configuration specified in the Access Control Configuration. If your network is implementing Registration or Assisted Remediation, the Portal Configuration defines the branding and behavior of the website used by the end user during the registration or remediation process.

AAA Configuration

The name of the AAA Configuration specified in the Access Control Configuration.

Load Balancing

Edit Internal Load Balancing

The Load Balancing panel displays the status of ExtremeXOS/Switch Engine/EOS firmware. By default, ExtremeXOS/Switch Engine/EOS Firmware status will be set to Manual Configuration.

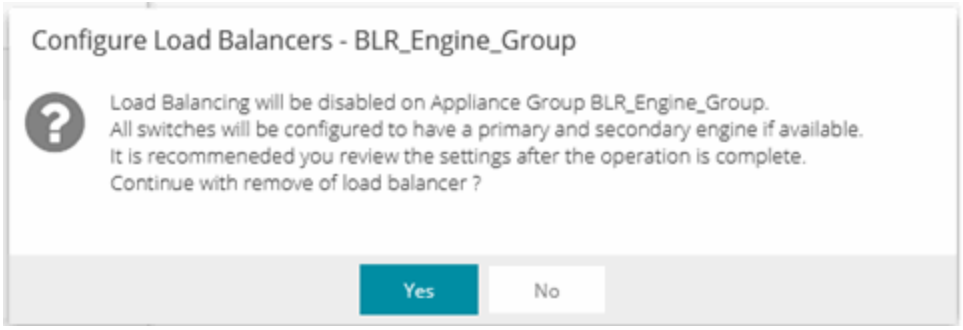
Select the Edit Internal Load Balancing button to open the Internal Load Balancer Window, which includes the following configuration types. The default configuration is Manual Configuration.

- Manual Configuration
- Standard
- Round Robin
- Sticky Round Robin

Edit External Load Balancing

The Load Balancing panel displays the status of External Load Balancer(s). By default, the External Load Balancer status is Disabled.

Select the **Edit External Load Balancing** button to open the External Load Balancer Window, where you can add, edit, delete or reorder Load Balancer IP addresses. If you delete all the load balancer addresses, a confirmation message window displays after the last IP address is deleted:

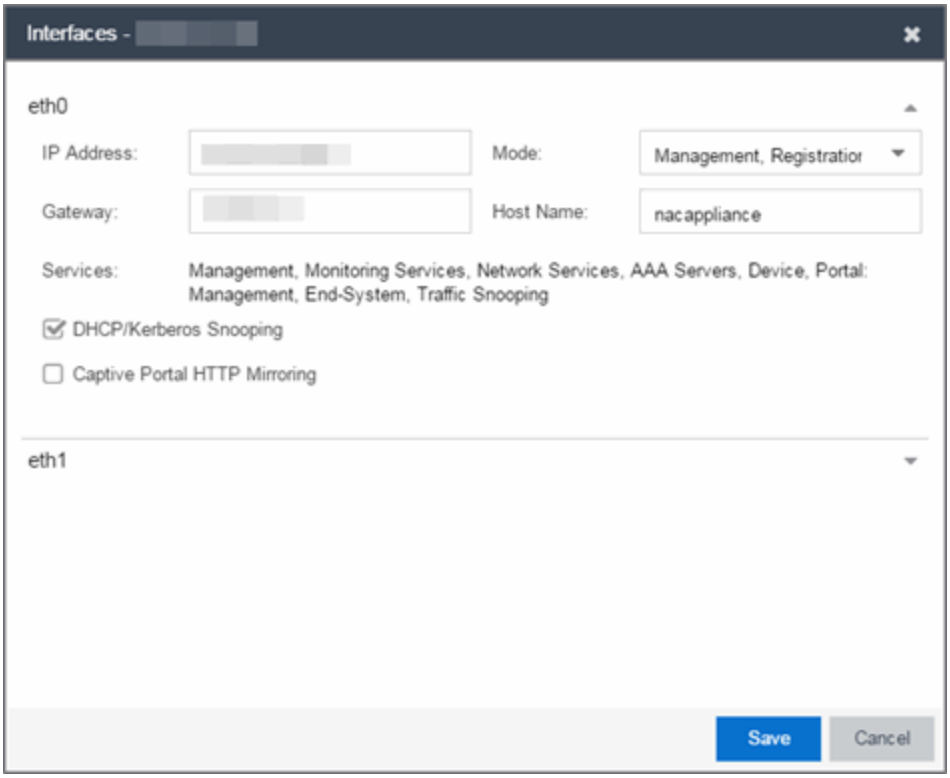


Select **Yes** to continue.

Interfaces Window

Use this ExtremeCloud IQ Site Engine window to configure the interfaces on an ExtremeControl engine. Interface configuration enables you to separate management traffic from end-system traffic, providing another layer of protection for sensitive data. It also provides the ability to snoop mirrored traffic on other ports.

This window is accessed from the **Control** > **Access Control** tab by selecting an Access Control engine, opening the **Details** tab, and selecting the **Edit** button in the Interface Summary section.



Interface Modes

There are five different modes that can be configured for an interface: Management, Registration & Remediation, Management Only, Registration & Remediation Only, Listening Only, Advanced Configuration, and Off. The mode determines the type of traffic permitted on the interface and the services provided by the interface.

You can configure all the interfaces on an engine; however, you cannot change the management interface and you are only permitted to configure one interface to enable management traffic.

Management, Registration & Remediation – This mode is the in-band management mode where both management traffic and registration, assessment, and remediation traffic use the same interface. In this mode, the engine does not limit traffic to each of the services.

Management Only – In this mode, the engine binds all management services to this interface. This includes:

- traffic to ExtremeCloud IQ Site Engine and other engines (JMS and HTTP)
- all traffic to switches
- all LDAP and RADIUS traffic
- traffic for the following services: SSH daemon, SNMP daemon, and RADIUS server
- traffic for captive portal administration, sponsorship, pre-registration, and screen preview (on ports 80 and 443)
- traffic for WebView pages and ExtremeCloud IQ Site Engine web services (on ports 8080 and 8443)

Registration & Remediation Only – In this mode, the engine binds all registration and remediation services to this interface. All traffic to end-systems is initiated through this interface, including:

- assessment traffic
- NetBIOS for IP and hostname resolution
- traffic for registration pages, remediation pages, and self-registration (on ports 80 and 443)
- all agent communication traffic (on ports 8080 and 8443)

Listen Only – In this mode, the engine enables DHCP and Kerberos snooping to be performed on the interface. No IP address or hostname can be assigned to the interface.

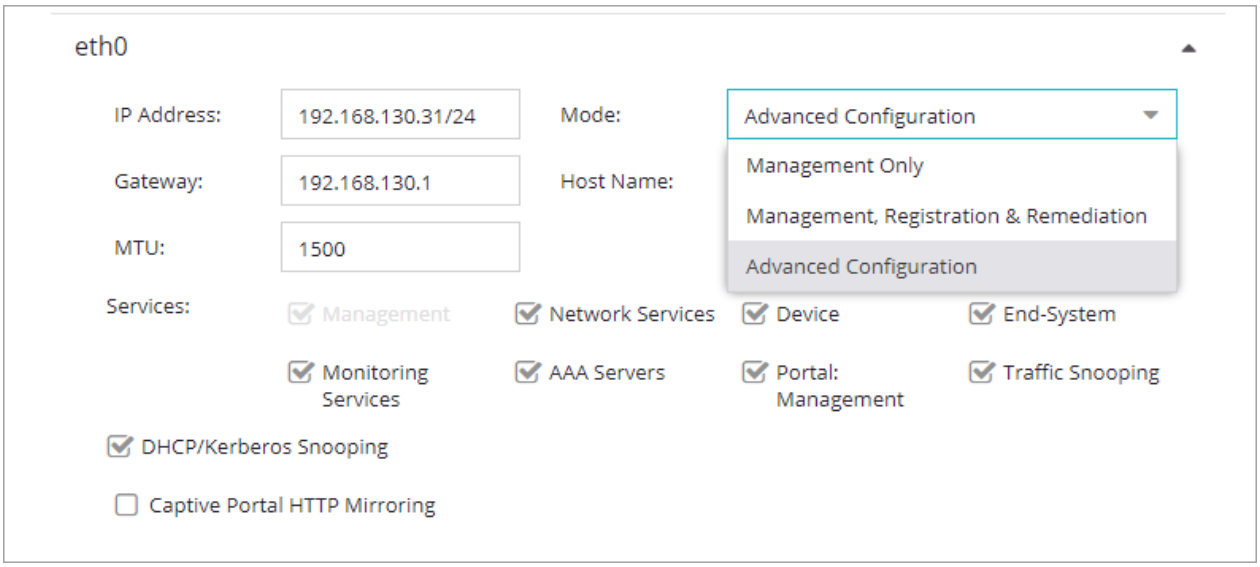
Advanced Configuration - This mode enables you to configure the services that are provided by the selected interface, using the link in the Services field. This is useful for ExtremeControl deployments in MSP or MSSP environments.

Off – The interface is disabled and not used in any way.

Services

The Services field displays the services that are provided by the ExtremeControl engine interface, as determined by the selected interface mode. Each mode provides a different set of services on the interface.

If the mode is set to Advanced Configuration, the services list becomes a link that launches an Edit window where you can select or deselect the services provided by the interface. This granularity is useful for ExtremeControl deployments in MSP or MSSP environments.



NOTE: Only one interface can have **End-System** enabled when using the OAUTH2 social login. The End-System service is part of the Management, Registration, and Remediation mode, so it can also be enabled in Advanced Configuration.

The following list describes the various services that are provided by the different modes:

- **Management** - The communication to and from the ExtremeCloud IQ Site Engine server. Sub-services include JMS, Web Services, and Syslog.
  NOTE: The Management service cannot be moved from eth0.
- **Monitoring Services** - The services used to monitor or contact an engine. Sub-services include the SSH daemon and SNMP agent.
- **Network Services** - The communication to external servers that provide networking services. Sub-services include DNS servers and NTP servers.
  NOTE: The Network Services service can only be applied to one interface.
- **AAA Servers** - The communication used by external servers for authentication and authorization. Sub-services include RADIUS servers and LDAP servers.
  NOTE: The AAA Servers service can only be applied to one interface.
- **Device** - The communication to and from a NAS (switch, router, VPN, or wireless controller). Sub-services include SNMP, RADIUS, RFC3576, SSH/Telnet, and TFTP.
- **Portal: Management** - the captive portal registration management services for an engine.
- **End-System** - The communication to and from end-systems. Sub-services include portal registration and remediation, assessment, NetBIOS, and DNS proxy.
- **Traffic Snooping** - DHCP and Kerberos snooping on the interface. This service is listed if the DHCP/Kerberos Snooping option is set to Enabled.

DHCP/Kerberos Snooping

Use the DHCP/Kerberos Snooping option to enable or disable DHCP and Kerberos snooping on the interface. DHCP snooping is used for IP resolution and OS detection. Kerberos snooping is used for user name detection and elevated access.

Captive Portal HTTP Mirroring

This is an advanced option that enables the interface to accept mirrored HTTP traffic which is used to display the captive portal to end users. This option is an alternative to using Policy-Based Routing and DNS Proxy.

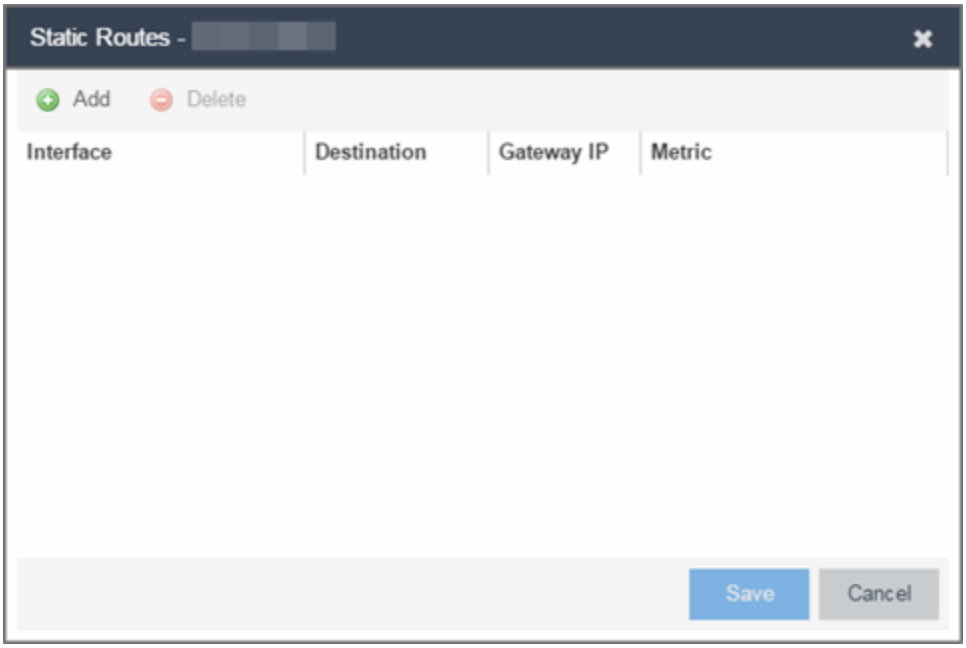
Tagged VLANs

If the mirrored traffic includes an 802.1Q VLAN tag, then the list of VLANs to capture must be explicitly stated in this field by entering a comma-separated list of VLAN IDs from 1 to 4094. If the mirrored traffic is not tagged then this field can be left blank.

Static Route Configuration Window

This window displays the static routes used for advanced routing configuration. Use the toolbar buttons to add, edit, or delete a route.

This window is accessed from the **Control** > **Access Control** tab by selecting an Access Control engine, opening the **Details** tab, and selecting the **Static Routes** button in the Interface Summary section.



Interface
The ExtremeControl engine interface used for the static route.

Destination
The IP address used to define the subnet or individual device whose traffic is assigned to the route.

Gateway IP
The IP address of the device where traffic matching the Network value is sent.

Metric
A number used to configure route precedence. The lower the number, the higher the precedence.

How To Use Access Control

The **How To** section contains Help topics that give you instructions for performing tasks in the **Access Control** tab.

How to Use Device Type Profiling

This Help topic describes how to set up device type profiling in your ExtremeControl Configuration using device type rule groups. Device type profiling lets you assign Access Control profiles to end-systems based on operating system family, operating system, or hardware type. This allows you to use the end-system's device type to determine the end user's level of network access control and whether the end-system is scanned. For more information on device type groups, see the Add/Edit Device Type Group Window Help topic.

NOTE: Assessment provides the most accurate determination of device type. If the initial device type determination is not based on assessment results, it can be less reliable. For that reason, device type rule groups should be based on broad families of device types.

Here are some examples of how device type profiling can be used to determine network access:

- When an end user with valid credentials logs in to the network on a registered iPad versus a registered Windows 10 machine, they receive a lower level of network access.
- When an end user registers a Windows machine using its MAC address, another user cannot spoof that MAC address using a Linux system. (Device profiling does not resolve this issue in environments with dual boot machines.)
- If an end user exports a certificate from a corporate PC to an iPad and successfully authenticates with 802.1x, the iPad is not allowed full network access.

Device Profiling Use Case

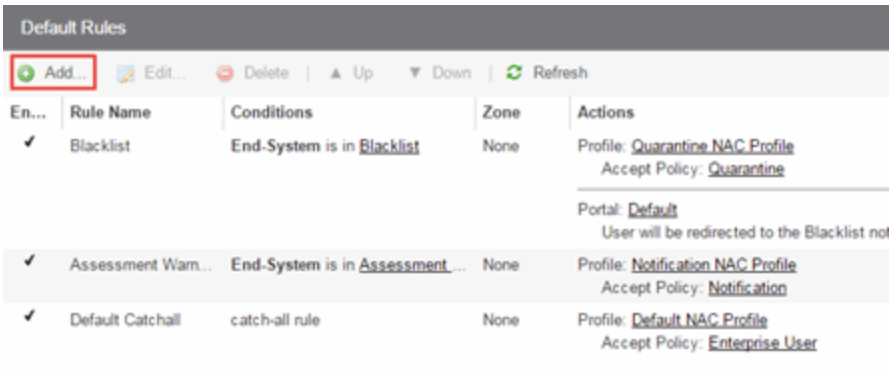
This section provides high-level instructions for configuring device type profiling for a sample use case. In this scenario, the network administrator has the following network access requirements:

- All Windows registered devices should be assigned the "Default Access Control Profile."
- All Windows 10 registered devices should be assigned the "Windows10 Profile."
- All Linux registered devices should be assigned the "Default Access Control Profile." In addition, a new Linux version called SuperLinux needs to be added to the Linux family device type.
- All HP Printers should be assigned the "HP Printer Profile."

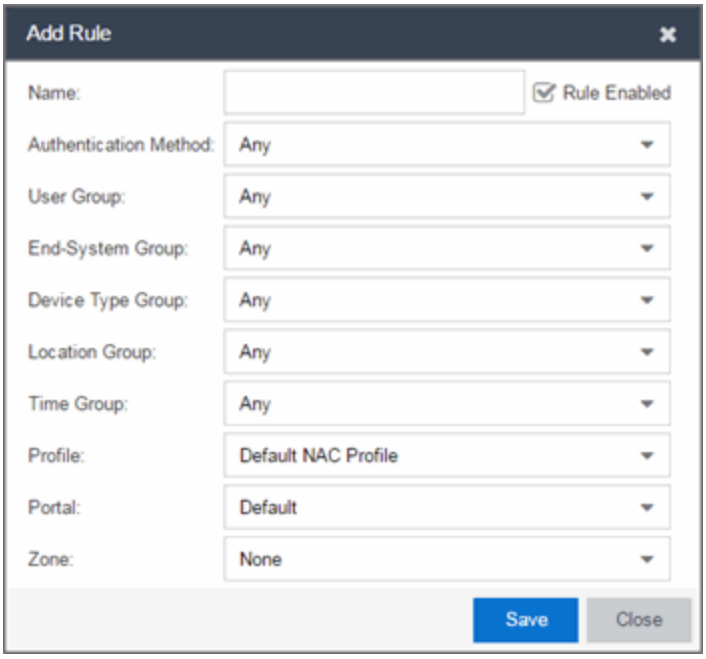
To do this, create four rules in your Access Control configuration that use device type as criteria for matching rules to end-systems authenticating to the network. The following instructions assume that you already created your profiles: Basic Profile, Windows10 Profile, and HP Printer Profile.

1. Expand the Default left-panel tree (Control > ExtremeControl> Access Control Configurations > Default).

2. Select the Rules left-panel option and select the **Add** button in the right panel.

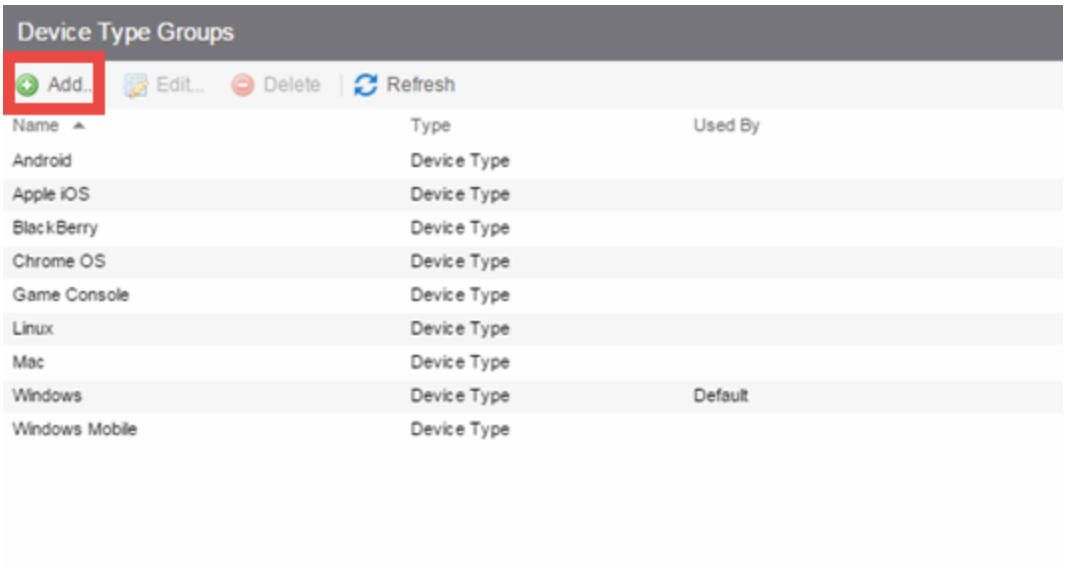


3. Create a rule that assigns the Default Access Control Profile to all Registered Guests using Windows devices as shown below.

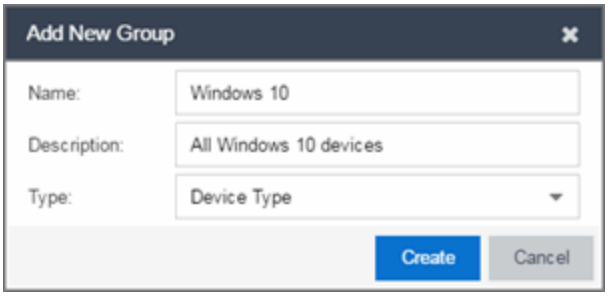


4. Create a rule that assigns the Windows10 Profile to all Windows 10 registered devices. To do this, you need to create a new Windows 10 device type group.
    a. From the Access Control Configurations left-panel tree, expand the Group Editor tree.

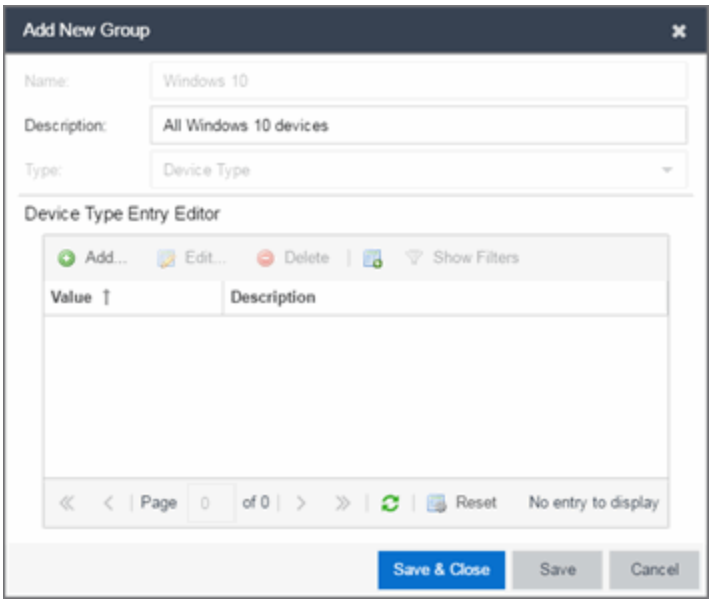
b. Select Device Type Groups and select the **Add** button in the right panel.



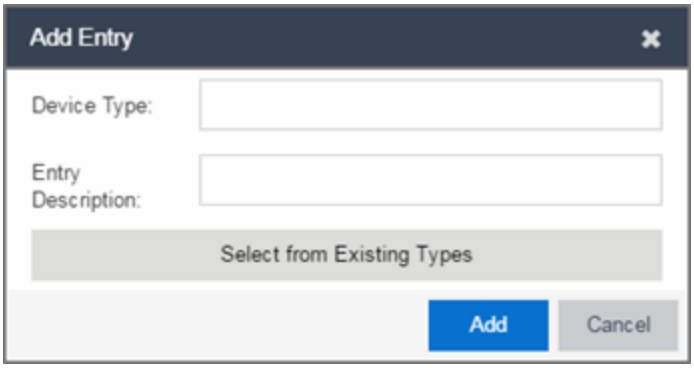
c. Create a new device type group with the name Windows 10.



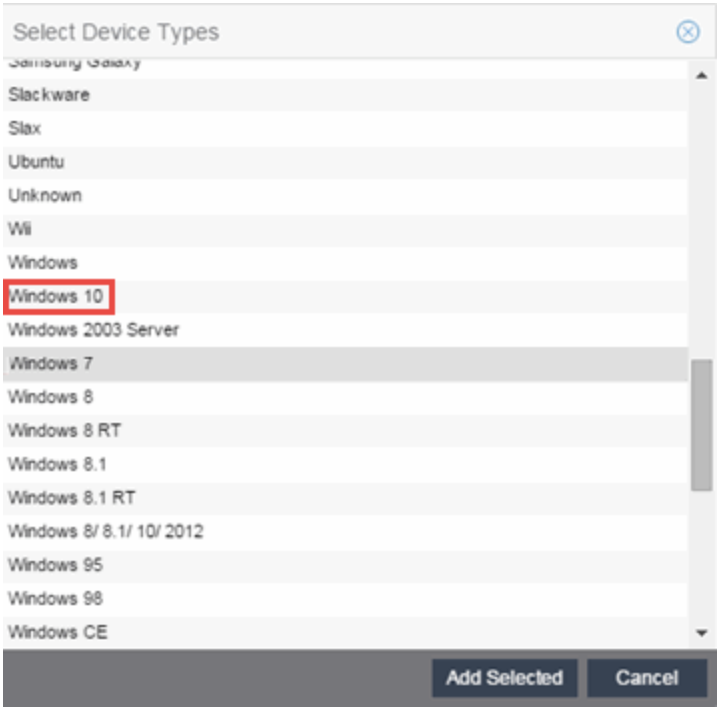
d. Select **Create**. The Device Type Entry Editor displays.



e. Select the **Add** button. The Add Entry window displays.



f. Select the **Select from Existing Types** button and in the Select Device Types window, select Windows 10.



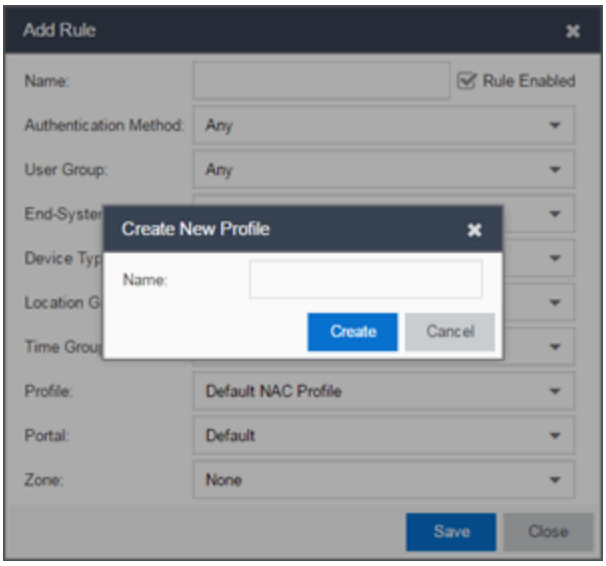
g. Select the **Add Selected** button.

h. Select the **Save & Close** button on the Add New Group window.

i. You can then create the rule.

j. Select the Access Control Configurations > Default > Rules left-panel option and select the **Add** button in the right panel.

k. In the Profile drop-down list, select **New**. The Create New Profile window displays.

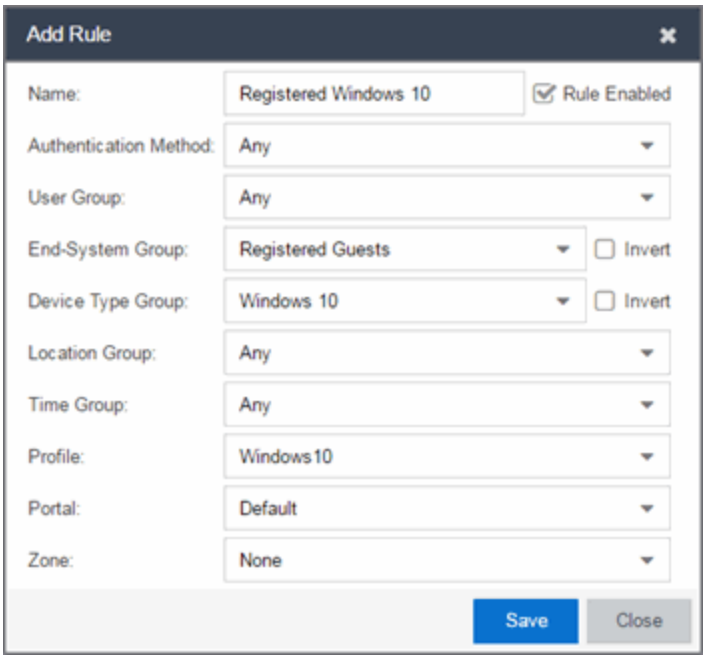


l. Enter the name **Windows10** in the **Name** field and select the **Create** button.

The Access Control Profile window opens.

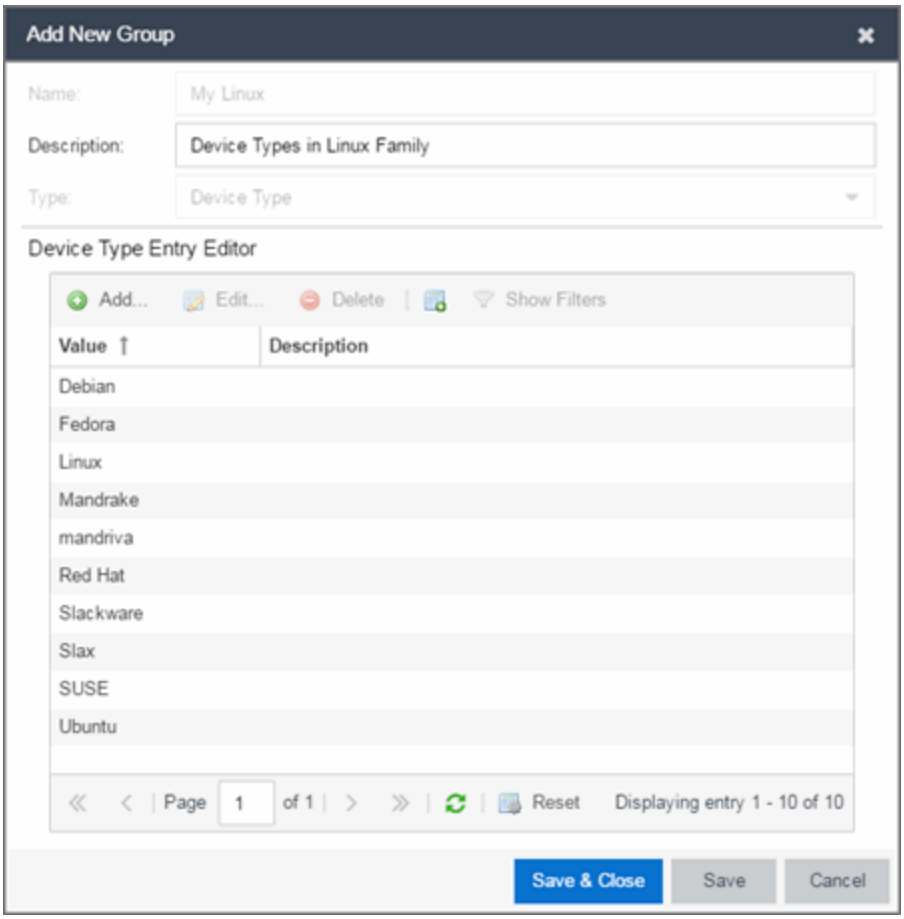
m. Select **Save**.

n. Configure the rule as shown in the screenshot below.

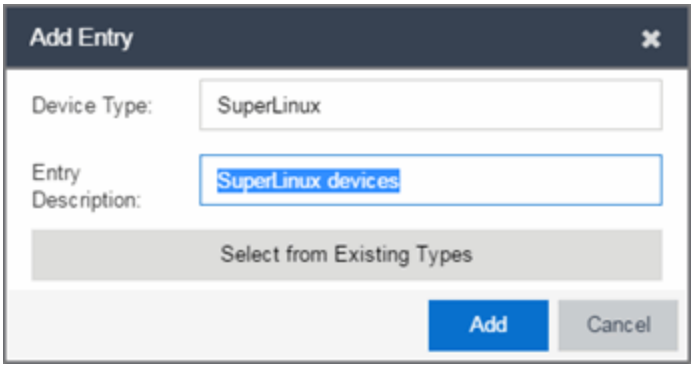


o. Select **Save**.

5. Create a rule that assigns the Default Access Control Profile to all Linux registered devices and add the SuperLinux version to the Linux family device type. To do this, you need to create a new Linux device type group that includes SuperLinux.
    a. Create the My Linux device type group to include the devices in the Linux device type group using the **Select from Existing Types** button in the Add Entry window as discussed in step 4f above.



    b. Select the **Add** button and in the Add Entry window, create the **SuperLinux** Device Type as shown below.

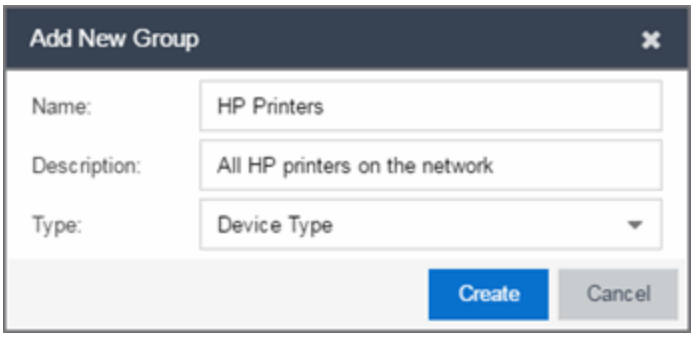


c. Select **Add** to save the SuperLinux device type to the My Linux device type group.

d. Select the **Save & Close** button on the Add New Group window.

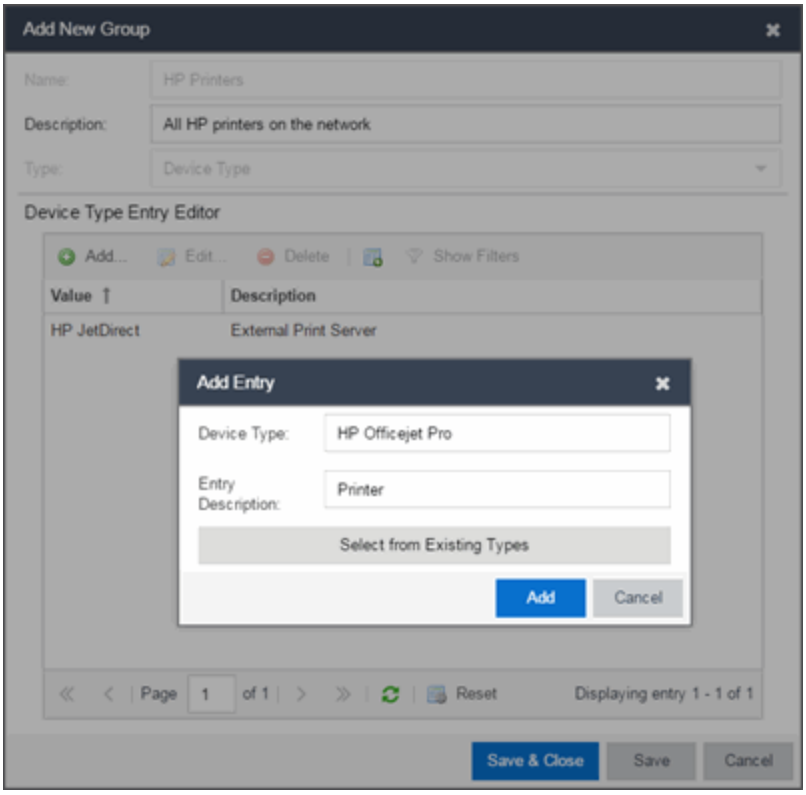
6. Create a rule that assigns the HP Printer Profile to all HP printers on the network. To do this, create a new HP Printers device type group.

   a. Open the Add New Group window by selecting the **Add** button on the Access Control Configurations > Group Editor > Device Type Groups panel.



   b. Select **Create**. The Device Type Entry Editor section displays.

   c. Add the HP Printers via the Add Entry window by selecting the **Add** button as shown below.



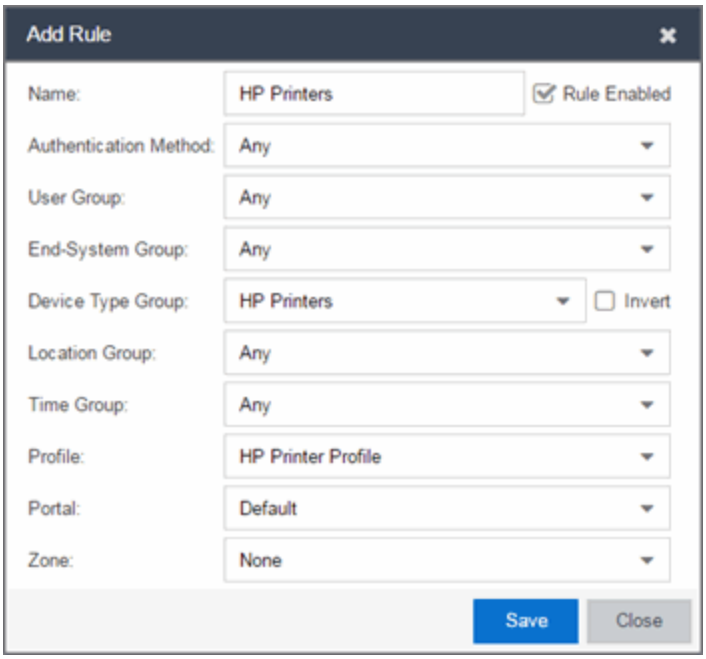
d. Select **Save & Close** to save the HP Printers group.

e. Select Rules in the left-panel tree (Access Control Configurations > Default > Rules).

f. Select **Add** in the right-panel to open the Add Rule window.

g. Select the New option in the Profile drop-down list and create the **HP Printer Profile**.

h. Create the HP Printers rule using the following criteria.



i. Select **Save**.

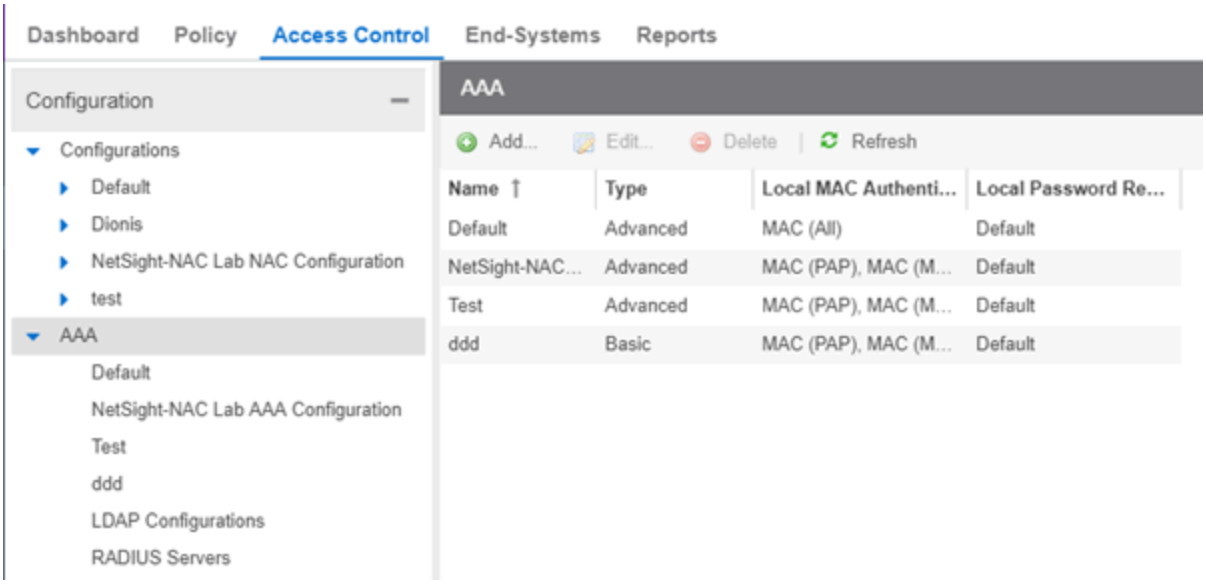
7. Your Access Control Configuration now contains the following rules used to determine network access and assessment requirements based on device type.

How to Configure LDAP for End Users and Hosts via Active Directory

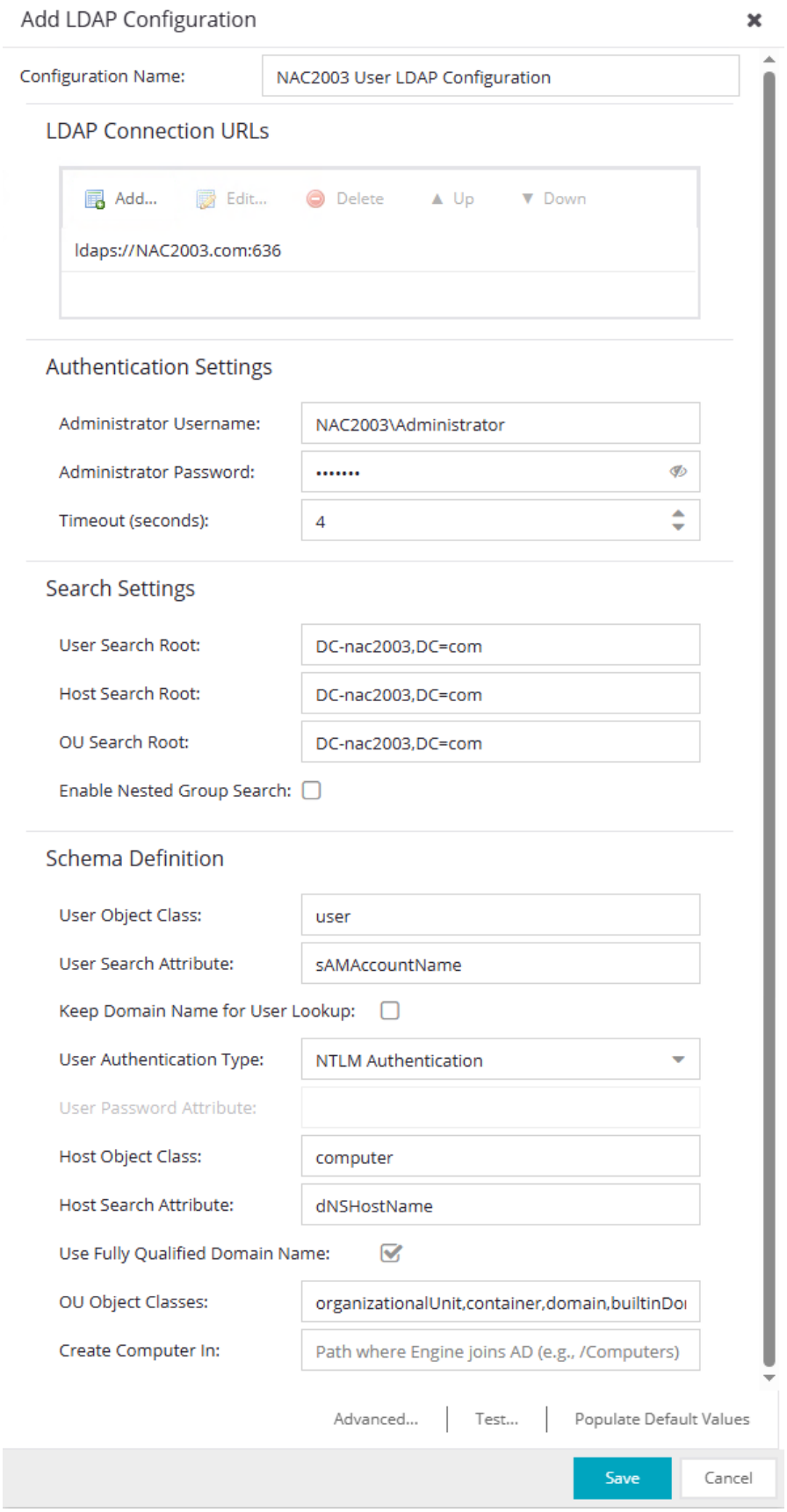
This Help topic provides instructions for creating LDAP configurations in Access Control that provide authentication and authorization for network end users and host machines via Active Directory.

In Access Control, you can create an Advanced AAA configuration that contains one mapping rule for your host machines and two mapping rules for your users. These mappings are the same except for their LDAP configuration. You need to create two LDAP configurations: one for the hosts mapping and one for the users mapping. The LDAP configurations are identical except for the User Search Attribute. When you have completed these instructions, Access Control uses the new AAA configuration to authenticate both end users and host machines via your Active Directory server.

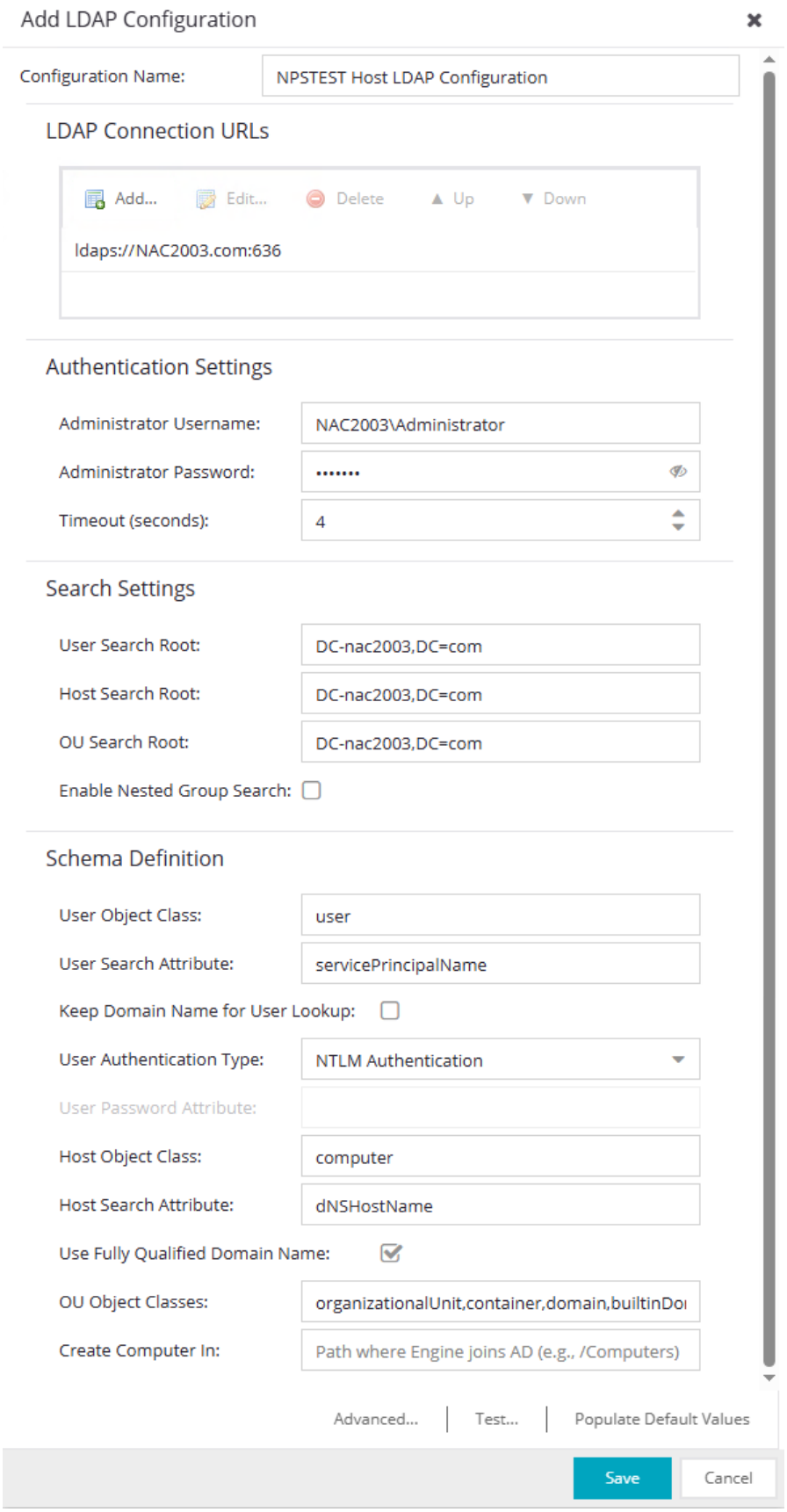
1. Select **Control > Access Control** > **Configuration** tab.
2. In the left-panel tree, select the **AAA** tab to open the AAA Configuration window to the right.



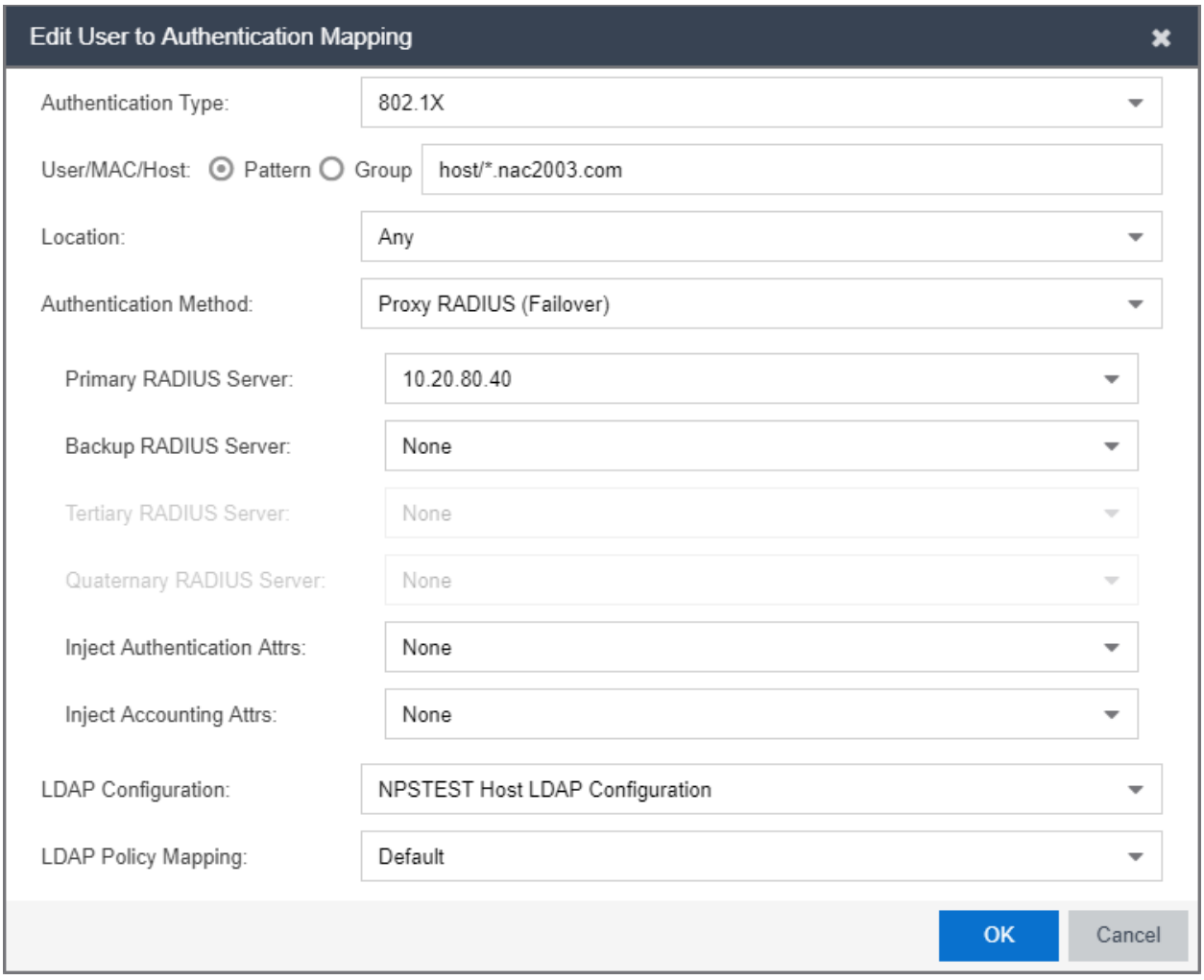
3. Select the **Add** button in the AAA Configuration panel create a new AAA Configuration.
4. Select LDAP Configuration in the left-panel tree to open the LDAP Configuration window.
5. Create an LDAP configuration for use with end users that authenticate to the network using the sample below as a guide. Select **Save**.


Add LDAP Configuration
Configuration Name:
NAC2003 User LDAP Configuration
LDAP Connection URLs
Add...
Edit...
Delete
Up
Down
ldaps://NAC2003.com:636
Authentication Settings
Administrator Username:
NAC2003\Administrator
Administrator Password:
Timeout (seconds):
4
Search Settings
User Search Root:
DC-nac2003,DC=com
Host Search Root:
DC-nac2003,DC=com
OU Search Root:
DC-nac2003,DC=com
Enable Nested Group Search:
Schema Definition
User Object Class:
user
User Search Attribute:
sAMAccountName
Keep Domain Name for User Lookup:
User Authentication Type:
NTLM Authentication
User Password Attribute:
Host Object Class:
computer
Host Search Attribute:
dNSHostName
Use Fully Qualified Domain Name:
OU Object Classes:
organizationalUnit,container,domain,builtinDo
Create Computer In:
Path where Engine joins AD (e.g., /Computers)
Advanced...
Test...
Populate Default Values
Save
Cancel

6. Open the Add LDAP Configuration window to add another LDAP configuration that will be used for host machines that authenticate to the network using the sample below as a guide. Note that the only difference between the two LDAP configurations is the User Search Attribute. Select **Save**.

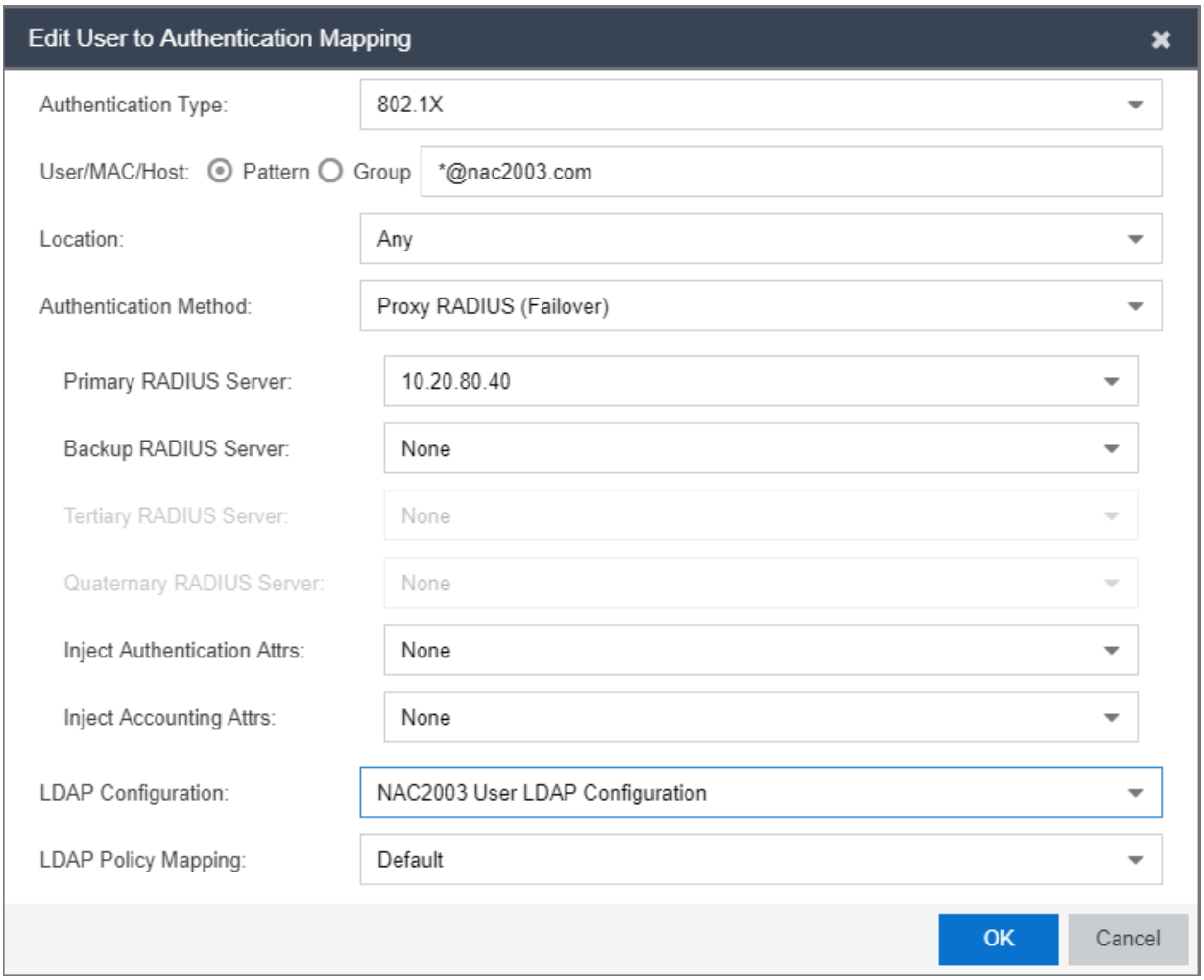

Add LDAP Configuration
Configuration Name:
NPSTEST Host LDAP Configuration
LDAP Connection URLs
Add...
Edit...
Delete
Up
Down
ldaps://NAC2003.com:636
Authentication Settings
Administrator Username:
NAC2003\Administrator
Administrator Password:
Timeout (seconds):
4
Search Settings
User Search Root:
DC-nac2003,DC=com
Host Search Root:
DC-nac2003,DC=com
OU Search Root:
DC-nac2003,DC=com
Enable Nested Group Search:
Schema Definition
User Object Class:
user
User Search Attribute:
servicePrincipalName
Keep Domain Name for User Lookup:
User Authentication Type:
NTLM Authentication
User Password Attribute:
Host Object Class:
computer
Host Search Attribute:
dNSHostName
Use Fully Qualified Domain Name:
OU Object Classes:
organizationalUnit,container,domain,builtinDo
Create Computer In:
Path where Engine joins AD (e.g., /Computers)
Advanced...
Test...
Populate Default Values
Save
Cancel

7. In the left-panel tree, select an AAA Configuration to open the Advanced AAA Configuration window.
8. In the Authentication Rules panel of the Advanced AAA Configuration window, select the **Add** button to open the Add User to Authentication Mapping window.
9. Create your first mapping rule to capture machine authentications using the sample below as a guide. In the example below, **host/*.nac2003.com** captures the machine authentications for the NAC2003 active directory domain. Be sure to select the host LDAP Configuration you create. Select **OK**.

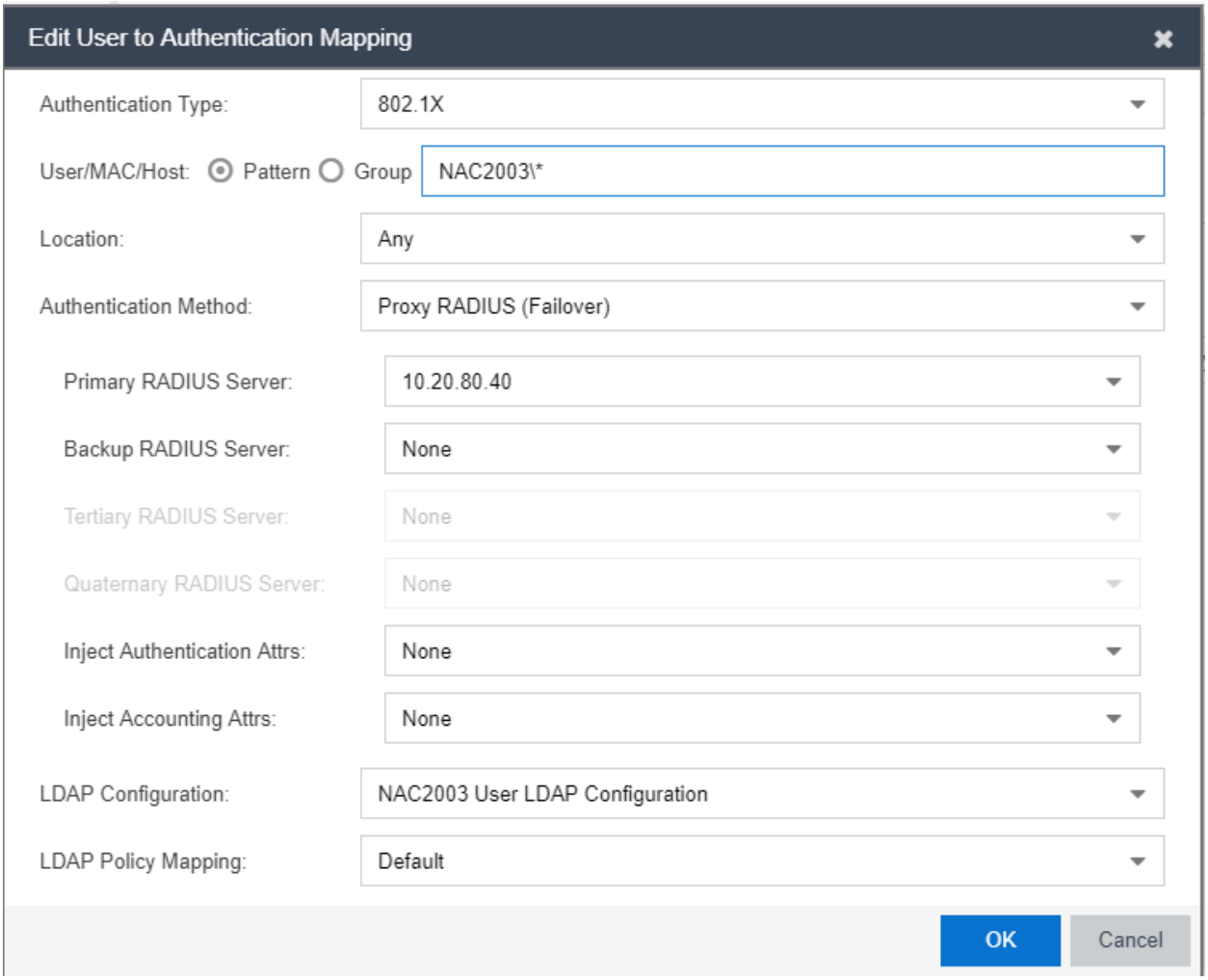


10. Create your second mapping rule to capture end user authentications using the sample below as a guide. In the example below, ***@nac2003.com** captures all users logging in to the NAC2003 active directory domain when they authenticate with their username in the format <username>@<domain>. Be sure to select the end user LDAP Configuration you create. Select

OK.



11. Create your third mapping rule to capture other end user authentications using the sample below as a guide. In the example below, **NAC2003*** captures all users logging in to the NAC2003 active directory domain when they authenticate with their username in the format <domain>\<username>. Be sure to select the end user LDAP Configuration you create. Select **OK**.



12. In the left-panel tree, select an AAA Configuration to open the Advanced AAA Configuration window. Use the **Up** and **Down** buttons to move your new mappings above the "Any" mappings in the list of mappings. Select **Save**.

You can configure your LDAP policy mappings and/or LDAP user groups based on the attributes from either your host or user LDAP configurations.

How to Change the Assessment Agent Adapter Password

This Help topic provides instructions for changing the password on the assessment agent adapter on your network assessment servers, including agent-less, Nessus, or a third-party assessment agent (an assessment agent not supplied or supported by ExtremeCloud IQ Site Engine). The assessment agent adapter enables communication between the ExtremeControl engine and the assessment servers, and the password is used by the assessment agent adapter to authenticate Access Control engine assessment requests.

This password must match the password specified in the Access Control Options as the Assessment Agent Adapter Credentials (Administration > Options > Identity and Access > Assessment Server). If you change the password on the assessment agent adapter, change assessment agent adapter credentials in the Access Control options as well, or connection between the engine and assessment servers is lost and assessments is not performed.

To change the assessment agent adapter password:

1. Go to the install directory for the assessment agent adapter on the assessment server. This can be a Nessus server or the Access Control engine if you are using on-board agent-less assessment. On an Access Control engine, the install directory is **/opt/nac/saint**.
2. Run the **sha1.sh** script (on an Access Control engine, the script is located in located in **/opt/nac/saint/util**) using the new password as the argument. The script produces a hash string that looks something like:
   9ba2db465ff11b0bdfd188f7ee87b10fc3a145dc
3. Open the **users.properties** file (on an Access Control engine, the file is located in **/opt/nac/saint/users.properties**) and replace the existing hash string with the new one:
   `admin=<new string>`
4. Restart the assessment agent adapter. On an Access Control engine, the command is `aglsctl restart`.

How to Set ExtremeControl Options

Use the Options window (**Administration > Options**) to set options for ExtremeControl. In the Options window, the right-panel view changes depending on what you have selected in the left-panel tree. Expand the Access Control folder in the tree to view all the different options you can set.

Instructions on setting the following Access Control options:

- Advanced Settings
- Assessment Server
- Data Persistence
- End-System Event Cache
- Enforce Warning Settings
- Features
- Notification Engine
- Policy Defaults
- Status Polling and Timeout

Advanced Settings

Use the Advanced Settings panel to configure advanced settings for Access Control. These settings apply to all users on all clients.

1. Select **Administration > Options** in ExtremeCloud IQ Site Engine. The Options window opens.
2. In the left-panel tree, expand the Access Control folder and select Advanced Settings.
3. Use the **Resource Allocation Capacity** option configure the ExtremeCloud IQ Site Engine resources allocated to end-system and configuration processing services. The greater the number of end-systems and engines in your Access Control deployment, the more resources it requires.
    - Low - For low performance shared systems.
    - Low-Medium - For medium performance shared systems, or low performance dedicated systems
    - Medium - For medium performance shared systems, or medium performance dedicated systems.
    - Medium-High - For high performance shared systems, or medium performance dedicated systems.

- High - For high performance dedicated systems.
- Maximum - For extremely high performance dedicated systems.

4. Use the **Hybrid Mode** option to enable Hybrid Mode for Layer 2 Controllers. Hybrid Mode enables a Layer 2 Access Control Controller engine to act as a RADIUS proxy for switches, like an Access Control engine. Select this option to enable Hybrid Mode for your Layer 2 Controllers at a global level. When the option is selected, the **Configuration** tab for a Layer 2 Controller displays an option to enable Hybrid Mode for that specific controller. Disabling Hybrid Mode at the global level when a controller has switches has a similar effect to deleting an engine: the switches have the controller removed as a reference.
5. Select **Save** or select the **Autosave** checkbox.

Assessment Server

Use the Assessment Server view to provide assessment agent adapter credentials. The options apply to all users on all clients.

The assessment agent adapter credentials are used by the ExtremeControl engine when attempting to connect to network assessment servers, including Extreme Networks Agent-less, Nessus, or a third-party assessment server (an assessment server that is not supplied or supported by ExtremeCloud IQ Site Engine). The password is used by the assessment agent adapter (installed on the assessment server) to authenticate assessment server requests. Access Control provides a default password you can change, if desired. However, if you change the password here, you need to change the password on the assessment agent adapter as well, or connection between the engine and assessment agent adapter is lost and assessments are not performed. For instructions, see How to Change the Assessment Agent Adapter Password.

1. Select **Administration > Options**. The Options window opens.
2. In the left-panel tree, expand the Access Control folder and select Assessment Server.
3. Specify the assessment agent adapter credentials.
4. Select **Save** or select the **Autosave** checkbox.

Data Persistence

Use the Data Persistence view to customize how ExtremeCloud IQ Site Engine ages-out or deletes end-systems, end-system events, and end-system health results (assessment results) from the tables and charts in the End-Systems tab. These settings apply to all users on all clients.

1. Select **Administration > Options**. The Options window opens.
2. In the left-panel tree, expand the ExtremeControl folder and select Data Persistence.
3. In the **Age End-Systems** section, enter the number of days the Data Persistence Check uses as criteria for aging end-systems. Each day, when the Data Persistence check runs, it searches

the database for end-systems ExtremeCloud IQ Site Engine has not received an event for in the number of days specified (90 days by default). It removes those end-systems from the tables in the End-Systems tab.

4. If you select the **Remove Associated MAC Locks and Occurrences in Groups** checkbox, the aging check also removes any MAC locks or group memberships associated with the end-systems being removed. The **Remove Associated Registration Data** checkbox is selected by default, so the aging check also removes any registration data associated with the end-systems being removed.
5. In the **End-System Event Persistence** section, select the checkbox if you want ExtremeCloud IQ Site Engine to store non-critical end-system events, which are events caused by an end-system reauthenticating. End-system events are stored in the database. Each day, when the Data Persistence check runs, it removes end-system events which are older than the number of days specified (90 days by default).
6. In the **End-System Information Event** section, select the checkbox if you want ExtremeCloud IQ Site Engine to generate an Access Control event when end-system information is modified.
7. In the **Health Result Persistence** section, specify how many health result (assessment results) summaries and details are saved and displayed in the End-Systems tab for each end-system. By default, the Data Persistence check saves the last 30 health result summaries for each end-system along with detailed information for the last five health result summaries per end-system.
   There are two additional options:
   - You can specify to only save the health result details for quarantined end-systems (with the exception of agent-based health result details, which are always saved for all end-systems).
   - You can specify to save duplicate health result summaries and detail. By default, duplicate health results obtained during a single scan interval are **not** saved. For example, if the assessment interval is one week, and an end-system is scanned five times during the week with identical assessment results each time, the duplicate health results are not saved (with the exception of administrative scan requests such as Force Reauth and Scan, which are always saved). This reduces the number of health results saved to the database. If you select this option, all duplicate results are saved.
8. Set the time you would like the Data Persistence Check to be performed each day.
9. In the **Transient End-Systems** section, configure the number of days to keep transient end-systems in the database before they are deleted as part of the nightly database cleanup task. The default value is 1 day. A value of 0 disables the deletion of transient end-systems. Transient end-systems are Unregistered end-systems and have not been seen for the specified number of days. End-systems are not deleted if they are part of an End-System group or there are MAC locks associated with them. Select the **Delete Rejected End-Systems** checkbox if you want end-systems in the Rejected state to be deleted as part of the

cleanup. You can also delete transient end-systems using the Tools > End-System Operations > Data Persistence option.

10. Select **Save** or select the **Autosave** checkbox.

End-System Event Cache

End-system events are stored daily in the database. In addition, the end-system event cache stores in memory the most recent end-system events and displays them in the End-System Events tab. This cache enables ExtremeCloud IQ Site Engine to quickly retrieve and display end-system events without having to search through the database. Use the End-System Event Cache view to configure the amount of resources used by the end-system event cache. This setting applies to all users on all clients.

1. Select **Administration > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the ExtremeControl folder and select End-System Event Cache.
3. Specify the parameters to use when searching for older events outside of the cache. (The search is initiated by using the **Search for Older Events** button in the End-System Events tab.) The search is ended when any one of the parameters is reached.
    - Maximum number of days to go back when searching
    - Maximum number of results to return from search
    - Maximum time to spend searching for events
4. Specify the number of events to cache. Keep in mind the more events you cache, the faster data is returned, but caching uses more memory.
5. The End-System Event Cache also keeps a secondary cache of events by MAC address. This means a particular end-system's events can be more quickly accessed in subsequent requests. Specify the number of MAC addresses kept in the secondary cache. Keep in mind that the more MAC addresses you cache, the more memory used. Also, note the secondary cache can include events not in the main cache, but were retrieved by scanning the database outside the cache boundary.
6. Select **Save** or select the **Autosave** checkbox.

Enforce Warning Settings

Use the Enforce Warning Settings view to specify warning messages you don't want displayed during the Enforce engine audit.

When an engine configuration audit is performed during an Enforce operation, warning messages can display in the audit results listed in the Enforce window. If an engine has a warning associated with it, you are given the option to acknowledge the warning and proceed with the enforce anyway.

These settings enable you to select specific warning messages that you do not want to have displayed in the audit results. This enables you to proceed with the Enforce without having to acknowledge the

warning message. For example, you can have an ExtremeControl configuration that always results in one of these warning messages. By selecting that warning here, it is ignored in future audit results and you no longer have to acknowledge it before proceeding with the Enforce.

1. Select **Administration > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the ExtremeControl folder and select Enforce Warnings. The Enforce Warnings view opens.
3. Select the checkbox in the Ignore column next to the warning messages you don't want displayed.
4. Select **Save** or select the **Autosave** checkbox.

Setting Features Options

Use the Features view to automatically create new Policy mappings and profiles. If you are not using these features, you can disable them to remove sections that pertain only to those features from certain ExtremeCloud IQ Site Engine windows.

Notification Engine Options

Use the Notification Engine view to define the default content contained in ExtremeControl notification action messages. For example, with an email notification action, you can define the information contained in the email subject line and body. With a syslog or trap notification action, you can specify certain information you want contained in the syslog or trap message. These settings apply to all users.

There are certain "keywords" that you can use in your email, syslog, and trap messages to provide specific information. Following is a list of the most common keywords used. For a complete list of available keywords for ExtremeControl notifications, see the Keywords Help topic.

- $type - the notification type.
- $trigger - the notification trigger.
- $conditions - a list of the conditions specified in the notification action.
- $ipaddress - the IP address of the end-system that is the source of the event.
- $macaddress - the MAC address of the end-system that is the source of the event.
- $switchIP - the IP address of the switch where the end-system connected.
- $switchPort - the port number on the switch where the end-system connected.
- $username - the username provided by the end user upon connection to the network.

1. Select **Administration > Options**. The Options window opens.
2. In the left-panel tree, expand the ExtremeControl folder and select Notification Engine. The Notification Engine view opens.

3. Use the fields to define the default content contained in notification action messages. For a definition of each field, see the Notification Engine view Help topic.
4. In the Advanced section, set parameters for the Action and Event queues processed by the Notification engine.
5. Select **Save** or select the **Autosave** checkbox.

Policy Defaults

Use the Policy Defaults view to specify a default policy role for each of the four access policies. These default policy roles display as the first selection in the drop-down lists when you create an ExtremeControl profile. For example, if you specify an Assessment policy called "New Assessment" as the Policy Default, then "New Assessment" automatically displays as the first selection in the Assessment Policy drop-down list in the New ExtremeControl Profile window.

ExtremeCloud IQ Site Engine supplies seven policy role names from which you can select. You can add more policies in the Edit Policy Mapping window, where you can also define policy to VLAN associations for RFC 3580-enabled switches. When a policy is added, it becomes available for selection in this view.

1. Select **Administration > Options**. The Options window opens.
2. In the left-panel tree, expand the ExtremeControl folder and select Policy Defaults.
3. Select the desired policies.
    - The **Accept policy** is applied to an end-system when an end-system has been authorized locally by the ExtremeControl Engine and has passed an assessment (if an assessment was required), or the "Replace RADIUS Attributes with Accept Policy" option is used when authenticating the end-system.
    - The **Assessment policy** is applied to an end-system while it is being assessed (scanned).
    - The **Failsafe policy** is applied to an end-system when it is in an Error connection state. An Error state results if the end-system's IP address could not be determined from its MAC address, or if there was a scanning error and an assessment of the end-system could not take place.
    - The **Quarantine policy** is applied to an end-system if the end-system fails an assessment.
4. Select **Save** or select the **Autosave** checkbox.

Status Polling and Timeout

Use the Status Polling and Timeout view to specify polling and timeout options for ExtremeControl engines. These settings apply to all users on all clients.

1. Select **Administration > Options**. The Options window opens.
2. In the left-panel tree, expand the ExtremeControl folder and select Status Polling and Timeout.
3. In the **ExtremeControl Appliance Enforce Timeout** section, specify the amount of time ExtremeCloud IQ Site Engine waits for an enforce response from the engine before determining the ExtremeControl engine is not responding. During an enforce, an ExtremeControl engine responds every second to report that the enforce operation is either in-progress or complete. Typically, you do not need to increase this timeout value, unless you are experiencing network delays that require a longer timeout value.
4. In the **ExtremeControl Inactivity Check** section, you can enable a check to verify end-system ExtremeControl activity is taking place on the network. If no end-system activity is detected, an ExtremeControl Inactivity event is sent to the ExtremeControl Events view. You can use the **Alarms and Events** tab to configure custom alarm criteria based on the ExtremeControl Inactivity event to create an alarm, if desired.
5. In the **Status Polling** section, select the **Length of Timeout**, which specifies the amount of time ExtremeCloud IQ Site Engine waits when communicating with ExtremeControl engines for status polling before determining contact failed. If ExtremeCloud IQ Site Engine does not receive a response from an engine in the defined amount of time, ExtremeCloud IQ Site Engine considers the engine to be "down" and the engine icon changes from a green up-arrow to a red down-arrow in the left-panel tree. The engine status refers to Messaging connectivity, not SNMP connectivity. This means that if the engine is "down," ExtremeCloud IQ Site Engine is not able to enforce a new configuration to it.
6. Specify the **Polling Interval**, which is the frequency ExtremeCloud IQ Site Engine polls the ExtremeControl engines to determine engine status.
7. Select **Save** or select the **Autosave** checkbox.

How to Set Up Registration

The Extreme Networks ExtremeControl Solution provides support for Registration which forces any new end-system connected on the network to provide the user's identity in a web page form before being permitted access to the network. Registration utilizes Registration Web Server functionality installed on an Access Control engine to enable end users to register their end-systems and automatically obtain network access without requiring the intervention of network operations. For more information on Registration and an overview of how it works, see the Registration section of the Concepts help file.

NOTE: For important information on web browser requirements for end-systems connecting through ExtremeCloud IQ Site Engine, refer to the Access Control Configuration Considerations Help topic.

This Help topic describes the specific steps that must be performed when deploying Registration on your network. The steps vary depending on whether you are using Access Control engines and/or Layer 2 Access Control Controller engines on your network. (Registration is not supported on the Layer 3 Access Control Controller engines.)

For Access Control engines you must:

- Identify the location in your network topology for the Access Control installation.
- Define the access policy for authorizing unregistered end-systems.
- Configure policy-based routing on your network.
- Configure Registration parameters in ExtremeCloud IQ Site Engine.

For Layer 2 Access Control Controller engines you must:

- Configure Registration parameters in ExtremeCloud IQ Site Engine.

The Registration Web Server is pre-installed on the Access Control engine. For instructions on installing and configuring a Access Control engine, refer to your engine Installation Guide.

NOTE: It is important to add a DNS entry from the Fully Qualified Domain Name (FQDN) of the Access Control engine (both Access Control Engines and Access Control Controllers) into the DNS servers deployed on the network so that the device running ExtremeCloud IQ Site Engine is able to resolve queries to these DNS servers. Otherwise, a short delay occurs in returning the Registration web page to end users on the network.

Information and instructions on:

- ExtremeControl Configuration
  - Identifying ExtremeControl Engines Location
  - Defining the Unregistered Access Policy
  - Configuring Policy-Based Routing
- Configuring ExtremeCloud IQ Site Engine (for ExtremeControl Engine and ExtremeControl Controller Engines)

ExtremeControl Configuration

Perform the following steps when you are deploying Registration in a network that utilizes ExtremeControl engines. These steps are not necessary if you are utilizing only Access Control Controller engines on your network.

Identifying Access Control Engines Location

Although several Access Control Engines can be deployed on the entire network depending on the number of connecting end-systems, only one Access Control Engine is required to serve as the Registration Web Server. The location of this Access Control Engine is important for the implementation of web redirection for unregistered end-systems on the network. The Access Control Engine serving as the Registration Web Server must be installed on a network segment directly connected to a router or routers that exist in the forwarding path of HTTP traffic from unregistered end-systems. This is because policy-based routing is configured on this router or routers to redirect the web traffic sourced from unregistered end-systems to this Access Control Engine. It is important to note that only the Access Control Engine that you wish to serve as the Registration Web Server needs to be positioned in such a manner. All other Access Control Engines can be positioned at any location on the network, with the only requirement being that access layer switches are able to communicate to the engines.

Typically, the Access Control Engine serving as the Registration Web Server is positioned on a network segment directly connected to the distribution layer routers on the enterprise network, so that any HTTP traffic sourced from unregistered end-systems that are connected to the network's access layer can be redirected to that Access Control Engine. As an alternative, the Access Control Engine can be positioned on a network segment directly connected to the router providing connectivity to the Internet or internal web server farm. In this scenario, the HTTP traffic sourced from unregistered end-systems would be redirected to the Access Control Engine before reaching the Internet or internal web servers.

Defining the Unregistered Access Policy

When you implement Registration, you assign the Unregistered Access Control Profile defined in ExtremeCloud IQ Site Engine (ExtremeCloud IQ Site Engine) as the Default Profile for all end-systems connected to the engine group. The Unregistered Access Control Profile specifies that end-systems

are **not** assessed for security posture compliance (at this time) and authorizes end-systems on the network with the "Unregistered" access policy. With this configuration, end-systems are first forced to register to the network, and after successful registration, can be assessed for security posture compliance and subsequently quarantined or permitted network access.

Note that an end-system group can be configured to exempt certain devices from having to register to the network, based on authentication type, MAC address, or user name. For example, an end-system group for the MAC OUI of the printer vendor for the network can be configured to exempt printers from having to register for network access.

Creating the Unregistered Access Policy

The Unregistered access policy must permit unregistered end-systems access to ARP, DHCP, DNS, and HTTP; particularly HTTP communication to the Access Control Engine implementing the Registration Web Server functionality. For a network composed of EOS policy-enabled switches in the access layer, you must create the appropriate network access services and rules for the Unregistered *policy role* in ExtremeCloud IQ Site Engine's **Control** > **Policy** tab to meet these requirements, and enforce those changes to the policy-enabled switches. For a network composed of RFC 3580-enabled switches, you must ensure appropriate network services are enabled for the VLAN(s) associated to the Unregistered access policy.

For EOS policy-enabled Access Layer Switches

When configuring the Unregistered policy role (using ExtremeCloud IQ Site Engine's **Policy** tab) for EOS policy-enabled switches, there are two required configurations:

- A rule must be added that permits HTTP traffic (i.e. TCP destination port equaling 80) on the network.
- The rule must specify a class of service action that rewrites the ToS value of the HTTP traffic to a value of '*y*'. This value should match the decimal equivalent used in your policy-based routing that is used on the router.

If Assisted Remediation is already deployed with the Quarantine policy role appropriately configured for web redirection on EOS policy-enabled access layer switches, the simplest way to configure the Unregistered policy role in ExtremeCloud IQ Site Engine is to copy and paste the Quarantine policy role under the **Roles** tab in ExtremeCloud IQ Site Engine and rename this new policy role "Unregistered".

In addition, the **Policy** tab's Default Policy Domain includes an Unregistered role that is already configured with a service called Redirect Web Services, that includes an "Allow HTTP and Redirect" rule configured with the Access Control Web Redirect Class of Service.

Perform the following steps in ExtremeCloud IQ Site Engine to configure your Unregistered policy role.

NOTE: The ExtremeCloud IQ Site Engine Default Policy Domain includes an Access Control Web Redirect Class of Service you can use. Make sure that the ToS rewrite value is set to the appropriate value for your network. If you already created a Class of Service with ToS rewrite functionality for Assisted Remediation, you can use that same Class of Service for Registration and start with step number 3 below.

1. In ExtremeCloud IQ Site Engine, access the **Administration** > **Options** tab and select Policy Manager in the left-panel.
2. In the Default Class of Service Mode section, select **Role-Based Rate Limits/Transmit Queue Configuration** to enable the Role-based Class of Service mode on your network devices.
3. Create a new Class of Service that implements the ToS rewrite functionality:
    a. Open the Class of Service left-panel (**Control** > **Policy** tab > Class of Service).
    b. Right-click the Class of Service navigation tree and select Create CoS.
    The Create CoS window opens.
    c. Enter a name for the class of service (for example, "Web Redirection").
    d. Select **OK**.
    e. Select the **802.1p Priority** checkbox and use the drop-down list to select the **802.1p priority** to associate with the class of service.
    f. Select the **Edit** button next to the ToS field and enter a value (hex).
    g. The new Class of Service is automatically saved.
4. Create an "Allow HTTP" rule to a service currently included in your Unregistered policy role.
    a. Right-click a service in the Roles/Services left-panel and select **Create Rule**.
    b. Enter a name for the rule (for example, "Allow HTTP") and select **All Devices** in the **Rule Type(s)** drop-down list.
    c. Select **OK**.
    d. Select the new rule in the left-panel to display the rule details in the right panel.
    e. Enter a **Description** for the rule.
    f. Select **Enabled** in the **Rule Status** drop-down list.
    g. In the Traffic Description section, select the **Edit** button.

    The Edit Traffic Description window displays.
    h. Select **Layer 4 - Application Transport** in the **Traffic Classification Layer** drop-down list.
    i. Select **IP TCP Port Destination** in the **Traffic Classification Type** drop-down list.
    j. Select **HTTP (80)** in the **Well-Known Value** drop-down list.

k. Do not enter an IP address value.

l. Select **OK**.

m. In the Actions section, select **Permit Traffic** in the **Access Control** drop-down list.

n. Select CoS you created in step 2 ("Web Redirection") in the **Class of Service** drop-down list.

o. In the **Open/Manage Domain(s)** drop-down list at the top of the tab, select **Save Domain**.

5. Enforce these policy configurations to your network devices by selecting **Enforce Preview** in the **Enforce** drop-down list.

   The **Enforce Preview** window displays.

6. Verify the information you are enforcing is correct and select the **Enforce** button.

For RFC 3580-compliant Access Layer Switches

A VLAN must be identified to which unregistered end-systems will be assigned upon connecting to the network. You can make this the same VLAN assigned to end-systems when they are being assessed or quarantined. The VLAN must provision network services to an unregistered end-system that permit the end-system to open a web browser; specifically HTTP, DHCP, ARP, and DNS. Furthermore, it is required that IP connectivity between the end-system and the ExtremeControl Engine implementing the Registration Web Server functionality is operational.

The VLAN to which unregistered end-systems are assigned must be appropriately configured on all access layer switches where end-systems will be registering to the network. Access Control lists can be configured at the default gateway router's interface for the unregistered VLAN to restrict particular types of traffic sourced from end-systems within this VLAN to other areas of the network; withstanding the previously described provisioning requirements for this VLAN.

For Both EOS policy-enabled and RFC 3580-compliant Access Layer Switches

Now that you have defined the Unregistered policy role for EOS policy-enabled switches and/or the VLAN assigned to unregistered end-systems for RFC 3580-compliant switches, you must associate this policy role to the appropriate VLAN on the Access Control tab.

1. In ExtremeCloud IQ Site Engine, access the Control > **Access Control** tab.
2. Select the **Unregistered NAC Profile** entry in the Configuration > Profiles left-panel menu.
3. In the **Accept Policy** drop-down list, select **Manage Policy Mappings**.

   The **Manage Policy Mappings** window displays.

4. Select the **Unregistered** policy and select the **Edit** button.

   The **Edit Policy Mapping** window displays.

5. Select **Unregistered** in the **Policy Role** drop-down list.

6. Select the **Save** button.
7. Select **Close** to close the **Manage Policy Mappings** window.

Your Unregistered access policy is now configured to permit unregistered end-systems the ability to communicate to the ExtremeControl Engine serving as the Registration Web Server. In the next step, the authentication, authorization, and assessment of unregistered end-systems will be specified.

Configuring the Unregistered ExtremeControl Profile

Now that you have created the Unregistered access policy, you can customize the Unregistered ExtremeControl Profile. The Unregistered NAC Profile is defined by default in ExtremeCloud IQ Site Engine to specify that an unregistered end-system is **not** assessed for security posture compliance and that it is authorized on the network with the "Unregistered" policy. Therefore, unregistered end-systems are immediately assigned to the "Unregistered" policy when connected to EOS policy-capable access layer switches without being assessed. The authentication, assessment, and authorization settings of the Unregistered NAC profile can be changed as required by your organization. When you have configured the Unregistered NAC Profile, it can be selected as the default profile for an engine group (as described in a later section) where end-systems will be required to register to the network.

To change the Unregistered NAC Profile, use the following steps.

1. In ExtremeCloud IQ Site Engine, access the Control > **Access Control** tab.
2. Expand Configuration > Profiles in the left panel.
3. Select the Unregistered NAC Profile in the left panel.
4. Select the desired authentication, assessment, and configuration settings.
5. Select **Save**.

Configuring Policy-Based Routing

As described above, the ExtremeControl Engine serving as the Registration Web Server must be located on a network segment directly connected to a router or routers that exist in the transmission path of all traffic from any end-system that is not registered. This is because policy-based routing (PBR) must be configured on the routers to redirect the web traffic sourced from unregistered end-systems to that ExtremeControl Engine.

If EOS policy-enabled switches are deployed on the network, this is done by configuring policy-based routing to forward all HTTP traffic with a ToS field of '*y*' to the next-hop address of the Engine serving as the Registration Web Server. If RFC 3580-enabled switches are deployed on the network, this is done by configuring policy-based routing to forward all HTTP traffic with the source IP address on the subnet (s)/VLAN(s) associated to the Unregistered access policy, to the next-hop address of the Engine serving as the Registration Web Server.

In addition, if you are adding multiple ExtremeControl Engines for redundancy, the network needs to be configured for redundant policy-based routing as well.

For EOS policy-enabled Access Layer Switches

Let's consider an example where the Unregistered access policy is associated to a policy role on EOS policy-enabled switches that uses the "Allow HTTP" classification rule to assign HTTP traffic the "Web Redirection" class of service. This class of service rewrites the ToS field in the HTTP traffic to a value of 0x40 (or 64 base 10), equivalent to a DSCP value of 16. (The DSCP is the value defined in the six most significant bits of the 8-bit ToS field.) Furthermore, the Unregistered access policy is associated to VLANs 10, 20, and 30 on RFC 3580-enabled switches on the network which map to subnets 10.1.10.0/24, 10.1.20.0/24, and 10.1.30.0/24, respectively. The following steps describe how to configure policy-based routing on an N-Series router or Cisco IOS-based router when Registration is deployed for EOS policy-enabled access layer switches.

1. Configure an entry in the access-list 102 to identify HTTP traffic with a DSCP of 16.
   access-list 102 permit tcp any any eq 80 dscp 16
2. Use a route-map to configure the access-list 102 ACL to redirect HTTP traffic from end-systems to the next-hop IP address of the ExtremeControl Engine serving as the Registration Web Server, where "xxx.xxx.xxx.xxx" is the IP addresses of the Engine. Note that multiple next hop IP addresses can be specified in the route-map if multiple Engines are serving as Registration Web Servers.
   route-map 101
   match ip address 102
   set next-hop xxx.xxx.xxx.xxx
3. Apply the route map for the PBR configuration to the routed interface receiving the HTTP traffic from unregistered end-systems by entering the routed interface configuration prompt and executing the following command.
   ip policy route-map 101

For RFC 3580-compliant Access Layer Switches

Let's consider an example where the Unregistered access policy is associated to VLANs 10, 20, and 30 on RFC 3580-enabled switches on the network which map to subnets 10.1.10.0/24, 10.1.20.0/24, and 10.1.30.0/24, respectively. The following steps describe how to configure policy-based routing on an N-Series router or Cisco IOS-based router when Registration is deployed for RFC 3580-compliant access layer switches.

1. Configure an entry in the access-list 102 to identify HTTP traffic sourced from subnets 10.1.10.0/24, 10.1.20.0/24, and 10.1.30.0/24.
   access-list 102 permit tcp 10.1.10.0.0.0.0.255 any eq 80
   access-list 102 permit tcp 10.1.20.0.0.0.0.255 any eq 80
   access-list 102 permit tcp 10.1.30.0.0.0.0.255 any eq 80
2. Use a route-map to configure the access-list 102 ACL to redirect HTTP traffic from end-systems to the next-hop IP address of the ExtremeControl Engine serving as the Registration Web Server, where "xxx.xxx.xxx.xxx" is the IP addresses of the Engine. Note that multiple next hop IP addresses can be specified in the route-map if multiple Engines are serving as

Registration Web Servers.

```
route-map 101
match ip address 102
set next-hop xxx.xxx.xxx.xxx
```

3. Apply the route map for the PBR configuration to the routed interface receiving the HTTP traffic from unregistered end-systems by entering the routed interface configuration prompt and executing the following command.

```
ip policy route-map 101
```

Setting up Redundancy on ExtremeControl Engines

When adding multiple ExtremeControl Engines for redundancy, the network needs to be configured for redundant policy-based routing as well. This is performed on the router in which policy-based routing is configured. Use the same commands described in the previous two sections except for the two following changes:

- In step 2, in addition to the single IP address set as the next-hop IP address, enter a list of IP addresses of the redundant Engines. For example:

```
set next-hop xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx
```

- In step 3, when adding the ip policy route-map to the router interface, specify an additional command called "ip policy pinger on". This command attempts to ping the first IP address that is specified in the next-hop to determine its availability. If it is not available, the next IP in the list of next-hops will be pinged and then used, if it is available.
  For example:

```
ip policy route-map 101
ip policy pinger on
```

With policy-based routing and the Unregistered NAC Profile configured, Registration settings can be specified and then enabled on the network, as described in the next section.

Configuring the Access Control Tab (for ExtremeControl Engines and Controllers)

Perform the following steps when you are deploying Registration in a network that utilizes ExtremeControl engines and/or Layer 2 ExtremeControl Controllers. (Registration is not supported on Layer 3 Controller engines.)

Use the Configuration section of the Access Control tab left-panel menu to configure parameters for the Registration web pages served from the ExtremeControl engine. All ExtremeControl engines are initially assigned a default portal configuration. Use this tab to view and edit the default configuration or create new configurations. When you define your portal configuration, enforce the Access Control configuration to your engine(s).

Use the following steps to define your portal configuration and enforce it to the engine:

1. In ExtremeCloud IQ Site Engine, access the Control > **Access Control** tab.
2. In the left panel, expand the Configuration section and select Captive Portals.
3. Select an existing captive portal and select **Edit** or select **Add** to create a new portal.
4. Select the portal configuration settings for your network using the Network Settings, Administration, and Website Configuration tabs, available in the left panel:
    a. Network Settings — view network web page parameters. These parameters are shared by both the Remediation and the Registration web pages. Be aware that if you deploy both the assessment/remediation and registration features, any changes will affect the web pages for both features.
    b. Administration — configure settings for the registration administration web page and grant access to the page for administrators and sponsors.
    c. Website Configuration — configure Guest Settings, Authentication Settings, Survivable Registration, and Assessment/Remediation. Additionally, use this to configure the Look & Feel of the website.
5. When you have finished making your changes to the portal configuration, select **Save**.
6. Enforce the Access Control configuration to the engine group.
7. To exempt certain end-systems or end users from having to register to the network, you can configure end-system groups based on authentication type, MAC address, or user name. For example, an end-system group for the MAC OUI of the printer vendor for the network can be configured to exempt printers from having to register for network access.

Registration is now enabled for all end-systems connecting to this engine group, with the exception of those end-systems and end users that have been exempted based on group membership.

How to Configure Pre-Registration

This Help topic describes how to configure and use the ExtremeControl pre-registration feature as a part of Secure Guest Access or Authenticated Registration. With pre-registration, guest users can be registered in advance and given a username and password, allowing for a more streamlined and simple registration process when the guest user connects to the network. This can be particularly useful in scenarios where guest users are attending a company presentation, sales seminar, or a training session.

Pre-registration allows IT to delegate control of the network registration process to less technical personnel such as company receptionists, administrative assistants, or training personnel. Using the pre-registration web portal, selected personnel can easily register guest users in advance of an event, and print out a registration voucher that provides the guest user with their appropriate registration credentials. The guest user then follows the instructions on the voucher to connect to the corporate network.

This topic includes information and instructions on:

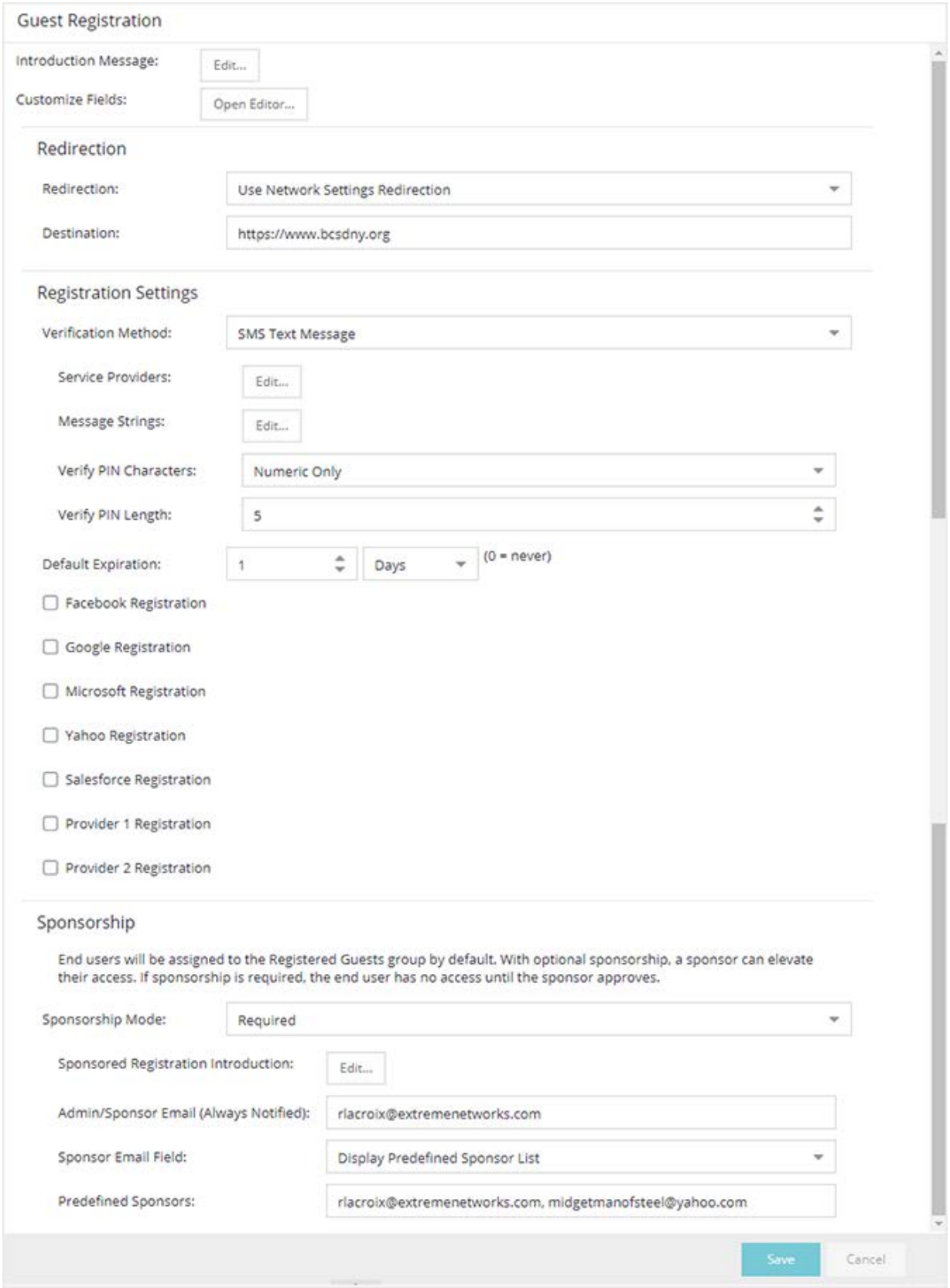
- Configuring Pre-Registration
- Pre-Registering Guest Users
    - Pre-Registering a Single User
    - Pre-Registering Multiple Usersv

Configuring Pre-Registration

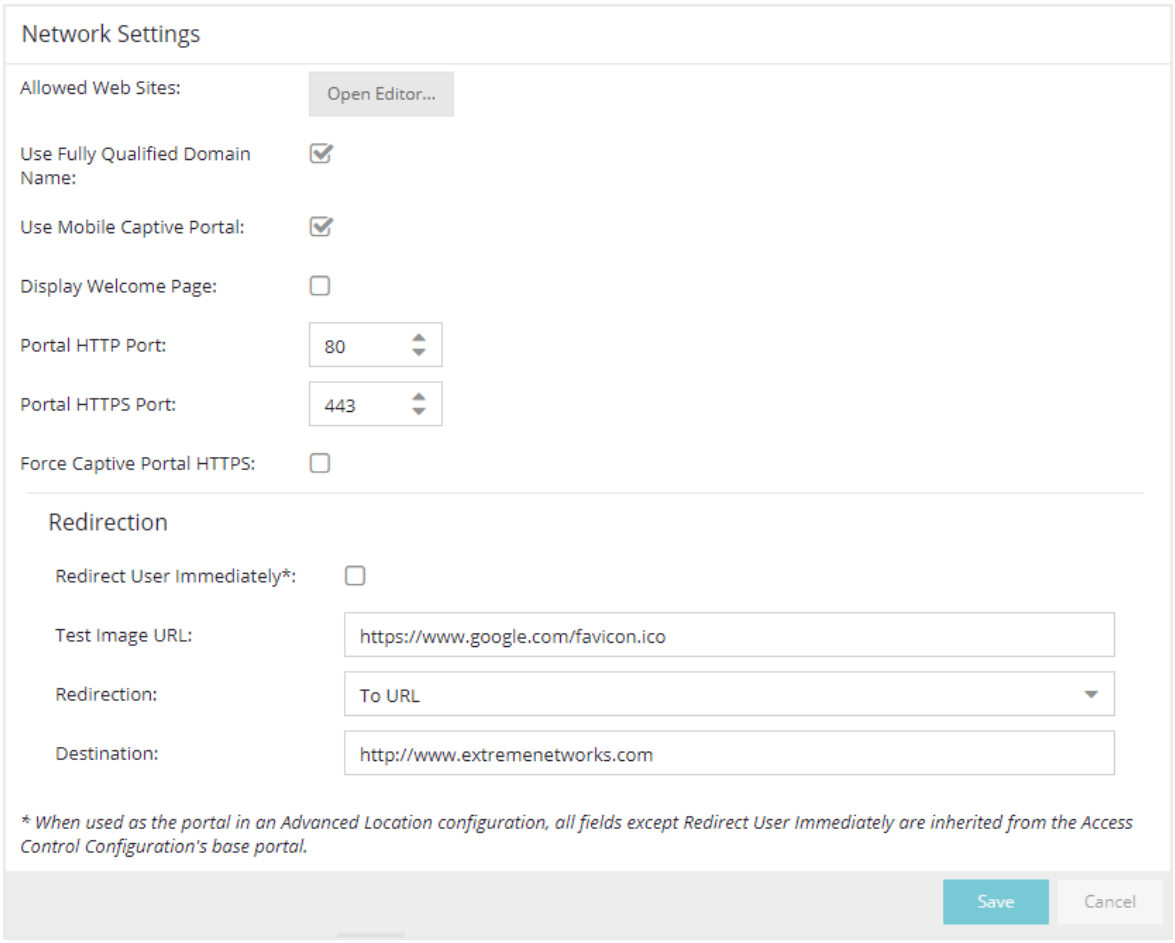
Following are instructions for configuring pre-registration in your portal configuration.

1. Open the **Control** > **Access Control** tab.
2. Select **Portal Configurations** > **Website Configuration** in the left-panel navigation tree.
3. Select Guest Access or Authenticated Registration (depending on the access type you are configuring).

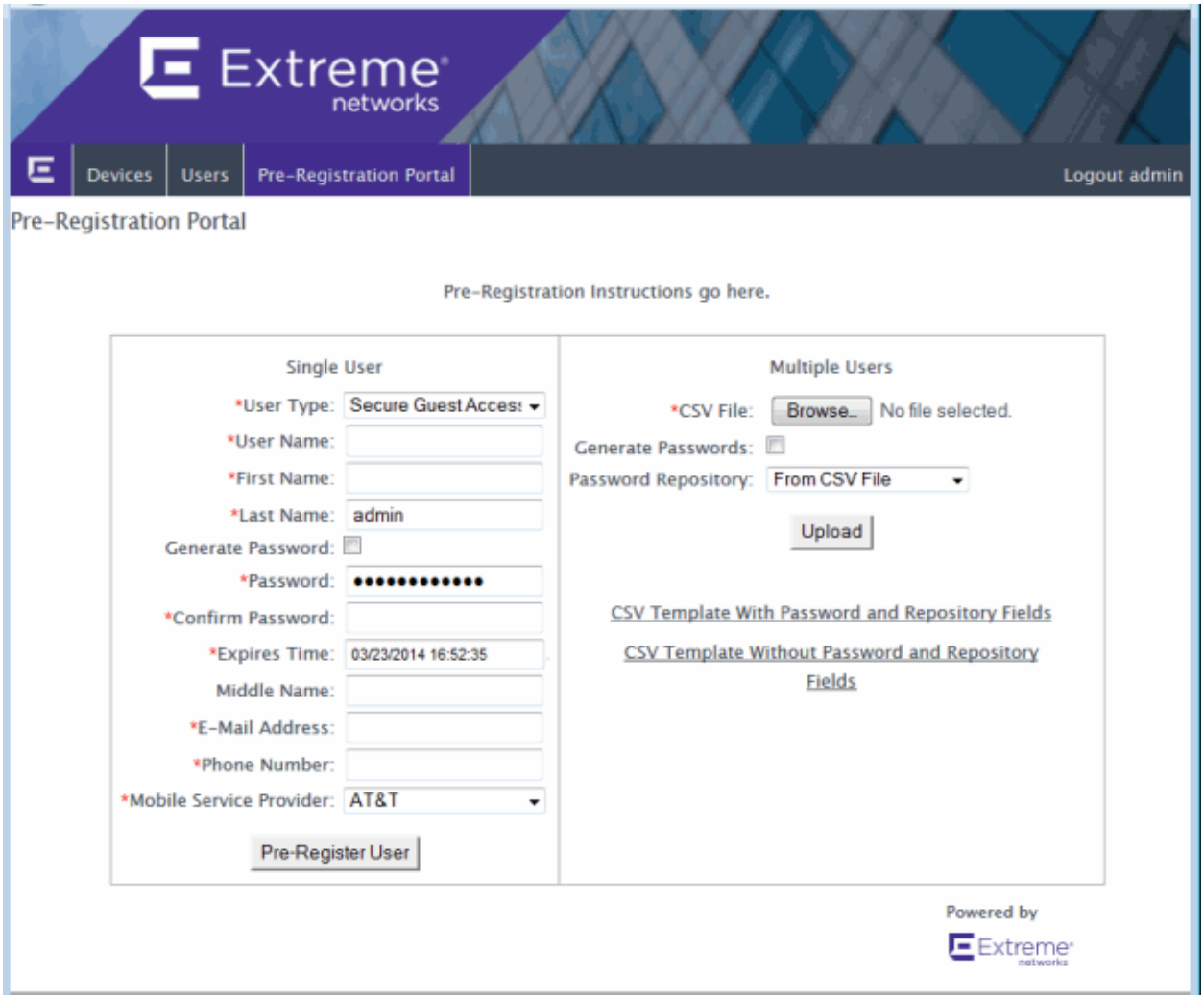
NOTE: If neither panel is available in the Website Configuration navigation tree, select Website Configuration in the left-panel and select the appropriate configuration.


Guest Registration
Introduction Message:
Edit...
Customize Fields:
Open Editor...
Redirection
Redirection:
Use Network Settings Redirection
Destination:
https://www.bcsdny.org
Registration Settings
Verification Method:
SMS Text Message
Service Providers:
Edit...
Message Strings:
Edit...
Verify PIN Characters:
Numeric Only
Verify PIN Length:
5
Default Expiration:
1
Days
(0 = never)
Facebook Registration
Google Registration
Microsoft Registration
Yahoo Registration
Salesforce Registration
Provider 1 Registration
Provider 2 Registration
Sponsorship
End users will be assigned to the Registered Guests group by default. With optional sponsorship, a sponsor can elevate their access. If sponsorship is required, the end user has no access until the sponsor approves.
Sponsorship Mode:
Required
Sponsored Registration Introduction:
Edit...
Admin/Sponsor Email (Always Notified):
rlacroix@extremenetworks.com
Sponsor Email Field:
Display Predefined Sponsor List
Predefined Sponsors:
rlacroix@extremenetworks.com, midgetmanofsteel@yahoo.com
Save
Cancel

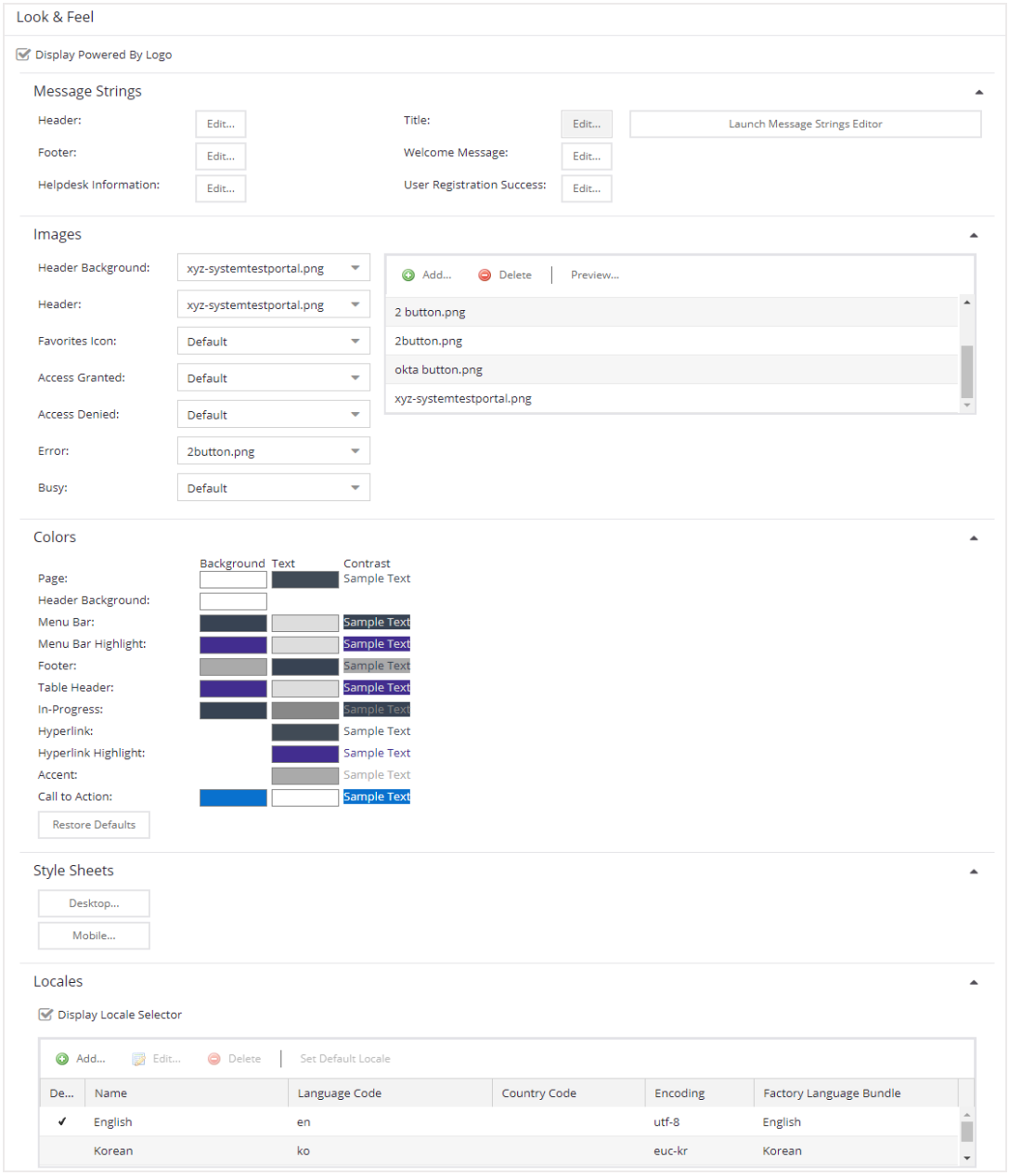
4. Select the **Enable Pre-Registration Portal** checkbox and specify whether personnel are able to register a single user, multiple users, or both single and multiple users.
5. Set the **Generate Password Characters** and **Generate Password Length** options. ExtremeControl uses these options when generating passwords for guest users to use when connecting to the network. These settings are shared by Authenticated Registration and Secure Guest Access. Changing it for one access type also changes it for the other.
6. For Authenticated Registration, select the Network Settings view to configure the connection URL specified on the Guest User Voucher (for example, www.ExtremeNetworks.com). Enter the URL in the **Redirection To URL** field. For Secure Guest Access, the Guest User Voucher provides instructions for connecting directly to the secure SSID.



7. Select **Save** to save your changes. Enforce your Access Control Configuration to your engines.
8. Access the Pre-Registration Portal by entering the following URL in a browser window: `https://<Access ControlEngineIP>/pre_registration`

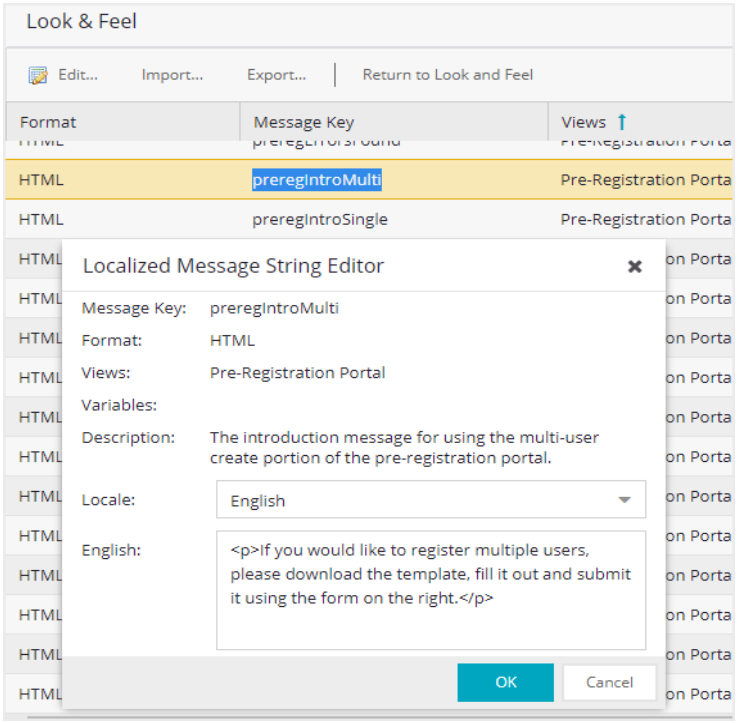


9. At the top of the portal web page are instructions for the people performing the pre-registrations. To modify and edit these instructions:
    a. In the **Control** > **Access Control** tab, select I&A Configurations > Portal in the left-panel navigation tree.
    b. Select a Portal Configuration and select Website Configuration > Look & Feel to open the Look & Feel panel.



c. Select the Message Strings **Launch Message Strings Editor** button. The Message Strings Editor window opens.

d. Scroll down to the "preregIntroMulti" or "preregIntroSingle" message key and double-click that line. The Modify Localized Entry window opens.



e. Enter any changes or modifications you wish to make to the instructions, and select **OK** to close the window.

f. Enforce the changes to your engines.

g. Refresh the browser window to see the new instructions in the Pre-Registration Portal.

10. The following sections provides information on how to pre-register a single user (when you want to pre-register one user at time) or multiple users (when you have a larger group of users to pre-register).

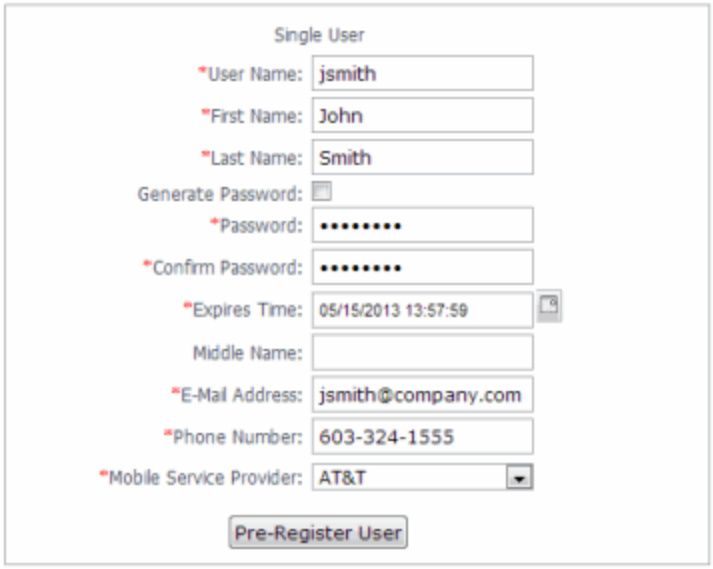
Pre-Registering Guest Users

After you have configured pre-registration, provide the URL for the Pre-Registration Portal (`https://<Access ControlEngineIP>/pre_registration`) to the personnel who are pre-registering guests. This can be network administrators or it can be personnel such as company receptionists, administrative assistants, or training personnel. (These users must be configured with administrative login privileges to access the web page).

The following sections provide steps for pre-registering single or multiple users in the Pre-Registration Portal.

Pre-Registering a Single User

Use the instructions in this section to pre-register a single end user using the Single User panel in the Pre-Registration Portal.



1. Enter the information for the guest user you want to pre-register. Fields with a red asterisk are required.
    - User Name — Enter the user name for the guest user when connecting to the network. Usernames must be unique and cannot already exist in the local password repository. Usernames are case sensitive. For example, "JSmith" and "jsmith" would be considered two different usernames.
    - First Name/Last Name — Enter the guest user's first and last name. The name is printed on the voucher along with their registration credentials.
    - Password/Confirm Password — Enter and confirm the password for the guest user connecting to the network. Select the **Generate Password** checkbox if you want ExtremeCloud IQ Site Engine to automatically generate a password for you.
    - Password Repository — When you pre-register the user, their credentials are automatically added to the local password repository specified here. Local Password Repositories are configured in the AAA Configuration window. (You only see this field if you have multiple repositories.)
    - Expires Time — Select a registration expiration date from the calendar. The time is automatically set to 0:00:00, which is midnight. You can enter a specific time, if desired.

NOTE: You can add additional fields to be displayed here using the Manage Custom Fields window accessed from the Customize Fields link in the Edit Portal Configuration window's Authenticated Registration view or Secure Guest Access view. However the Pre-Registration web page always displays the First Name and Last Name fields even if they are not selected as visible/required in the Manage Custom Fields window. This is because it is important for the first and last name to be included on the pre-registration voucher printed out.

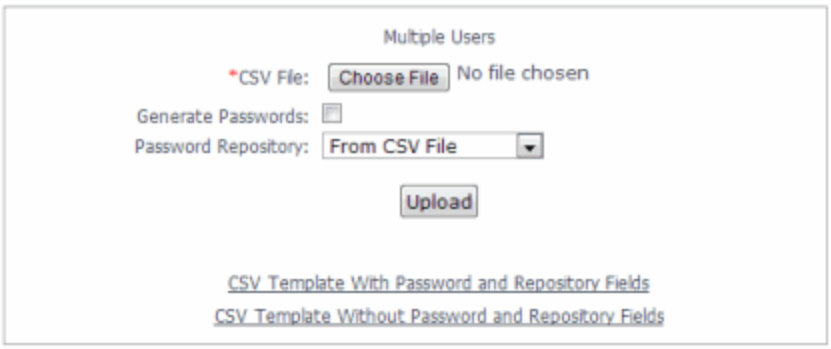
2. Select the **Pre-Register User** button to register the user. The user is added to the local password repository and added to the Registration Administration web page.
3. A voucher (see example below) is generated that provides registration instructions and the guest user's registration credentials. Print out this voucher to give to the guest user.

IMPORTANT: The voucher must be printed out immediately, as there is no way to go back and print out a voucher after you leave the web page. If you do not print out the voucher, the voucher needs to be created by hand. In the event that the "Generate Password" option was used, you need to modify the guest user password using the registration administration page or local repository administration.

1. To register another user, you must re-access the Pre-Registration page by using the browser's back button or re-entering the URL.

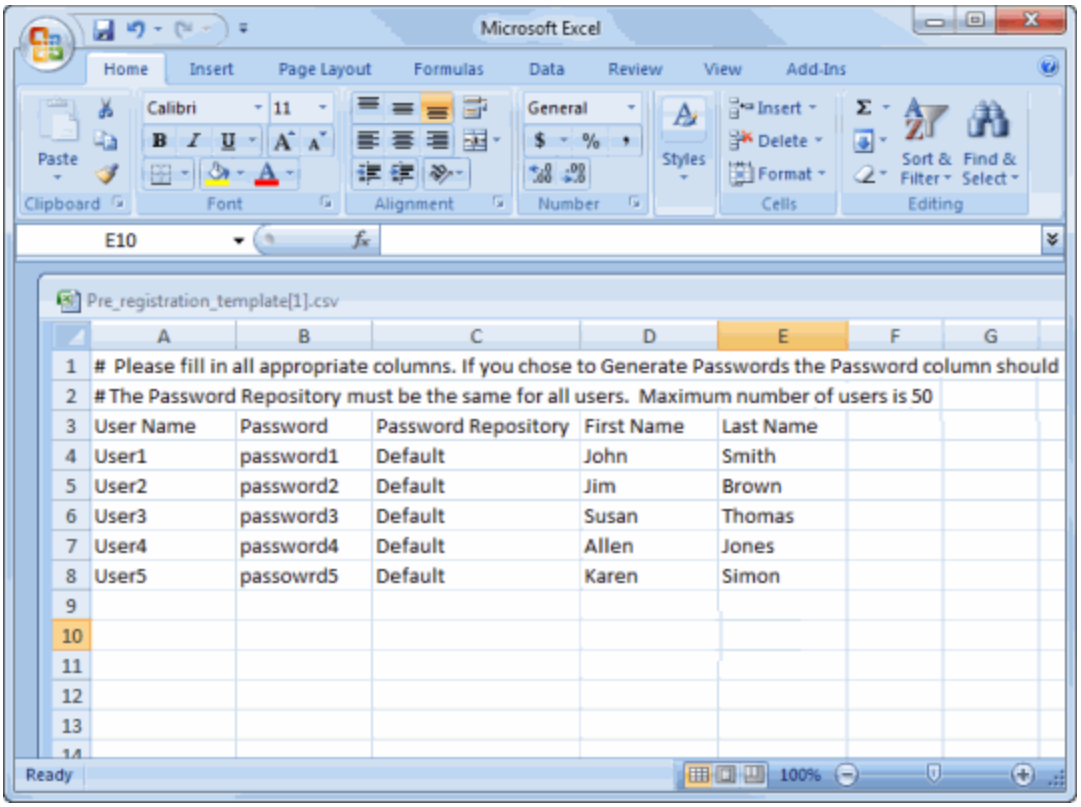
Pre-Registering Multiple Users

Use the instructions in this section to pre-register multiple end users at one time using the Multiple Users panel in the Pre-Registration Portal. When pre-registering multiple users, create a CSV file to provide all the user credential information in table form. Then, upload the file to ExtremeCloud IQ Site Engine to perform the pre-registration.



1. Select the CSV Template link to open a template CSV file where you create your list of guest users to pre-register. You can use a CSV template that includes password and password

repository fields or not, depending on your network requirements. Do not change any of the column headings in the file.



Following is an explanation of the columns that need to be filled in for each user, depending on the template you selected.

- User Name — Enter the username for the guest user connecting to the network. Usernames must be unique and cannot already exist in the local password repository. Usernames are case sensitive. For example, "JSmith" and "jsmith" would be considered two different usernames. (If you do try to pre-register existing usernames along with new usernames, you are notified of the error and given the option to continue registering the new names.)
- Password — Enter the password for the guest user connecting to the network. If you want ExtremeCloud IQ Site Engine to automatically generate end user passwords, leave the password column blank and select the **Generate Passwords** checkbox on the Multiple Users panel.
- Password Repository — When you pre-register the user, their credentials are automatically be added to the local password repository specified here. Local Password Repositories are configured in the AAA Configuration window. If you are using the Default repository, you can use the Password Repository drop-down list (in the Multiple

Users section) to select Default, and then you don't have to enter the Password Repository for each entry.

- First Name/Last Name — Enter the guest user's first and last name. The name is printed on the voucher along with their registration credentials.

NOTE: You can add additional columns to be included in the template using the Manage Custom Fields window accessed from the Customize Fields link in the Edit Portal Configuration window's Authenticated Registration view and Secure Guest Access view, however, the template always displays the First Name and Last Name fields even if they are not selected as visible/required in the Manage Custom Fields window. This is because it is important for the first and last name to be included on the pre-registration voucher you print.

---

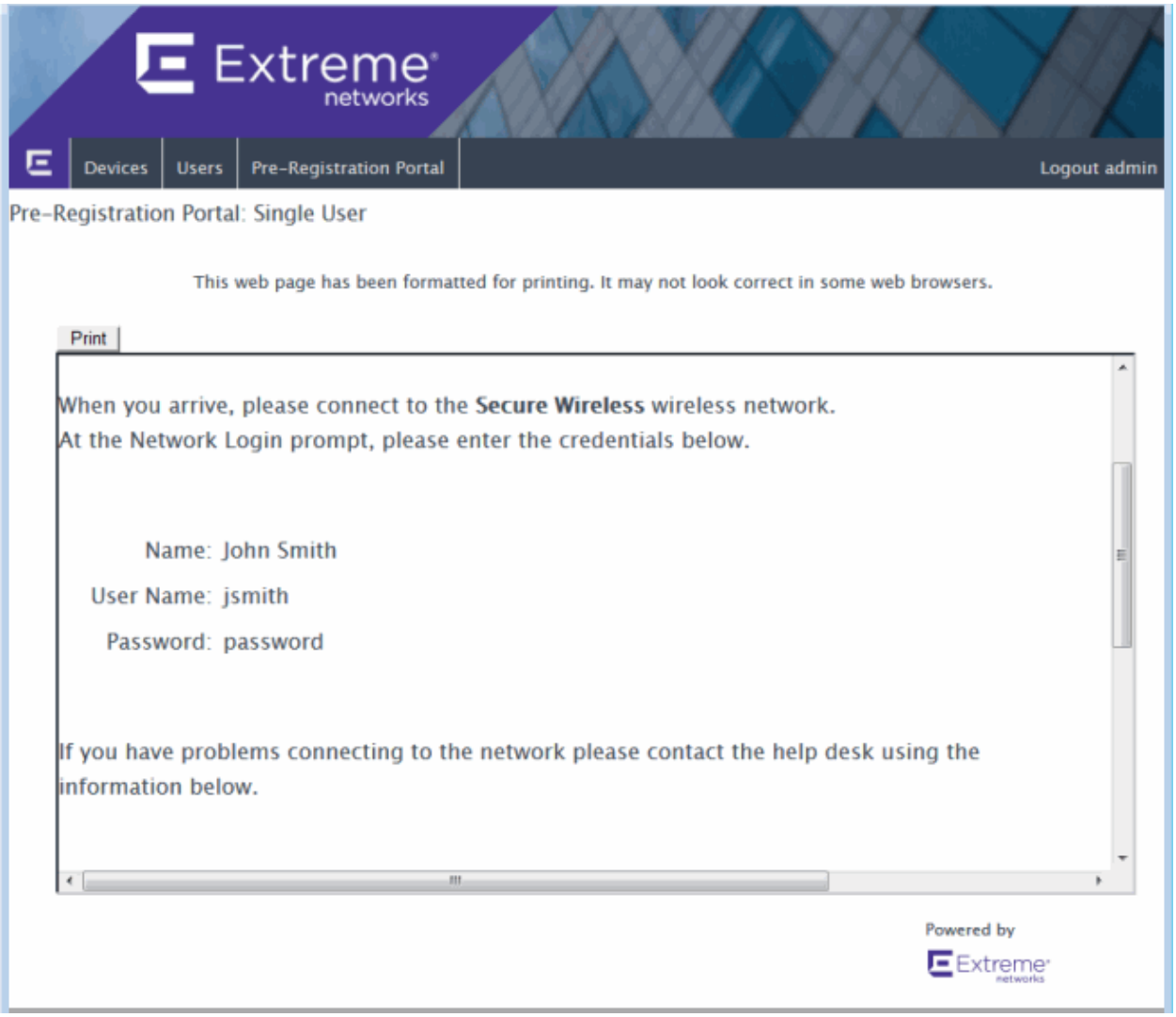
2. When you have finished entering the guest user information, save and close the file.
3. Back in the Multiple Users panel, enter the path and filename for the CSV file by using the **Browse** button to browse to the file on your system.
4. If your CSV file includes a Password Repository, use the Password Repository drop-down list to specify whether to use the default repository or the repository specified in the file.
5. Select the **Upload** button. Users are added to the local password repository and to the Registration Administration web page.
6. Individual vouchers (see an example below) are generated that provide registration instructions and the guest user's registration credentials for each guest user. Print out these vouchers to give to the guest users.

IMPORTANT: Vouchers must be printed out immediately, as there is no way to go back and print out a voucher after you leave the web page. If you do not print out the vouchers, the vouchers have to be created by hand. In the event that the "Generate Password" option is used, you need to modify the guest user passwords using the registration administration page or local repository administration.

---

7. To register another user, you must re-access the Pre-Registration Portal by using the browser's back button or re-entering the URL.

Sample Guest User Voucher



- Portal Configuration

How to Enable RADIUS Accounting

This Help topic describes how to use RADIUS accounting to provide real-time end-system connection status in ExtremeCloud IQ Site Engine. RADIUS accounting collects various end-system session data that ExtremeCloud IQ Site Engine uses to determine connection status for each end-system session. This can be useful for compliance purposes, enabling you to determine both when an end-system session started and when it was terminated.

RADIUS accounting is also used to monitor switches for Auto Tracking, CEP (Convergence End Point), and Switch Quarantine authentication sessions, when used in conjunction with the Monitoring or Network Access switch authentication access types. (For more information, see the Auth. Access Type section of the Add/Edit Switch Window Help topics.)

You must be running Access Control engine version 4.0 or higher to take advantage of RADIUS accounting functionality in ExtremeCloud IQ Site Engine.

For Extreme Networks stackable and standalone devices (A-Series, B-Series, C-Series, D-Series, G-Series, and I-Series), ExtremeCloud IQ Site Engine uses a combination of SNMP and CLI (command line interface) to configure RADIUS accounting on the switch. Before enabling RADIUS accounting on these devices, read through Considerations for Fixed Switching Devices below.

NOTES: RADIUS accounting is not supported on the Access Control Controller.

Use the following steps to enable RADIUS accounting:

1. Enable RADIUS accounting on your switches and controllers using the instructions appropriate for your devices.

   For Extreme Networks devices or ExtremeWireless Controller devices running firmware version 9.21.x.x or newer:

   a. **If you are editing an existing device:** In the right-panel **Switches** tab, select the devices you want to perform RADIUS accounting and select the **Edit** button. The Edit Switches in Access Control Appliance Group window opens.
   If you are adding a new device: Select **Add** in the right-panel **Switches** tab and the Add Switches to Access Control Appliance Group window opens.

   b. Set the RADIUS Accounting option to **Enabled**. Select **OK**.

   c. Enforce to your engines.

   For ExtremeWireless Controller devices running firmware versions older than 9.21.x.x:

   a. RADIUS accounting must be enabled manually on the controller using the ExtremeWireless Assistant or the device CLI (command line interface).

b. Be sure to configure the Access Control engine IP address as the IP address of the RADIUS server. Refer to your wireless controller User Guide for instructions on enabling RADIUS accounting via the ExtremeWireless Assistant, or the CLI Reference Guide for the exact CLI command syntax to use.

For third-party switching devices:

a. RADIUS accounting must be enabled manually on the device using the device CLI (command line interface).

b. Be sure to configure the Access Control engine IP address as the RADIUS accounting server. Refer to your device documentation for the exact command syntax.

2. If you are doing RADIUS accounting in an Access Control environment where the primary RADIUS server is being used for redundancy in a single Access Control engine configuration (Basic AAA configuration only), then enable the Proxy RADIUS Accounting Requests option in the Edit RADIUS Server window.

   a. In the Edit Basic AAA Configurations window, use the Configuration Menu button in the Primary RADIUS Server field to open the Manage RADIUS Servers window.

   b. Select the RADIUS Server and select **Edit**.

   c. Enable the Proxy RADIUS Accounting Requests option. Select **OK**.

   d. Enforce to your engine.

With RADIUS accounting enabled, you now see real-time connection status in the ExtremeCloud IQ Site Engine **End-Systems** tab and Dashboard.

Considerations for Fixed Switching Devices

ExtremeCloud IQ Site Engine uses a combination of SNMP and CLI (command line interface) to configure RADIUS accounting on Extreme Networks stackable and standalone devices (A-Series, B-Series, C-Series, D-Series, G-Series, and I-Series). Due to a limitation on the SNMP interface, the configuration can be read via SNMP, but must be written to the device via CLI. Before enabling RADIUS accounting on these devices, read through the following considerations.

NOTE: These considerations do not apply to A4, B5, and C5 devices running firmware version 6.81 and higher. Those devices support RADIUS accounting configuration using SNMP.

- The devices must be assigned a Device Access profile that provides Write access and includes CLI credentials for Telnet or SSH. Profiles and CLI credentials are configured using the Authorization/Device Access tool's **Profiles** tab.
- Before you enforce a new RADIUS server configuration to your fixed switching devices, you should verify that your CLI credentials are configured according to the settings in your new configuration. This is because the Enforce process first writes the RADIUS server configuration to the switch using SNMP, and then writes the RADIUS accounting configuration to the switch

using Telnet or SSH. If CLI credentials are not configured according to the new RADIUS server configuration, then the RADIUS accounting configuration are not written to the switches.

For example, by default you can Telnet to a fixed switching device using username=admin (with no password or a blank password). But, if you configure a new RADIUS configuration with an Auth Access Type (or Realm Type)=Any, then change the Device Access for the switches to use the IAS credentials, in order for ExtremeCloud IQ Site Engine to successfully write the RADIUS accounting information to the switches during Enforce.

Fixed switches only permit one accounting server to be configured. If a primary and secondary Access Control Engine are configured for the switch, only the primary engines accounting configuration is written to the switch. If a secondary engine is configured, a warning is displayed.

Considerations for ExtremeXOS/Switch Engine Devices

ExtremeCloud IQ Site Engine uses CLI access to perform RADIUS accounting configuration operations on ExtremeXOS/Switch Engine devices. CLI credentials for the device are obtained from the device profile and must be configured in the Authorization/Device Access tool.

Guest and IoT Manager Configuration in ExtremeCloud IQ Site Engine and Access Control (Legacy)

Guest & IoT Manager (GIM) is an application that allows you to access and manage guest user and end-system (device) activity information. Through ExtremeCloud IQ Site Engine and ExtremeControl, GIM provides non-IT personnel with the tools to configure limited system access for guest users and/or devices based on authorization constraints you define.

NOTE:	Beginning in ExtremeCloud IQ Site Engine 26.11.10, GIM performs a version compatibility check as it connects to ExtremeCloud IQ Site Engine. If you are attempting to connect to an incompatible version of ExtremeCloud IQ Site Engine, GIM displays an error message.

Non-IT personnel who are designated as provisioners can provide limited access to other guest users for a specified amount of time for specific purposes. For example, your company is conducting product training for customers at one of your offices. You provide the front desk employee at the site provisioner access so he or she can provide participating customers limited guest user access to your system for that day only. Refer to Extreme Control Guest and IoT Manager Configuration for more information about provisioner and guest user access.

Connecting GIM to ExtremeControl

GIM uses a REST API to communicate with ExtremeCloud IQ Site Engine through an Access Control engine. In order for GIM to access the REST API, it must be authorized to do so by configuring the appropriate GIM capability in the Authorization Group configuration in ExtremeCloud IQ Site Engine. The REST API allows GIM to store its configuration data in the ExtremeCloud IQ Site Engine database.

Use the following steps to create an Authorization Group and add users to that Authorization Group:

1. Open the **Administration > Users tab** in ExtremeCloud IQ Site Engine.
2. Create a new Authorization Group for users with access to the GIM REST API.
3. Select **Save**.
4. Create users and add them to the new Authorization Group.
5. Select **Save**.
6. Access the Administrator Application of GIM.
7. Open the **Administration** > **Access Control Engine** tab in GIM.
8. Open the **Engine Details** tab.

9. Enter the information for the Access Control engine you are using for GIM. For additional information, see Configuring Engine Details on page 49 of the Extreme Control Guest and IoT Manager Configuration document.

NOTE:	Enter the credentials of the user or users added to the GIM REST API Authorization Group in the **Admin Username** and **Admin Password** fields.

Configuring the RADIUS Protocol for GIM Authentication

After adding users to the GIM Authorization Group, enter the IP address and RADIUS shared secret in ExtremeCloud IQ Site Engine and in GIM to allow the Access Control engine to authenticate provisioners in GIM.

1. Open the **Control** > **Access Control** tab in ExtremeCloud IQ Site Engine.
2. Expand the Engines folder in the left panel.
3. Select the Engine Group through which provisioners are authenticating.
4. Open the **Guest and IoT Managers** tab in the right panel.
5. Select **Add**.

   The **Add Guest and IoT Manager** window opens.
6. Enter the GIM IP address.
7. Enter a Shared Secret and copy it to a safe location.

NOTE:	The shared secret functions as a password, allowing GIM and the RADIUS server (the Access Control engine) to communicate. Use a strong shared secret difficult for others to guess.

8. Access the Administrator Application of GIM.
9. Open the **Administration** > **Access Control Engine** tab in GIM.
10. Open the **RADIUS** tab.
11. Enter the RADIUS information on the tab. For additional information, see Configuring RADIUS Settings on page 50 of the Extreme Control Guest and IoT Manager Configuration document.

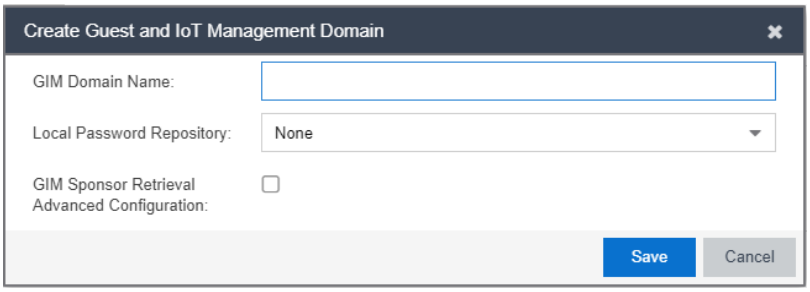
The Access Control engine is configured as the RADIUS server for GIM. Configure each GIM application with an IP Address and Shared Secret in ExtremeCloud IQ Site Engine.

Creating and Configuring a GIM Domain

A GIM domain contains all of the configuration information. GIM domains are created in ExtremeCloud IQ Site Engine and the configuration within that domain is configured in GIM.

To create a GIM domain in ExtremeCloud IQ Site Engine:

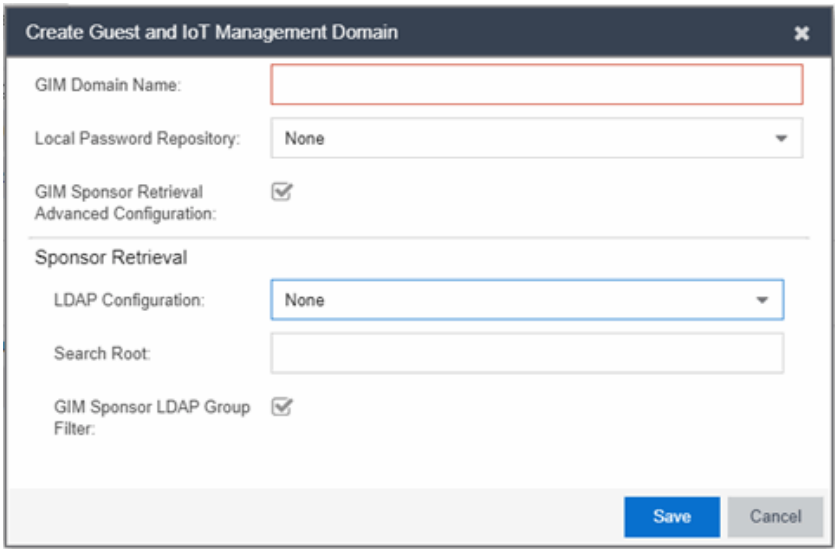
1. Open the **Control** > **Access Control** tab in ExtremeCloud IQ Site Engine.
2. Expand the Engines folder in the left panel.
3. Select the Engine Group through which provisioners are authenticating.
4. Open the **Details** tab in the right panel.
5. Select **Edit** in the Guest and IoT Configuration section of the tab. The **Edit Guest and IoT Manager Configuration** window opens.
6. Select **New** from the drop-down list to create a new domain. The **Create Guest and IoT Management Domain** window opens.



7. Enter the name of your GIM domain and select **New** in the **Local Password Repository** drop-down list to create a new password repository for GIM. The **Create Repository** window opens.
8. Enter a name for the local password repository you are using for your GIM provisioners and users.
9. Select **Create**.The **Edit Local Password Repository** window opens.
10. Select **Add**. The **Edit User** window opens.
11. Enter the information for at least one user.
12. Select **OK**.
13. Select the local password repository you created in the **Local Password Repository** drop-down list in the **Create Guest and IoT Management Domain** window.
14. To customize the sponsor retrieval in your GIM Domain, select the GIM Sponsor Retrieval Advanced Configuration check box and choose a different LDAP configuration and Search Root specifically for sponsor look-ups.

NOTE: Not enabling the GIM Sponsor Retrieval Advanced Configuration defaults sponsor retrieval to use an LDAP configuration based solely on the Sponsor Group configured in GIM.

a. The Sponsor Retrieval panel displays.



b. Select, create, or modify the LDAP Configuration from the drop-down list.

c. Enter the Search Root.

d. Optionally, you can select the check box to enable the GIM Sponsor LDAP Group filter, which further filters the search for a sponsor using the GIM-configured Sponsor LDAP Group.

NOTE: Not selecting the GIM Sponsor LDAP Group filter ignores yours Sponsor Group setting in GIM and uses the LDAP configuration and Search Root you define in the Create Guest and IoT Management Domain window for sponsor look-ups.

15. Select **Save**.

The templates, users, devices, and other information configured in the GIM application are stored in the GIM domain.

NOTE: While the domain is stored in ExtremeCloud IQ Site Engine, the only part of the GIM domain configured in ExtremeCloud IQ Site Engine is the authentication method used by GIM provisioners and users.

Configuring GIM Authentication

In GIM, the Administrator creates provisioners via the Administration login. Provisioners then provide network access to users or devices using the Provisioner login.

Local Password Repository

When you create a provisioner while logged into GIM as an Administrator, ExtremeCloud IQ Site Engine saves the provisioner credentials in the default local password repository associated with the GIM Domain.

When you provide network access to users or devices in GIM, those credentials are also saved in the local password repository associated with the GIM Domain.

LDAP

Provisioners can also authenticate via Active Directory associated with an LDAP Configuration in ExtremeCloud IQ Site Engine. For provisioners for which both LDAP and a local password repository are available as authentication methods, the methods can be independent or work in conjunction with each other (for example, if LDAP authentication fails, ExtremeCloud IQ Site Engine checks the local password repository for valid credentials).

To configure LDAP as an authentication method:

1. Access GIM as the Administrator.
2. Open the **Onboarding Template** tab and select **Add**.
3. Open the **Advanced** tab.
4. Enter the Active Directory field against which authentication is verified (for example, `cn=gimGroup1,dc=extremenetworks,dc=com`). The entire path must match for authentication to be successful.

   Some common Active Directory objects used include:

   - cn=common name
   - dn=distinguished name
   - dc=domain controller
   - ou=organizational unit

5. Access ExtremeCloud IQ Site Engine.
6. Open the **Control** tab.
7. Select the **Access Control** tab.

8. Select the **Configuration** > **Configurations** tab in the left-panel tree.
9. Expand the Access Control Configuration associated with the Access Control Engine Group to which GIM is associated.
10. Select **AAA**.
11. Configure the LDAP configuration to provide authentication and authorization for network end users and host machines via Active Directory.
12. Save the LDAP configuration.
13. Expand the Access Control Configuration associated with the Access Control Engine Group to which GIM is associated.
14. Select **AAA**.
15. Configure the Authentication Rules table to authenticate via your LDAP configuration, your local repository, or both by adding both to the table. If using both authentication methods, ensure the authentication method you want to take precedence is listed first in the table.
16. Select **Save**.

The Access Control Engine now authenticates GIM users based on the Access Control Configuration.

IMPORTANT:	Via the legacy NAC Manager java application, ensure **Manual Set (Accurate)** is listed first in the Device Type Detection Source Precedence Order in the Edit Appliance Settings window on the Device Type Detection tab. This is the default precedence, and is required for GIM-assigned device types to affect authentication.

Once GIM is fully connected to ExtremeCloud IQ Site Engine and Access Control, follow the steps outline in the Extreme Control Guest and IoT Manager Configuration document.

Configuring Multiple Active Directory Domains

You can configure multiple Active Directory (AD) domains to authenticate users that reside on Active Directories that do not have trust between them. Additionally, you can configure multiple authentication rules so that if authentication to one fails, ExtremeControl can automatically attempt to authenticate against a second domain.

Requirements

Prior to configuring multiple AD domains:

- Ensure all AD servers communicate using DNS name.
- Validate multi-domain functionality works for your network.

Validating Multiple AD Domain Functionality

To ensure you can configure multiple AD domains for authentication on your network, ExtremeControl must be able to resolve all Directory service domains correctly. DNS resolution is required for multiple AD domain functionality to work properly. For example, if you are using a third-party DNS server (e.g. Infoblox), ExtremeControl is able to resolve all domains correctly. If one of AD's is acting as a DNS server, configure it (using DNS conditional forwarding) to resolve other Domains.

Additionally, ExtremeControl runs the `wbinfo` command line tool to check the reachability of AD servers to which it joined. In this multi-join scenario, ExtremeControl runs `wbinfo` against all joined Directory Services.

After AD domains are configured, you can **Test AD Authentication** in ExtremeControl from the right-click context menu of an Engine in **Control > Access Control > Engines.**

Joining Multiple Active Directory Domains

After you verify you can configure multiple Active Directory domains on your network, perform the following to configure the functionality:

1. Access the **Advanced AAA Configurations** tab.
2. Select **All Domains** in the **Join AD Domain** drop-down list.

NOTE: If multiple Active Directory domains are configured, ExtremeControl attempts to join them all.

3. Select **Add** in the Authentication Rules section to open the **Add/Edit User to Authentication Mapping** window.
4. Configure multiple authentication rules with an **Authentication Method** of **LDAP Authentication** in the Authentication Rules section.
5. Select the **Fall-through if Authentication Failed** checkbox if you want ExtremeControl to attempt to authenticate a user against the next AAA authentication rule in the table if the current authentication rule fails or times out. If this checkbox is not selected and authentication fails, the user is not authenticated and ExtremeCloud IQ Site Engine does not attempt to authenticate using any other rules in the table.
6. Select **OK**.
7. Select **Save**.

ExtremeControl attempts to join to all Domains you configure in the AAA authentication rules. If ExtremeControl is not able to join to any Domains, then a timer runs and attempts to keeps trying to rejoin. When ExtremeControl joins a particular domain, then a separate health check timer runs to ensure AD server is reachable.

Multiple AD domains are configured and if you enabled fall-through for your rules, ExtremeControl automatically attempts to authenticate against the next rule in the table.

Important Note

If duplicate users exist in multiple Active Directory domains with the same password, the AAA rule(s) with user pattern (for example, Domain*) needs to be configured for the user to match the domain name and use the AAA rule correctly.

For example, a user **administrator** exists in 2 Active Directory domain servers and the following is configured in AAA rule:

- All LDAP Authentication using Domain_A.com server - fall through enabled
- All LDAP Authentication using Domain_B.com server

When **administrator** joined, the Domain_B domain tries to authenticate the user. The **administrator** user is successfully authenticated to the Domain_A.com server because the user does exist in Domain_A.com server. To avoid this, configure the AAA rule with user pattern as seen below:

- User matching Domain_A* (or *@domain_a.com) using Domain_A.com server - fall through enabled
- User matching Domain_B* (or *@domain_b.com) using Domain_B.com server

How to Set Up Access Policies and Policy Mappings

Access policies define the appropriate level of access to network resources allocated to a connecting end-system based on the end-system's authentication and/or assessment results. There are four access policies defined in an ExtremeControl profile: Accept policy, Quarantine policy, Failsafe policy, and Assessment policy. When an end-system connects to the network, it is assigned one of these access policies, as determined by the Access Control profile assigned to the matching Access Control rule and the end-system state.

In your Access Control profiles, each access policy is associated to a *policy mapping* that defines exactly how an end-system's traffic is handled when the access policy is applied.

A policy mapping specifies the policy role (created in the **Policy** tab) and other RADIUS attributes included as part of a RADIUS response to a switch. The RADIUS attributes required by the switch are defined in the RADIUS Attributes to Send field configured in the Edit Switch window. Policy mappings are configured in the Edit Policy Mapping Configuration window.

How you set up your access policies depends on whether your network utilizes Access Control Controller engines and/or Access Control engines. In addition, if your network utilizes Access Control engines, your setup depends on whether your network contains EOS switches that support Policy, third-party switches that support RFC 3580, or switches that support RADIUS attributes that are defined manually.

For Access Control Controllers:

If your network utilizes Access Control L2/L3 controller engines, the access policies specified in Access Control profiles are mapped to policy roles that are defined in a default policy configuration already configured on the controller. It is recommended that you review this default policy configuration using the **Policy** tab. To do this, you must create a policy domain in the **Policy** tab specifically for the Access Control Controller, assign the Access Control Controller to the domain, then import the policy configuration from the device into **Policy** tab. Review the policy roles and make any rule changes required for your environment. When you have finished modifying the policy configuration, you must enforce it back to the Access Control Controller.

For Access Control Appliances:

If your network utilizes Access Control engines, the access policies specified in Access Control profiles are mapped to policy roles that must be created and defined in the **Policy** tab and enforced to the policy-enabled switches in your network. If you have RFC 3580-enabled switches in your network, ExtremeCloud IQ Site Engine lets you associate your policy roles to a VLAN ID or VLAN Name using the Policy Mappings panel. This allows your Access Control engines to send the appropriate VLAN attribute instead of a policy role to those switches that are RFC 3580-enabled.

Policy mappings have a Location option that allows different VLAN IDs to be returned for a policy based on the location the authentication request originated from. This is useful in networks that have a VoIP/voice VLAN that is defined on multiple switches, but that VLAN maps to a unique VLAN ID on each switch. (For more information, see the section on Location in the Edit Policy Mapping Configuration Window Help topic.)

NOTE: If you have RFC 3580-enabled switches in your network, be sure to verify that the DHCP Resolution Delay Time option is set correctly in your Appliance Settings (Tools > Manage Advanced Configurations> Global and Appliance Settings). This option specifies the number of seconds an Access Control engine waits after an authentication completes before attempting to resolve the end-system's IP address. When modifying this delay, keep in mind that for RFC 3580 devices, the engine links down/up a port to force the end-system to get a new IP address when ExtremeCloud IQ Site Engine determines that the VLAN has changed. If the delay time specified is less than the amount of time the end-system needs to renew its IP address, then the Access Control engine can resolve the end-system's IP address incorrectly (to the previously held IP), or additional delay can be introduced as the resolution process attempts to resolve the address based on the configured retry interval. This is a problem when either registration or assessment is enabled: the registration process never completes or takes an unacceptable amount of time to complete, or the Access Control engine could attempt to scan the incorrect IP address. Be sure to take into account the amount of time required for an end-system to get a new IP address when setting the delay time value.

Setting Up Your Access Policies

Before you begin working with the **Access Control** tab, use these steps to define the policy mapping criteria (policy roles, corresponding VLAN IDs, etc.) available for selection for each access policy.

1. For each Access Control profile, create a worksheet listing the four Access Control policies. For each access policy, associate a policy role (created in the **Policy** tab), and the policy role's corresponding VLAN ID, if you are using RFC 3580-enabled switches in your network. For a description of each access policy, and some guidelines for creating corresponding policy roles, see the section on Access Policies in the Concepts file.

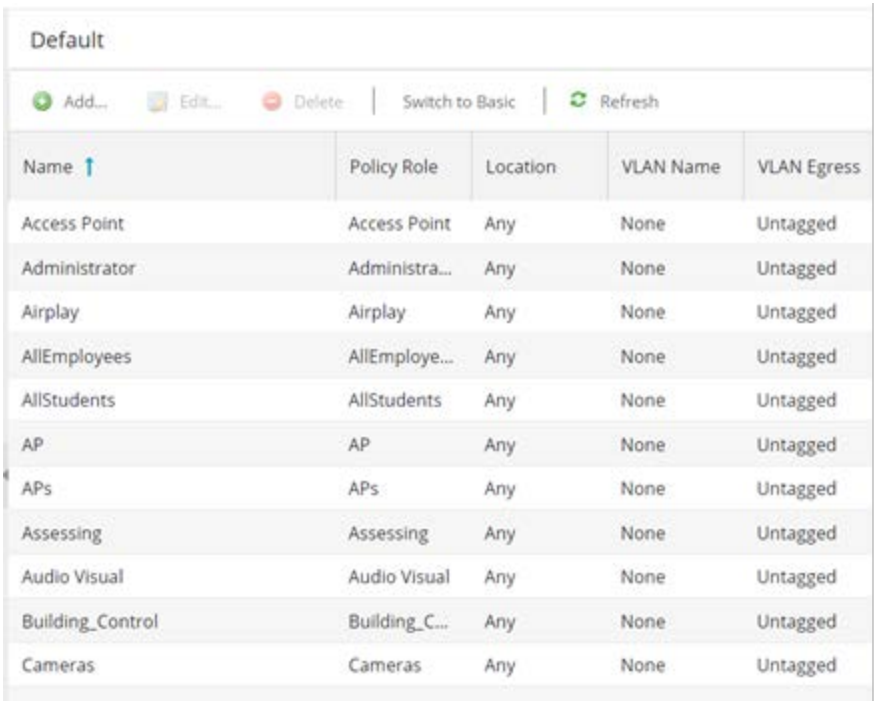
   NOTE: If your network uses Access Control engines with only RFC 3580-enabled switches, instead of listing policy roles, simply create a list of policy names that correspond to the VLANs you are using in your network. One tip is to use policy names that identify the corresponding VLAN name for ease of selection when you are creating your Access Control profiles.

   Here's an example of a worksheet for an Access Control profile that contains both policy-enabled and RFC 3580 switches:

Access Policy	Policy Role	VLAN ID
Accept Policy	Enterprise User	[2] Enterprise User VLAN
Quarantine Policy	Quarantine	[4] Quarantine VLAN
Failsafe Policy	Failsafe	[5] Failsafe VLAN
Assessment Policy	Assessing - Strict	[6] Assessing - Strict VLAN

2. For Access Control Controllers, use the **Policy** tab to verify that the policy configuration contains the required policy roles, and that the configuration has been enforced to the Access Control Controller. See the instructions above.
3. For Access Control engines, verify each policy role listed on your worksheet is created in ExtremeCloud IQ Site Engine's **Policy** tab and enforced to the policy-enabled switches in your network. If you have RFC 3580-enabled switches in your network, verify that your VLANs have been created on the switches in your network.
4. Define the policy mappings that map each access policy to the appropriate policy role as specified in your worksheet.
    a. Select a policy mapping configuration from the Access Control Configurations > Access Control Profiles > Policy Mappings left-panel option.
    b. In your Access Control profile, your policy mappings are available for selection when you define your Accept, Quarantine, Failsafe, or Assessment access policy.

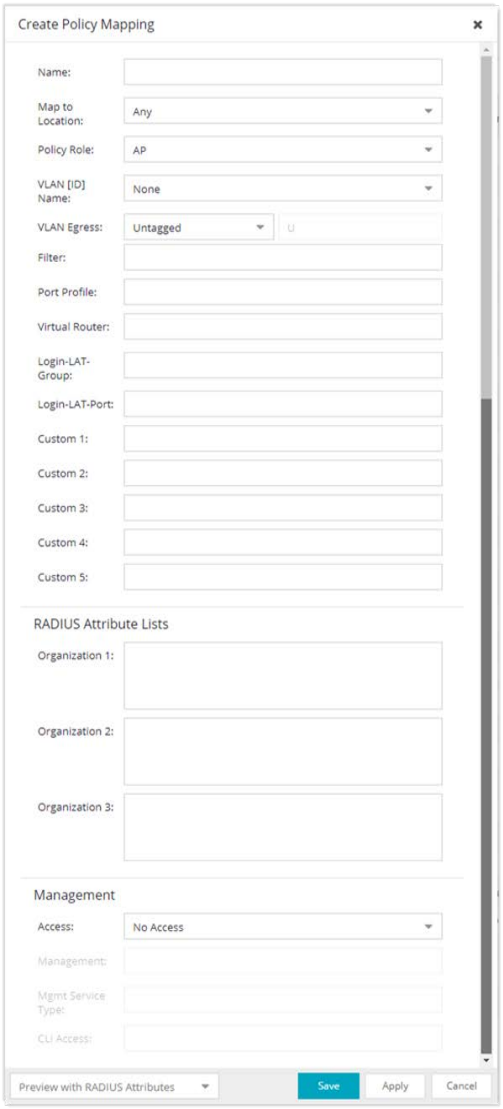
       The Policy Mapping Configuration right-panel opens.



c. Select between a Basic policy mapping and an Advanced policy mapping, depending on your network needs by selecting **Switch to Advanced** or **Switch to Basic** at the top of the panel.Typically, the Basic policy mapping configuration is used unless your devices require customization or when using locations in your mappings. If Basic Policy Mapping is used, then the **Add** new policy mapping, as well as **Edit** policy mapping, gives the option to show the advanced options.

   Access Control provides a list of default policy mappings you can use. Be aware if you use one of the default mappings, you still need to verify that the policy role specified in the mapping is part of your Access Control Controller policy configuration and/or is created and enforced to the policy-enabled switches in your network via the **Policy** tab.

d. To add a new policy mapping, select the **Add** button to open the Add Policy Mapping window.



For the new policy mapping, enter a mapping name and specify a policy role (created in the **Policy** tab) and other required RADIUS attributes included in the RADIUS response to a switch. Select **OK** to add the mapping. Note that the required RADIUS attributes for your switches are defined in the RADIUS Attributes to Send field configured in the Edit Switch window, as shown below.

e. Select **OK** to close the Edit Policy Mapping Configuration window.

How to Configure Credential Delivery for Secure Guest Access

Secure Guest Access provides secure network access for wireless guests via 802.1x PEAP by sending a unique username, password, and access instructions for the secure SSID to guests via an email address or mobile phone (via SMS text). Use the instructions in this Help topic to configure the method used to send guests their credentials and access instructions for the secure SSID.

Configuration Steps

The Credential Delivery method is configured in your portal configuration. Depending on the method you specify, the appropriate custom fields must be configured for display on the Registration web page, so that end users can enter the required information.

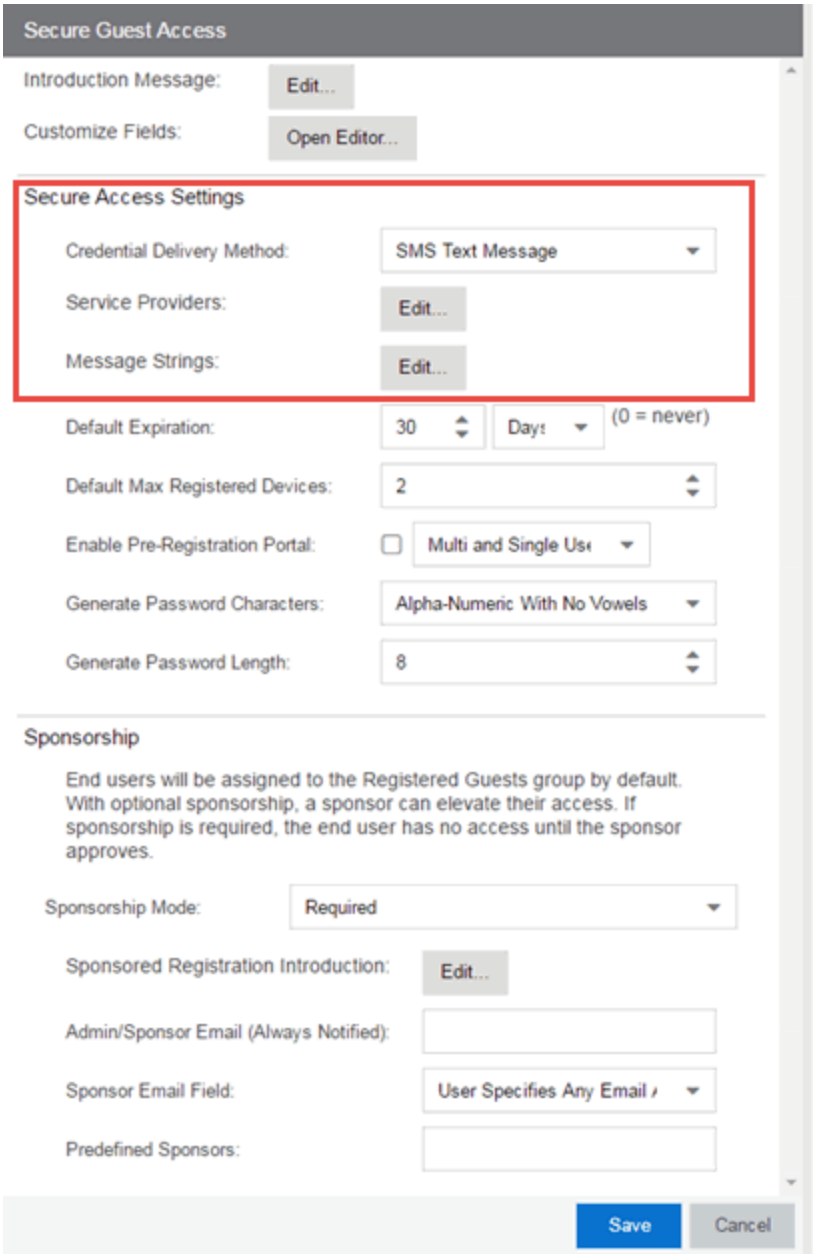
The following table provides a description of each credential delivery method and lists their custom field requirements.

User Verification Method	Description	Custom Field Requirement
Captive Portal	The credential information is displayed on the Registration web page.	There are no Custom Field requirements.
Email	The end user must enter a valid email address on the Registration web page.	The Email Address Custom Field must be set to **Required**.
SMS Gateway	The SMS Gateway provider must support SMTP API. The SMS Gateway provider converts the email to an SMS text message. The end user must enter a mobile phone number on the Registration web page.	The Phone Number Custom Field must be set to **Required**.
SMS Gateway or Email	The SMS Gateway provider must support SMTP API. The SMS Gateway provider converts the email to an SMS text message. The end user must enter a mobile phone number or email address on the Registration web page.	The Phone Number and Email Address Custom Fields must be set to **Visible**.

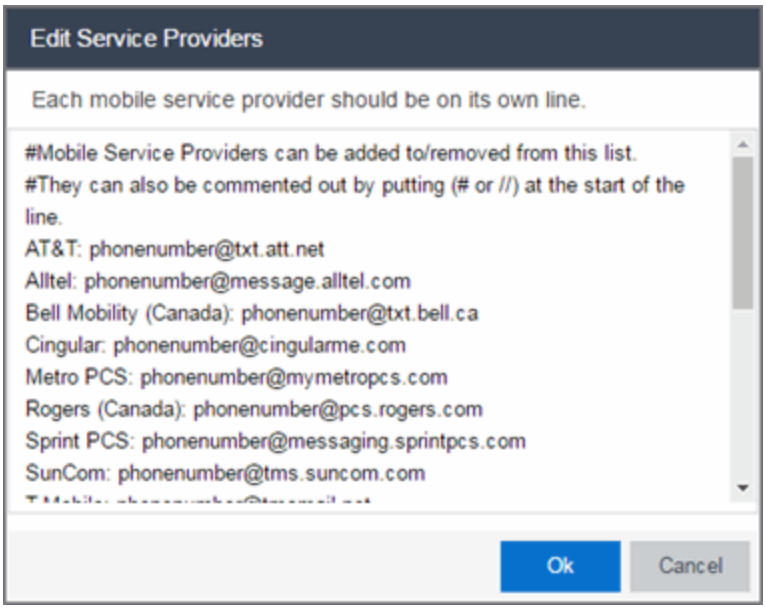
User Verification Method	Description	Custom Field Requirement
SMS Text Message	The mobile provider converts the email to an SMS text message. The end user must enter a valid mobile phone number on the Registration web page.	The Phone Number Custom Field must be set to **Required**.
SMS Text or Email	The mobile provider converts the email to an SMS text message. The end user must enter a valid mobile phone number or email address on the Registration web page.	The Phone Number and Email Address Custom Fields must be set to **Visible**.

Use the following steps to configure credential delivery for Secure Guest Access in your portal configuration.

1. In the **Access Control** tab, access the Portal Configuration. Select Secure Guest Access in the Portal Configuration tree. (If you don't see this selection, select Features in the tree and enable the Secure Guest Access feature.)
2. In the Secure Guest Access panel, use the drop-down list to select the desired Credential Delivery Method (refer to the table above).



3. If you selected the **SMS Text Message** or the **SMS Text or Email** Credential Delivery method, select the Service Providers **Edit** button to configure the list of mobile service providers from which end users can select the Registration web page. The Mobile Service Provider List provides a default list of providers that can be edited to include the appropriate service providers for your geographic location.



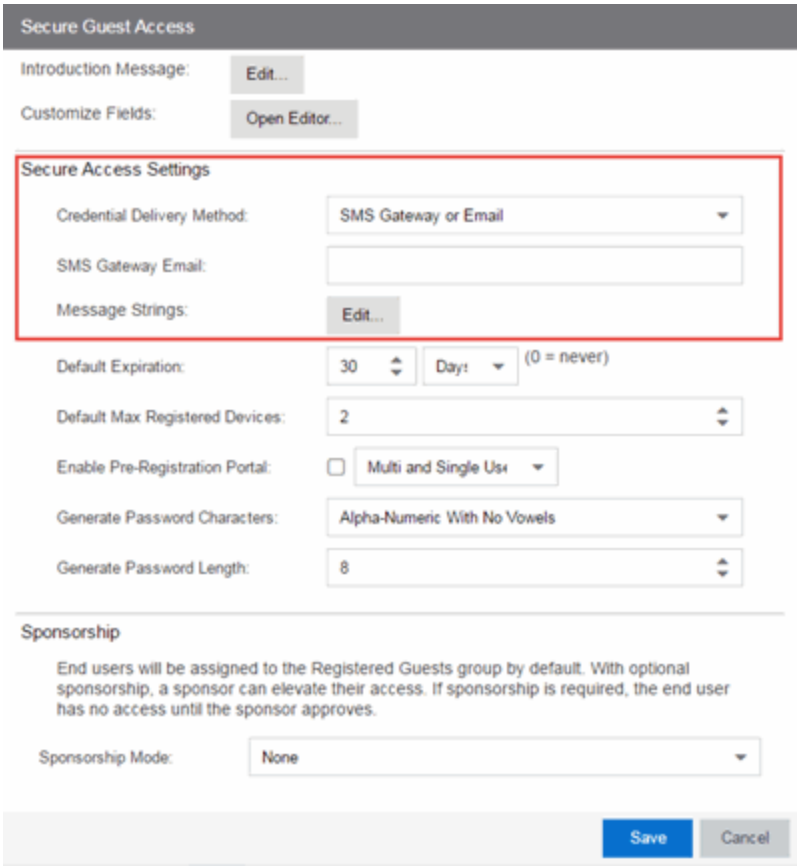
You can comment out entries by preceding each line with either a # or // to enable temporary editing of the file without removing the text.

The list requires one service provider entry per line, using the following format: <Provider>:phonenumber@<specificdomain>.

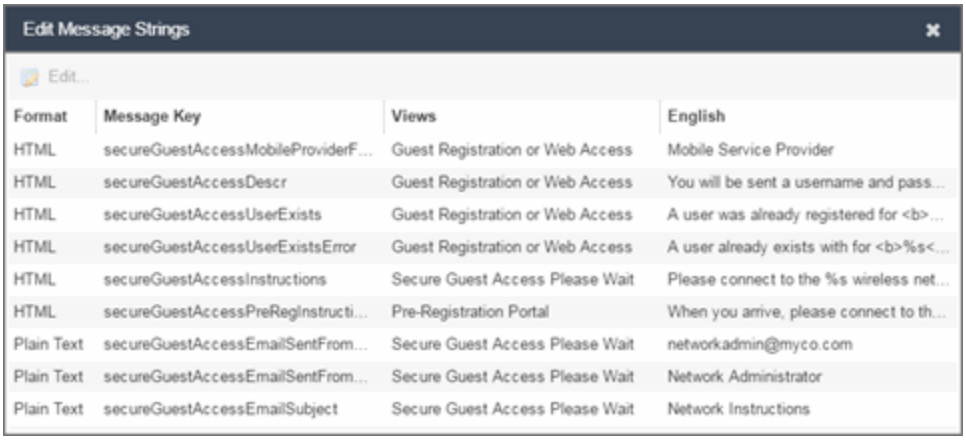
When the end user registers, they only see the <Provider> portion in the drop-down list of providers on the Registration web page.

Select **OK** to close the window.

4. If you have selected the **SMS Gateway** or **SMS Gateway or Email** method, enter the SMS Gateway Email address provided by the SMS Gateway provider.



5. For all methods, select the Message Strings **Edit** button to open the Message Strings Editor where you can customize the text displayed on the Registration web page and the messages sent to the end user.



You need to modify different message strings sent to the end user, depending on the delivery method or methods you selected. Double-click the message to open a window where you can edit the message text.

NOTE: When customizing message strings for text messaging (SMS Gateway or SMS Text Message) it is best to keep the message length as short as possible (under the maximum 160 characters limit). Some providers break long messages into multiple messages and other providers truncate the message, which could cause important information to be missing from the text message the guest receives.

- **Email** — This method uses the following strings:

  secureGuestAccessEmailMsgBody — the default message shouldn't need to be changed.

  secureGuestAccessEmailSentFromAddress — you need to change the default message to the appropriate email address for your company.

  secureGuestAccessEmailSentFromName — the default message shouldn't need to be changed.

  secureGuestAccessEmailSubject — the default message shouldn't need to be changed.

- **SMS Gateway** — Depending on your SMS Gateway provider and their required format, modify the following message strings using appropriate variables to customize the dynamic data such as phone number.

  secureGuestAccessSMSMsgBody

  secureGuestAccessSMSSubject

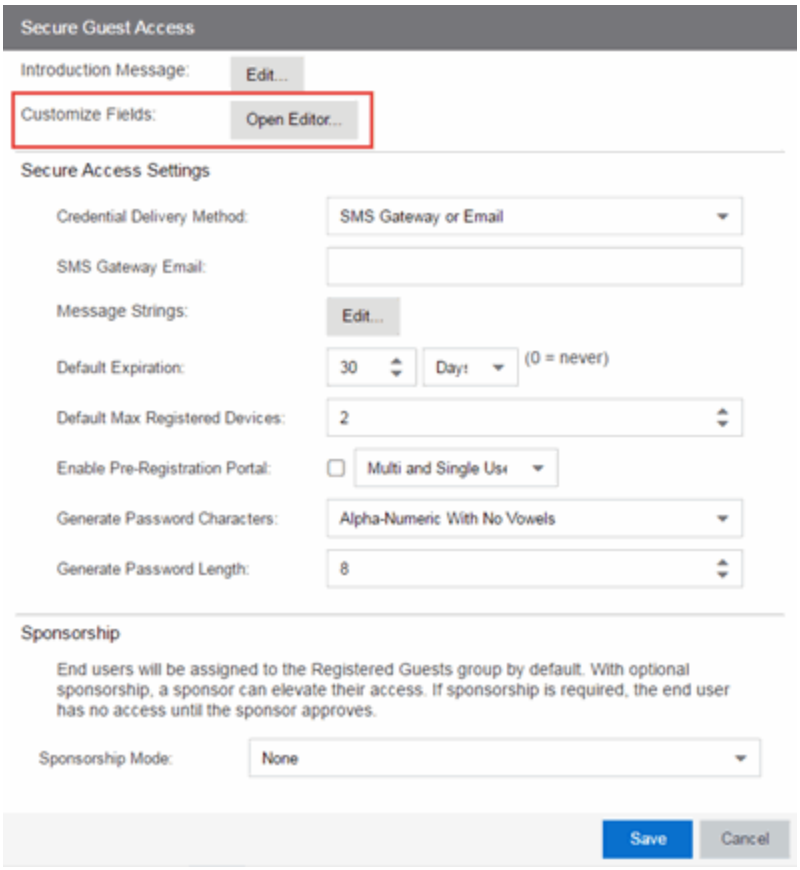
- **SMS Text Message** — This method uses the following strings. The default messages shouldn't need to be changed.

  secureGuestAccessSMSMsgBody

  secureGuestAccessSMSSubject

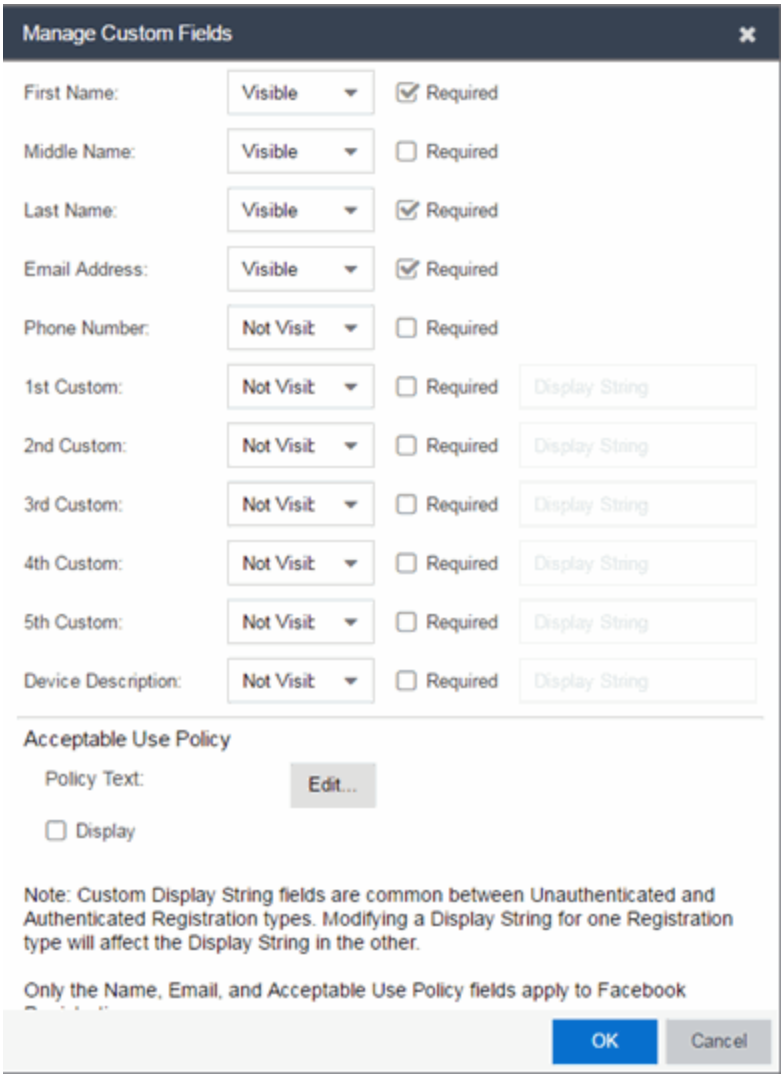
Select **OK** to close the window.

6. Select the Customize Fields **Open Editor** button to open the Manage Custom Fields window.



7. Set the appropriate custom fields to display on the Registration web page, depending on the delivery method you selected (refer to the table above). If you do not set these fields, ExtremeControl automatically sets them for you based on your delivery method.

   These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing them for one access type also changes them for the others. For more information, see the Manage Custom Fields Window.

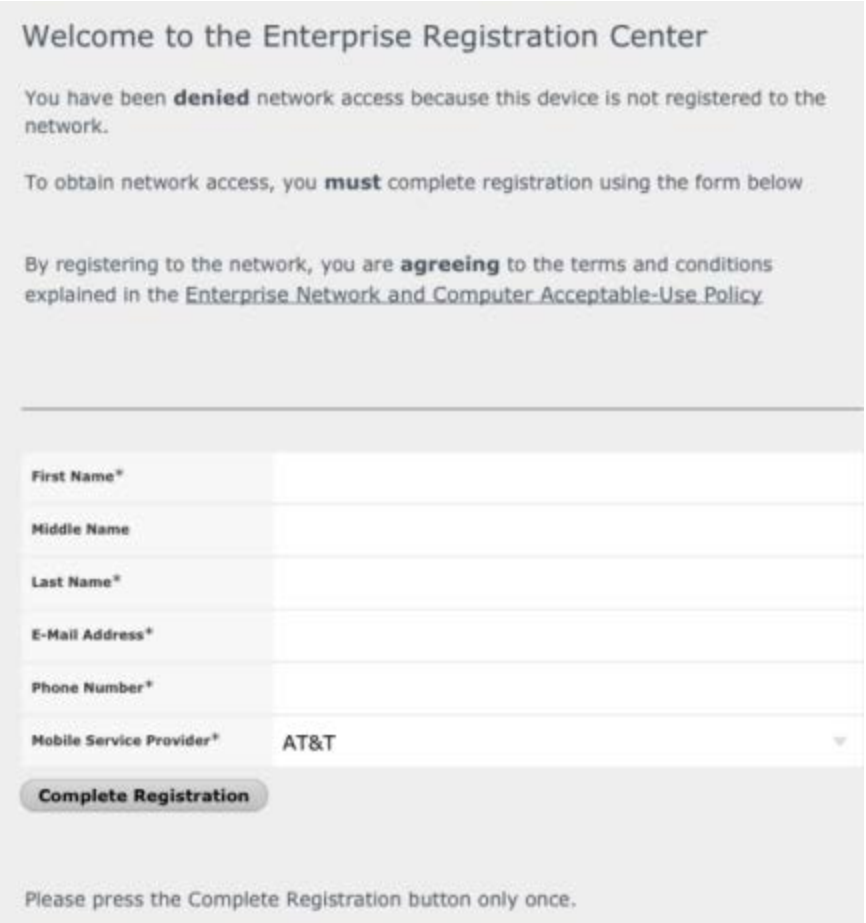


8. Select **OK** to close the window.
9. Back in the Portal Configuration, select **Save** to save your changes.
10. Enforce the new portal configuration to your engine(s).

    Credential delivery is now configured for your secure guest access.

How Secure Guest Access Works

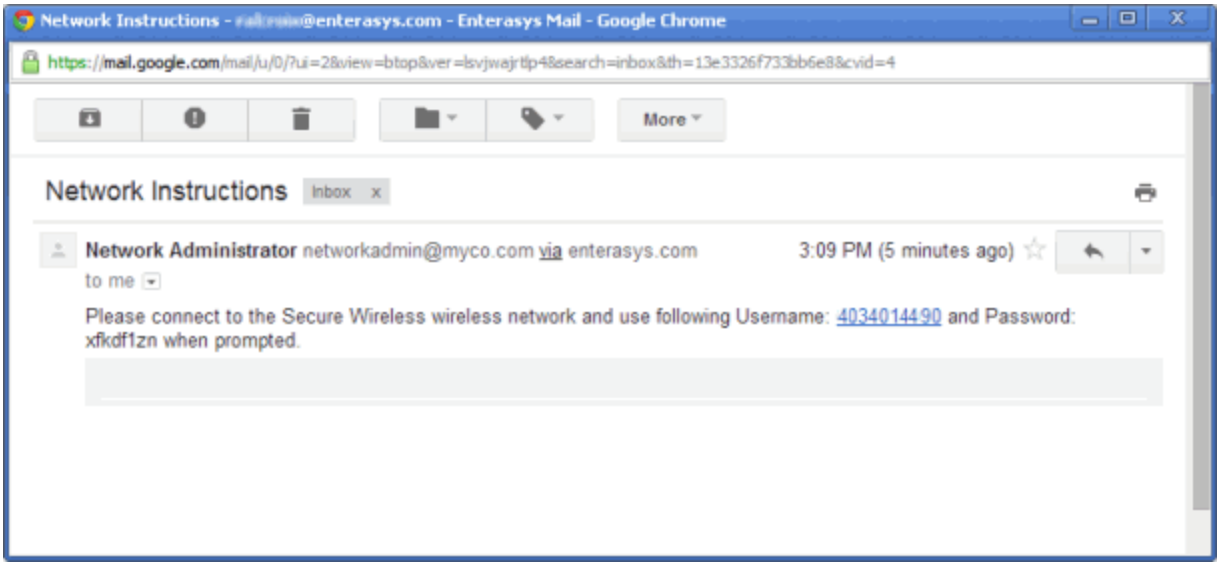
When a guest attempts to access the network, the Registration web page asks for their email address and/or phone number, and any other required/configured information.



When they select the Complete Registration button, they see the following screen that notifies them to check their email or phone for instructions on how to gain access to the network.



They are sent a username, password, and access instructions via an email or a phone text message.





When they connect to the Secure Wireless network, they will enter their username and password in this screen to gain access to the network.



For information on related help topics:

- Portal Configuration

How to Configure Verification for Guest Registration

Guest registration requires end users to enter their name and contact information on a Registration web page in order to gain access to the network. However, in many cases, end users provide false names and contact information because they don't want their personal information to be used for other purposes. In those cases, network administrators do not have a way to contact the user in the event of an Acceptable Use Policy (AUP) violation or in the case of an emergency.

With verification, guest end users registering to the network are required to enter a verification code that is sent to their email address or mobile phone (via SMS text) before gaining network access. This ensures that network administrators have at least one way to contact the end user.

Configuration Steps

The verification feature is supported for both Guest Registration and Guest Web Access, and is configured using the Verification Method options in your portal configuration. Depending on the verification method you specify, the appropriate custom fields must be configured for display on the Registration web page, so that end users can enter the required information.

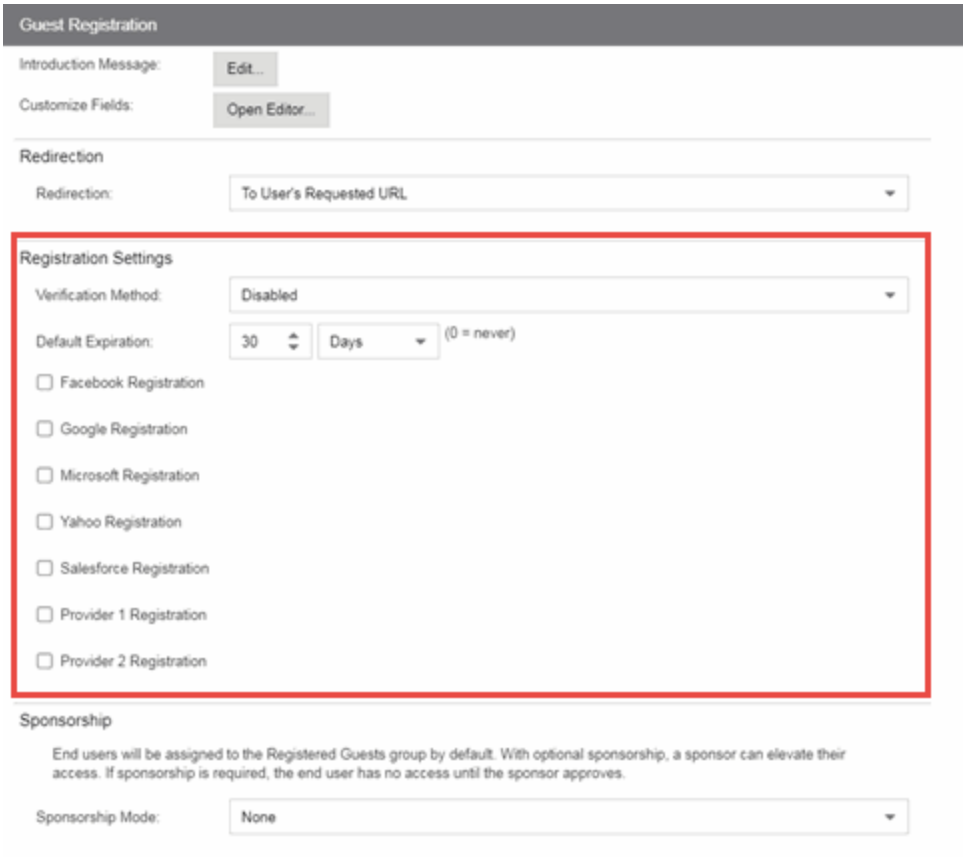
The following table provides a description of each verification method and lists their custom field requirements.

User Verification Method	Description	Custom Field Requirement
Email	The end user must enter a valid email address on the Registration web page or Guest Web Access login page.	The Email Address Custom Field must be set to **Required**.
SMS Gateway	The SMS Gateway provider must support SMTP API. The SMS Gateway provider converts the email to an SMS text message. The end user must enter a mobile phone number on the Registration web page or Guest Web Access login page.	The Phone Number Custom Field must be set to **Required**.

User Verification Method	Description	Custom Field Requirement
SMS Gateway or Email	The SMS Gateway provider must support SMTP API. The SMS Gateway provider converts the email to an SMS text message. The end user must enter a mobile phone number or email address on the Registration web page or Guest Web Access login page.	The Phone Number and Email Address Custom Fields must be set to **Visible**.
SMS Text Message	The mobile provider converts the email to an SMS test message. The end user must enter a valid mobile phone number on the Registration web page or Guest Web Access login page.	The Phone Number Custom Field must be set to **Required**.
SMS Text or Email	The mobile provider converts the email to an SMS test message. The end user must enter a valid mobile phone number or email address on the Registration web page or Guest Web Access login page.	The Phone Number and Email Address Custom Fields must be set to **Visible**.

Use the following steps to configure verification in your portal configuration.

1. In ExtremeCloud IQ Site Engine, access the Portal Configuration. Select the Guest Registration or Guest Web Access selection in the Portal tree, depending on what access type your network is using. (If you don't see these selections, select Website Configuration in the tree and enable the appropriate feature.)
2. In the Guest Registration or Guest Web Access panel, use the drop-down list to select the desired Verification Method (refer to the table above). The Guest Registration panel is shown below.



3. If you selected the **SMS Text Message** or the **SMS Text or Email User Verification** method, select the Service Providers link to configure the list of mobile service providers from which end users can select the Registration web page or Guest Web Access login page. The Mobile Service Provider List provides a default list of providers that can be edited to include the appropriate service providers for your geographic location.

   You can comment out entries by preceding each line with either a # or // to enable temporary editing of the file without removing the text.

   The list requires one service provider entry per line, using the following format: <Provider>:phonenumber@<specificdomain>.

   When the end user registers, they will see only the <Provider> portion in the drop-down list of providers on the Registration web page.

   Select **OK** to close the window.

4. If you have selected the **SMS Gateway** or **SMS Gateway or Email** method, enter the SMS Gateway Email address provided by the SMS Gateway provider.

5. For all methods, select the Message Strings link to open the Message Strings Editor where you can customize the text displayed on the Registration web page or Guest Web Access login page, and the messages sent to the end user.

   You need to modify different message strings sent to the end user, depending on the verification method or methods you selected. Double-click on the message to open a window where you can edit the message text.

   - **Email** - This method uses the following strings:

     registrationVerificationEmailMsgBody - the default message shouldn't need to be changed.

     registrationVerificationEmailSentFromAddress - you need to change the default message to the appropriate email address for your company.

     registrationVerificationEmailSentFromName - the default message shouldn't need to be changed.

     registrationVerificationEmailSubject - the default message shouldn't need to be changed.

   - **SMS Gateway** - Depending on your SMS Gateway provider and their required format, modify the following message strings using appropriate variables to customize the dynamic data such as phone number.

     registrationVerificationSMSMsgBody

     registrationVerificationSMSSubject

   - **SMS Text Message** - This method uses the following strings. The default messages shouldn't need to be changed.

     registrationVerificationSMSMsgBody

     registrationVerificationSMSSubject

   Select OK to close the window.

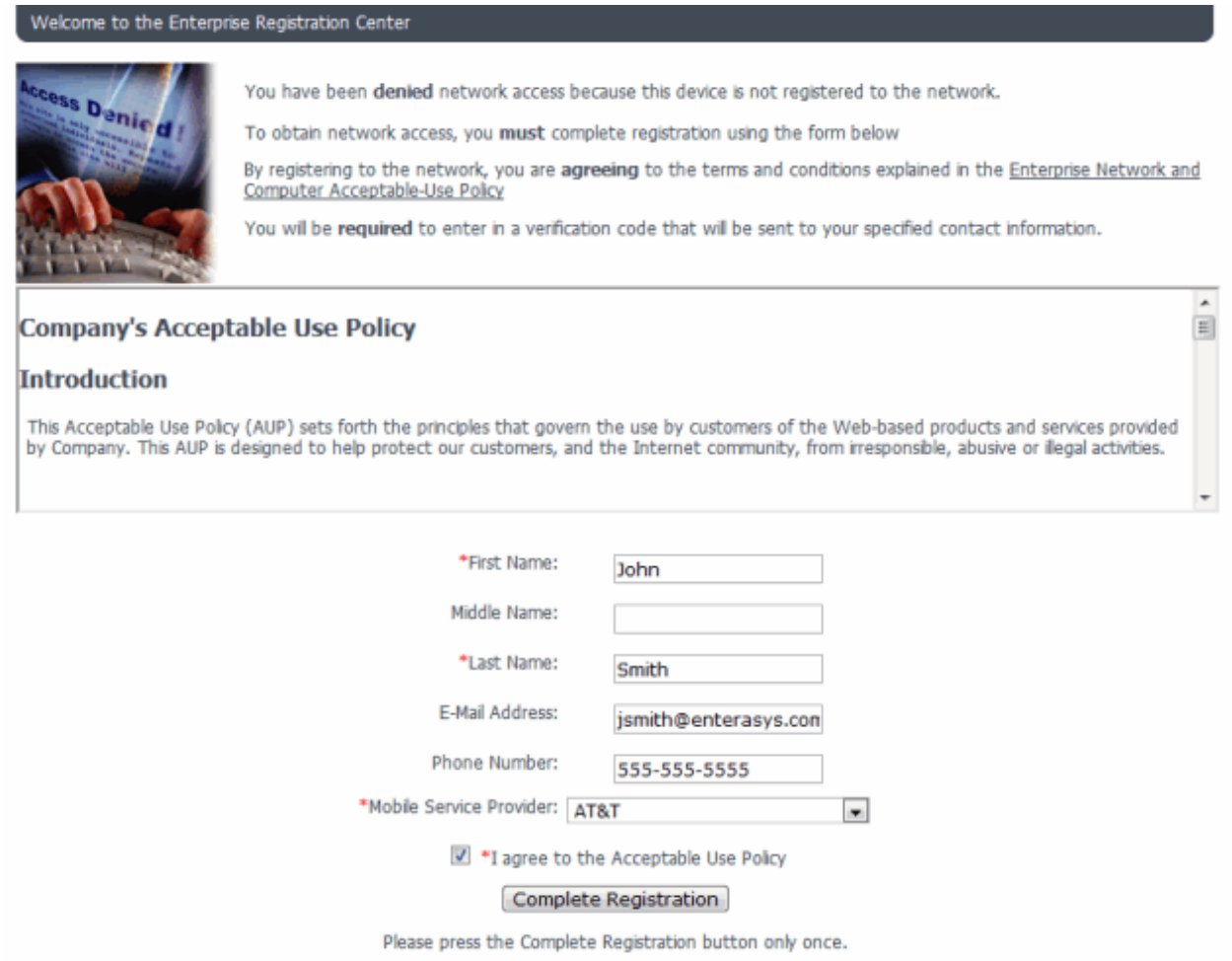
6. In the Web Page Customizations (Shared) section, select the Customize Fields link to open the Manage Custom Fields window.
7. Set the appropriate custom fields to display on the Registration web page or Guest Web Access login page, depending on the verification method you selected (refer to the table above). When you save your portal changes, the correct configuration of the custom fields are verified. These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing them for one access type also changes them for the others. For more information, see the Manage Custom Fields Window.

   Select **OK** to close the window.

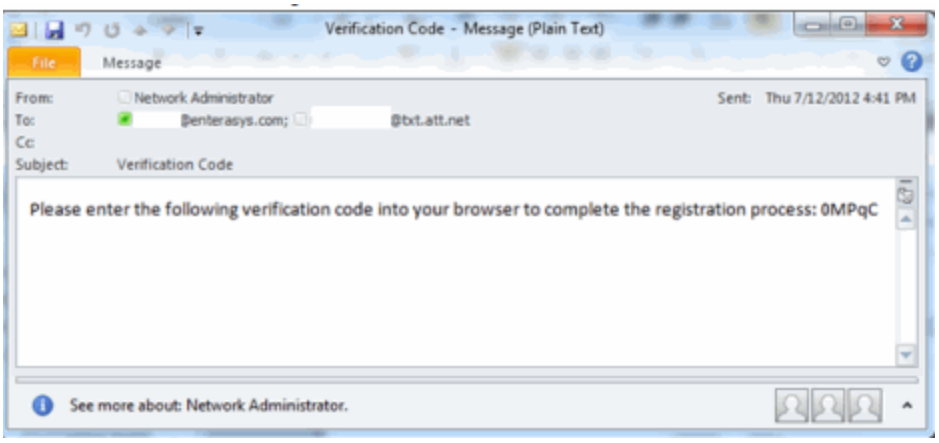
8. Back in the Portal Configuration, select **Save** to save your changes. Close the Portal Configuration window. Enforce the new portal configuration to your engine(s). Verification is now configured for your guest registration.

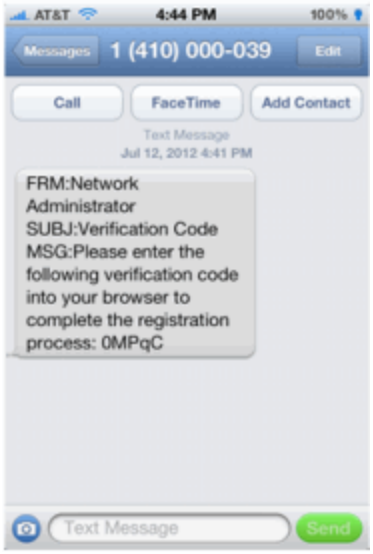
How User Verification Works

When a guest attempts to access the network, the Registration web page or Guest Web Access login page asks for their email address and/or phone number and mobile service provider, along with their normal contact information.

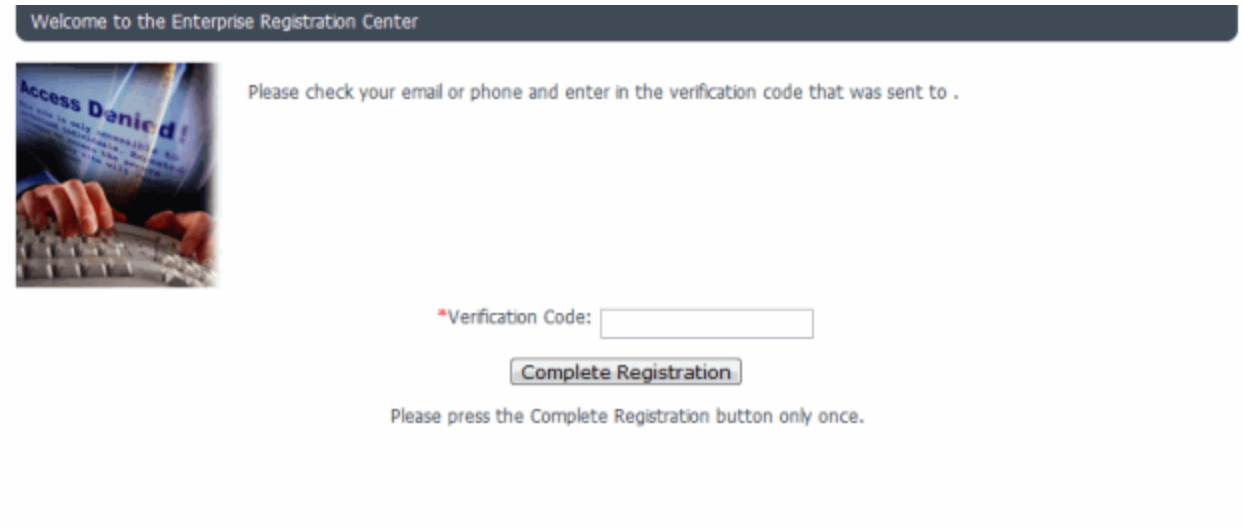


When they select the Complete Registration button, they are sent a verification code via an email or a phone text message.





The web page then prompts them for the code. When they enter the correct code that was generated for them and select the **Complete Registration** button, they are permitted access to the network. The verification code is valid for 15 minutes and cannot be reused after it is validated.


Welcome to the Enterprise Registration Center
Please check your email or phone and enter in the verification code that was sent to .
*Verification Code:
Complete Registration
Please press the Complete Registration button only once.

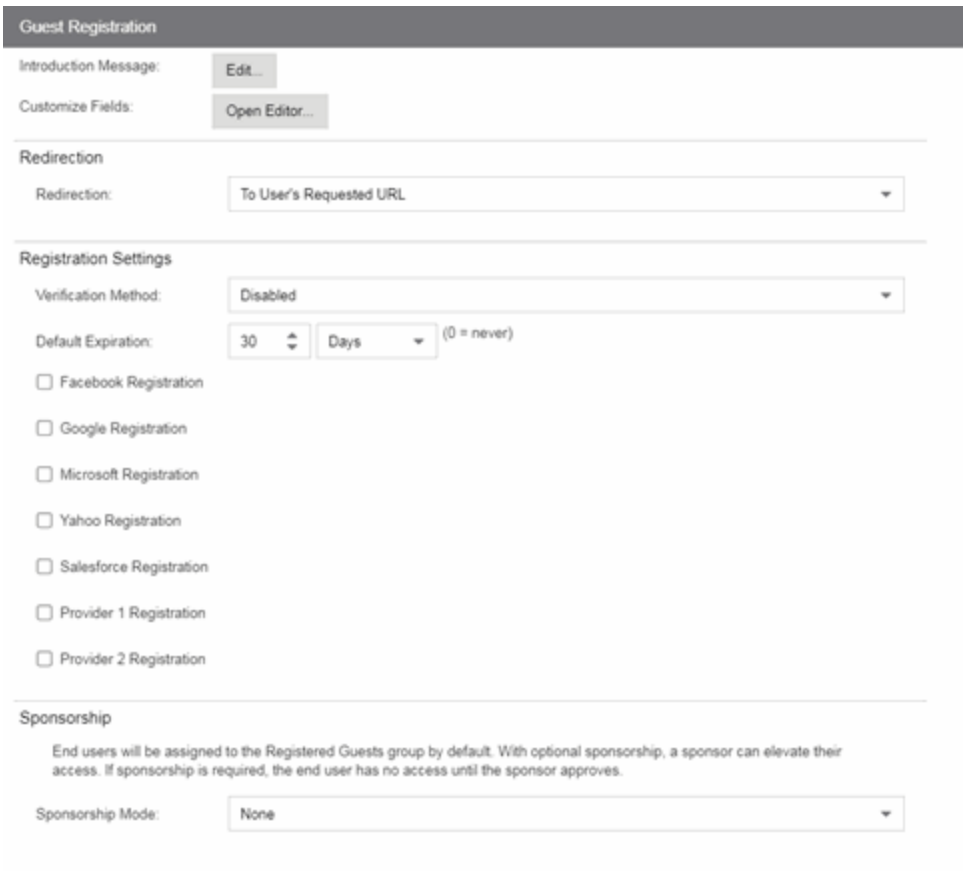
Configure Sponsorship for Guest Registration

This topic describes how to configure sponsorship for Guest Registration and Secure Guest Access. Sponsorship is configured as part of your portal configuration, and is accessed from the Guest Registration and Secure Guest Access views in the Portal section of the Portal Configuration panel.

With sponsored registration, end users are only allowed to register to the network when approved by a "sponsor," an internal trusted user to the organization. Sponsorship can provide the end user with a higher level of access than just guest access and allows the sponsor to fine-tune the level of access for individual end users. The end user registers and declares a sponsor's email address. The sponsor is notified and approves the registration, and can assign an elevated level of access, if desired.

To configure sponsorship:

1. Access the **Control** > **Access Control** tab.
2. In the left-panel tree, expand the **Access Control** Configurations > Portal and select the Guest Registration view or the Secure Guest Access view (depending on the access type you are configuring). The screenshot below shows the Guest Registration view.



3. In the Sponsorship section, select the **Sponsorship Mode** required. Additional settings display when you select optional or required sponsorship.
    - **None** - Sponsorship is not required and the end user is assigned to the Registered Guests End-System Group.
    - **Optional** - The end user is assigned to the Registered Guests End-System Group until sponsored. At that time, the sponsor can assign elevated access, if desired.
    - **Required** - The end user has no access until the sponsor approves the registration. The end user is added to the Registration Pending Access end-system group and is presented the sponsorship pending page until approved.
4. **Sponsored Registration Introduction** - Select the **Edit** button to open a window where you can edit the introductory message displayed to the end user.
5. **Admin/Sponsor Email** - Enter the person or group to notify when an end user requests sponsorship, typically the network ExtremeControl administrator, for example "IT@CompanyA.com." This email address is always notified, in addition to the sponsor email address entered by the end user when they register to the network.
6. **Sponsor Email Field** - Select an option for the sponsor email field on the registration web page.
    - **Do Not Display** - The field is not displayed, and the end user is not required to enter a sponsor email address. In this case, only the admin/sponsor email address (defined above) is notified when the end user registers.
    - **Display Predefined Sponsor List** - The end user must select a sponsor email from a list of predefined sponsors (defined below). The end user sees a drop-down list of sponsor email addresses and select the appropriate sponsor.
    - **User Specifies Any Email as Sponsor** - The end user can enter any email address as a sponsor's email address.
    - **User Must Specify Predefined Sponsor Email** - The end user must enter an email address that matches one of the predefined sponsors (defined below).
7. **Predefined Sponsors** - Enter one or more sponsor email addresses. If you have selected **Display Predefined Sponsor List** as your Sponsor Email Field option (above), these addresses are presented to the end user as a drop-down list, allowing them to select a sponsor email address. If you have selected **User Must Specify Predefined Sponsor Email** as your Sponsor Email Field option, then the sponsor email address entered by the end user must match an email address listed here. Email addresses can be separated by semi-colons (;) or commas (,) for example, jdoe@CompanyA.com;rsmith@CompanyA.com. Because commas are accepted separators, they should not be used in actual email addresses.
8. In the Portal Configuration window, select **Save** to save your changes. You need to enforce the new portal configuration to your engine(s).

For information on related help topics:

- Portal Configuration

How to Implement Facebook Registration

This Help topic describes the steps for implementing guest registration using Facebook as a way to obtain end user information.

In this scenario, the Guest Registration portal provides the option to register as a guest or log into Facebook in order to complete the registration process. If the end user selects the Facebook option, ExtremeCloud IQ Site Engine OAuth to securely access the end user's Facebook account, obtain public end user data, and use that data to complete the registration process.

NOTE: Guest OAuth (for example, Google, Yahoo) may not support native mobile browsers and display a “user agent” error. To access the network, use a standard browser application (e.g. Google Chrome).

Guest Registration using Facebook has two main advantages:

- It provides ExtremeCloud IQ Site Engine with a higher level of user information by obtaining information from the end user's Facebook account instead of relying on information entered by the end user.
- It provides an easier registration process for the end user. ExtremeCloud IQ Site Engine retrieves the public information from the end user's Facebook account and uses that information to populate the name and email registration fields.

This topic includes information and instructions on:

- Requirements for Facebook Registration
- Creating a Facebook Application
- Portal Configuration for Facebook
- How Facebook Registration Works
- Special Deployment Considerations
    - Networks using DNS Proxy

Requirements

These are the configuration requirements for Facebook Registration.

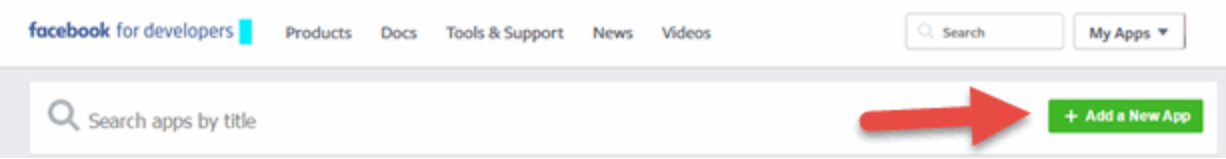
- The ExtremeControl engine must have Internet access in order to retrieve user information from Facebook.
- The Access Control Unregistered access policy must provide access to the Facebook site (either enable all SSL or make allowances for Facebook servers).

- A Unique Facebook application must be created on the Facebook Developers page (see instructions below).
- The Portal Configuration must have Facebook Registration enabled and include the Facebook Application ID and Secret (see instructions below).

Creating a Facebook Application

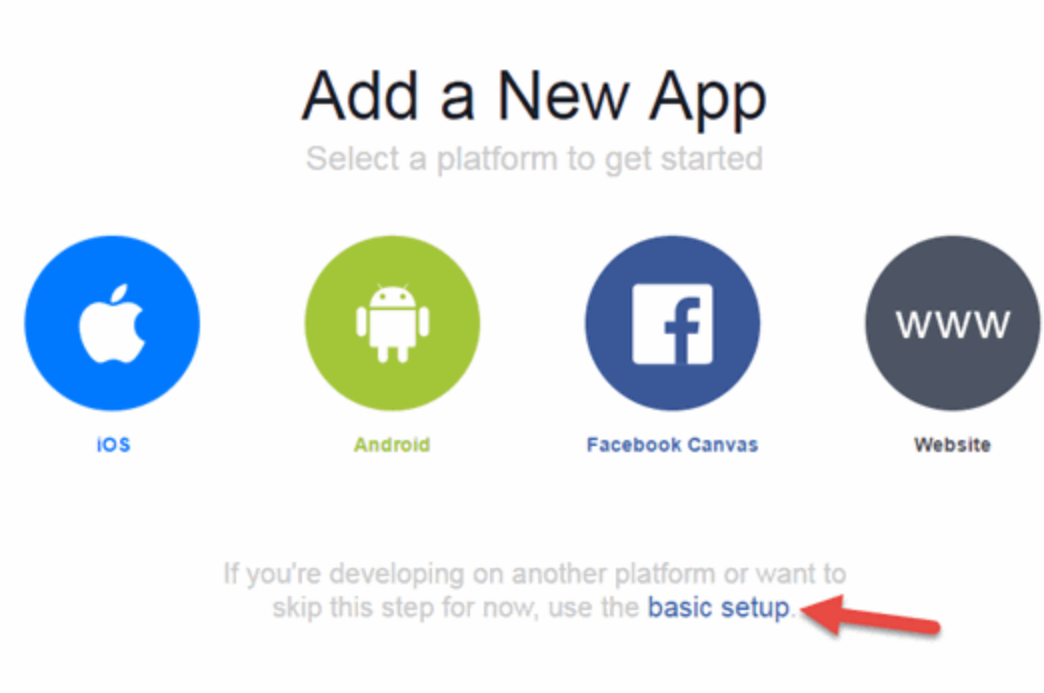
When implementing guest registration using Facebook, you must first create a Facebook application. This generates an Application ID and Application Secret that are required as part of the ExtremeCloud IQ Site Engine OAuth process. Use the following steps to create a Facebook application.

1. Access the Facebook Developers page at https://developers.facebook.com/apps/. If you already have a Developers account you can log in, otherwise you must create a Developers account.
2. When logged in, select the **Add a New App** button.



The Add a New App window opens.

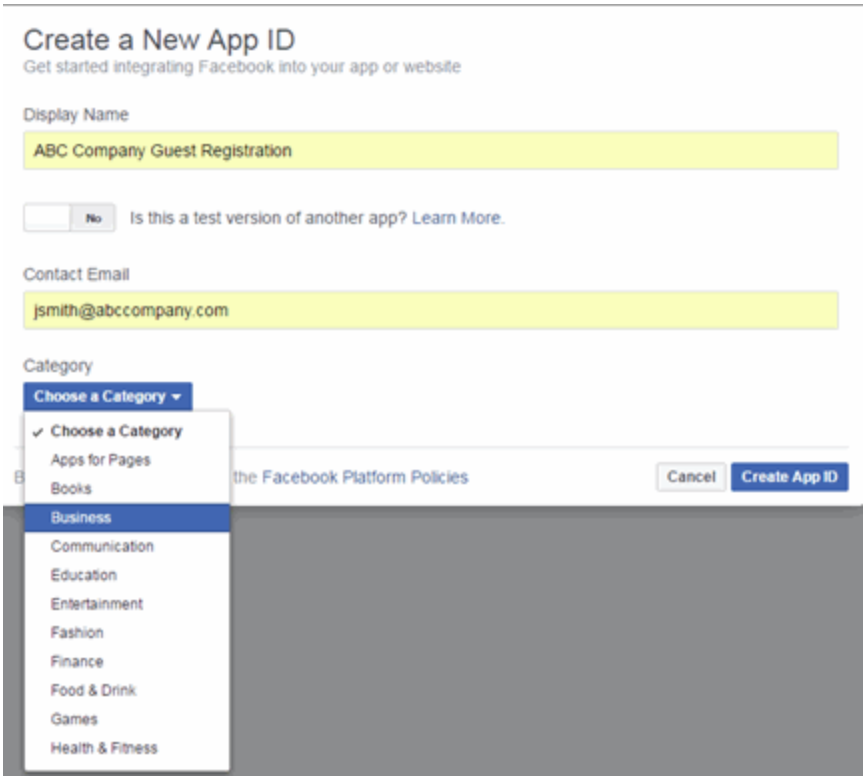
3. Select the **basic setup** link at the bottom of the window.



The Create a New App ID window opens.

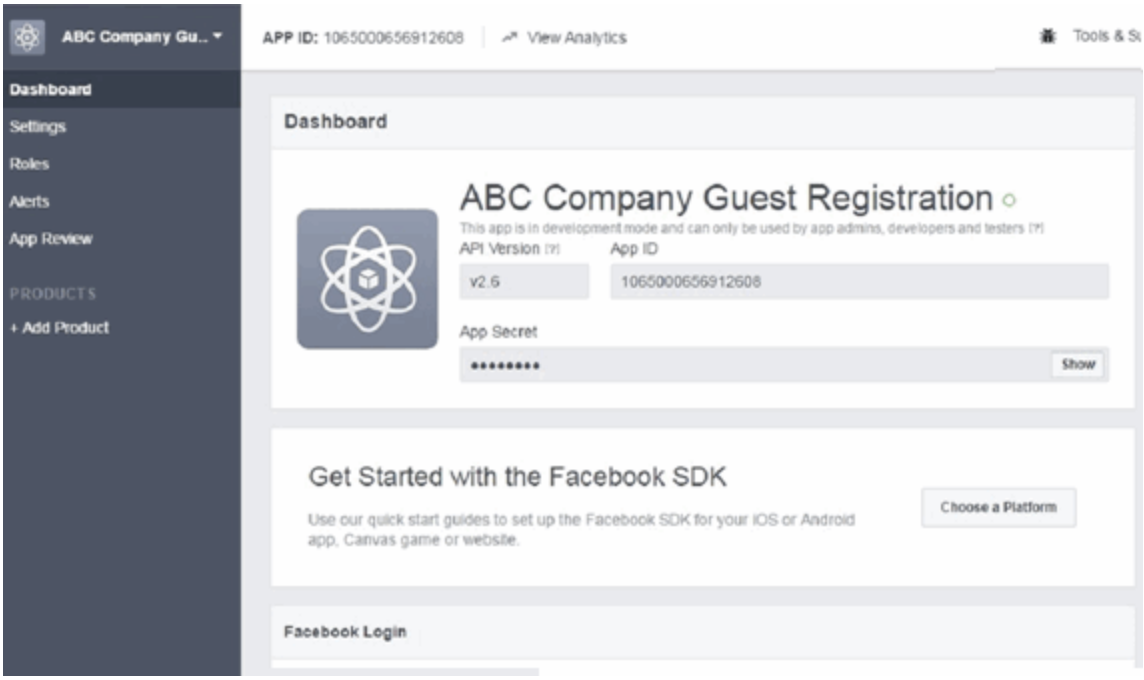
4. Enter a **Display Name**, enter a **Contact Email**, and select a **Category** for your app.

   The **Display Name** is the name of the app presented to the end-user when they grant ExtremeCloud IQ Site Engine access to their Facebook information and should clearly indicate what its purpose is, for example, Extreme Networks Guest Registration.



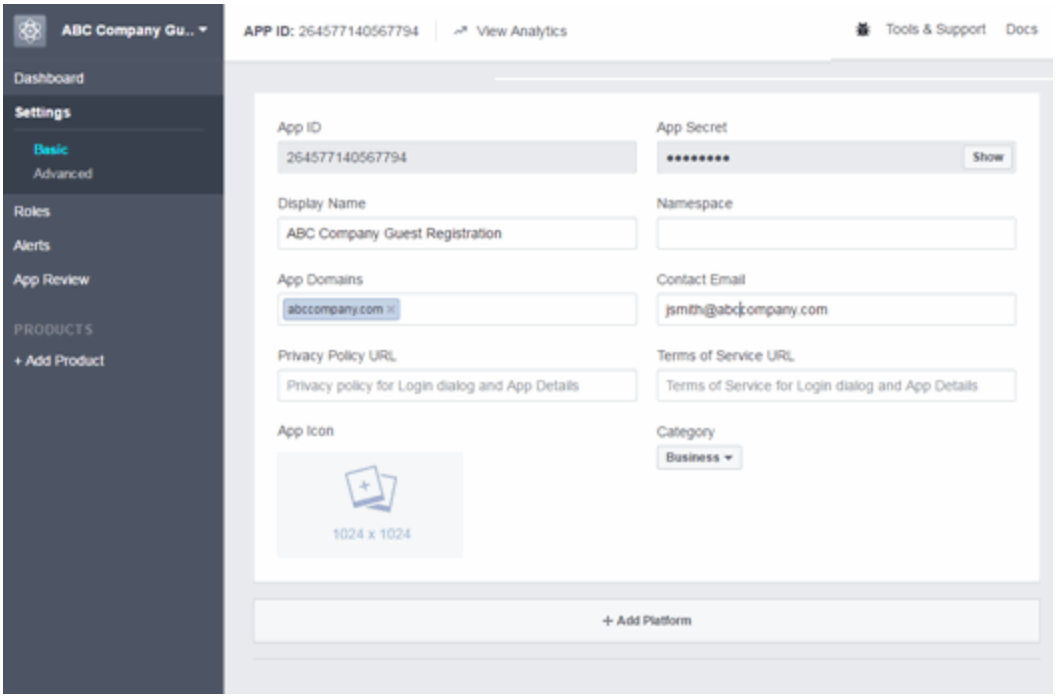
5. Select **Create App ID**.

   The Dashboard panel opens and displays information about the new app including an App ID and an App Secret.



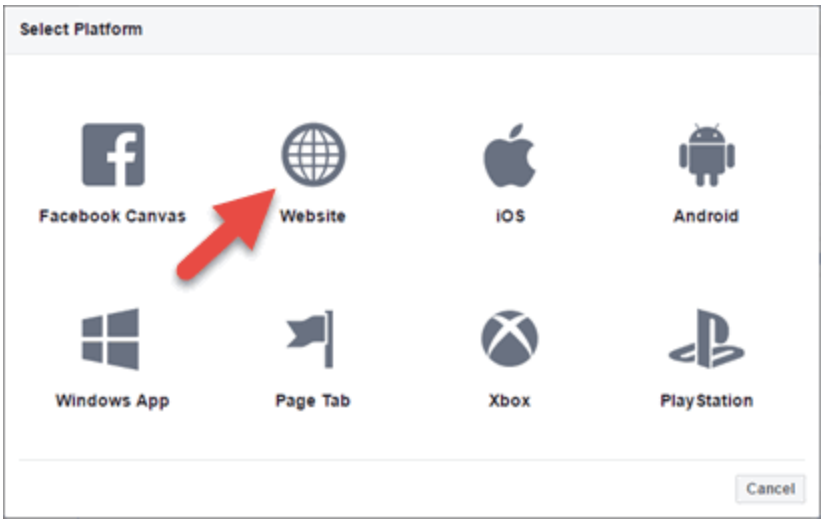
6. Select **Settings** in the left panel.

   The Settings panel's **Basic** tab opens.



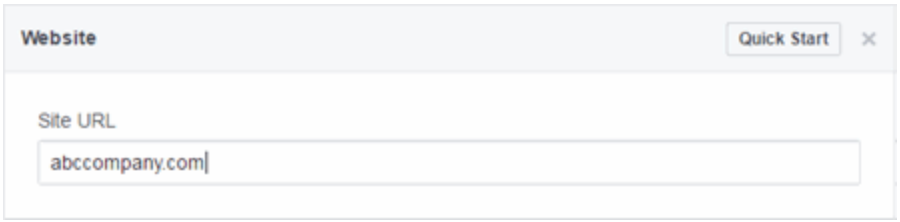
7. Enter in a valid domain name for the ExtremeControl engines in the **App Domains** field. For example, if the Access Control engine to which users are connecting is Access Control engine.AbcCompany.com, enter "abccompany.com" in the **App Domains** field.
8. Select **Add Platform**.

   The Select Platform window opens.



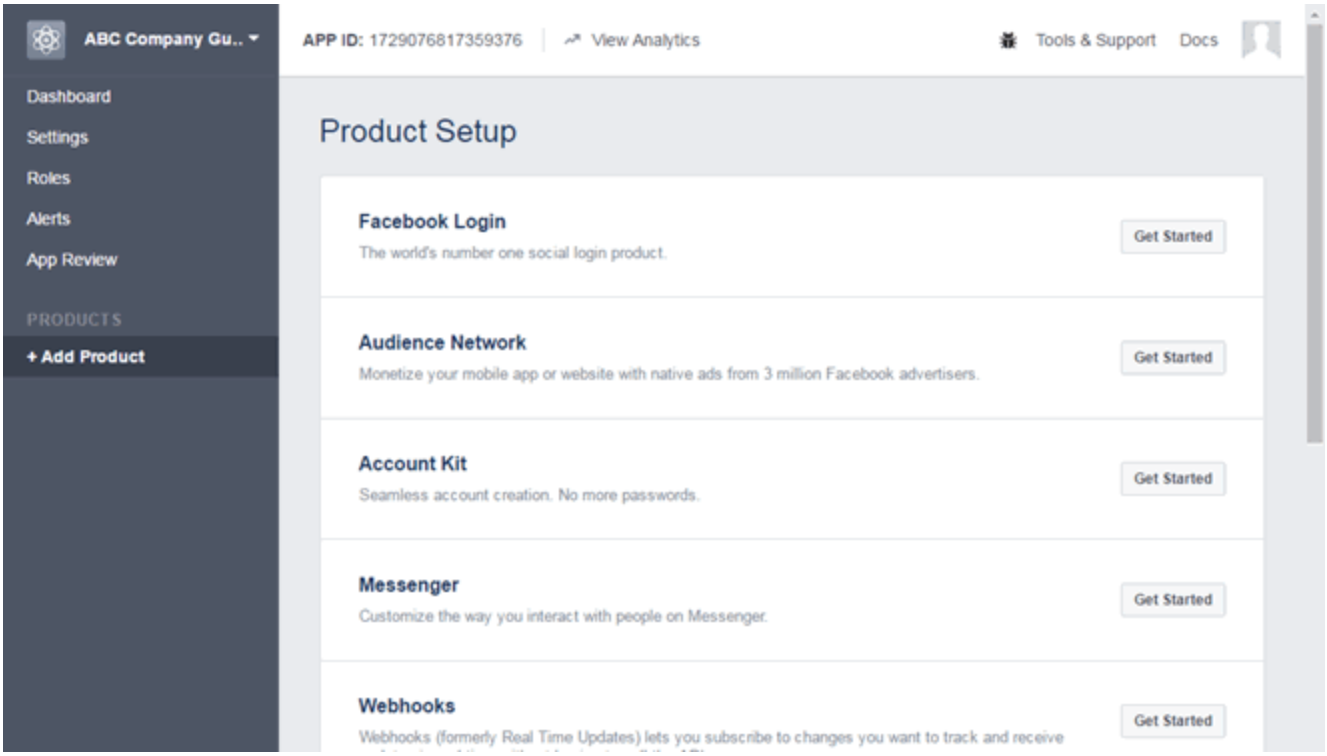
9. Select **Website**.

   The Website panel displays on the **Basic** tab.



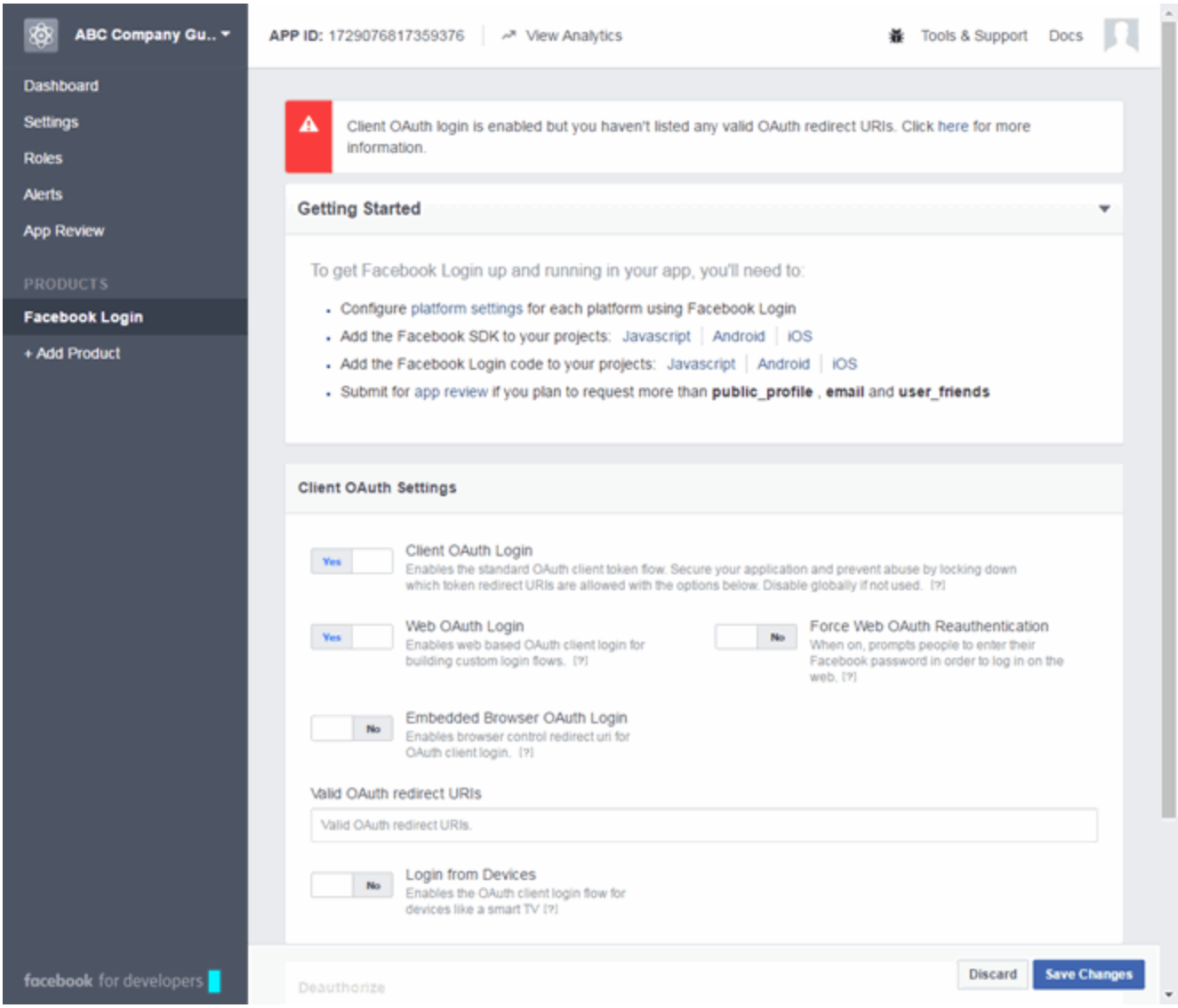
10. Enter the domain name you added in the **App Domains** field in step 7 in the **Site URL** field.
11. Select **Save Changes**.
12. Select **Add Product** in the left panel.

    The Product Setup panel opens.



13. Select the Facebook Login **Get Started** button.

    The Getting Started panel opens.



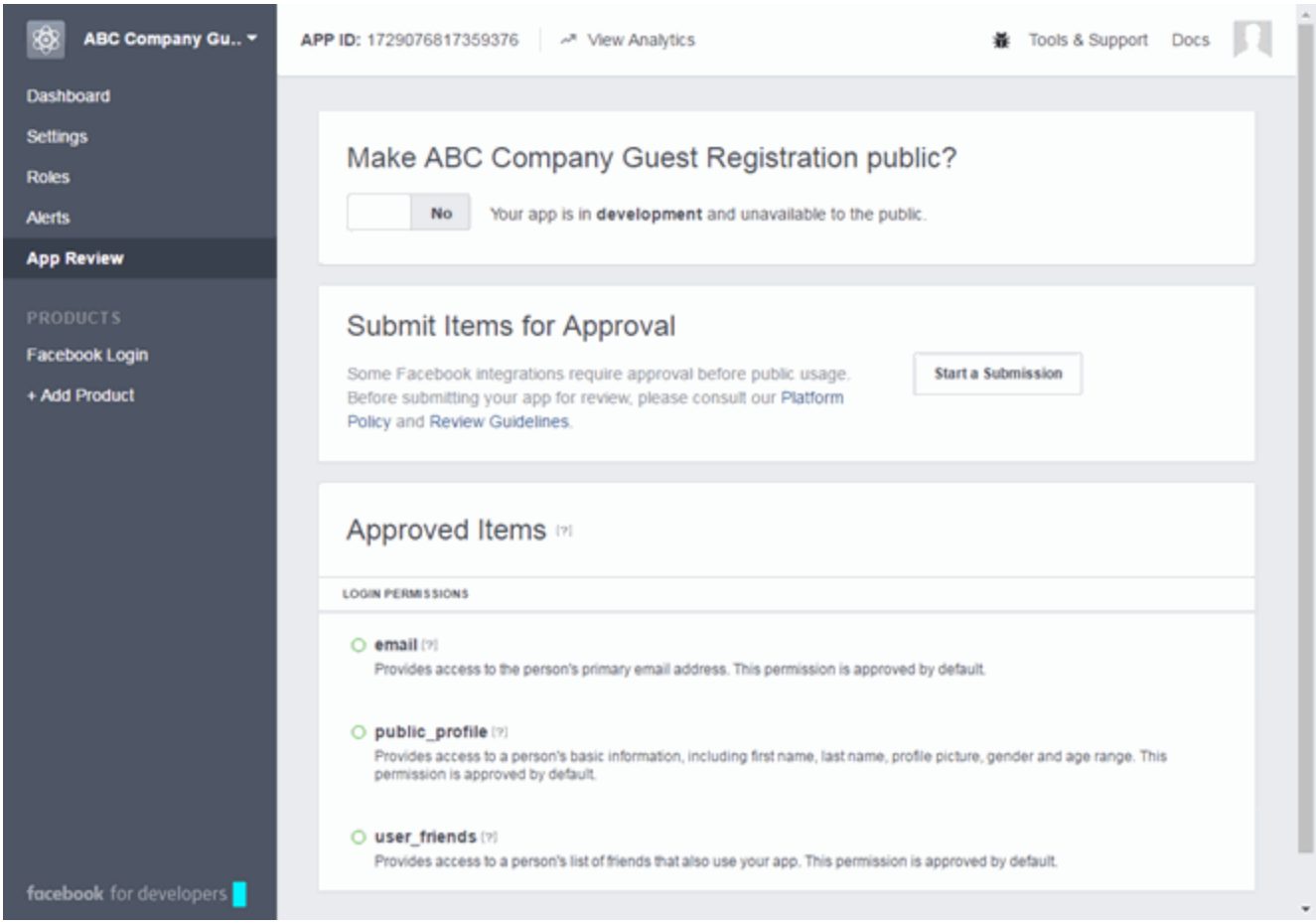
14. Enter the **Valid OAuth redirect URIs**. A redirect URI is required to redirect the user back to the engine with an Access Token ExtremeCloud IQ Site Engine uses to access the user account and retrieve the user data. The Redirection URI should be in the following format:

    https://<Access ControlengineFQDN>/fb_oauth

    A Redirection URI must be added for each Access Control engine where end users can register via Facebook.

15. Select **Save Changes**.
16. Select **App Review** in the left panel.

    The App Review panel opens.



17. Select the **No** button in the **Make *<Display Name>* public** field to change the button to **Yes**.

    A Confirmation window displays.

18. Select **Confirm**.

    The Approved Items section displays a list of default permissions that provide access to end user data. (For more information on setting permissions, see https://developers.facebook.com/docs/facebook-login/permissions#reference.)

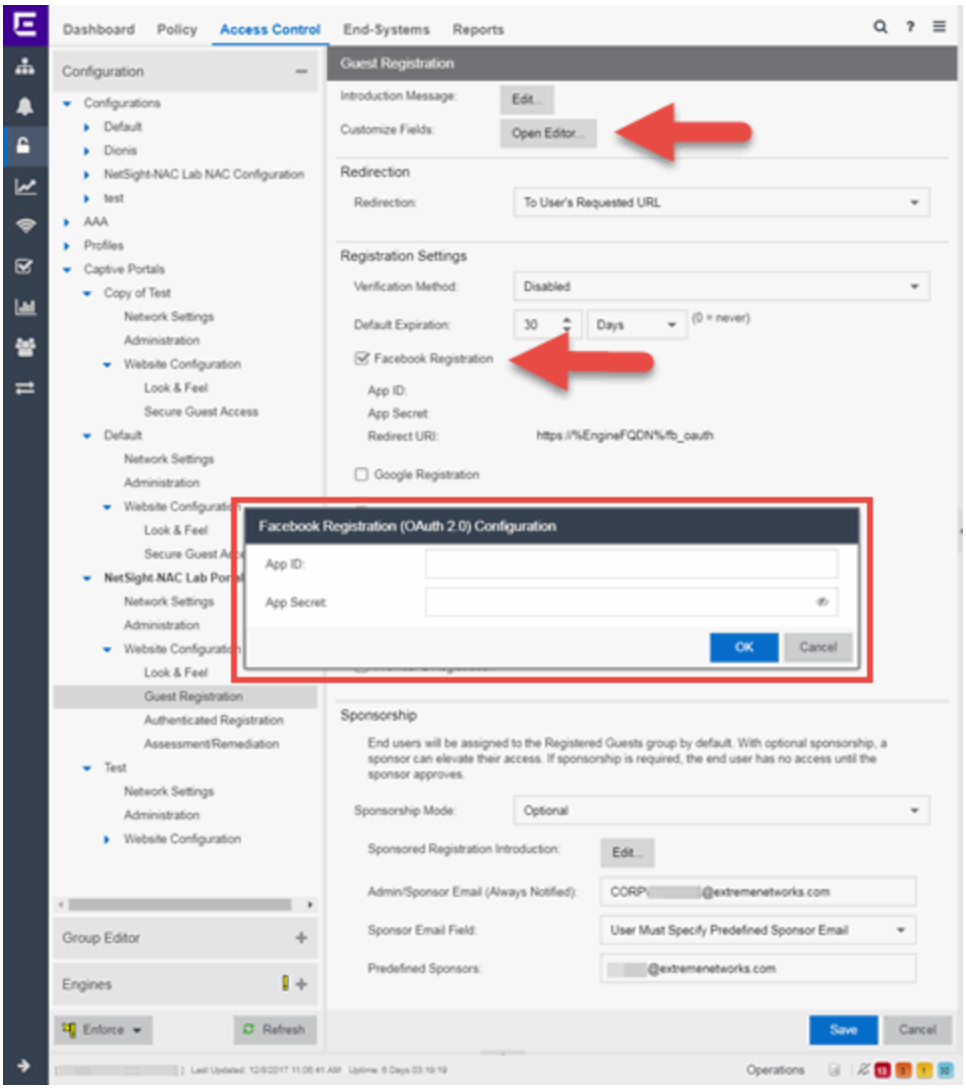
    Your application is created and ready to use.

    You need to add the App ID and App Secret to your portal configuration.

Portal Configuration

The Application ID and Application Secret assigned during the creation of the Facebook application must be provided in the Portal Configuration in order for the entire process to complete properly.

1. Open the **Control** > **Access Control** tab.
2. In the left-panel tree, expand the Access Control Configurations > Portal tree and select Guest Registration.



3. In the Customize Fields section, select the **Open Editor** button to open the Manage Custom Fields window where you can change registration portal fields. Facebook registration uses only the First Name, Last Name, and Email Address fields, and the Display Acceptable Use Policy (AUP) option. All other fields only apply to regular guest registration. If the Display AUP option is selected, the captive portal verifies that the AUP has been acknowledged before redirecting the user to Facebook.
4. Select the Facebook Registration checkbox.
5. Enter the Facebook App ID and Facebook App Secret.

6. Select **Save**. Warning messages display stating that Verification Method and Sponsorship are not used for Facebook registration, and that an FDQN is required will be enabled.
7. Enforce the new configuration to your engines.

How Facebook Registration Works

After you have configured Facebook registration using the steps above, this is how the registration process works:

1. The end user attempts to access an external Web site. Their HTTP traffic is redirected to the captive portal.
2. In the Guest Registration Portal, the end user selects the option to register using Facebook.
3. The end user is redirected to the Facebook login. If Acceptable Use Policy option is configured, the captive portal verifies that the AUP has been acknowledged before redirecting the user to Facebook.
4. When logged in, the end user is presented with the information that ExtremeCloud IQ Site Engine receives from Facebook.
5. The end user grants ExtremeCloud IQ Site Engine access to the Facebook information and is redirected back to the captive portal where they see a "Registration in Progress" message.
6. Facebook provides the requested information to ExtremeCloud IQ Site Engine, which uses it to populate the user registration fields.
7. The registration process completes and network access is granted.
8. The word "Facebook" is added to the user name so you can easily search for Facebook registration via the Registration Administration web page.

Special Deployment Considerations

Read the following deployment consideration prior to configuring Facebook Registration.

Wireless Clients

To provide access to your network via a wireless connection, create an L7 host record for the **Unregistered Role** on your Wireless Controller for `facebook.com`. This domain is subject to change and can vary based on location.

Networks using DNS Proxy

Facebook Registration for networks redirecting HTTP traffic to the captive portal using DNS Proxy requires additional configuration.

In order for Facebook Registration to work properly with DNS Proxy, **all** domains/URLs necessary to properly load the Facebook web page must be added to the Allowed URLs/Allowed Domains section of the captive portal configuration. Otherwise, the ExtremeControl engine resolves DNS queries for these components to the Access Control engine IP causing the page to not load properly.

As of July 26, 2014, you must add the following domains in order for Facebook registration to work with DNS Proxy. These domains are subject to change and can vary based on location.

Facebook.com
fbstatic-a.akamaihd.net
fbcdn-profile-a.akamaihd.net
fbcdn-photos-c-a.akamaihd.net

- Portal Configuration

How to Implement Google Registration

This Help topic describes the steps for implementing guest registration using Google as a way to obtain end user information.

In this scenario, the Guest Registration portal provides the option to register as a guest or log into Google in order to complete the registration process. If the end user selects the Google option, ExtremeCloud IQ Site Engine OAuth to securely access the end user's Google account, obtain public end user data, and use that data to complete the registration process.

NOTE: Guest OAuth (for example, Google, Yahoo) may not support native mobile browsers and display a "user agent" error. To access the network, use a standard browser application (e.g. Google Chrome).

Guest Registration using Google has two main advantages:

- It provides ExtremeCloud IQ Site Engine with a higher level of user information by obtaining information from the end user's Google account instead of relying on information entered by the end user.
- It provides an easier registration process for the end user. ExtremeCloud IQ Site Engine retrieves the public information from the end user's Google account and uses that information to populate the name and email registration fields.

This topic includes information and instructions on:

- Requirements for Google Registration
- Creating a Google Application
- Portal Configuration for Google
- How Google Registration Works
- Special Deployment Considerations
    - Networks using DNS Proxy

Requirements

These are the configuration requirements for Google Registration.

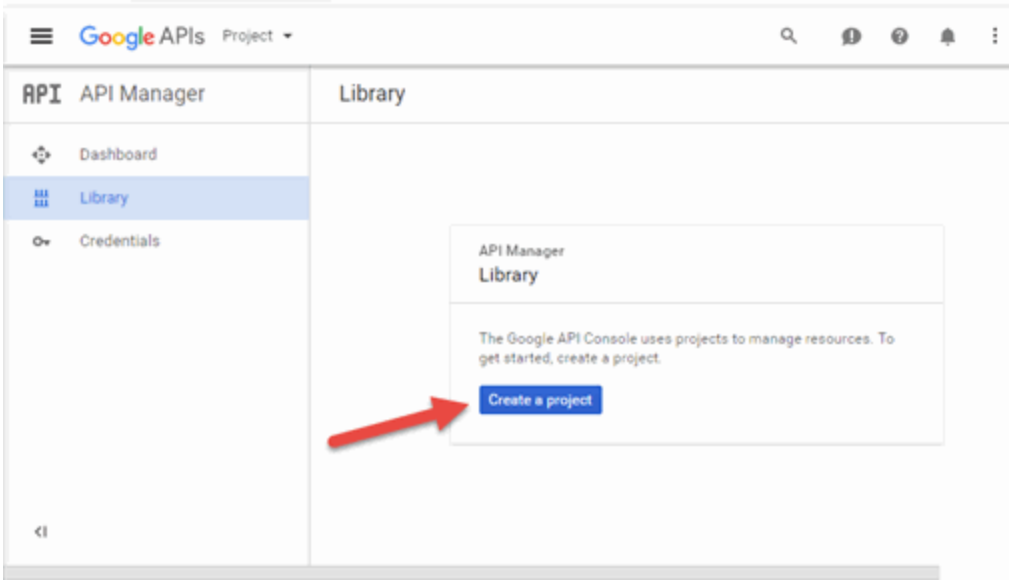
- The ExtremeControl engine must have Internet access in order to retrieve user information from Google.
- The Access Control Unregistered access policy must allow access to the Google site (either allow all SSL or make allowances for Google servers).

- The Access Control Unregistered access policy must allow access to HTTPS traffic to the Google OAuth servers.
- A Unique Google application must be created on the Google Developers page (see instructions below).
- The Portal Configuration must have Google Registration enabled and include the Google Application ID and Secret (see instructions below).

Creating a Google Application

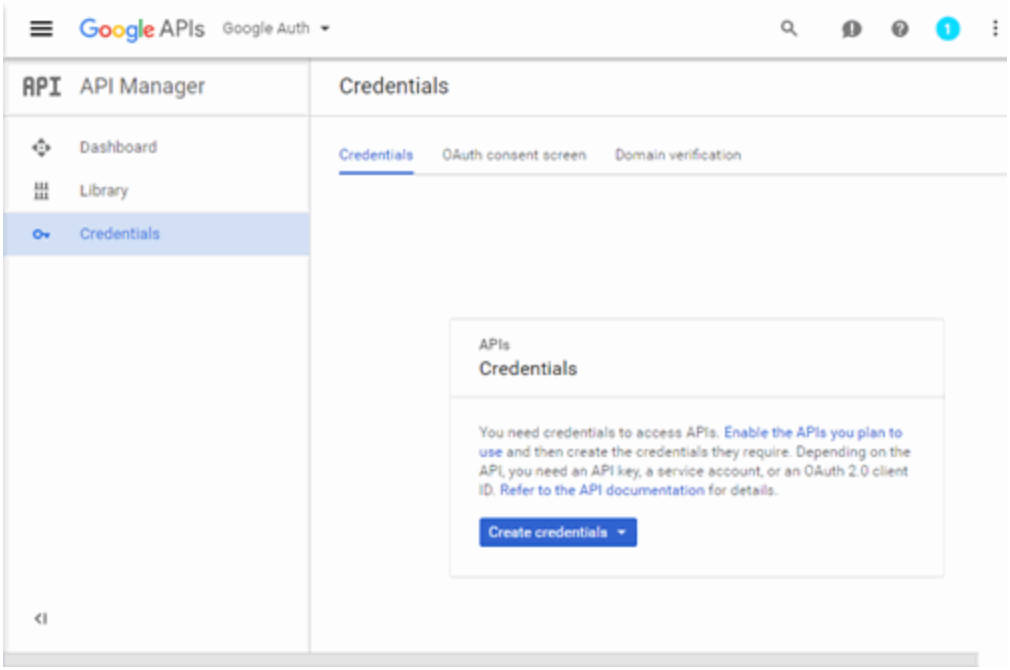
When implementing guest registration using Google, you must first create a Google application. This generates an Application ID and Application Secret that are required as part of the ExtremeCloud IQ Site Engine OAuth process. Use the following steps to create a Google application.

1. Access the Google Developers page at https://console.developers.google.com/projectselector/apis/library.
2. Log into your existing Developers account or create a new Developers account.
3. Select the **Create a project** button.



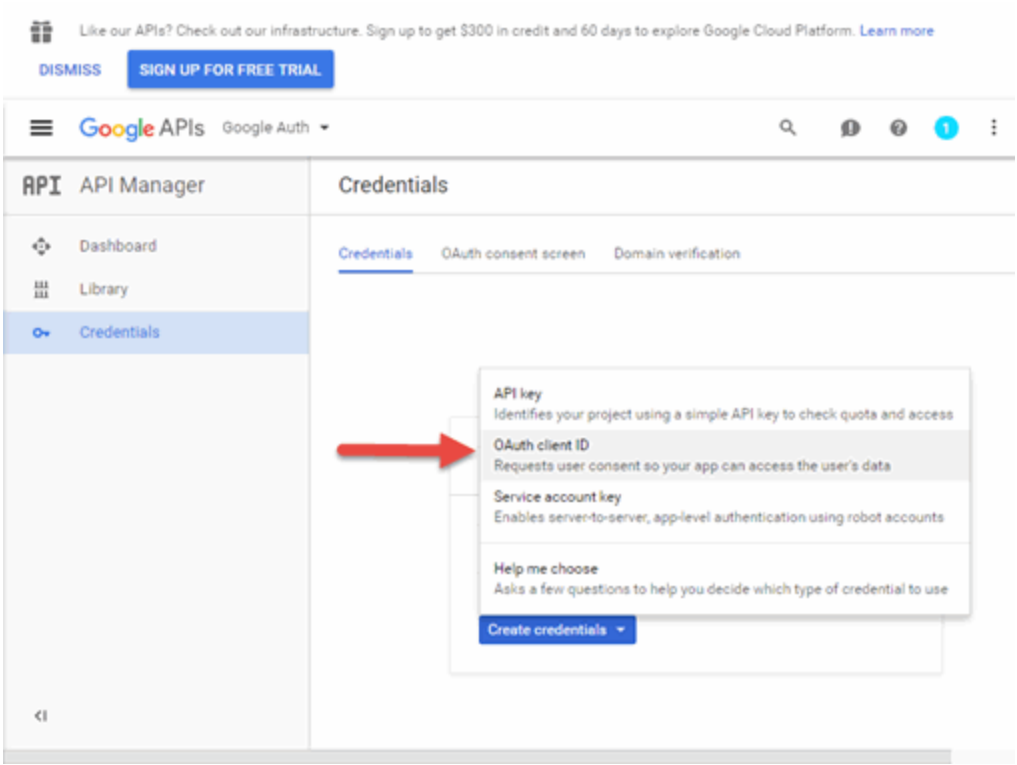
The New Project window opens.

4. Enter a **Project name** and select **Create**.
5. Select the **Credentials** link in the left-panel.



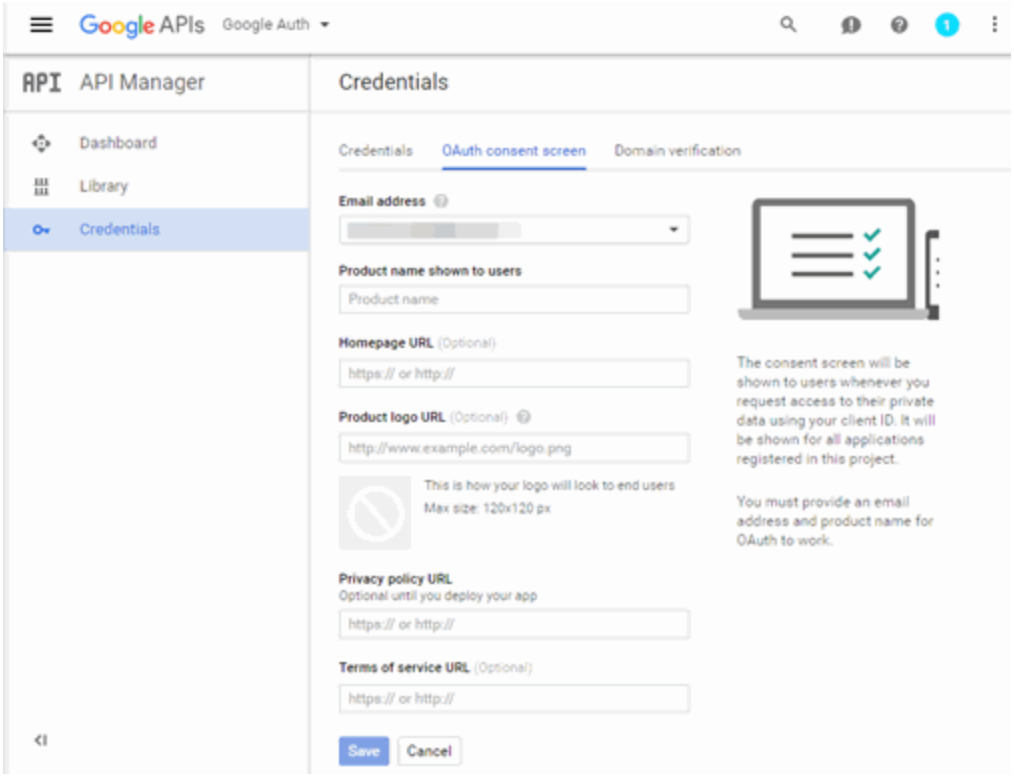
The Credentials panel opens.

6. Select the **Create credentials** button to open the drop-down list and select **OAuth client ID**.



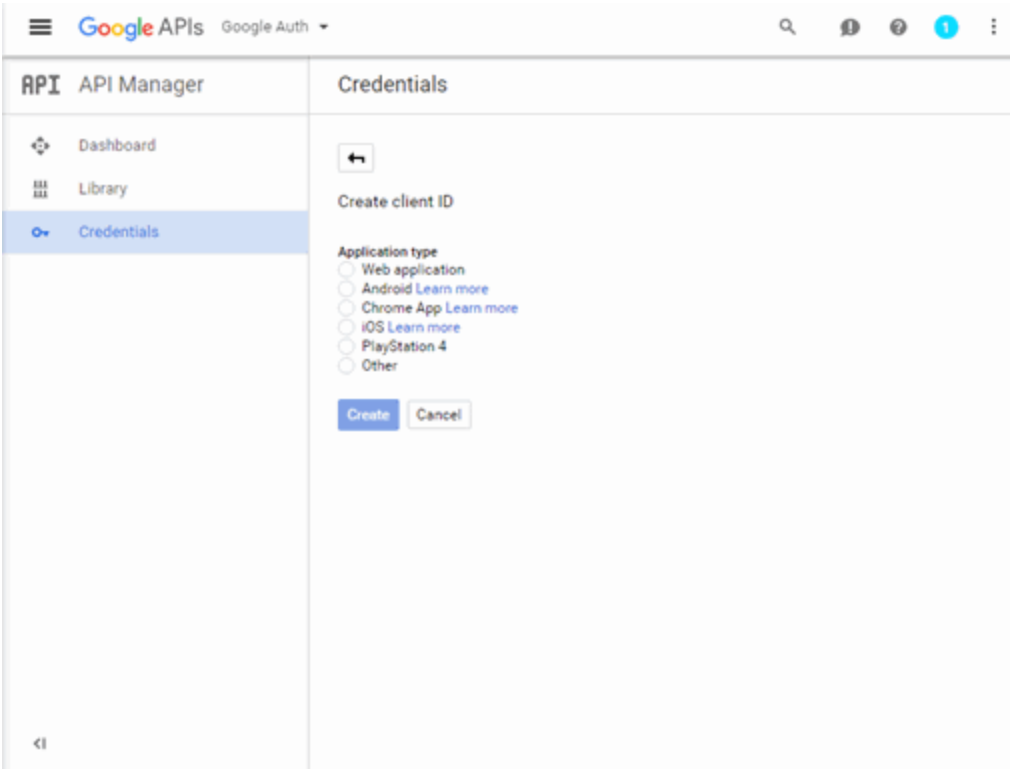
The Create client ID panel displays.

7. Select **Configure consent screen** to open the OAuth consent screen panel.



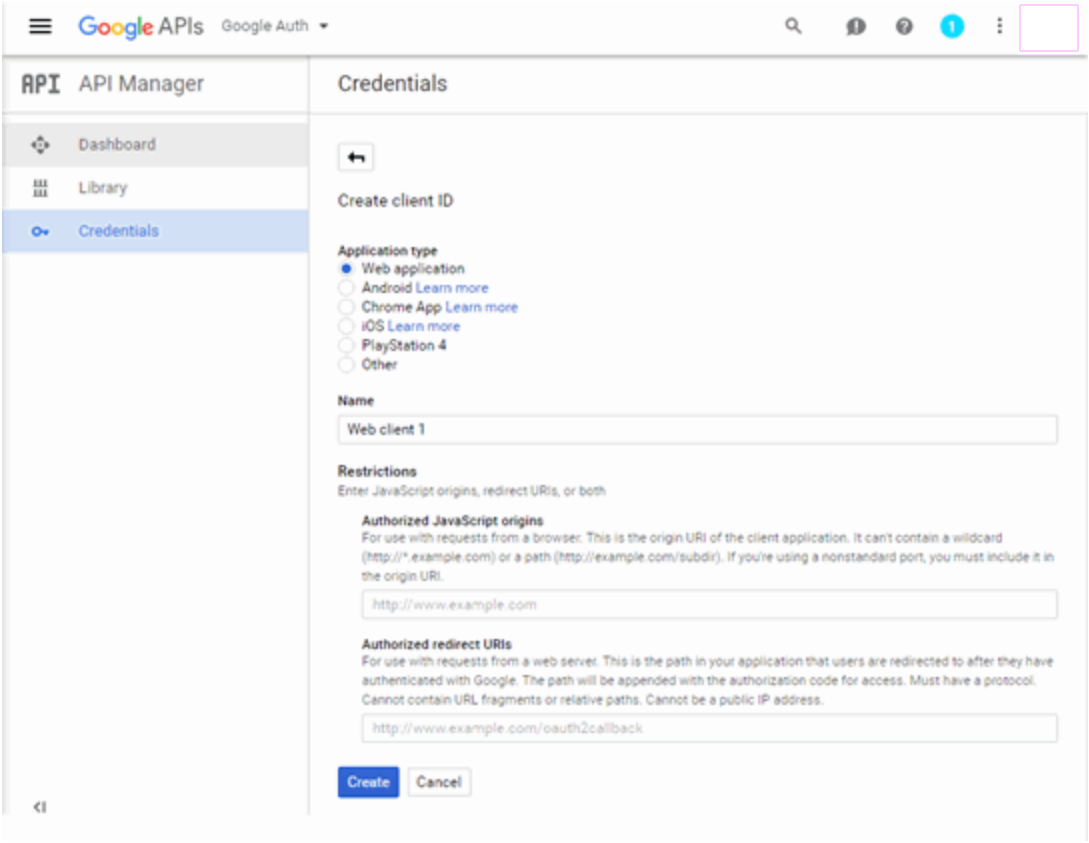
8. Select your email address, enter your product name, and enter the URL to any of the applicable resources for your company, then select **Save**.

   The Create client ID panel opens.



9. Select **Web application**.

   The panel expands to display additional fields.



10. Enter a name for the application in the **Name** field. Use a name that clearly indicates what its purpose is, for example, Extreme Networks Guest Registration.
11. Enter an **Authorized redirect URI** in the following format `https://<AccessControlengineFQDN>/google_oauth`. Google uses the **Authorized redirect URI** to redirect the user back to the engine with an Access Token.

    NOTES: Google OAuth APIs require your engine's FQDN resolves to a top level domain (.com, .net, .edu, .org, .mil, .gov, or .int. You cannot use a domain not classified as top level (e.g. MyGateway.MyCompany.Local) or the engines IP address, which can require you to reclassify your domain and hosts.

    Use only lowercase when entering the host and domain suffix (e.g. .com).
12. Enter the **Authorized redirect URI** for any additional Access Control engines registering end-users via Google.
13. Select **Create**.

    The **OAuth client** window displays, displaying your client ID and secret.



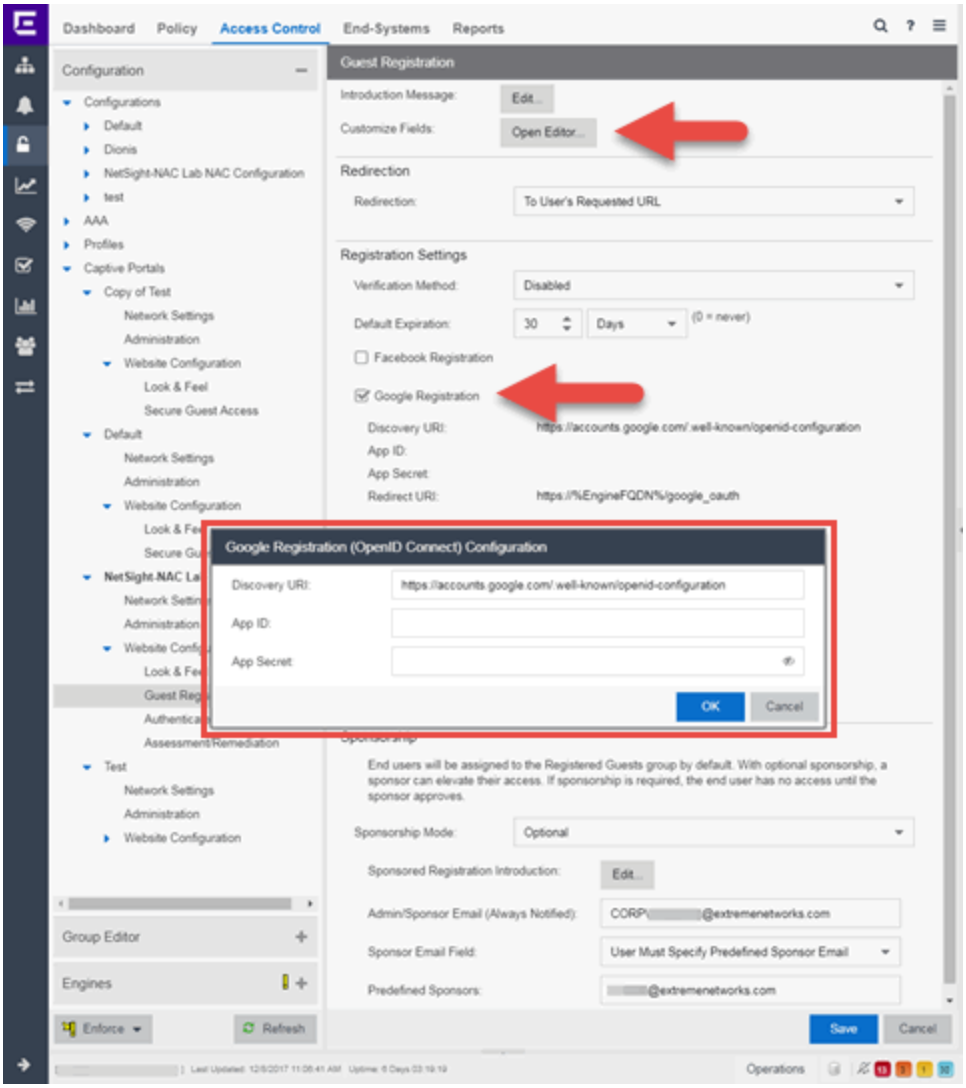
Your application is created and ready to use.

You need to add the client ID and client secret to your portal configuration.

Portal Configuration

The client ID and client secret assigned during the creation of the Google application must be provided in the Portal Configuration in order for the entire process to complete properly.

1. Open the **Control** > **Access Control** tab.
2. In the left-panel tree, expand the Configuration > Captive Portals > Website Configuration > and select Guest Registration.



3. In the Customize Fields section, select the **Open Editor** button to open the Manage Custom Fields window where you can change registration portal fields. Google registration uses only the First Name, Last Name, and Email Address fields, and the Display Acceptable Use Policy (AUP) option. All other fields only apply to regular guest registration. If the Display AUP option is selected, the captive portal verifies that the AUP has been acknowledged before redirecting the user to Google.
4. Select the **Google Registration** checkbox.
5. Select **Edit**.
6. Enter the client ID in the **Google App ID** field and the client secret in the **App Secret** field.
7. Select **Save**. Warning messages display stating that Verification Method and Sponsorship are not used for Google registration, and that an FDQN is required will be enabled.
8. Enforce the new configuration to your engines.

How Google Registration Works

After you have configured Google registration using the steps above, this is how the registration process works:

1. The end user attempts to access an external Web site. Their HTTP traffic is redirected to the captive portal.
2. In the Guest Registration Portal, the end user selects the option to register using Google.
3. The end user is redirected to the Google login. If Acceptable Use Policy option is configured, the captive portal verifies that the AUP has been acknowledged before redirecting the user to Google.
4. When logged in, the end user is presented with the information that ExtremeCloud IQ Site Engine receives from Google.
5. The end user grants ExtremeCloud IQ Site Engine access to the Google information and is redirected back to the captive portal where they see a "Registration in Progress" message.
6. Google provides the requested information to ExtremeCloud IQ Site Engine, which uses it to populate the user registration fields.
7. The registration process completes and network access is granted.
8. The word "Google" is added to the user name so you can easily search for Google registration via the Registration Administration web page.

Special Deployment Considerations

Read the following deployment consideration prior to configuring Google Registration.

To allow traffic to your network via a wireless connection, create an L7 host record for the **Unregistered Role** on your Wireless Controller for `accounts.google.com` and `gstatic.com`. These domains are subject to change and can vary based on location.

Networks using DNS Proxy

Google Registration for networks redirecting HTTP traffic to the captive portal using DNS Proxy requires additional configuration.

In order for Google Registration to work properly with DNS Proxy, **all** domains/URLs necessary to properly load the Google web page must be added to the Allowed URLs/Allowed Domains section of the captive portal configuration. Otherwise, the ExtremeControl engine resolves DNS queries for these components to the Access Control engine IP causing the page to not load properly.

As of February 2017, you must add the following domains in order for Google registration to work with DNS Proxy. This domain is subject to change and can vary based on location.

Accounts.google.com

- Portal Configuration

How to Implement Microsoft Registration

This Help topic describes the steps for implementing guest registration using Microsoft as a way to obtain end user information.

In this scenario, the Guest Registration portal provides the option to register as a guest or log into Microsoft in order to complete the registration process. If the end user selects the Microsoft option, ExtremeCloud IQ Site Engine OAuth to securely access the end user's Microsoft account, obtain public end user data, and use that data to complete the registration process.

NOTE: Guest OAuth (for example, Google, Yahoo) may not support native mobile browsers and display a “user agent” error. To access the network, use a standard browser application (e.g. Google Chrome).

Guest Registration using Microsoft has two main advantages:

- It provides ExtremeCloud IQ Site Engine with a higher level of user information by obtaining information from the end user's Microsoft account instead of relying on information entered by the end user.
- It provides an easier registration process for the end user. ExtremeCloud IQ Site Engine retrieves the public information from the end user's Microsoft account and uses that information to populate the name and email registration fields.

This topic includes information and instructions on:

- Requirements for Microsoft Registration
- Creating a Microsoft Application
- Portal Configuration for Microsoft
- How Microsoft Registration Works
- Special Deployment Considerations
    - Networks using DNS Proxy

Requirements

These are the configuration requirements for Microsoft Registration.

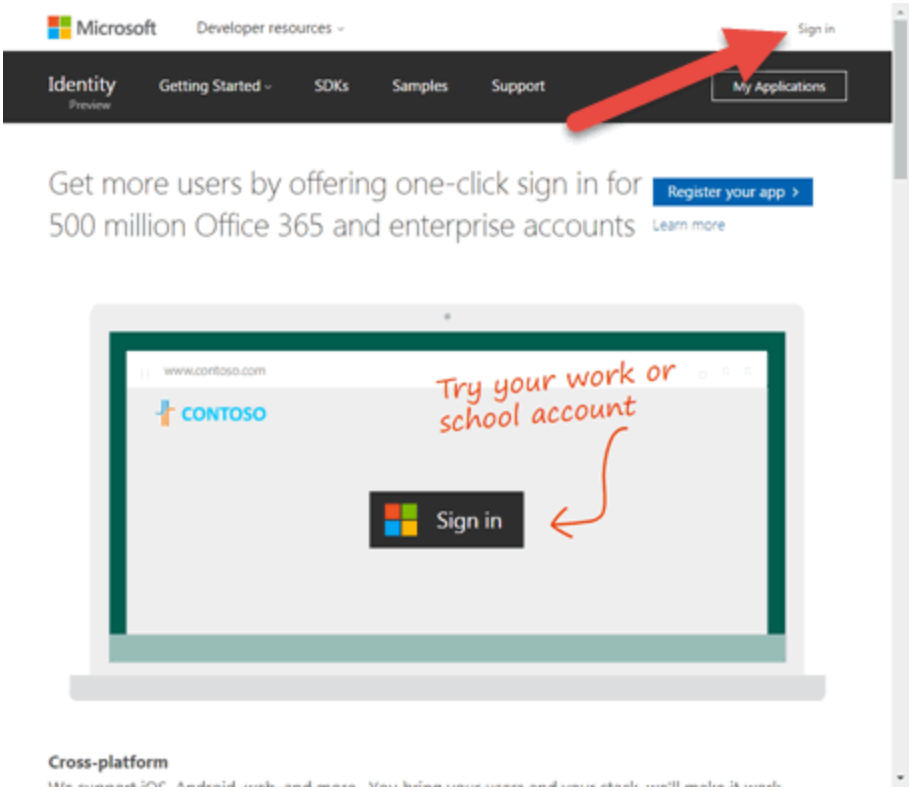
- The ExtremeControl engine must have Internet access in order to retrieve user information from Microsoft.
- The Access Control Unregistered access policy must provide access to the Microsoft site (either enable all SSL or make allowances for Microsoft servers).

- The Access Control Unregistered access policy must provide access to HTTPS traffic to the Microsoft OAuth servers.
- A Unique Microsoft application must be created on the Microsoft Developers page (see instructions below).
- The Portal Configuration must have Microsoft Registration enabled and include the Microsoft Application ID and Secret (see instructions below).

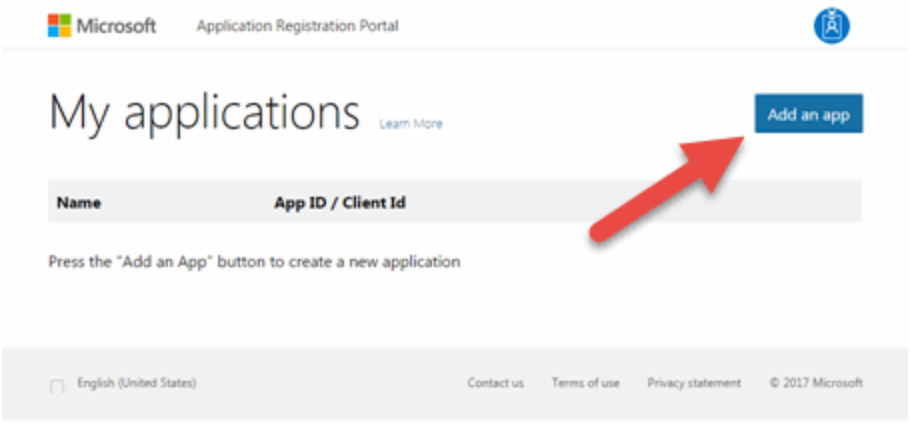
Creating a Microsoft Application

When implementing guest registration using Microsoft, you must first create a Microsoft application. This generates an Application ID and Application Secret that are required as part of the ExtremeCloud IQ Site Engine OAuth process. Use the following steps to create a Microsoft application.

1. Access the Microsoft Developers page at https://apps.dev.microsoft.com/#/appList.
2. Log into your existing account or create a new account by selecting the **Sign in** link in the top-right corner of the window.



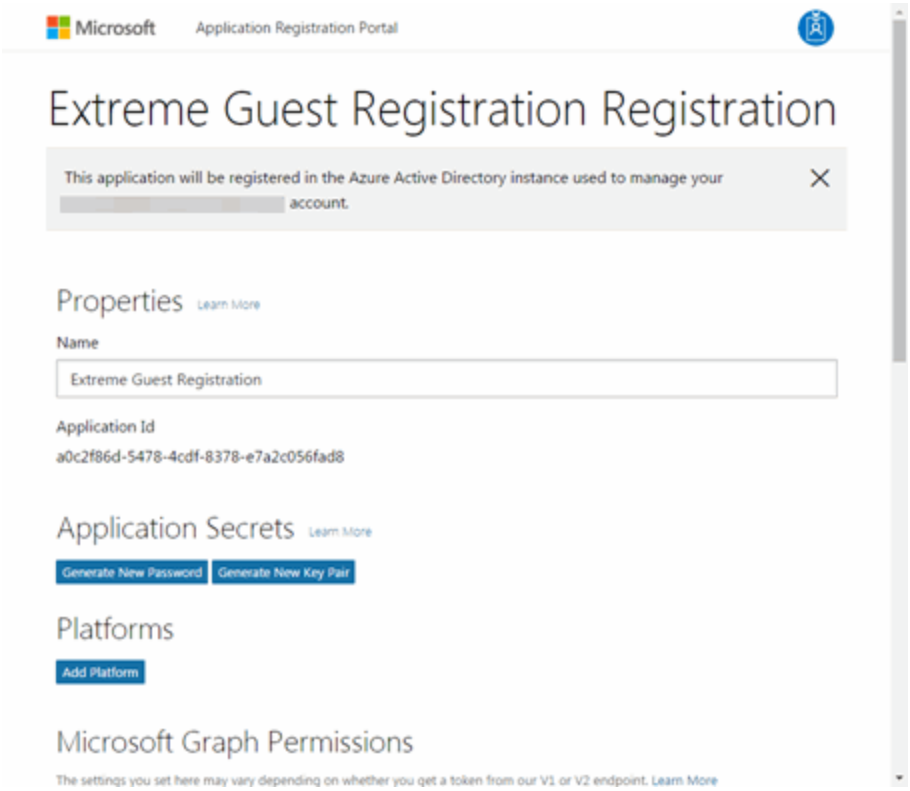
3. Select the **Add an app** button.



The New Application Registration window opens.

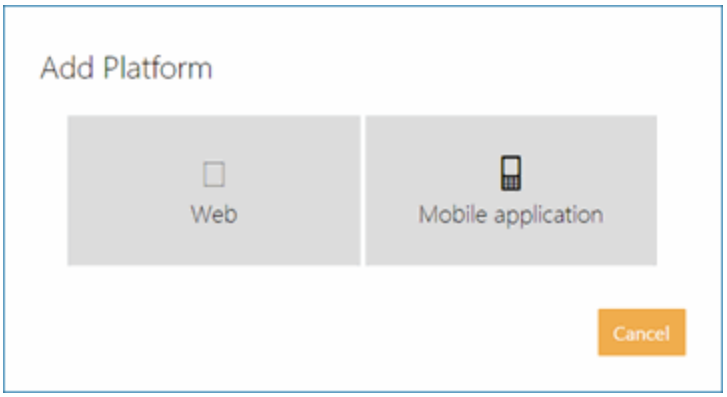
4. Enter a **Name** for the application. Use a name that clearly indicates it's purpose (e.g. Extreme Networks Guest Registration) and select **Create application**.

   The Application Registration window opens.



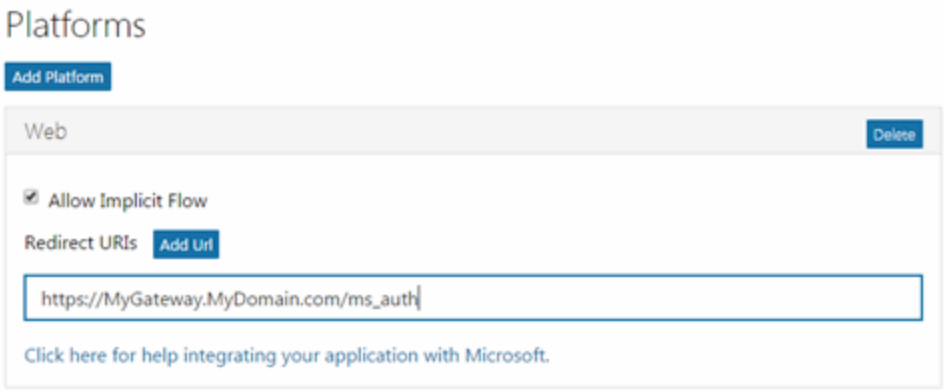
5. Select **Add Platforms** under Platforms.

   The Add Platform window opens.



6. Select **Web**.

   Additional fields display under Platforms enabling you to configure a web platform.

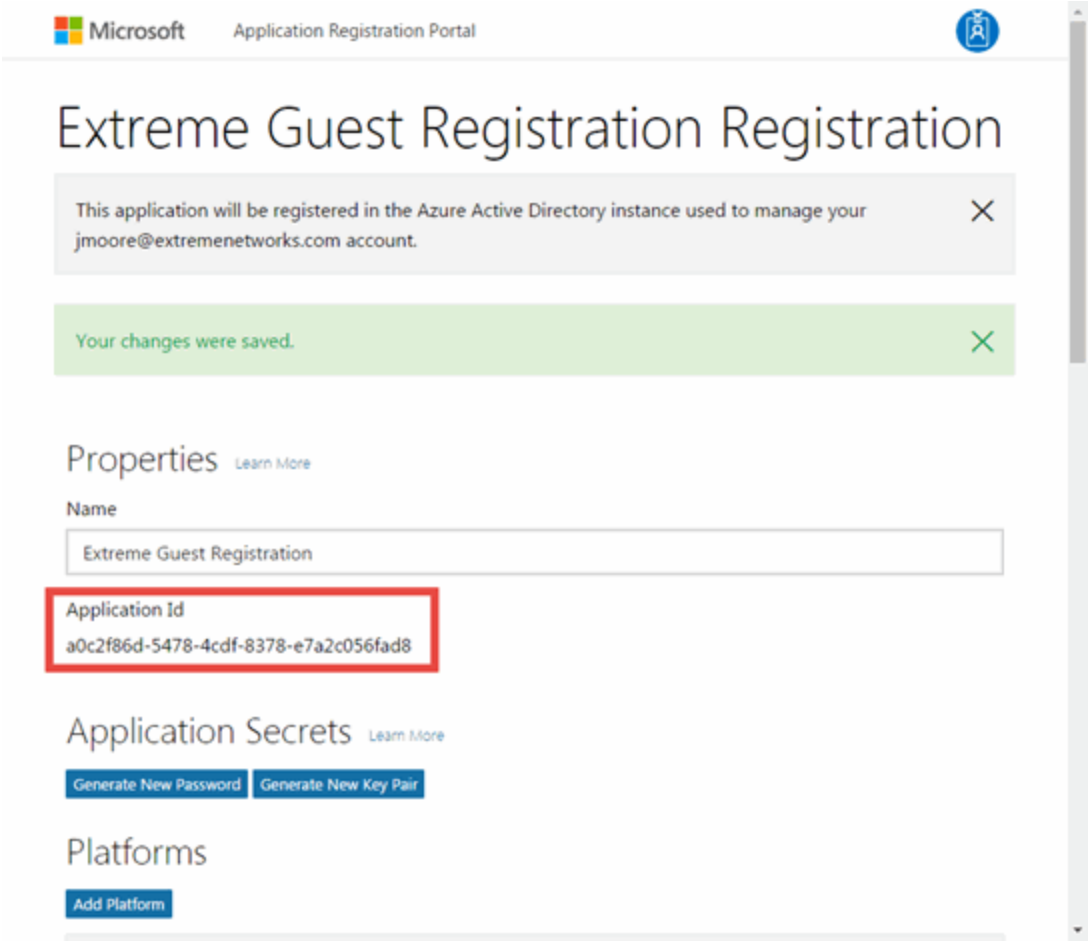


7. Enter a **Redirect URI** in the following format `https://<AccessControlengineFQDN>/ms_oauth`. Microsoft uses the **Redirect URI** to redirect the user back to the engine with an Access Token.

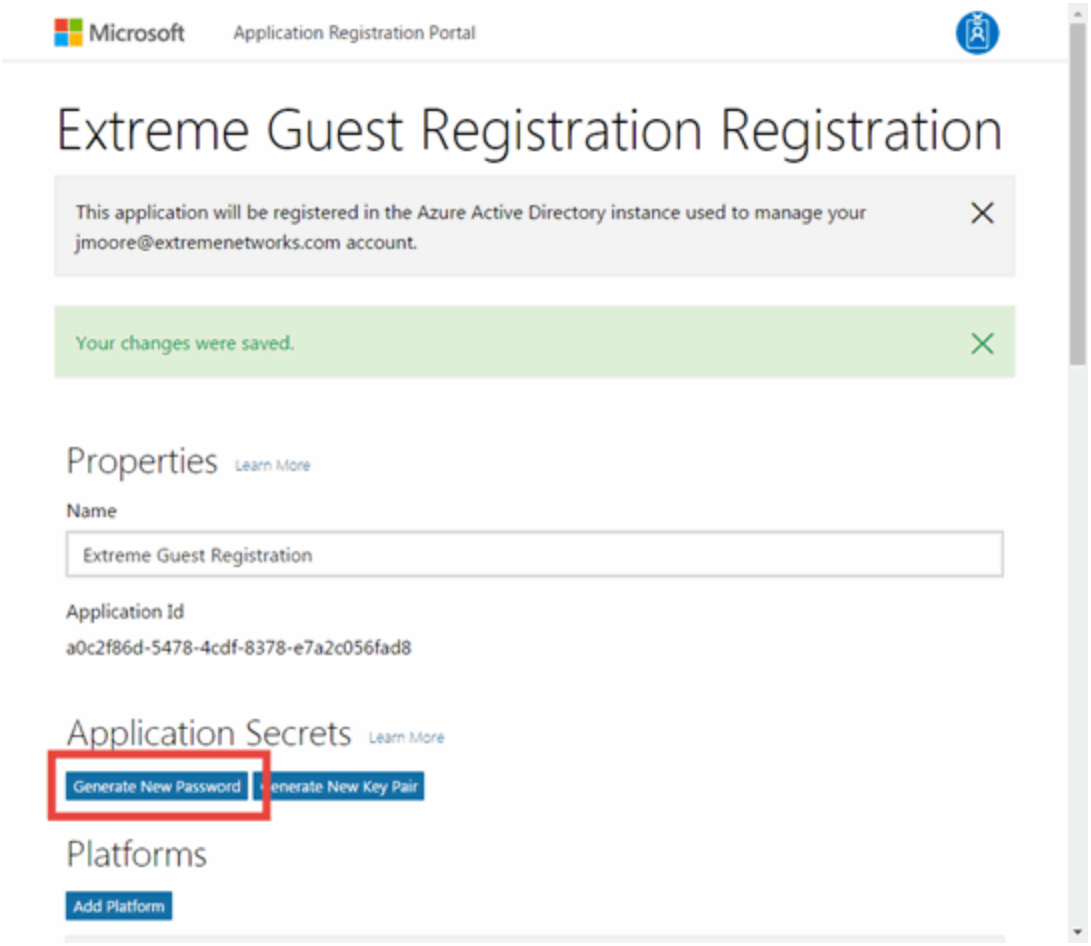
   NOTE: Microsoft applications can only use a limited set of redirect URI values.

8. Select **Add Url** to enter the **Redirect URI** for any additional Access Control engines registering end-users via Microsoft.

9. Copy the **Application Id** under Properties.



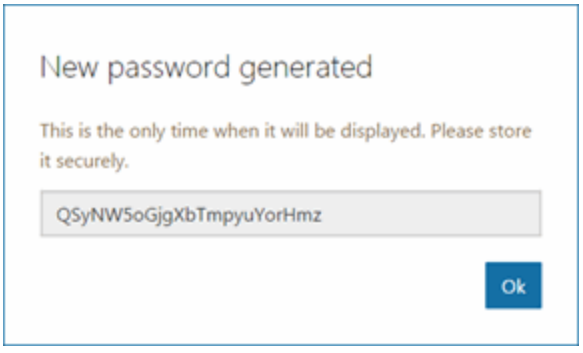
10. Select **Generate New Password** under Application Secrets.



The **New password generated** window displays.

11. Copy the application password.

IMPORTANT: Ensure you copy the password accurately. After the window is closed, you cannot access the password again.



12. Select **Save**.

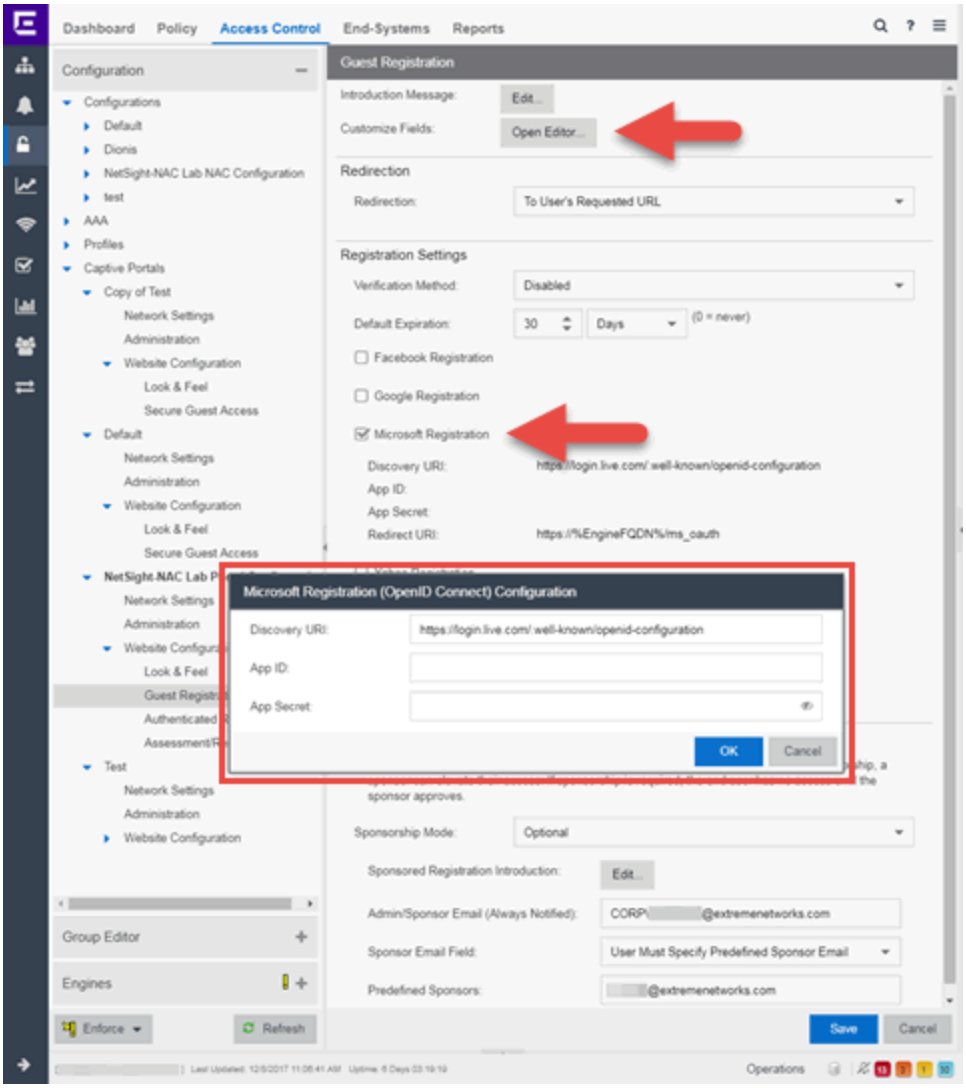
    Your application is created and ready to use.

    You need to add the **Application Id** and application password to your portal configuration.

Portal Configuration

The Application Id and application password assigned during the creation of the Microsoft application must be provided in the Portal Configuration in order for the entire process to complete properly.

1. Open the **Control** > **Access Control** tab.
2. In the left-panel tree, expand the Access Control Configurations > Portal tree and select Guest Registration.



3. In the Customize Fields section, select the **Open Editor** button to open the Manage Custom Fields window where you can change registration portal fields. Microsoft registration uses only the First Name, Last Name, and Email Address fields, and the Display Acceptable Use Policy (AUP) option. All other fields only apply to regular guest registration. If the Display AUP option is selected, the captive portal verifies that the AUP has been acknowledged before redirecting the user to Microsoft.
4. Select the **Microsoft Registration** checkbox.
5. Select **Edit**.
6. Enter the Application Id in the **Microsoft App ID** field and the application password in the **Microsoft App Secret** field.

7. Select **Save**. Warning messages display stating that Verification Method and Sponsorship are not used for Microsoft registration, and that an FDQN is required and will be enabled.
8. Enforce the new configuration to your engines.

How Microsoft Registration Works

After you have configured Microsoft registration using the steps above, this is how the registration process works:

1. The end user attempts to access an external Web site. Their HTTP traffic is redirected to the captive portal.
2. In the Guest Registration Portal, the end user selects the option to register using Microsoft.
3. The end user is redirected to the Microsoft login. If Acceptable Use Policy option is configured, the captive portal verifies that the AUP has been acknowledged before redirecting the user to Microsoft.
4. When logged in, the end user is presented with the information that ExtremeCloud IQ Site Engine receives from Microsoft.
5. The end user grants ExtremeCloud IQ Site Engine access to the Microsoft information and is redirected back to the captive portal where they see a "Registration in Progress" message.
6. Microsoft provides the requested information to ExtremeCloud IQ Site Engine, which uses it to populate the user registration fields.
7. The registration process completes and network access is granted.
8. The word "Microsoft" is added to the user name so you can easily search for Microsoft registration via the Registration Administration web page.

Special Deployment Considerations

Read the following deployment consideration prior to configuring Microsoft Registration.

To provide access to your network via a wireless connection, create an L7 host record for the **Unregistered Role** on your Wireless Controller for `login.live.com` and `auth.gfx.ms`. These domains are subject to change and can vary based on location.

Networks using DNS Proxy

Microsoft Registration for networks redirecting HTTP traffic to the captive portal using DNS Proxy requires additional configuration.

In order for Microsoft Registration to work properly with DNS Proxy, **all** domains/URLs necessary to properly load the Microsoft web page must be added to the Allowed URLs/Allowed Domains section of

the captive portal configuration. Otherwise, the ExtremeControl engine resolves DNS queries for these components to the Access Control engine IP causing the page to not load properly.

As of February 2017, you must add the following domains in order for Microsoft registration to work with DNS Proxy. These domains are subject to change and can vary based on location.

Login.live.com

- Portal Configuration

How to Implement Yahoo Registration

This Help topic describes the steps for implementing guest registration using Yahoo as a way to obtain end user information.

In this scenario, the Guest Registration portal provides the option to register as a guest or log into Yahoo in order to complete the registration process. If the end user selects the Yahoo option, ExtremeCloud IQ Site Engine OpenID to securely access the end user's Yahoo account, obtain public end user data, and use that data to complete the registration process.

NOTE: Guest OAuth (for example, Google, Yahoo) may not support native mobile browsers and display a “user agent” error. To access the network, use a standard browser application (e.g. Google Chrome).

Guest Registration using Yahoo has two main advantages:

- It provides ExtremeCloud IQ Site Engine with a higher level of user information by obtaining information from the end user's Yahoo account instead of relying on information entered by the end user.
- It provides an easier registration process for the end user. ExtremeCloud IQ Site Engine retrieves the public information from the end user's Yahoo account and uses that information to populate the name and email registration fields.

This topic includes information and instructions on:

- Requirements for Yahoo Registration
- Creating a Yahoo Application
- Portal Configuration for Yahoo
- How Yahoo Registration Works
- Special Deployment Considerations
    - Networks using DNS Proxy

Requirements

These are the configuration requirements for Yahoo Registration.

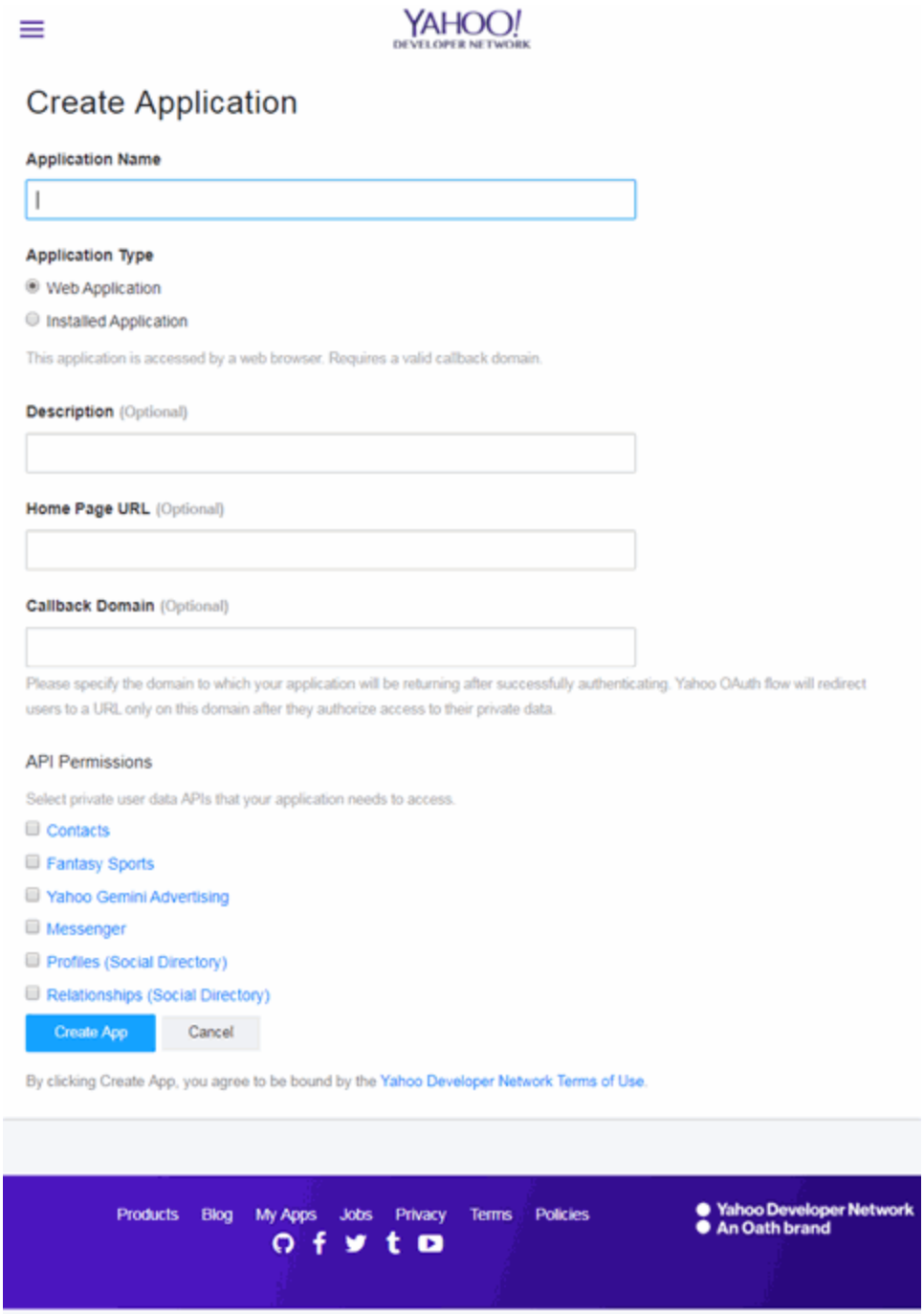
- The ExtremeControl engine must have Internet access in order to retrieve user information from Yahoo.
- The Access Control Unregistered access policy must provide access to the Yahoo site (either enable all SSL or make allowances for Yahoo servers).

- The Access Control Unregistered access policy must provide access to HTTPS traffic to the Yahoo OpenID servers.
- A Unique Yahoo application must be created on the Yahoo Developers page (see instructions below).
- The Portal Configuration must have Yahoo Registration enabled and include the Yahoo Application ID and Secret (see instructions below).

Creating a Yahoo Application

When implementing guest registration using Yahoo, you must first create a Yahoo application. This generates an Application ID and Application Secret that are required as part of the ExtremeCloud IQ Site Engine OpenID process. Use the following steps to create a Yahoo application.

1. Log into your existing account or create a new account.
2. Access the Create Application page at https://developer.yahoo.com/apps/create/.



3. Enter a name for the application in the **Application Name** field. Use a name that clearly indicates what its purpose is, for example, Extreme Networks Guest Registration.
4. Select **Web Application** for the **Application Type**.
5. Enter an **Callback Domain** in the following format `https://<AccessControlengineFQDN>`. Yahoo uses the **Callback Domain** to redirect the user back to the engine with an Access

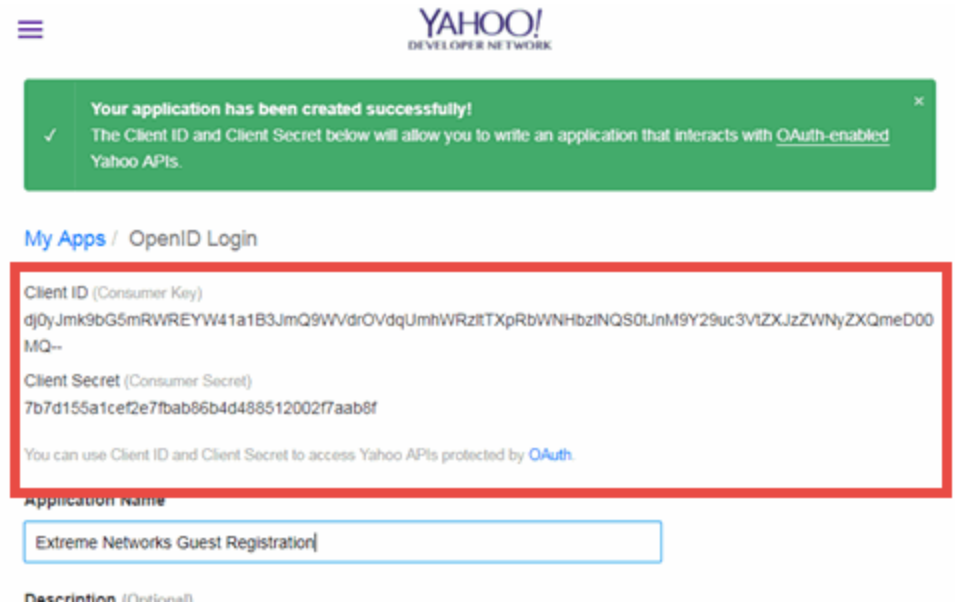
Token.

NOTES: Yahoo OAuth APIs require your engine's FQDN resolves to a top level domain (.com, .net, .edu, .org, .mil, .gov, or .int. You cannot use a domain not classified as top level (e.g. MyGateway.MyCompany.Local) or the engines IP address, which can require you to reclassify your domain and hosts.

Use only lowercase when entering the host and domain suffix (e.g. .com).

6. Select **Create App**.

   The Client ID and Client Secret display at the top of the window.



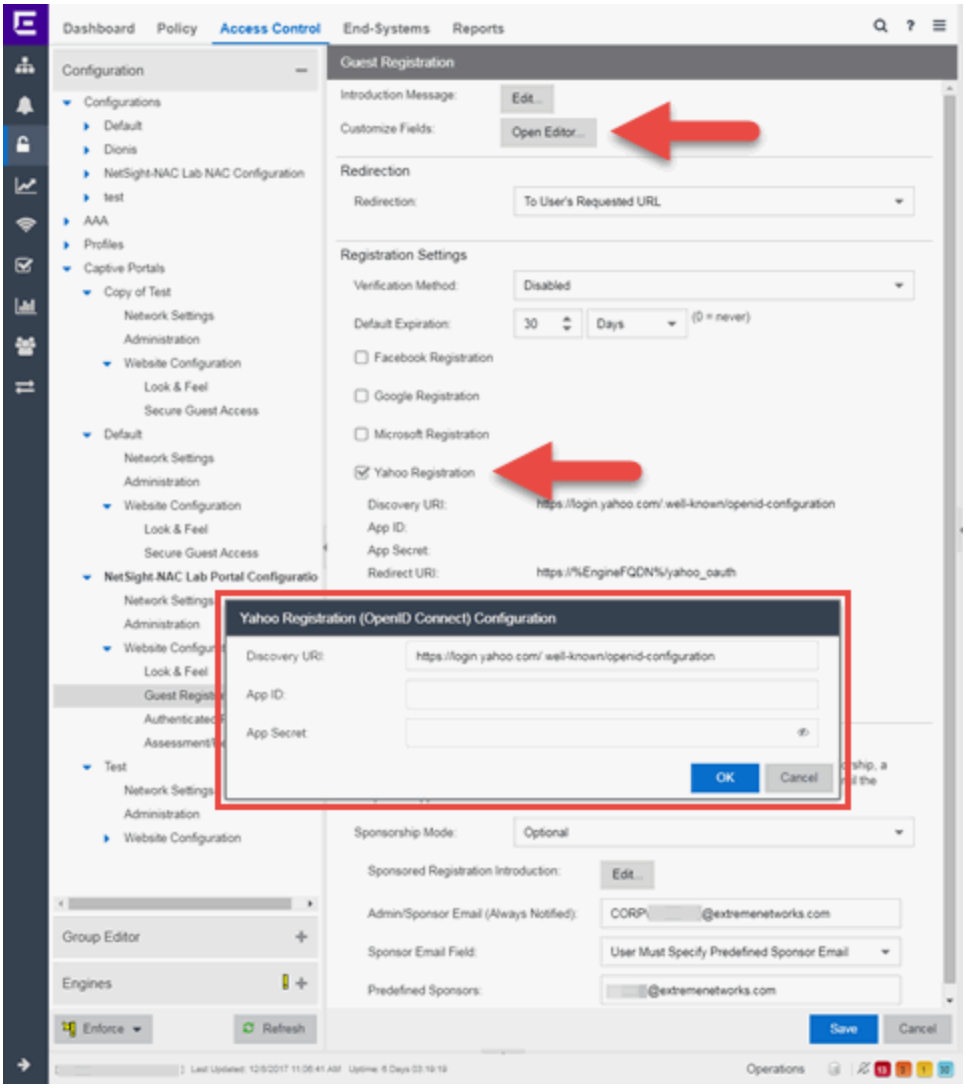
   Your application is created and ready to use.

   You need to add the client ID and client secret to your portal configuration.

Portal Configuration

The client ID and client secret assigned during the creation of the Yahoo application must be provided in the Portal Configuration in order for the entire process to complete properly.

1. Open the **Control** > **Access Control** tab.
2. In the left-panel tree, expand the Configuration > Captive Portals > Website Configuration > and select Guest Registration.



3. In the Customize Fields section, select the **Open Editor** button to open the Manage Custom Fields window where you can change registration portal fields. Yahoo registration uses only the First Name, Last Name, and Email Address fields, and the Display Acceptable Use Policy (AUP) option. All other fields only apply to regular guest registration. If the Display AUP option is selected, the captive portal verifies that the AUP has been acknowledged before redirecting the user to Yahoo.
4. Select the **Yahoo Registration** checkbox.
5. Select **Edit**.
6. Enter the Client ID in the **App ID** field and the Client Secret in the **App Secret** field.
7. Select **Save**. Warning messages display stating that Verification Method and Sponsorship are not used for Yahoo registration, and that an FDQN is required will be enabled.
8. Enforce the new configuration to your engines.

How Yahoo Registration Works

After you have configured Yahoo registration using the steps above, this is how the registration process works:

1. The end user attempts to access an external Web site. Their HTTP traffic is redirected to the captive portal.
2. In the Guest Registration Portal, the end user selects the option to register using Yahoo.
3. The end user is redirected to the Yahoo login. If Acceptable Use Policy option is configured, the captive portal verifies that the AUP has been acknowledged before redirecting the user to Yahoo.
4. When logged in, the end user is presented with the information that ExtremeCloud IQ Site Engine receives from Yahoo.
5. The end user grants ExtremeCloud IQ Site Engine access to the Yahoo information and is redirected back to the captive portal where they see a "Registration in Progress" message.
6. Yahoo provides the requested information to ExtremeCloud IQ Site Engine, which uses it to populate the user registration fields.
7. The registration process completes and network access is granted.
8. The word "Yahoo" is added to the user name so you can easily search for Yahoo registration via the Registration Administration web page.

Special Deployment Considerations

Read the following deployment consideration prior to configuring Yahoo Registration.

To provide access to your network via a wireless connection, create an L7 host record for the **Unregistered Role** on your Wireless Controller for `login.yahoo.com`. This domain is subject to change and can vary based on location.

Networks using DNS Proxy

Yahoo Registration for networks redirecting HTTP traffic to the captive portal using DNS Proxy requires additional configuration.

In order for Yahoo Registration to work properly with DNS Proxy, **all** domains/URLs necessary to properly load the Yahoo web page must be added to the Allowed URLs/Allowed Domains section of the captive portal configuration. Otherwise, the ExtremeControlengine resolves DNS queries for these components to the Access Controlengine IP causing the page to not load properly.

As of February 2017, you must add the following domains in order for Yahoo registration to work with DNS Proxy. This domain is subject to change and can vary based on location.

login.yahoo.com

- Portal Configuration

How to Implement Salesforce Registration

This Help topic describes the steps for implementing guest registration using Salesforce as a way to obtain end user information.

In this scenario, the Guest Registration portal provides the option to register as a guest or log into Salesforce in order to complete the registration process. If the end user selects the Salesforce option, ExtremeCloud IQ Site Engine uses OpenID to securely access the end user's Salesforce account, obtain public end user data, and use that data to complete the registration process.

NOTE: Guest OAuth (for example, Google, Yahoo) may not support native mobile browsers and display a "user agent" error. To access the network, use a standard browser application (e.g. Google Chrome).

Guest Registration using Salesforce has two main advantages:

- It provides ExtremeCloud IQ Site Engine with a higher level of user information by obtaining information from the end user's Salesforce account instead of relying on information entered by the end-user.
- It provides an easier registration process for the end user. ExtremeCloud IQ Site Engine retrieves the public information from the end user's Salesforce account and uses that information to populate the name and email registration fields.

This topic includes information and instructions on:

- Requirements for Salesforce Registration
- Creating a Salesforce Application
- Portal Configuration for Salesforce
- How Salesforce Registration Works
- Special Deployment Considerations
    - Networks using DNS Proxy

Requirements

These are the configuration requirements for Salesforce Registration.

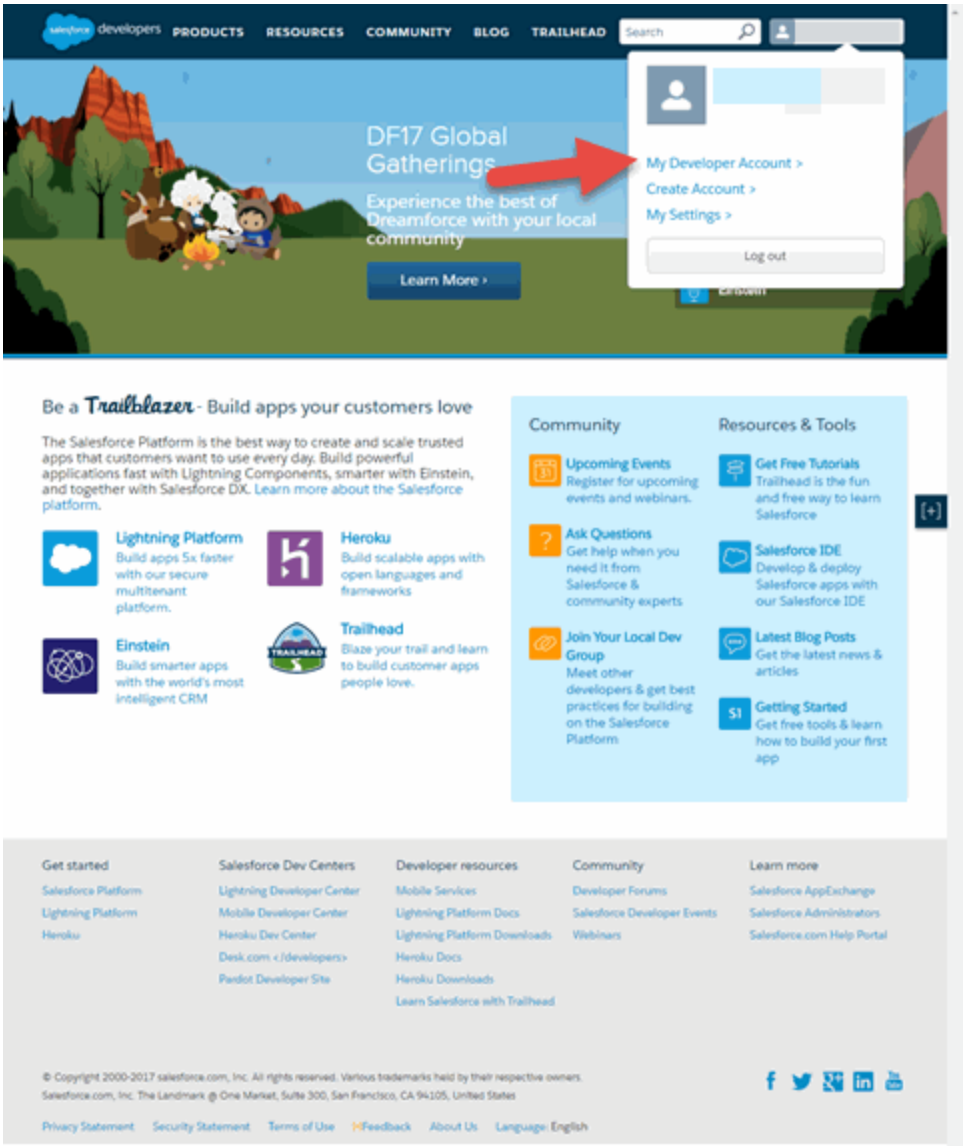
- The ExtremeControl engine must have Internet access in order to retrieve user information from Salesforce.
- The Access Control Unregistered access policy must provide access to the Salesforce site (either enable all SSL or make allowances for Salesforce servers).

- The Access Control Unregistered access policy must provide access to HTTPS traffic to the Salesforce OpenID servers.
- A Unique Salesforce application must be created on the Salesforce Developers page (see instructions below).
- The Portal Configuration must have Salesforce Registration enabled and include the Salesforce Application ID and Secret (see instructions below).

Creating a Salesforce Application

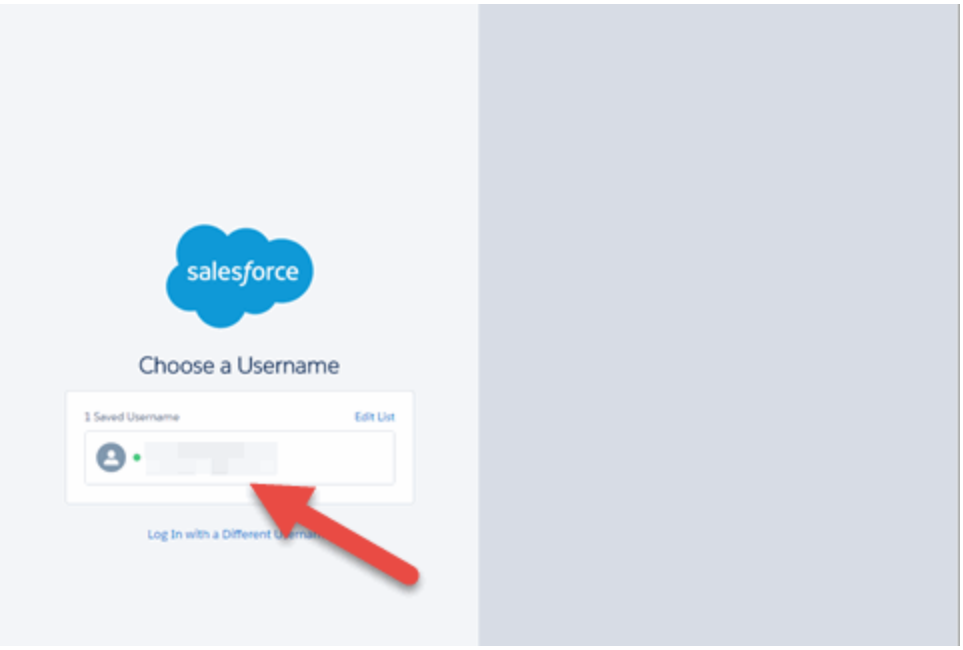
When implementing guest registration using Salesforce, you must first create a Salesforce application. This generates an Application ID and Application Secret that are required as part of the ExtremeCloud IQ Site Engine OpenID process. Use the following steps to create a Salesforce application.

1. Access the Salesforce Developers page at https://developer.salesforce.com/signup.
2. Log into your existing Developers account or create a new Developers account.
3. Select the **My Developer Account** button from the profile drop-down list.



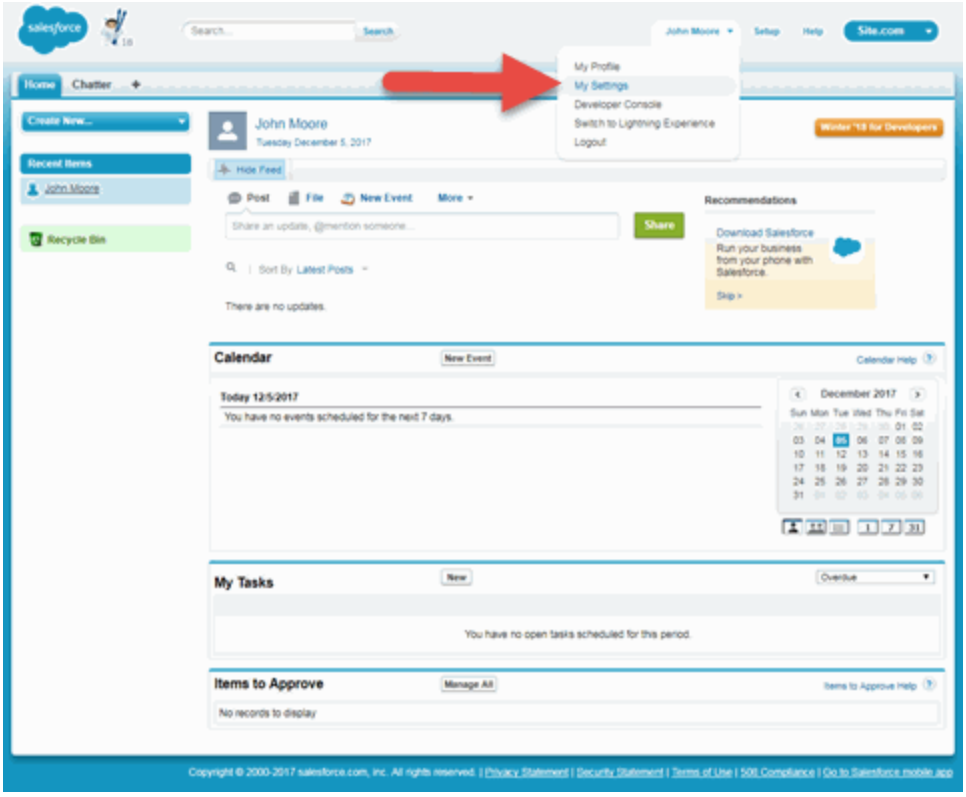
The Developer Account login window opens.

4. Select your account.



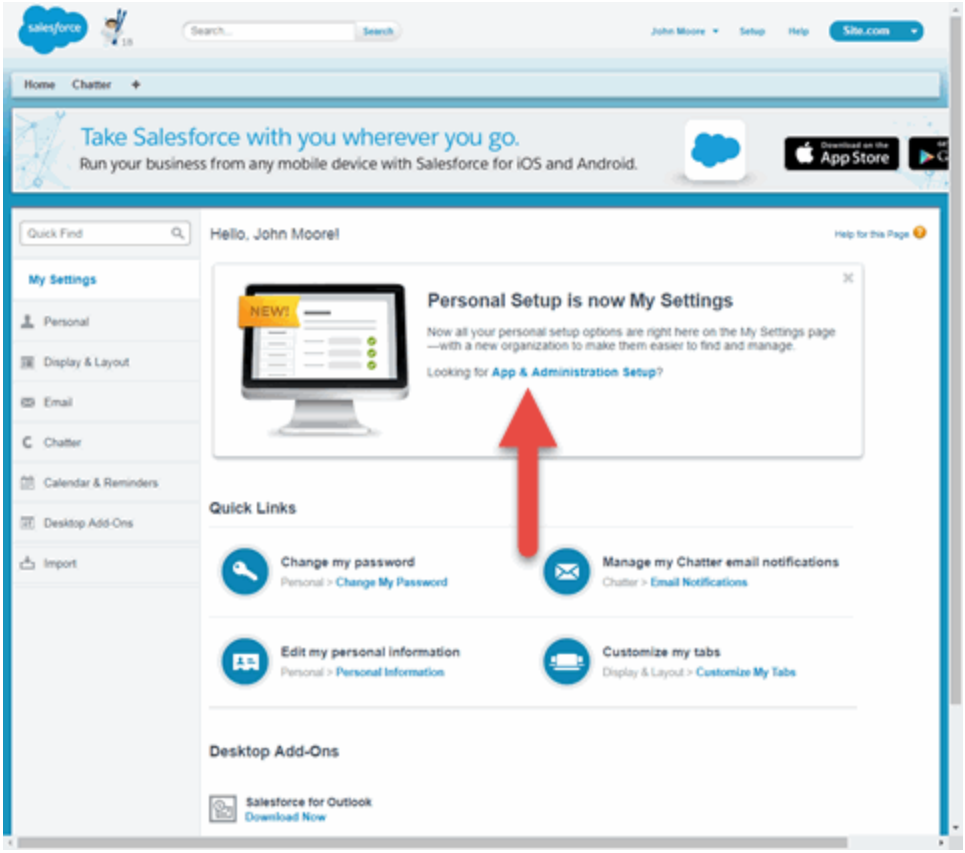
The **Developer Home** window opens.

5. Select **My Settings** from the Profile drop-down list.



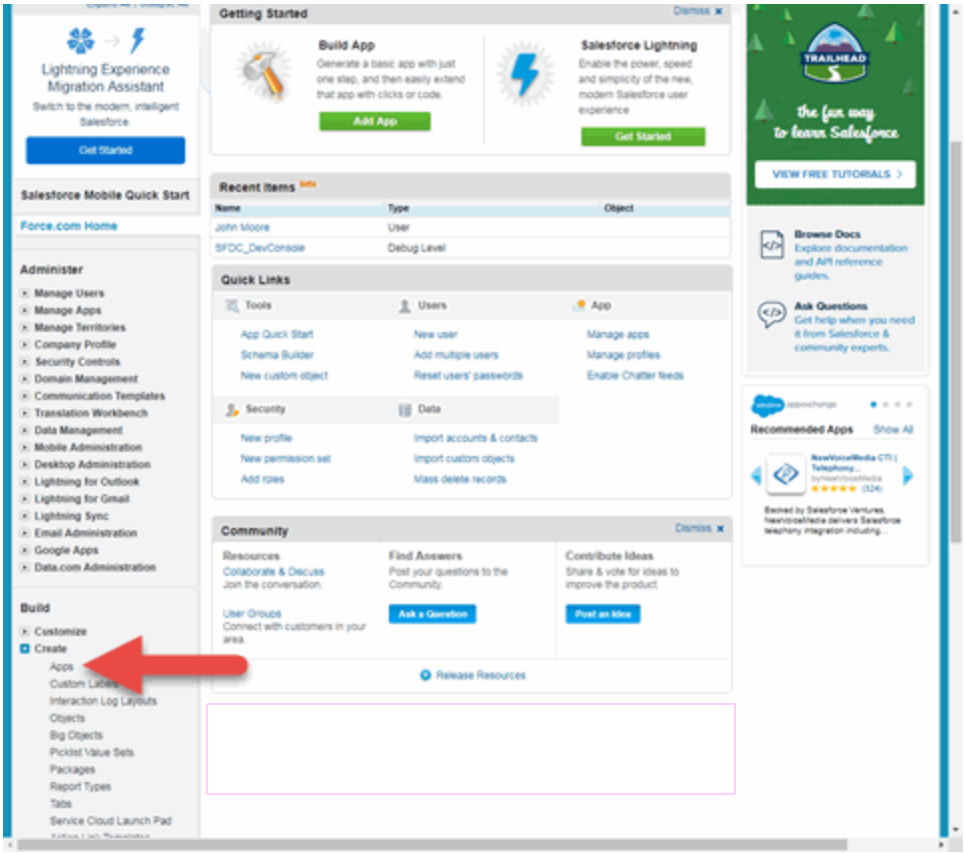
The **My Settings** window opens.

6. Select **App & Administration Setup**.



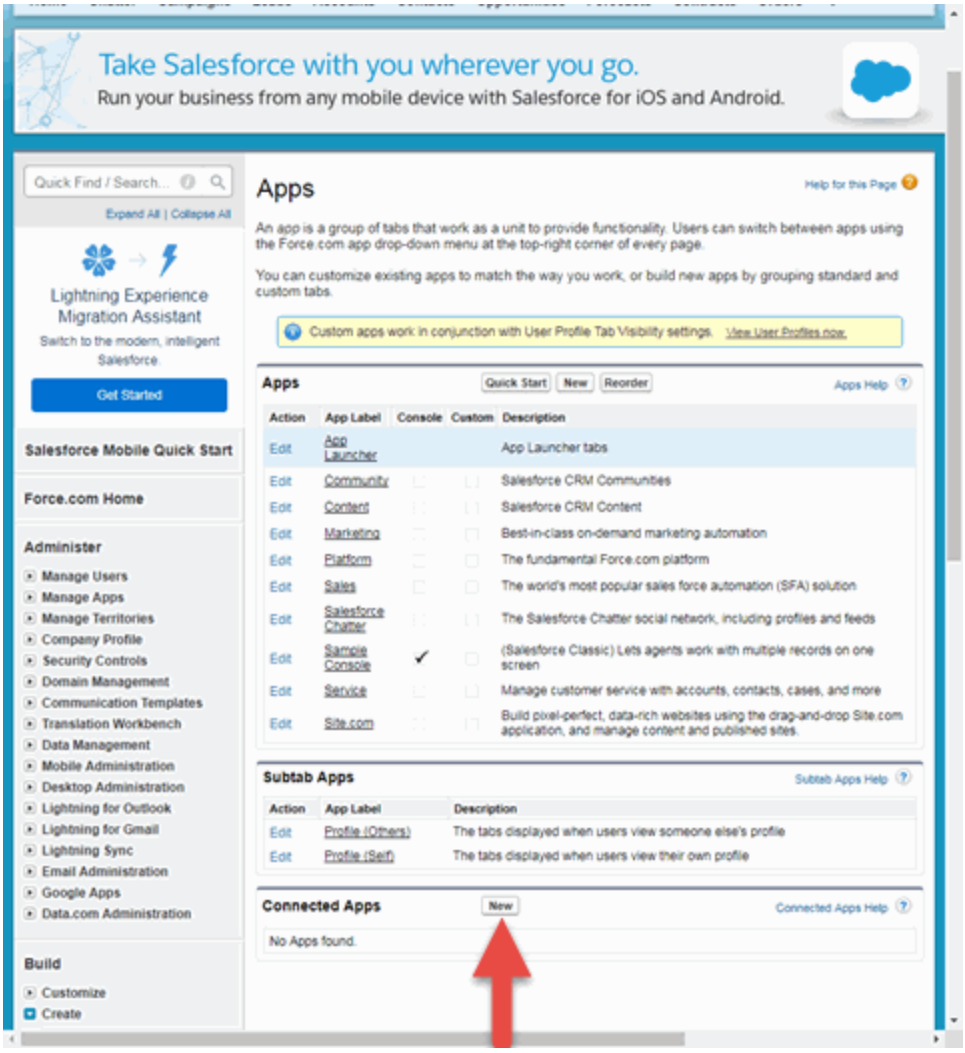
The **App & Administration Setup** window opens.

7. Select **Apps** from within the Build > Create menu.



The **Apps** window opens.

8. Select the **New** button in the Connected Apps section.



The New Connected App window opens.

9. Enter a **Connected App Name**, **API Name**, **Contact Email**, and select the **Enable OAuth Settings** checkbox.

   The API (Enable OAuth Settings) section of the window expands to display additional fields.

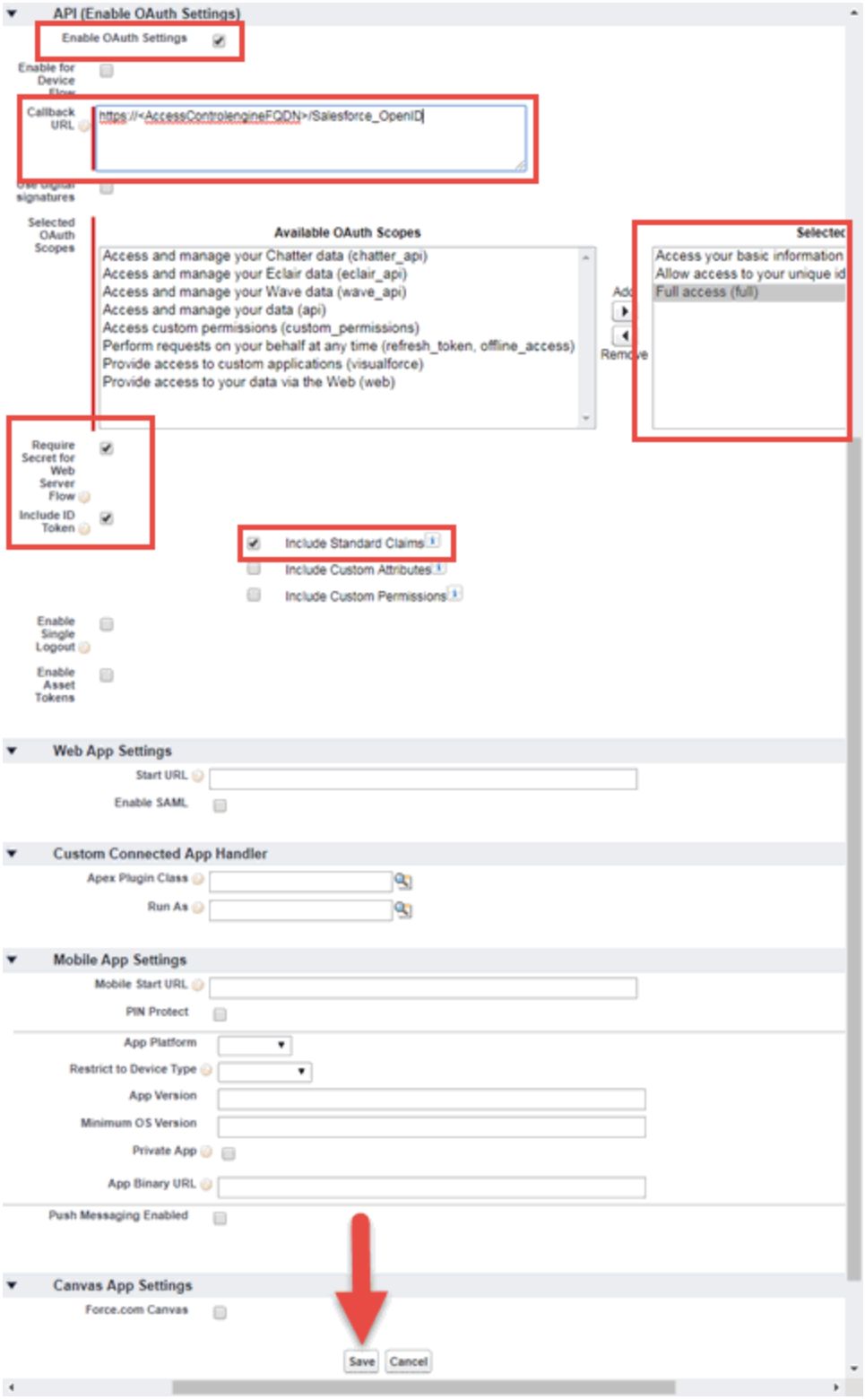
10. Select **Enable OAuth Settings**.

11. Enter a **Callback URL** in the following format `https://<AccessControlengineFQDN>/Salesforce_oauth`. Salesforce uses the **Authorized redirect URI** to redirect the user back to the engine with an Access Token.

NOTES: Salesforce OpenID APIs require your engine's FQDN resolves to a top level domain (.com, .net, .edu, .org, .mil, .gov, or .int. You cannot use a domain not classified as top level (e.g. MyGateway.MyCompany.Local) or the engines IP address, which can require you to reclassify your domain and hosts.

Use only lowercase when entering the host and domain suffix (e.g. .com).

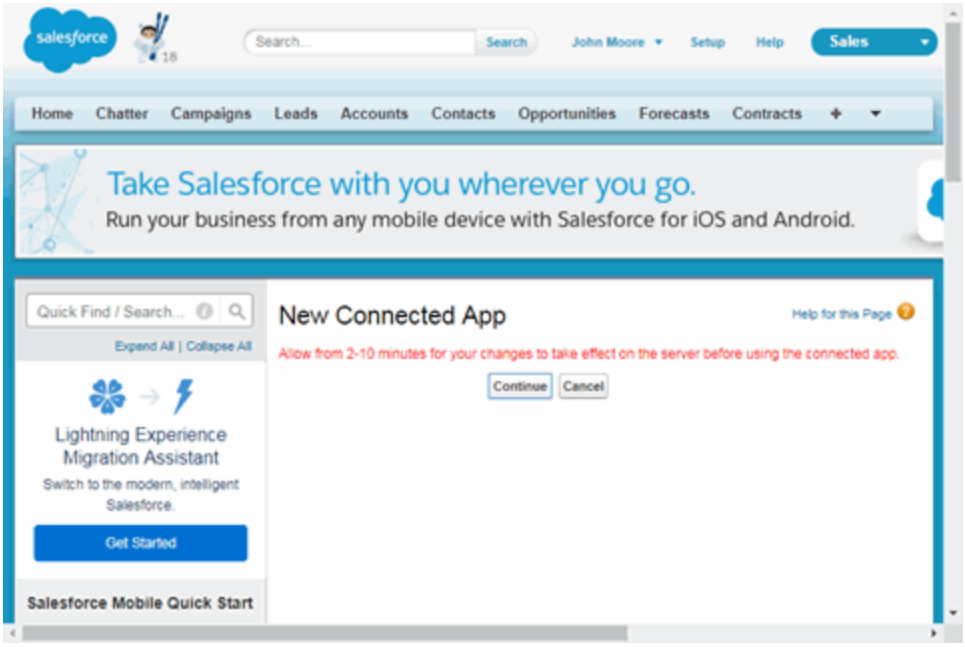
12. Select **Access your basic information (id, profile, email, address, phone)**, **Full access (full)**, and **Allow access to your unique identifier (openid)**, then select the **Add** icon in the Selected OAuth Scopes section of the window to add the scopes to the Selected OAuth Scopes list.
13. Select the **Require Secret for Web Server Flow**, **Include ID Token** and **Include Standard Claims** checkboxes.


API (Enable OAuth Settings)
Enable OAuth Settings
Enable for Device Flow
Callback URL
https://<AccessControlengineFQDN>/Salesforce_OpenID
Use digital signatures
Selected OAuth Scopes
Available OAuth Scopes
Access and manage your Chatter data (chatter_api)
Access and manage your Eclair data (eclair_api)
Access and manage your Wave data (wave_api)
Access and manage your data (api)
Access custom permissions (custom_permissions)
Perform requests on your behalf at any time (refresh_token, offline_access)
Provide access to custom applications (visualforce)
Provide access to your data via the Web (web)
Selected
Access your basic information
Allow access to your unique id
Full access (full)
Add
Remove
Require Secret for Web Server Flow
Include ID Token
Include Standard Claims
Include Custom Attributes
Include Custom Permissions
Enable Single Logout
Enable Asset Tokens
Web App Settings
Start URL
Enable SAML
Custom Connected App Handler
Apex Plugin Class
Run As
Mobile App Settings
Mobile Start URL
PIN Protect
App Platform
Restrict to Device Type
App Version
Minimum OS Version
Private App
App Binary URL
Push Messaging Enabled
Canvas App Settings
Force.com Canvas
Save
Cancel

14. Select **Save**.

    Your application is created and ready to use.

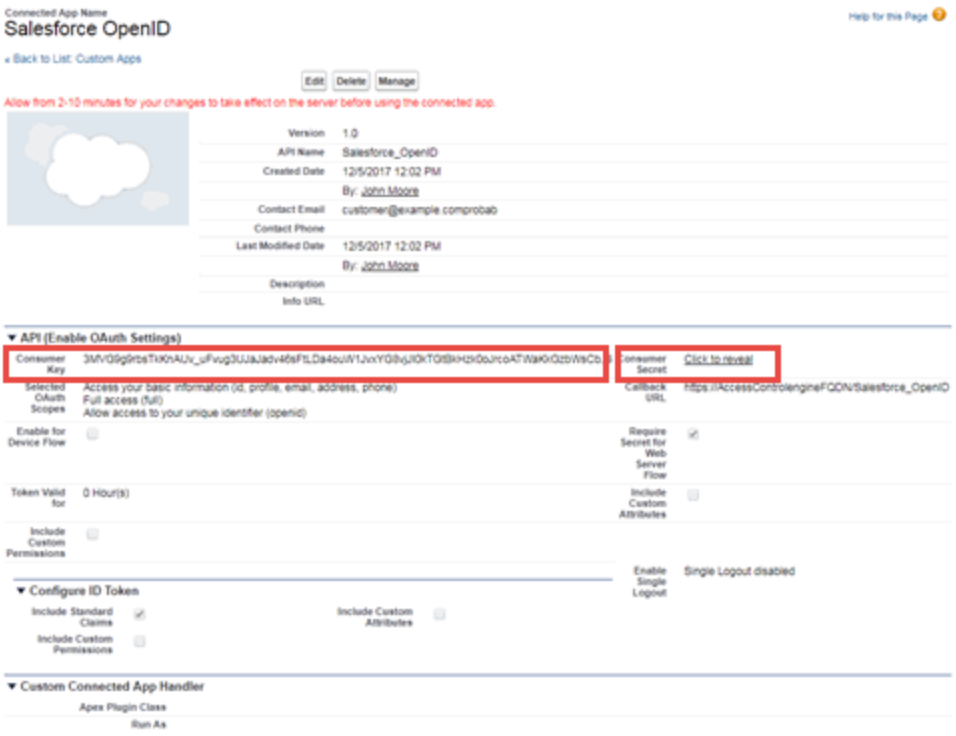
    The **New Connected App** window opens.



15. Select **Continue**.

    The **Connected App** window opens.

16. Select the **Click to reveal** link in the **Consumer Secret** field and copy the **Consumer Secret** and **Consumer Key**.

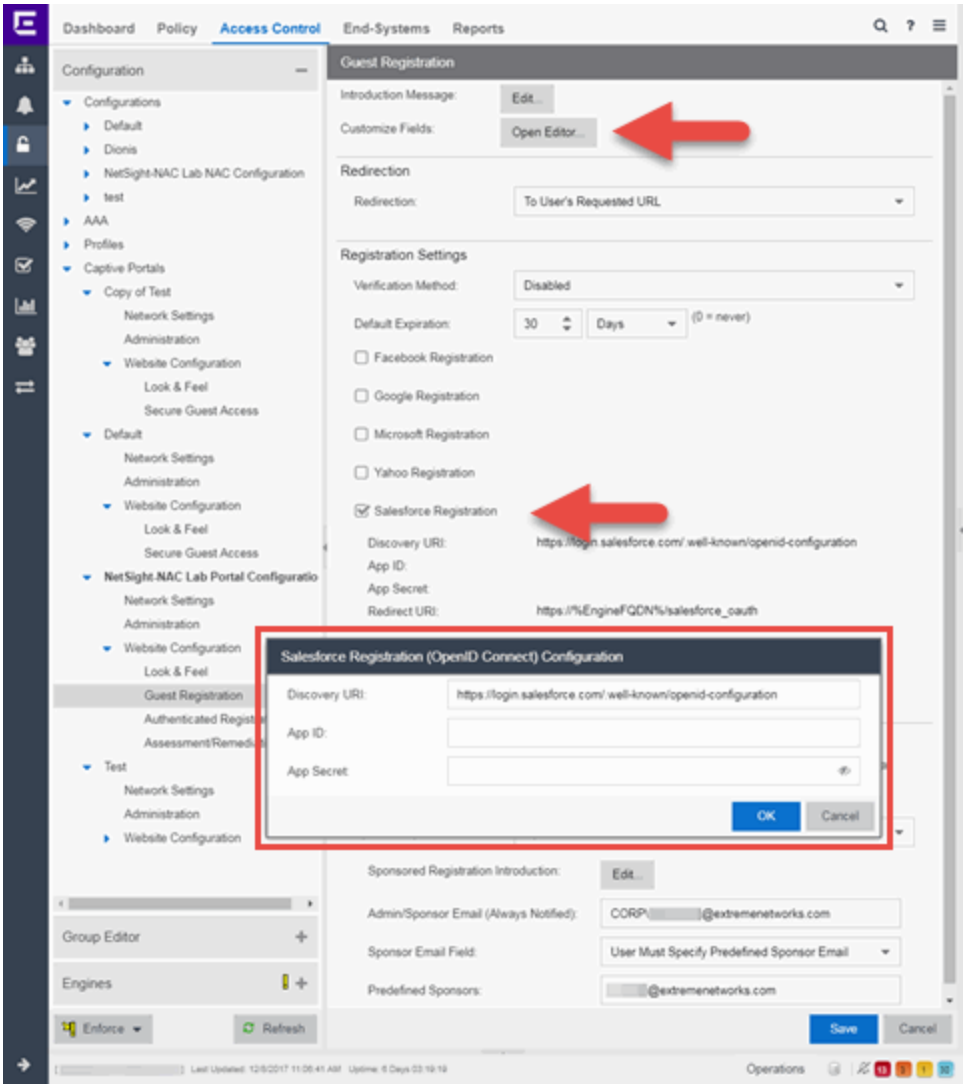


You need to add the Consumer Key and Consumer Secret to your portal configuration.

Portal Configuration

The client ID and client secret assigned during the creation of the Salesforce application must be provided in the Portal Configuration in order for the entire process to complete properly.

1. Open the **Control** > **Access Control** tab.
2. In the left-panel tree, expand the Access Control Configurations > Portal tree and select Guest Registration.



3. In the Customize Fields section, select the **Open Editor** button to open the Manage Custom Fields window where you can change registration portal fields. Salesforce registration uses only the First Name, Last Name, and Email Address fields, and the Display Acceptable Use Policy (AUP) option. All other fields only apply to regular guest registration. If the Display AUP option is selected, the captive portal verifies that the AUP has been acknowledged before redirecting the user to Salesforce.
4. Select the **Salesforce Registration** checkbox.
5. Enter the Consumer Key in the **App ID** field and the Consumer Secret in the **App Secret** field.
6. Select **Save**. Warning messages display stating that Verification Method and Sponsorship are not used for Salesforce registration, and that an FDQN is required will be enabled.
7. Enforce the new configuration to your engines.

How Salesforce Registration Works

After you have configured Salesforce registration using the steps above, this is how the registration process works:

1. The end user attempts to access an external Web site. Their HTTP traffic is redirected to the captive portal.
2. In the Guest Registration Portal, the end user selects the option to register using Salesforce.
3. The end user is redirected to the Salesforce login. If Acceptable Use Policy option is configured, the captive portal verifies that the AUP has been acknowledged before redirecting the user to Salesforce.
4. When logged in, the end user is presented with the information that ExtremeCloud IQ Site Engine receives from Salesforce.
5. The end user grants ExtremeCloud IQ Site Engine access to the Salesforce information and is redirected back to the captive portal where they see a "Registration in Progress" message.
6. Salesforce provides the requested information to ExtremeCloud IQ Site Engine, which uses it to populate the user registration fields.
7. The registration process completes and network access is granted.
8. The word "Salesforce" is added to the user name so you can easily search for Salesforce registration via the Registration Administration web page.

Special Deployment Considerations

Read the following deployment consideration prior to configuring Salesforce Registration.

To provide access to your network via a wireless connection, create an L7 host record for the **Unregistered Role** on your Wireless Controller for `login.Salesforce.com`. This domain is subject to change and can vary based on location.

Networks using DNS Proxy

Salesforce Registration for networks redirecting HTTP traffic to the captive portal using DNS Proxy requires additional configuration.

In order for Salesforce Registration to work properly with DNS Proxy, **all** domains/URLs necessary to properly load the Salesforce web page must be added to the Allowed URLs/Allowed Domains section of the captive portal configuration. Otherwise, the ExtremeControl engine resolves DNS queries for these components to the Access Control engine IP causing the page to not load properly.

As of February 2017, you must add the following domains in order for Salesforce registration to work with DNS Proxy. This domain is subject to change and can vary based on location.

login.Salesforce.com

- Portal Configuration

How to Implement Microsoft Entra ID Registration with OpenID

This topic describes how to implement authenticated registration using OAuth 2.0 OpenID Connect with Microsoft Entra ID (formerly Azure AD). For more information, watch the Entra ID with OpenID video.

A common use case for this configuration is to apply different network authorizations to different users based on their security group membership in Entra ID.

This topic includes the following information and instructions:

- Requirements for Entra ID Registration
- Create an Entra ID Application
- Configure the Captive Portal
- Configure User Groups
- Configure Access Control Rules
- Configure Custom Security Attributes and Extension Attributes
- Configure a Multiple NIC Environment
- Deployment Considerations

Requirements for Entra ID Registration

Entra ID registration has the following requirements:

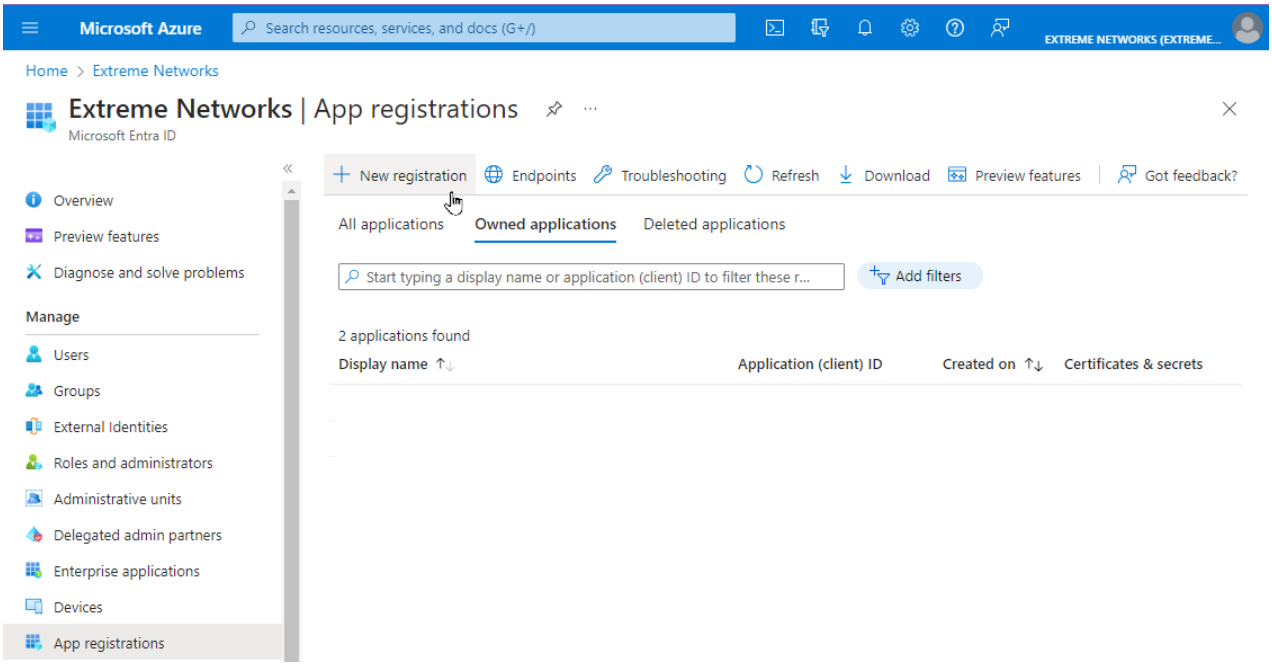
- The Access Control engine must have Internet access to retrieve user information from Microsoft.
- The ExtremeControl Unregistered access policy must allow access to the Microsoft site (either allow all SSL or make allowances for Microsoft servers).
- Create a unique Microsoft Entra ID application on the Microsoft Entra ID page (see Create an Entra ID Application).
- The Portal Configuration must have Microsoft Registration enabled and include the Microsoft registered Application ID and Application Secret (see Configure the Captive Portal).

NOTE: You must copy and paste some text values between applications during the registration and configuration.
When instructed, copy and save the required values. Some values are unique secret values that you cannot view or receive again.

Create an Entra ID Application

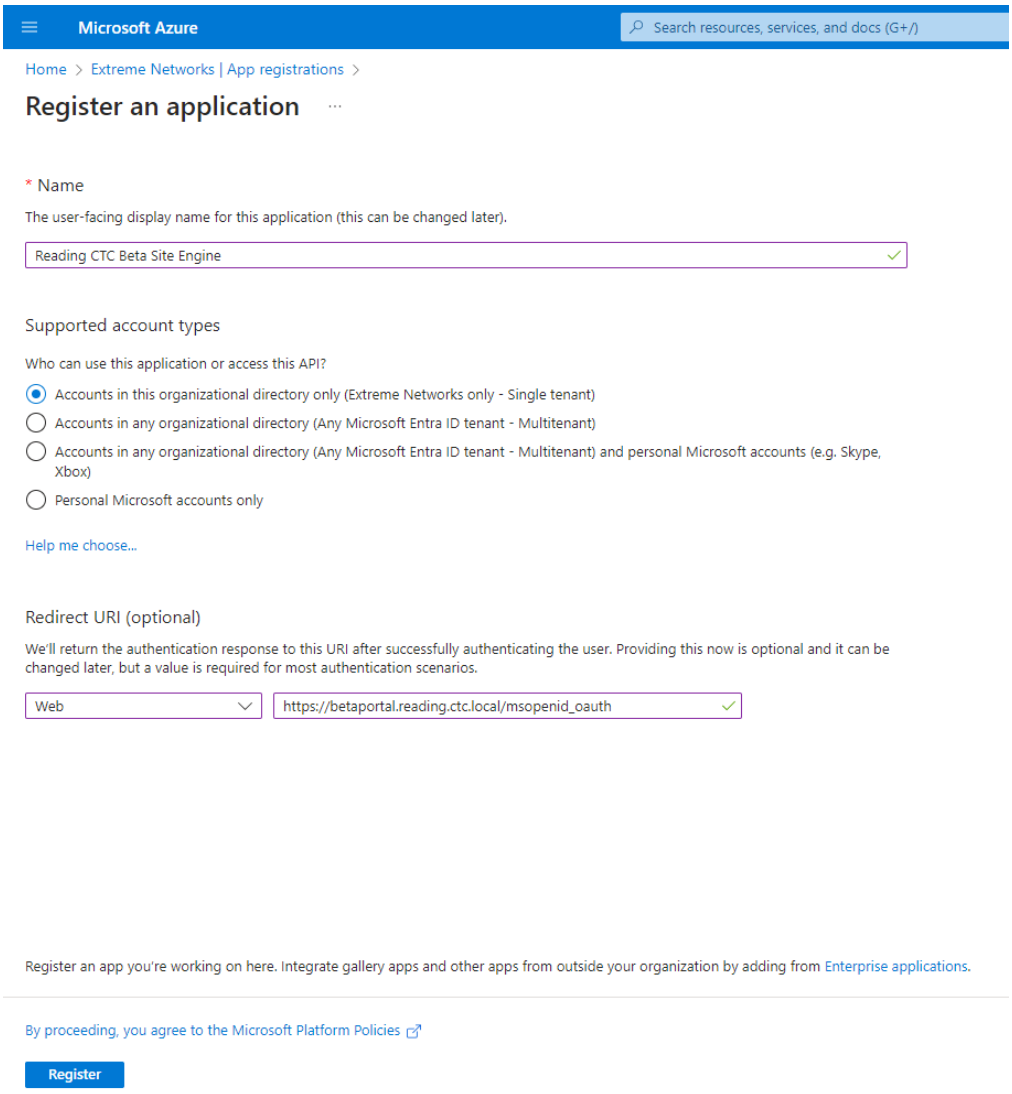
To implement authenticated registration using Entra ID and OpenID Connect, you must first create an Entra ID application. Registering the application generates an Application ID and Application Secret that ExtremeCloud IQ Site Engine requires. To create and register an Entra ID application:

1. Sign in to the Microsoft Entra ID page with your administrator credentials at https://portal.azure.com or https://entra.microsoft.com.
2. Select **Manage Microsoft Entra ID > View**.
3. Select **App registrations > New registration**.



4. Enter the following information in the required fields:
   - **Name** – Enter a name for the Entra ID registered application
   - **Supported account types** – Select Accounts in this organization directory only – (Single tenant)
   - **Redirect URI (Optional)** – Select a platform: Web
   - **Redirect URI (Optional)** – Enter a URI that uses HTTP or HTTPS with the FQDN of the captive portal followed by /msopenid_oauth
   - **NOTE:** The best practice is to use HTTPS and install a trusted certificate as the Captive Portal Server Certificate on the Access Control Engine.

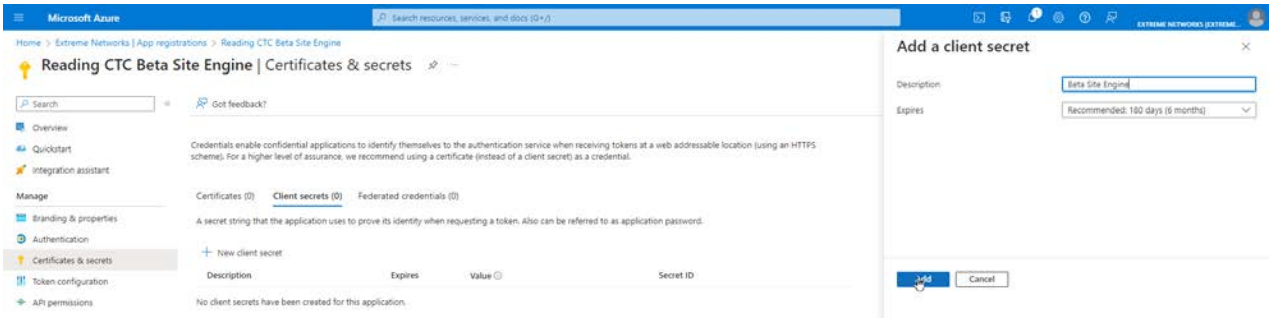
5. Select **Register**.



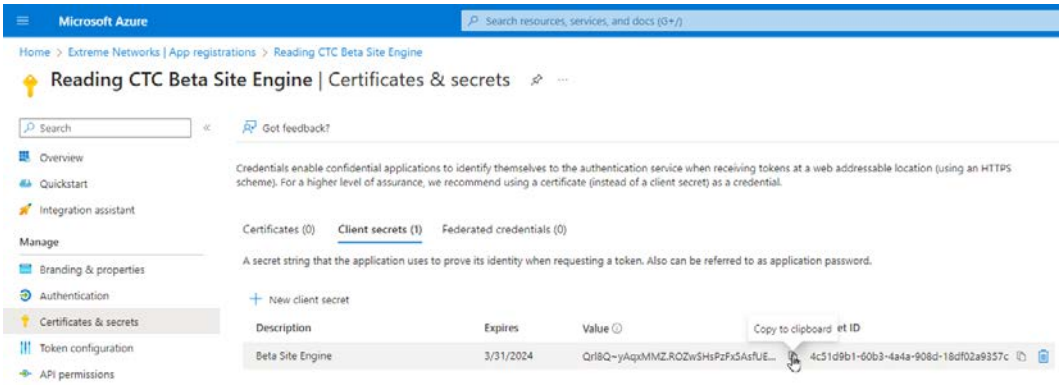
6. Select **Add a certificate or secret**, or in the left menu, select **Certificates & secrets**.
7. Select **New client secret**.
8. Enter the following information in the required fields:
    - **Description** – enter a description of the new credentials
    - **Expires** – specify how long the client secret is valid. When the client secret expires, users cannot authenticate.

- **NOTE:** You cannot modify the expiration of the client secret in Entra ID. The best practice is to create a new client secret before the existing one expires and update the value in ExtremeControl settings.

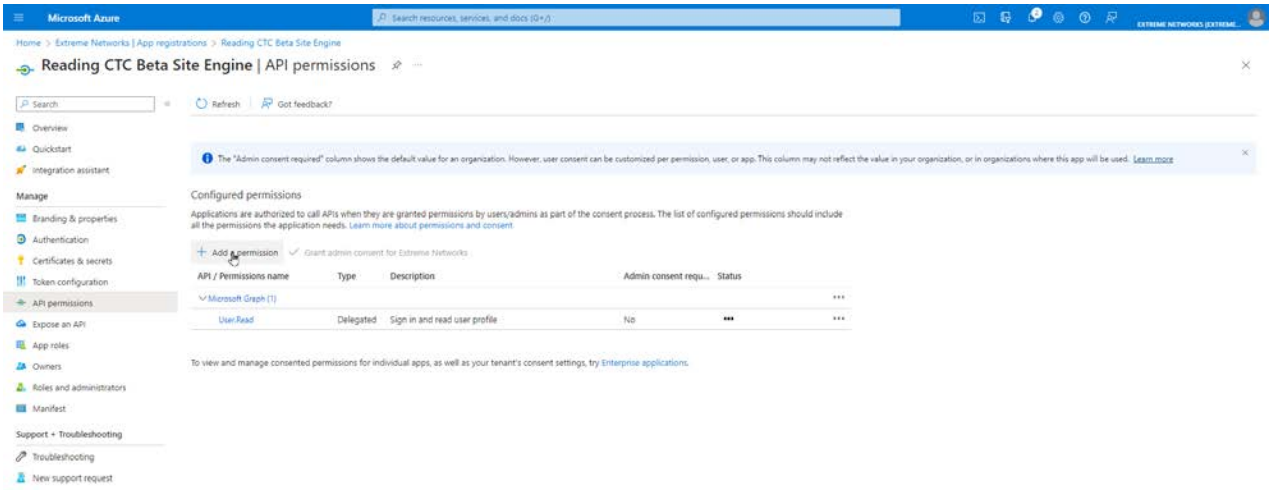
9. Select **Add**.



10. Copy the secret value to the clipboard. This is the only time that Entra ID displays the client secret. Save the secret value for your App Secret.

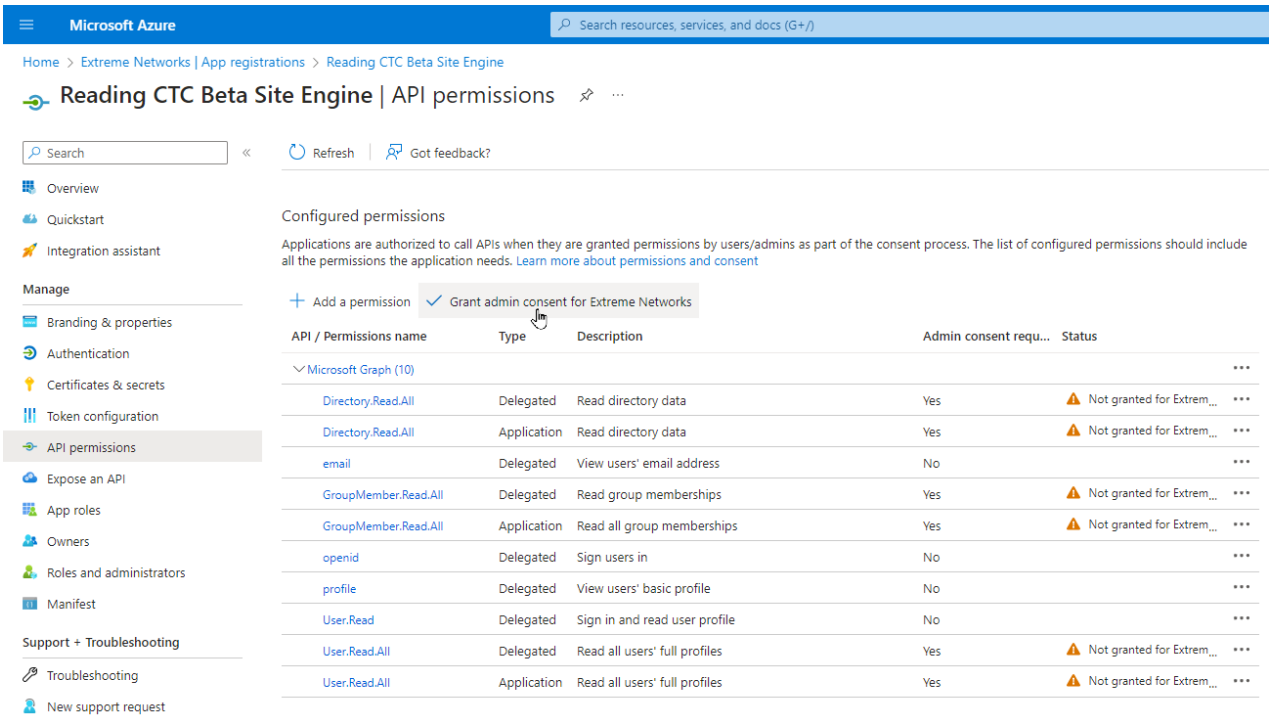


11. Select **API permissions > Add a permission**.



12. Select **Microsoft Graph > Delegated permissions**.
13. Select the following delegated permissions:
    - In the **OpenID group**, select:
      - **email**
      - **openid**
      - **profile**
14. If different users require different authorization based on security group membership, select the following additional delegated permissions:
    - In the **DirectoryRecommendations group**, select:
      - **DirectoryRecommendations.Read.All**
    - In the GroupMember group, select:
      - GroupMember.Read.All
    - In the User group, select:
      - User.Read.All
    - To check the values of Custom Security Attributes, select CustomSecAttributeAssignment:
      - CustomSecAttributeAssignment.Read.All
15. If you performed the previous step, select Application permissions, and add the following additional permissions:
    - In the DirectoryRecommendations group, select:
      - DirectoryRecommendations.Read.All
    - In the GroupMember group, select:
      - GroupMember.Read.All
    - In the User group, select:
      - User.Read.All
    - To check the values of Custom Security Attributes, select CustomSecAttributeAssignment:
      - CustomSecAttributeAssignment.Read.All
16. Select **Add permissions**.

17. Select **Grant admin consent for <your company domain>**, and select **Yes** to confirm.



18. Select **Overview**.
19. Copy the displayed **Application (client) ID** value. Save this value for your App ID.
20. Select **Endpoints**.
21. Copy the displayed **OAuth 2.0 token endpoint (v2)** value. Save this value for your Token Endpoint.
22. Copy the **OpenID Connect metadata document** value. Save this value for your Discovery URI.

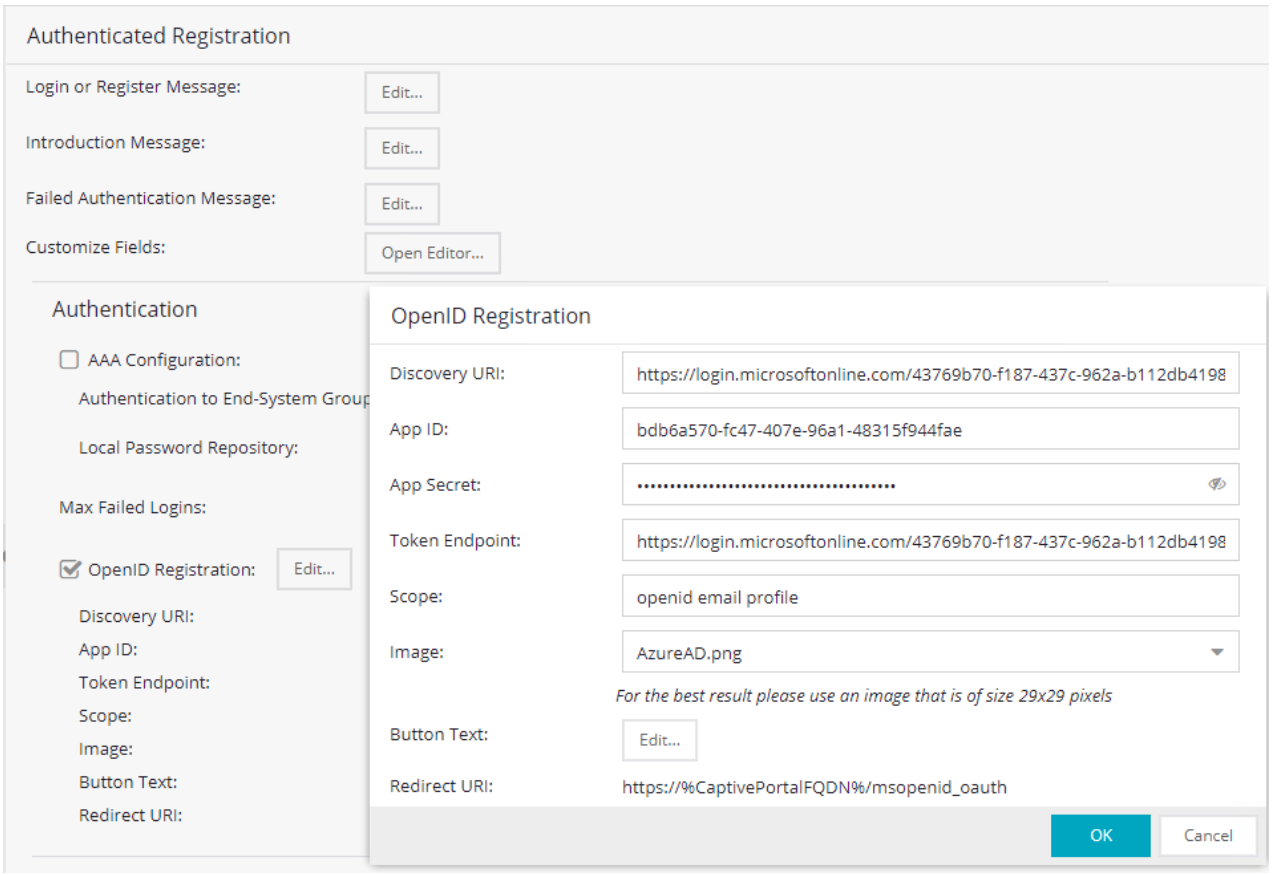
Configure the Captive Portal

In the Portal Configuration, enter the values that you saved when you created and registered the Entra ID application.

To configure authenticated registration using OpenID in the captive portal:

1. In ExtremeCloud IQ Site Engine, go to the **Control** > **Access Control** tab.
2. In the left-panel tree, go to **Configuration > Captive Portals >** *your portal* **> Website Configuration**.
3. Select **Authentication Settings**.
4. Select **Authenticated Registration**, and then select **Save**.
5. In the left-panel tree, go to **Website Configuration > Authenticated Registration**.

6. Select the **OpenID Registration** check box.
7. Select **Edit**.



8. Enter the following information in the required fields:
    - **Discovery URI** – enter the value copied as "OpenID Connect metadata document".
    - **App ID** – enter the value copied as "Application (client) ID".
    - **App Secret** – enter the value copied as "Client Secret".
    - **Token Endpoint** – enter the value copied as "OAuth 2.0 token endpoint (v2)".
    - **Scope** – enter "openid email profile".
    - **Group Source** – keep the default value, "Entra ID".
    - **Image** – optional picture to display to the user at the captive portal.
    - **Button Text** – text presented on the button. To define the text in different languages, use **Website Configuration > Look & Feel > Launch Message String Editor**.
    - **Redirect URI** – information only, not configurable. Indicates where the OpenID process redirects the user after the authentication is successful.

9. Select **Test Credentials...** to verify the connectivity, App ID, App Secret, and Token Endpoint.
10. Select **OK**.
11. Select **Save**.
12. Select **Enforce** to enforce the new configuration on your engines.

Configure User Groups

After you configure the captive portal for OpenID registration, use the following steps to configure a user group:

1. In ExtremeCloud IQ Site Engine, go to **Control** > **Access Control** > **Group Editor** > **User Groups**.
2. Select **Add**.
3. For **Name**, enter a name for the user group.
4. (Optional) For **Description**, enter a description for the user group.
5. For **Mode**, select Match Any or Match All to specify whether a user must match any or all of the attributes to be added to the group.
6. In the Create Group area, select **Add**.
7. For **Attribute Name**, enter one or any of the following:
    - **memberOf** to check the Entra ID security group membership
    - **extensionAttribute1** to check Entra ID Extension Attribute 1
    - **extensionAttribute2** to check Entra ID Extension Attribute 2
    - **extensionAttribute3** to check Entra ID Extension Attribute 3
    - **extensionAttribute4** to check Entra ID Extension Attribute 4
    - **extensionAttribute5** to check Entra ID Extension Attribute 5
    - **extensionAttribute6** to check Entra ID Extension Attribute 6
    - **extensionAttribute7** to check Entra ID Extension Attribute 7
    - **extensionAttribute8** to check Entra ID Extension Attribute 8
    - **extensionAttribute9** to check Entra ID Extension Attribute 9
    - **extensionAttribute10** to check Entra ID Extension Attribute 10
    - **extensionAttribute11** to check Entra ID Extension Attribute 11
    - **extensionAttribute12** to check Entra ID Extension Attribute 12
    - **extensionAttribute13** to check Entra ID Extension Attribute 13
    - **extensionAttribute14** to check Entra ID Extension Attribute 14

- **extensionAttribute15** to check Entra ID Extension Attribute 15
- **<custom security attribute>** to check Entra ID for a Custom Security Attribute
-

NOTE: You can add one or more of the attributes, in any order.

You can use the predefined Attribute Names and Attribute Values from Entra ID (memberOf and extensionAttribute1 through extensionAttribute15).

If you do not use the predefined names and values, add a Custom Security Attribute name and value to check and match with your Entra ID configuration.

8. For **Attribute Value**, enter the name of the security group (for memberOf), the value of the extension attribute (for extensionAttribute), or the value of the custom security attribute. You can match the exact name or value, or use the wildcard character (*).
9. Select **Save**.

Configure Access Control Rules

After you configure the captive portal and user groups, use the following steps to configure an Access Control rule:

1. In ExtremeCloud IQ Site Engine, go to **Control** > **Access Control** > **Configuration** > *your configuration* > **Rules**.
2. Select **Add**.
3. For **Name**, enter a name for the rule.
4. Select the **Rule Enabled** check box.
5. For **Description**, enter a description for the rule.
6. For **User Group**, select the user group that you created in Configure User Groups.
7. For **End System Group**, select **Web Authenticated Users**.
8. Select **Save**.
9. Select **Enforce** to enforce the new configuration on your engines.

Configure Custom Security Attributes and Extension Attributes

To configure custom security attributes and extension attributes:

1. In ExtremeCloud IQ Site Engine, go to **Control > Access Control > Configuration > Global & Engine Settings > Engine Settings >** *config name* **> Miscellaneous**.
2. To check the values of Custom Security Attributes in Entra ID, enable **Resolve Custom Security Attributes from EntraID**.
3. To check the values of Extension Attributes in Entra ID, enable **Resolve Extension Attributes from EntraID**.

Configure a Multiple NIC Environment

As a best practice for security, keep Management and Control traffic separate from user traffic.

After you configure the captive portal, user groups, and Access Control rules, you can configure a multiple NIC environment:

1. In ExtremeCloud IQ Site Engine, go to **Control** > **Access Control** > **Engines** > **Engine Groups** > *your group* > *your engine*.
2. Select **Details**, and then in the Interface Summary area, select **Edit**.
3. In the eth0 area, for **Mode**, select **Management Only**.
   The eth0 NIC is now configured for Management, Monitoring Services, Network Services, AAA Servers, Device, Portal: Management, and Traffic Snooping.
4. In the eth1 area, for **Mode**, select **Registration & Remediation Only**.
   The eth1 NIC is now configured for communication with End-System and Traffic Snooping, and also configured to communicate with Entra ID.
   IMPORTANT: Internet access must be available from the eth1 NIC.
5. In the eth1 area, for **Host Name**, enter the FQDN of the Redirect URI.
6. Select **Save**.
7. Select **Enforce** to enforce the new configuration on your engines.

Deployment Considerations

Read the following deployment considerations before you implement an Entra ID authenticated registration configuration:

- The best practice for the captive portal configuration is to use HTTPS and an FQDN.
- You can configure a High Availability Captive Portal by using multiple DNS records for the same FQDN.
- After a successful authentication at Entra ID, the web browser is redirected to the NIC of the Access Control Engine where the captive portal is enabled. If multiple NICs are configured, the lowest-numbered NIC that has Registration & Remediation enabled is used. For example, if you

configured Entra ID registration with OpenID and multiple NICs have the captive portal enabled, the lowest-numbered NIC is used for the web browser redirection.

- If the Access Control Engine is configured as a proxy, you must update the Allowed Web Sites.

- How to Update ExtremeControl Engine Server Certificates
- Manage Certificates

How to Implement 802.1X EAP-TTLS Authentication with Microsoft Entra ID

Multiple options exist for implementing IEEE 802.1X with Microsoft Entra ID (formerly Azure AD) integration. This topic describes how to implement 802.1X EAP-TTLS authentication and OAuth 2.0 authorization with Entra ID. For more information, watch the Entra ID with 802.1X video.

A common use case for this configuration is to apply different network authorizations to different users based on their security group membership in Entra ID.

This topic includes the following information and instructions:

- Requirements for Entra ID Registration
- Create an Entra ID Application
- Configure AAA Rules
- Configure User Groups
- Configure Access Control Rules
- Configure Custom Security Attributes and Extension Attributes
- Configure 802.1X on the End-System

Requirements for Entra ID Registration

Entra ID registration has the following requirements:

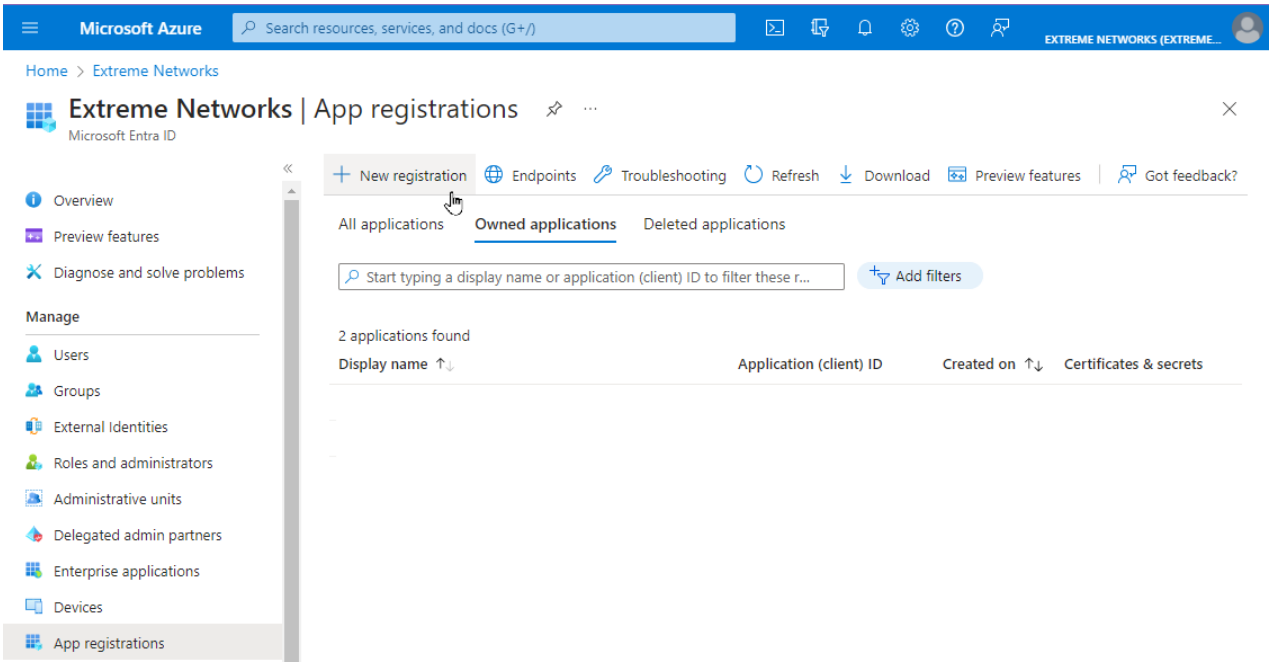
- The Access Control Engine must have Internet access to retrieve user information from Microsoft.
- Create a unique Microsoft Entra ID application on the Microsoft Entra ID page (see Create an Entra ID Application).
- The client must trust the RADIUS Certificate used by the Access Control Engine. Standard Windows clients reject the default self-signed certificate, and the authentication fails with the message "Authentication became stale".
- Multi-factor authentication (MFA) must be disabled for the app when you use EAP-TTLS.

NOTE: You must copy and paste some text values between applications during the registration and configuration.
When instructed, copy and save the required values. Some values are unique secret values that you cannot view or receive again.

Create an Entra ID Application

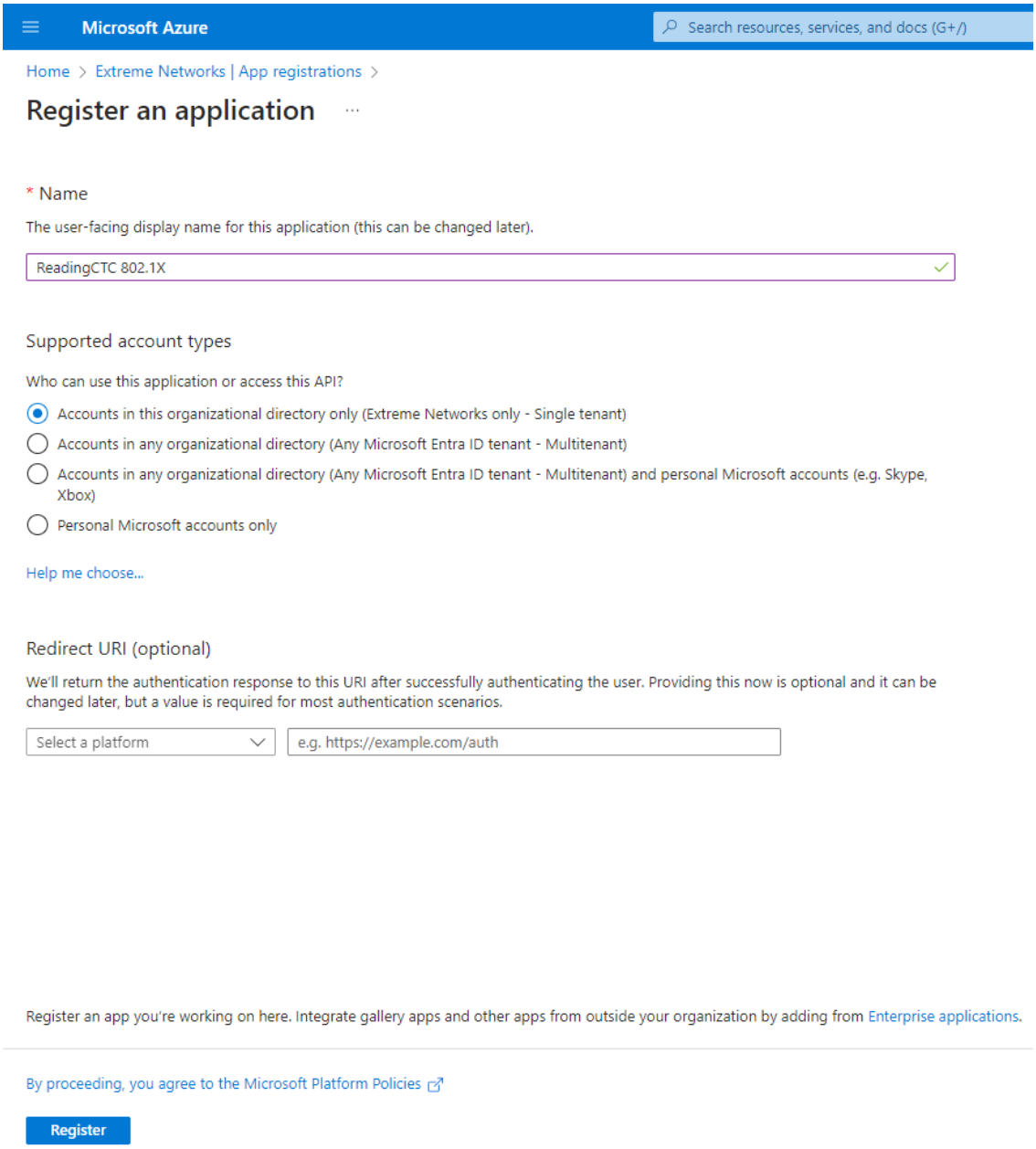
To implement 802.1X authentication using Entra ID and OAuth 2.0, you must first create an Entra ID application. Registering the application generates an Application ID and Application Secret that ExtremeCloud IQ Site Engine requires. To create and register an Entra ID application:

1. Sign in to the Microsoft Entra ID page with your administrator credentials at https://portal.azure.com or https://entra.microsoft.com.
2. Select **Manage Microsoft Entra ID > View**.
3. Select **App registrations > New registration**.



4. Enter the following information in the required fields:
   - **Name** – Enter a name for the Entra ID registered application
   - **Supported account types** – Select Accounts in this organization directory only – (Single tenant)

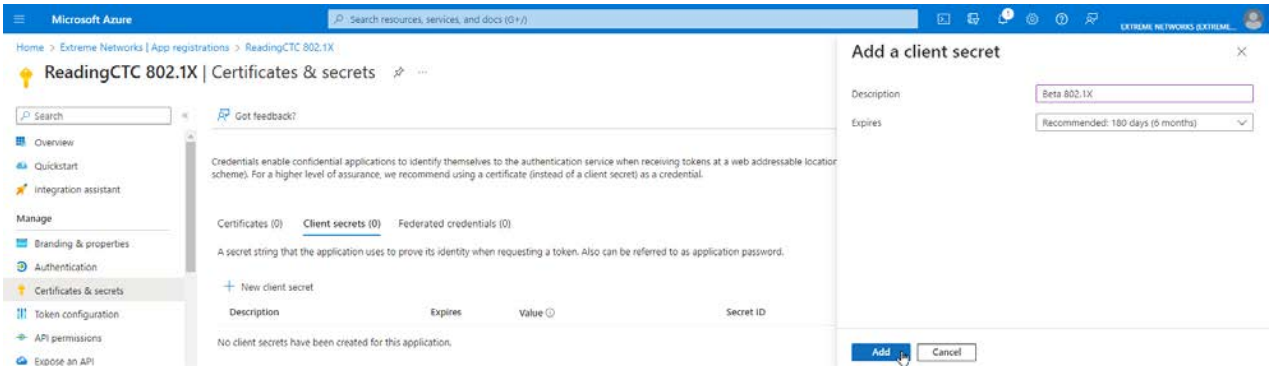
5. Select **Register**.



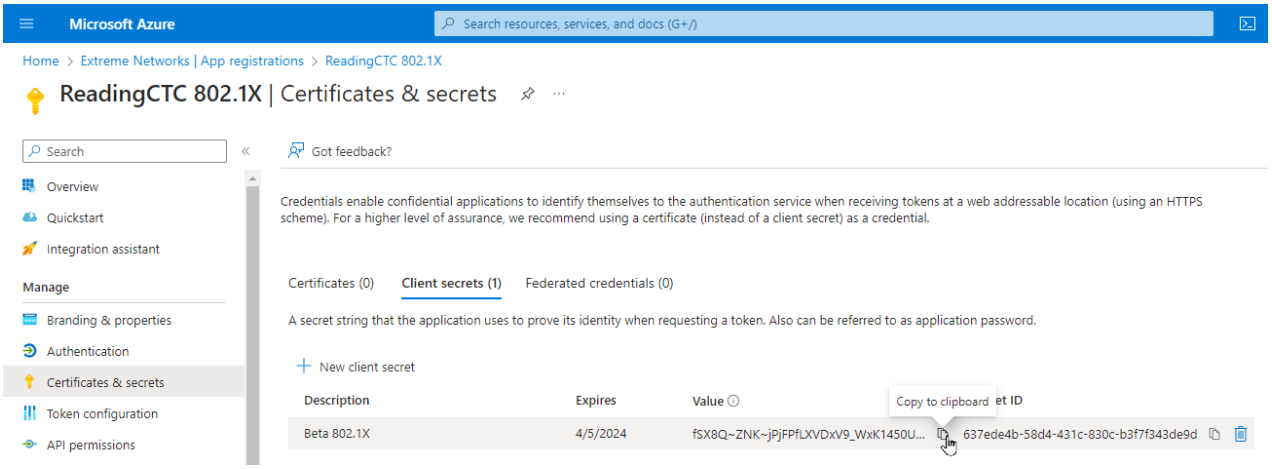
6. Select **Add a certificate or secret**, or in the left menu, select **Certificates & secrets**.
7. Select **New client secret**.
8. Enter the following information in the required fields:
    - **Description** – enter a description of the new credentials
    - **Expires** – specify how long the client secret is valid. When the client secret expires, users cannot authenticate.

- **NOTE:** You cannot modify the expiration of the client secret in Entra ID. The best practice is to create a new client secret before the existing one expires and update the value in ExtremeControl settings.

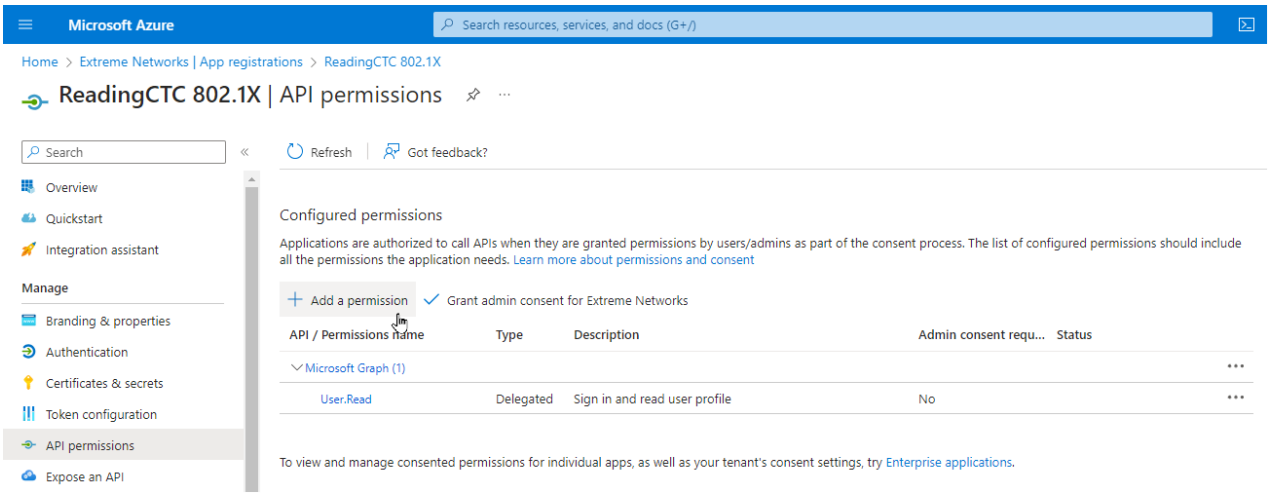
9. Select **Add**.



10. Copy the secret value to the clipboard. This is the only time that Entra ID displays the client secret. Save the secret value for your App Secret.

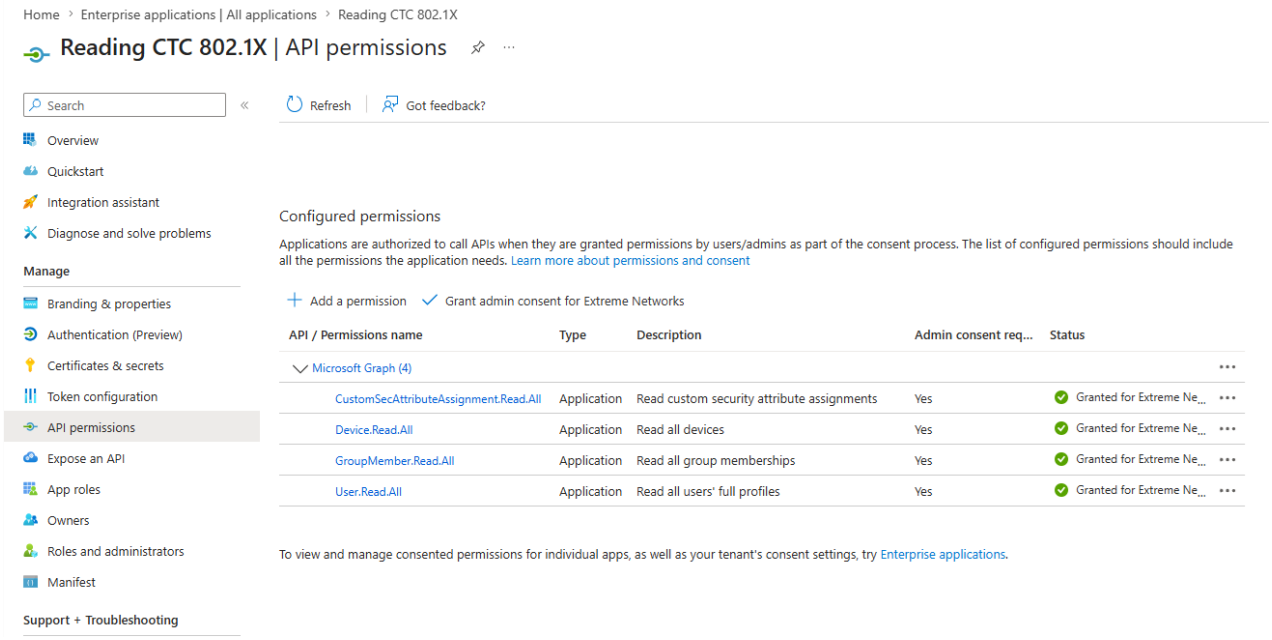


11. Select **API permissions > Add a permission**.



12. Select **Microsoft Graph > Delegated permissions**.
13. If different users require different authorization based on security group membership, select the following additional delegated permissions:
    - In the **DirectoryRecommendations group**, select:
        - **DirectoryRecommendations.Read.All**
    - In the **GroupMember group**, select:
        - **GroupMember.Read.All**
    - In the **User group**, select:
        - **User.Read.All**
    - To check the values of Custom Security Attributes, select **CustomSecAttributeAssignment**:
        - **CustomSecAttributeAssignment.Read.All**
14. If you performed the previous step, select **Application permissions**, and add the following additional permissions:
    - In the **DirectoryRecommendations group**, select:
        - **DirectoryRecommendations.Read.All**
    - In the **GroupMember group**, select:
        - **GroupMember.Read.All**
    - In the **User group**, select:

        - User.Read.All
    - To check the values of Custom Security Attributes, select CustomSecAttributeAssignment:
        - CustomSecAttributeAssignment.Read.All
15. Select **Add permissions**.
16. Select **Grant admin consent for <your company domain>**, and select **Yes** to confirm.



17. Select **Overview**.
18. Copy the displayed **Application (client) ID** value. Save this value for your App ID.
19. Select **Endpoints**.
20. Copy the displayed **OAuth 2.0 token endpoint (v2)** value. Save this value for your Token Endpoint.

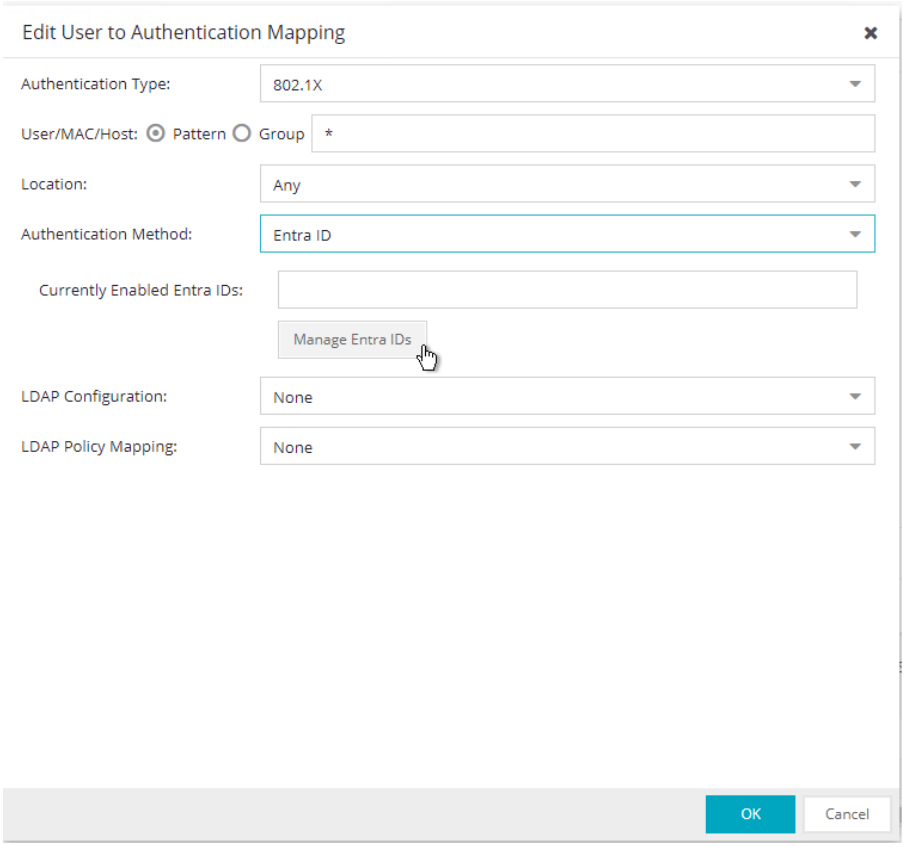
Configure AAA Rules

In the AAA Configuration, enter the values that you saved when you created and registered the Entra ID application.

To configure 802.1X authentication with Entra ID:

1. In ExtremeCloud IQ Site Engine, go to the **Control** > **Access Control** tab.
2. In the left-panel tree, go to **Configuration > AAA >** *your advanced configuration*.
3. In the Authentication Rules area, select **Add**.

4. For **Authentication Type**, select **802.1X**.
5. For **User/MAC/Host**, select **Pattern** of usernames to use the AAA rule.
6. For **Authentication Method**, select **Entra ID**.
7. Select **Manage Entra IDs**.



8. Select **Add**.
9. Enter the following information in the required fields:
    - **Enable** – select the check box.
    - **Entra ID Name** – enter the name of this Entra ID. The name has local meaning only.
    - **Realm** – specifies the Entra ID configuration to use based on the username. Realm is usually the part after the @ in the login username.
    - **App ID** – enter the value copied as "Application (client) ID".
    - **App Secret** – enter the value copied as "Client Secret".
    - **Token Endpoint** – enter the value copied as "OAuth 2.0 token endpoint (v2)".
10. Select **Test Credentials...** to verify the connectivity, App ID, App Secret, and Token Endpoint.
11. Select **OK**.

12. Select **Save**.
13. Select **Enforce** to enforce the new configuration on your engines.

Configure User Groups

After you configure the AAA rules for 802.1X, use the following steps to configure a user group:

1. In ExtremeCloud IQ Site Engine, go to **Control** > **Access Control** > **Group Editor** > **User Groups**.
2. Select **Add**.
3. For **Name**, enter a name for the user group.
4. (Optional) For **Description**, enter a description for the user group.
5. For **Mode**, select Match Any or Match All to specify whether a user must match any or all of the attributes to be added to the group.
6. In the Create Group area, select **Add**.
7. For **Attribute Name**, enter one or any of the following:
    - **memberOf** to check the Entra ID security group membership
    - **extensionAttribute1** to check Entra ID Extension Attribute 1
    - **extensionAttribute2** to check Entra ID Extension Attribute 2
    - **extensionAttribute3** to check Entra ID Extension Attribute 3
    - **extensionAttribute4** to check Entra ID Extension Attribute 4
    - **extensionAttribute5** to check Entra ID Extension Attribute 5
    - **extensionAttribute6** to check Entra ID Extension Attribute 6
    - **extensionAttribute7** to check Entra ID Extension Attribute 7
    - **extensionAttribute8** to check Entra ID Extension Attribute 8
    - **extensionAttribute9** to check Entra ID Extension Attribute 9
    - **extensionAttribute10** to check Entra ID Extension Attribute 10
    - **extensionAttribute11** to check Entra ID Extension Attribute 11
    - **extensionAttribute12** to check Entra ID Extension Attribute 12
    - **extensionAttribute13** to check Entra ID Extension Attribute 13
    - **extensionAttribute14** to check Entra ID Extension Attribute 14
    - **extensionAttribute15** to check Entra ID Extension Attribute 15
    - **<custom security attribute>** to check Entra ID for a Custom Security Attribute

- You can add one or more of the attributes, in any order.

  NOTE: You can use the predefined Attribute Names and Attribute Values from Entra ID (memberOf and extensionAttribute1 through extensionAttribute15).

  If you do not use the predefined names and values, add a Custom Security Attribute name and value to check and match with your Entra ID configuration.

8. For **Attribute Value**, enter the name of the security group (for memberOf), the value of the extension attribute (for extensionAttribute), or the value of the custom security attribute. You can match the exact name or value, or use the wildcard character (*).
9. Select **Save**.

Configure Access Control Rules

After you configure the 802.1X AAA rules and user groups, use the following steps to configure an Access Control rule:

1. In ExtremeCloud IQ Site Engine, go to **Control** > **Access Control** > **Configuration** > *your configuration* > **Rules**.
2. Select **Add**.
3. For **Name**, enter a name for the rule.
4. Select the **Rule Enabled** check box.
5. For **Description**, enter a description for the rule.
6. For **User Group**, select the user group that you created in Configure User Groups.
7. For **Authentication Method**, select **802.1X (TTLS)**.
8. Select **Save**.
9. Select **Enforce** to enforce the new configuration on your engines.

Configure Custom Security Attributes and Extension Attributes

To configure custom security attributes and extension attributes:

1. In ExtremeCloud IQ Site Engine, go to **Control > Access Control > Configuration > Global & Engine Settings > Engine Settings >** *config name* **> Miscellaneous**.

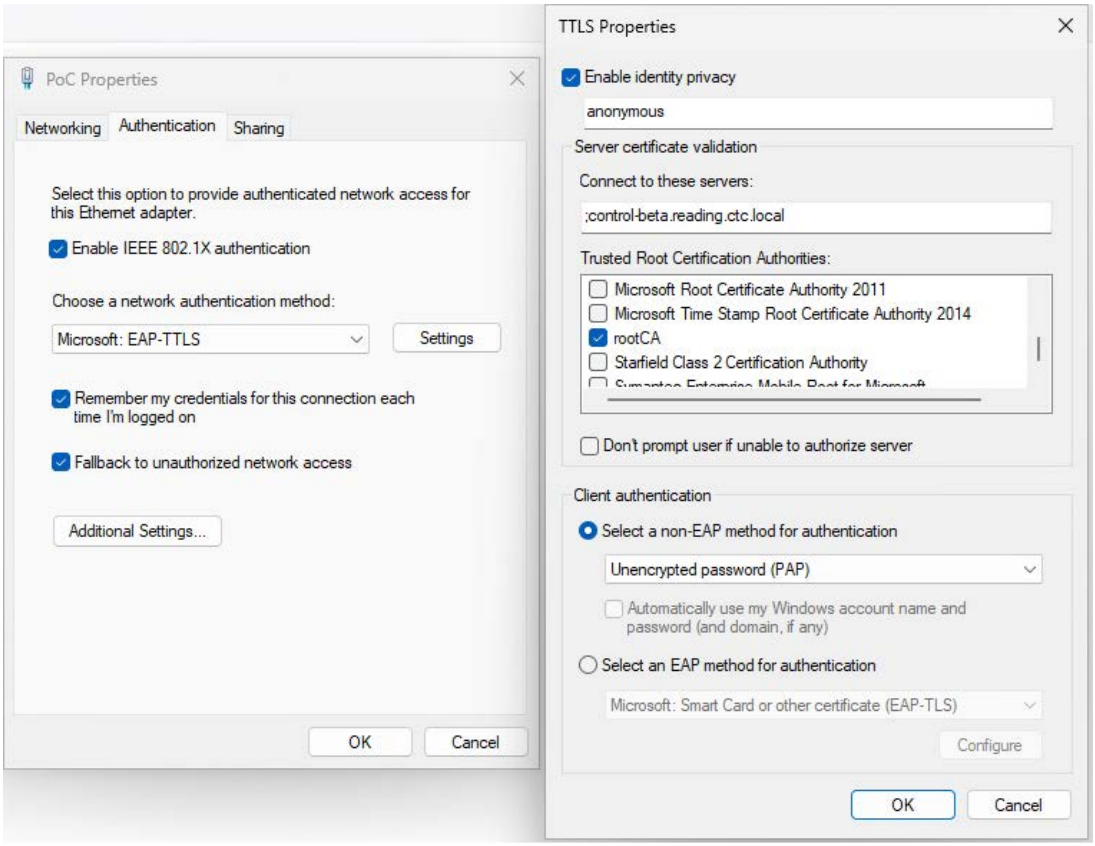
2. To check the values of Custom Security Attributes in Entra ID, enable **Resolve Custom Security Attributes from EntraID**.
3. To check the values of Extension Attributes in Entra ID, enable **Resolve Extension Attributes from EntraID**.

Configure 802.1X on the End-System

You must configure the end-system to use IEEE 802.1X authenticated network access. The following example uses a Windows 11 client.

After you configure the AAA rules, user groups, and Access Control rules, configure 802.1X on the end-system:

1. In Windows 11 search, type **view network connections**, and then select **Open**.
2. Right-click the network connection that you need to configure, and then select **Properties**.
3. Select the **Authentication** tab.
4. Verify that the **Enable IEEE 802.1X authentication** check box is selected.
5. For **Choose a network authentication method**, select **Microsoft: EAP TTLS**.
6. Select **Settings**.
7. In the **Trusted Root Certification Authorities** area of TTLS Properties, select the CA-issued certificate for your Access Control Engines.
8. In the **Client authentication** area of TTLS Properties, select **Select a non-EAP method for authentication**, and then select **Unencrypted password (PAP)** from the drop-down menu.



NOTE: The unencrypted password credentials travel through an encrypted tunnel.

9. Select **OK**, and then select **OK** again.

- How to Update ExtremeControl Engine Server Certificates
- Manage Certificates

How to Implement 802.1X EAP-TLS Authentication with Microsoft Entra ID

Multiple options exist for implementing IEEE 802.1X with Microsoft Entra ID (formerly Azure AD) integration. This topic describes how to implement 802.1X EAP-TLS authentication and OAuth 2.0 authorization with Entra ID.

A common use case for this configuration is to apply different network authorizations to different users or computers based on their security group membership in Entra ID.

This topic includes the following information and instructions:

- Requirements for Entra ID Registration
- Generate a RADIUS Certificate for Each Access Control Engine
- Upload Certificates
- Create an Entra ID Application
- Configure AAA Rules
- Configure User Groups
- Configure Access Control Rules
- Configure 802.1X on the End-System

Requirements for Entra ID Registration

Entra ID registration has the following requirements:

- The Access Control Engine must have Internet access to retrieve user information from Microsoft.
- Create a unique Microsoft Entra ID application on the Microsoft Entra ID page (see Create an Entra ID Application).
- The client must trust the RADIUS Certificate used by the Access Control Engine. Standard Windows clients reject the default self-signed certificate, and the authentication fails with the message "Authentication became stale".

NOTE: You must copy and paste some text values between applications during the registration and configuration.
When instructed, copy and save the required values. Some values are unique secret values that you cannot view or receive again.

Generate a RADIUS Certificate for Each Access Control Engine

To generate a server private key and a server certificate, and submit the certificate signing request to a Certificate Authority:

1. Generate a private key and certificate signing request.
2. Submit the request to a Certificate Authority.
3. Replace the Certificate or define certificate usage conditions.

Upload Certificates

Use the following steps to upload certificates to Trusted Authorities.

For more information, see the Trusted Authorities section in AAA Configurations.

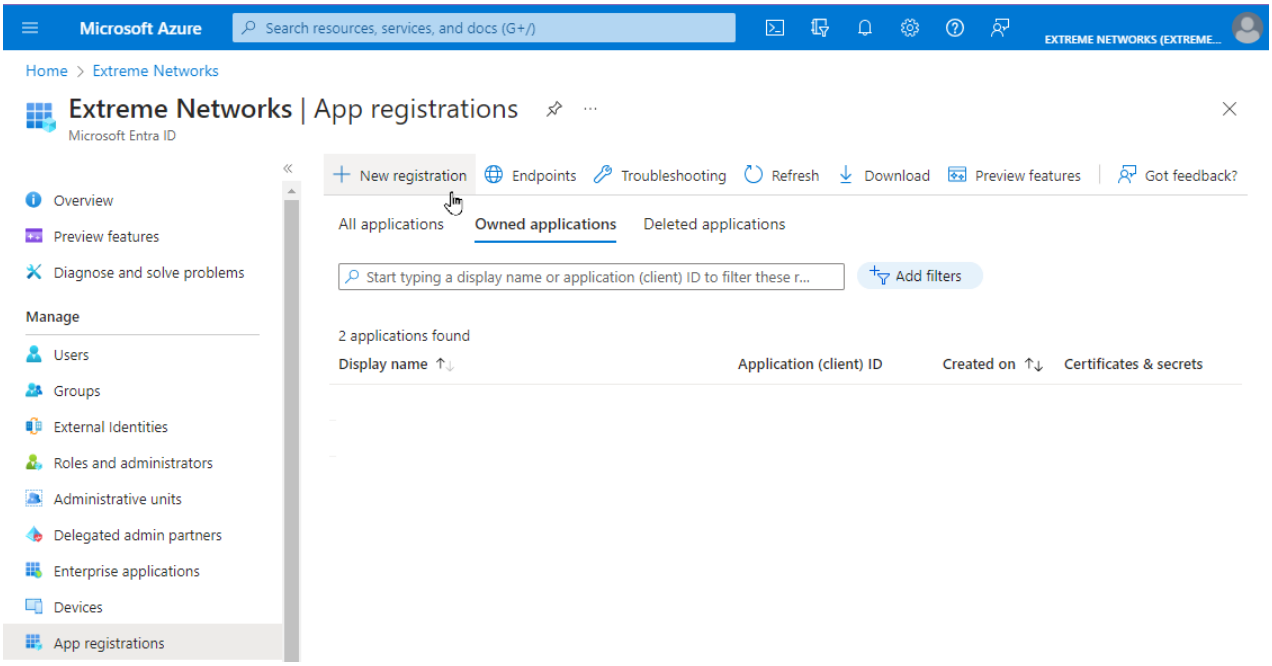
1. Upload the root CA certificate to Trusted Authorities.
2. Upload all intermediate CA certificates to Trusted Authorities.

Create an Entra ID Application

To implement 802.1X authentication using Entra ID and OAuth 2.0, you must first create an Entra ID application. Registering the application generates an Application ID and Application Secret that ExtremeCloud IQ Site Engine requires. To create and register an Entra ID application:

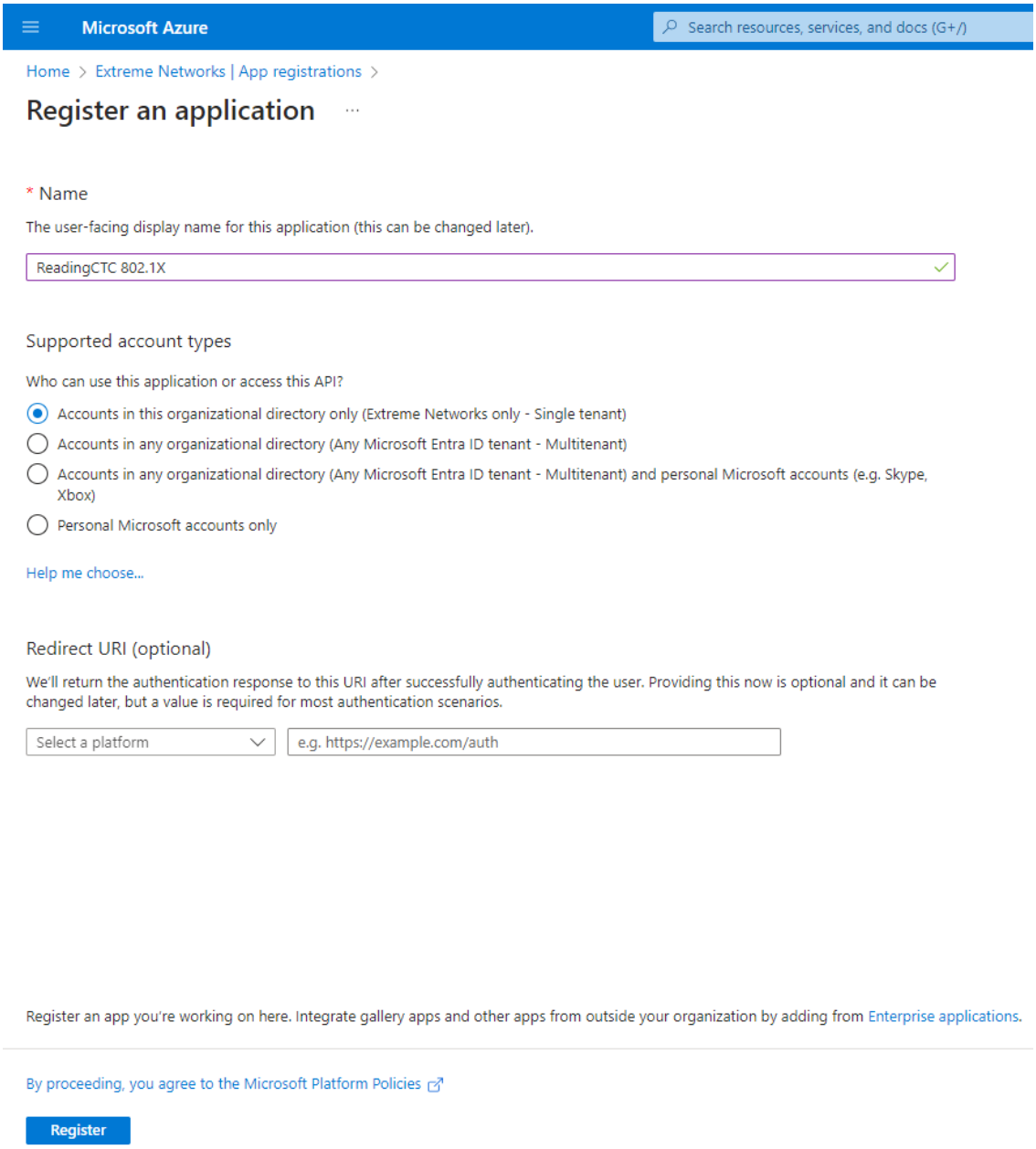
1. Sign in to the Microsoft Entra ID page with your administrator credentials at https://portal.azure.com or https://entra.microsoft.com.
2. Select **Manage Microsoft Entra ID > View**.

3. Select **App registrations > New registration**.



4. Enter the following information in the required fields:
    - **Name** - Enter a name for the Entra ID registered application
    - **Supported account types** - Select Accounts in this organization directory only - (Single tenant)

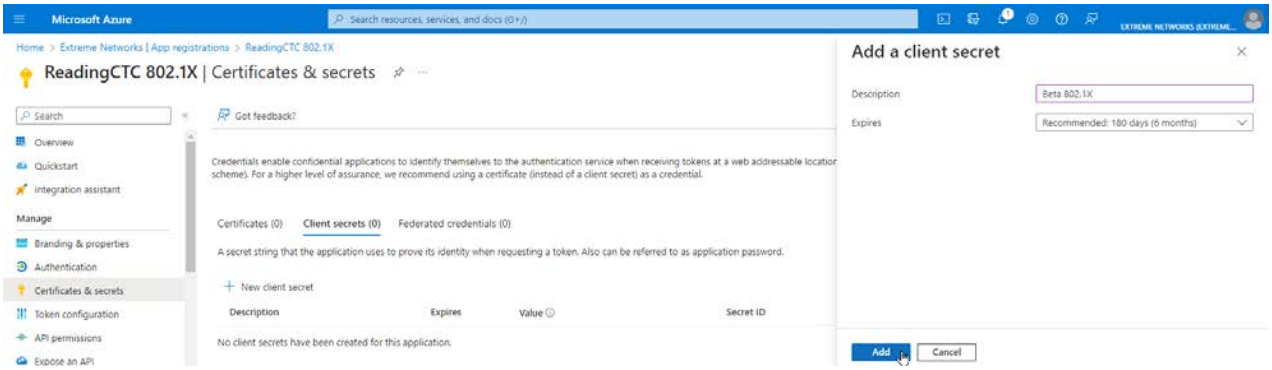
5. Select **Register**.



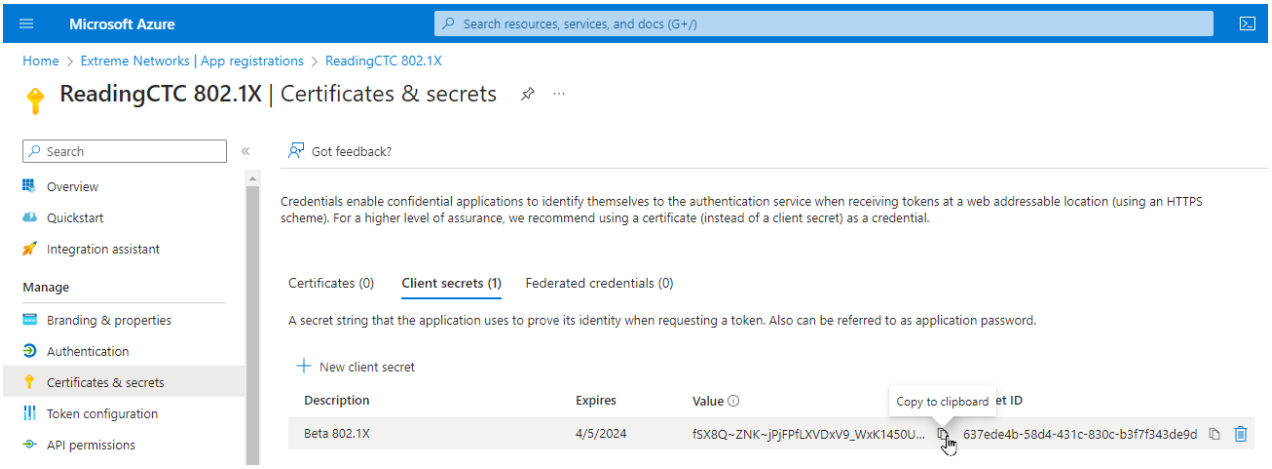
6. Select **Add a certificate or secret**, or in the left menu, select **Certificates & secrets**.
7. Select **New client secret**.
8. Enter the following information in the required fields:
    - **Description** – enter a description of the new credentials
    - **Expires** – specify how long the client secret is valid. When the client secret expires, users cannot authenticate.

- **NOTE:** You cannot modify the expiration of the client secret in Entra ID. The best practice is to create a new client secret before the existing one expires and update the value in ExtremeControl settings.

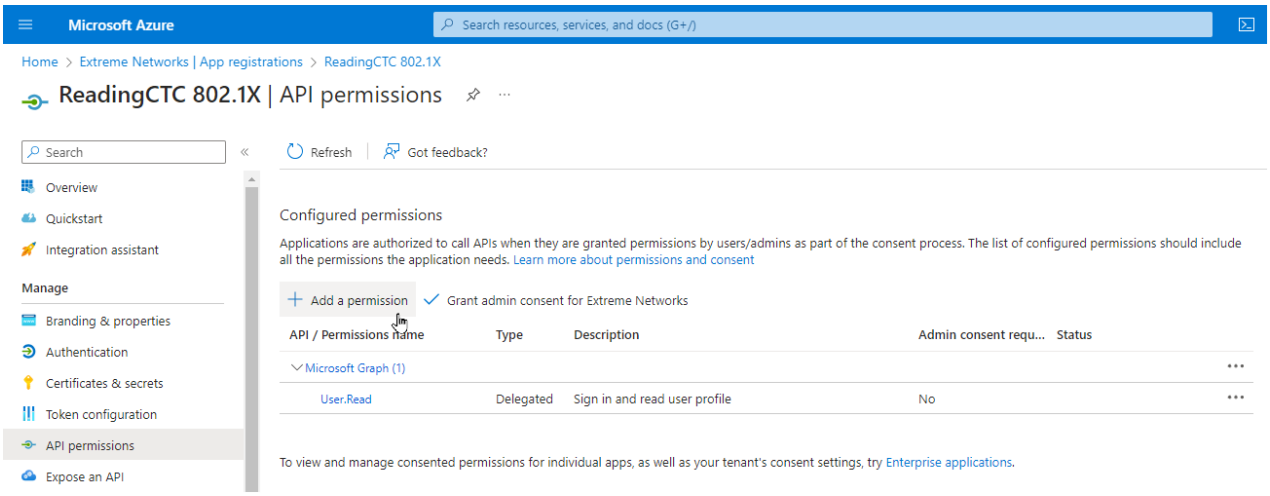
9. Select **Add**.



10. Copy the secret value to the clipboard. This is the only time that Entra ID displays the client secret. Save the secret value for your App Secret.

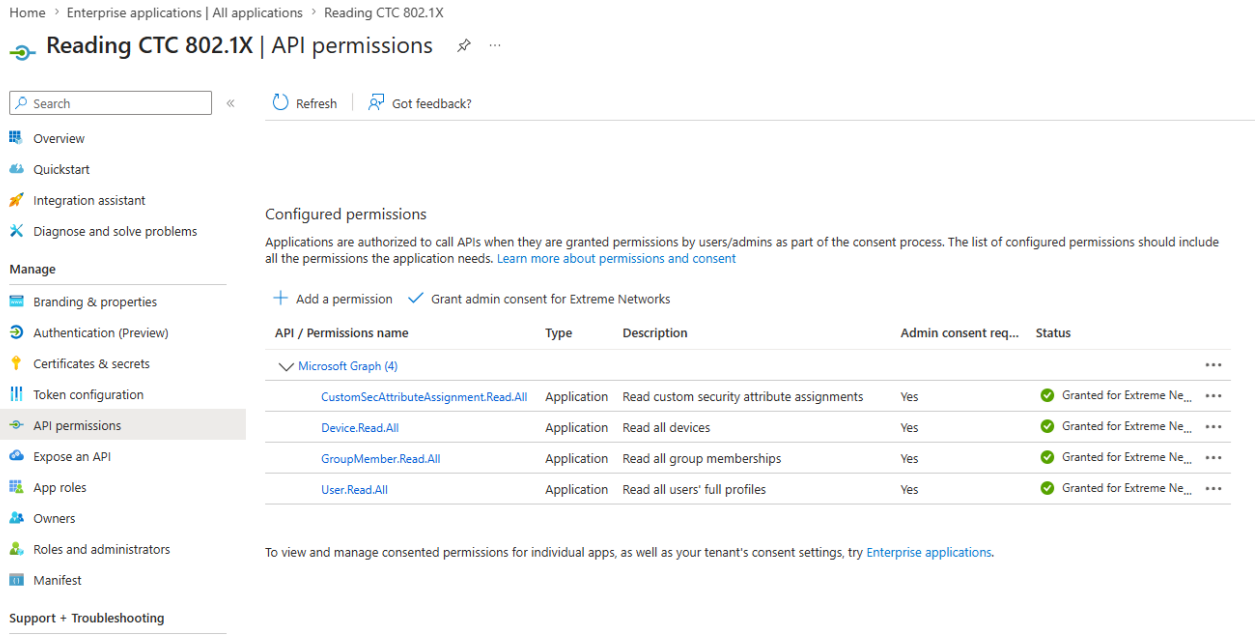


11. Select **API permissions > Add a permission**.



12. Select **Microsoft Graph > Application permissions**.
13. If different users require different authorization based on security group membership, select the following additional application permissions:
    - In the **GroupMember group**, select:
        - **GroupMember.Read.All**
    - In the **User group**, select:
        - **User.Read.All**
    - In the **Device group**, select:
        - **Device.Read.All**
    - To check the values of Custom Security Attributes, select **CustomSecAttributeAssignment**:
        - **CustomSecAttributeAssignment.Read.All**
14. Select **Add permissions**.

15. Select **Grant admin consent for <your company domain>**, and select **Yes** to confirm.



16. Select **Overview**.
17. Copy the displayed **Application (client) ID** value. Save this value for your App ID.
18. Select **Endpoints**.
19. Copy the displayed **OAuth 2.0 token endpoint (v2)** value. Save this value for your Token Endpoint.

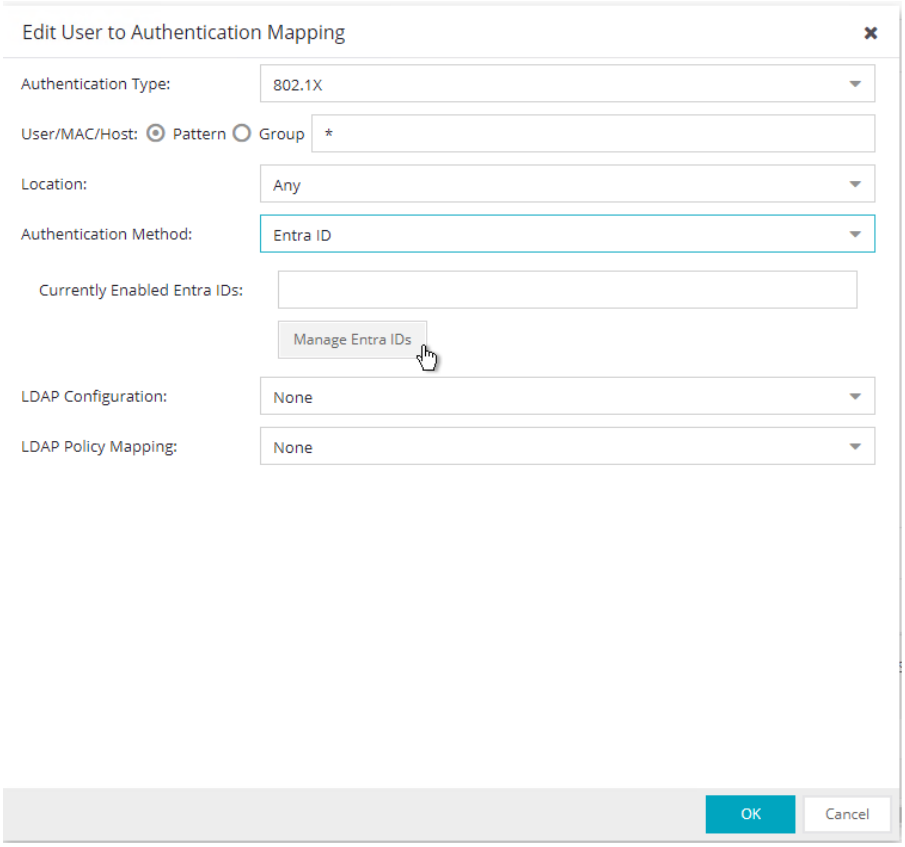
Configure AAA Rules

In the AAA Configuration, enter the values that you saved when you created and registered the Entra ID application.

To configure 802.1X authentication with Entra ID:

1. In ExtremeCloud IQ Site Engine, go to the **Control** > **Access Control** tab.
2. In the left-panel tree, go to **Configuration > AAA >** *your advanced configuration*.
3. In the Authentication Rules area, select **Add**.
4. For **Authentication Type**, select **802.1X**.
5. For **User/MAC/Host**, select **Pattern** of usernames to use the AAA rule.
6. For **Authentication Method**, select **Entra ID**.

7. Select **Manage Entra IDs**.



8. Select **Add**.
9. Enter the following information in the required fields:
    - **Enable** – select the check box.
    - **Entra ID Name** – enter the name of this Entra ID. The name has local meaning only.
    - **Realm** – specifies the Entra ID configuration to use based on the username. Realm is usually the part after the @ in the login username.
    - **App ID** – enter the value copied as "Application (client) ID".
    - **App Secret** – enter the value copied as "Client Secret".
    - **Token Endpoint** – enter the value copied as "OAuth 2.0 token endpoint (v2)".
10. Select **Test Credentials...** to verify the connectivity, App ID, App Secret, and Token Endpoint.
11. Select **OK**.
12. Select **Save**.
13. Select **Enforce** to enforce the new configuration on your engines.

Configure User Groups

A user group can validate user group membership and computer group membership.

After you configure the AAA rules for 802.1X, use the following steps to configure a user group:

1. In ExtremeCloud IQ Site Engine, go to **Control** > **Access Control** > **Group Editor** > **User Groups**.
2. Select **Add**.
3. For **Name**, enter a name for the user group.
4. (Optional) For **Description**, enter a description for the user group.
5. For **Mode**, select Match Any or Match All to specify whether a user must match any or all of the attributes to be added to the group.
6. In the Create Group area, select **Add**.
7. For **Attribute Name**, enter **memberOf** to check the Entra ID security group membership.
8. For **Attribute Value**, enter the name of the security group. You can match the exact name or value, or use the wildcard character (*).
9. Select **Save**.

NOTE:

The CN in the certificate must be in email format for user membership lookup against Entra ID.

The CN in the certificate must be in FQDN format for computer membership lookup against Entra ID.

If the Subject Alternative Name (SAN) in the certificate contains attribute 2 (usually called DNS or DNS Name), the value must follow the same rules as the CN.

Configure Access Control Rules

After you configure the 802.1X AAA rules and user groups, use the following steps to configure an Access Control rule:

1. In ExtremeCloud IQ Site Engine, go to **Control** > **Access Control** > **Configuration** > *your configuration* > **Rules**.
2. Select **Add**.
3. For **Name**, enter a name for the rule.
4. Select the **Rule Enabled** check box.
5. For **Description**, enter a description for the rule.

6. For **User Group**, select the user group that you created in Configure User Groups.
7. For **Authentication Method**, select **802.1X (TLS)**.
8. Select **Save**.
9. Select **Enforce** to enforce the new configuration on your engines.

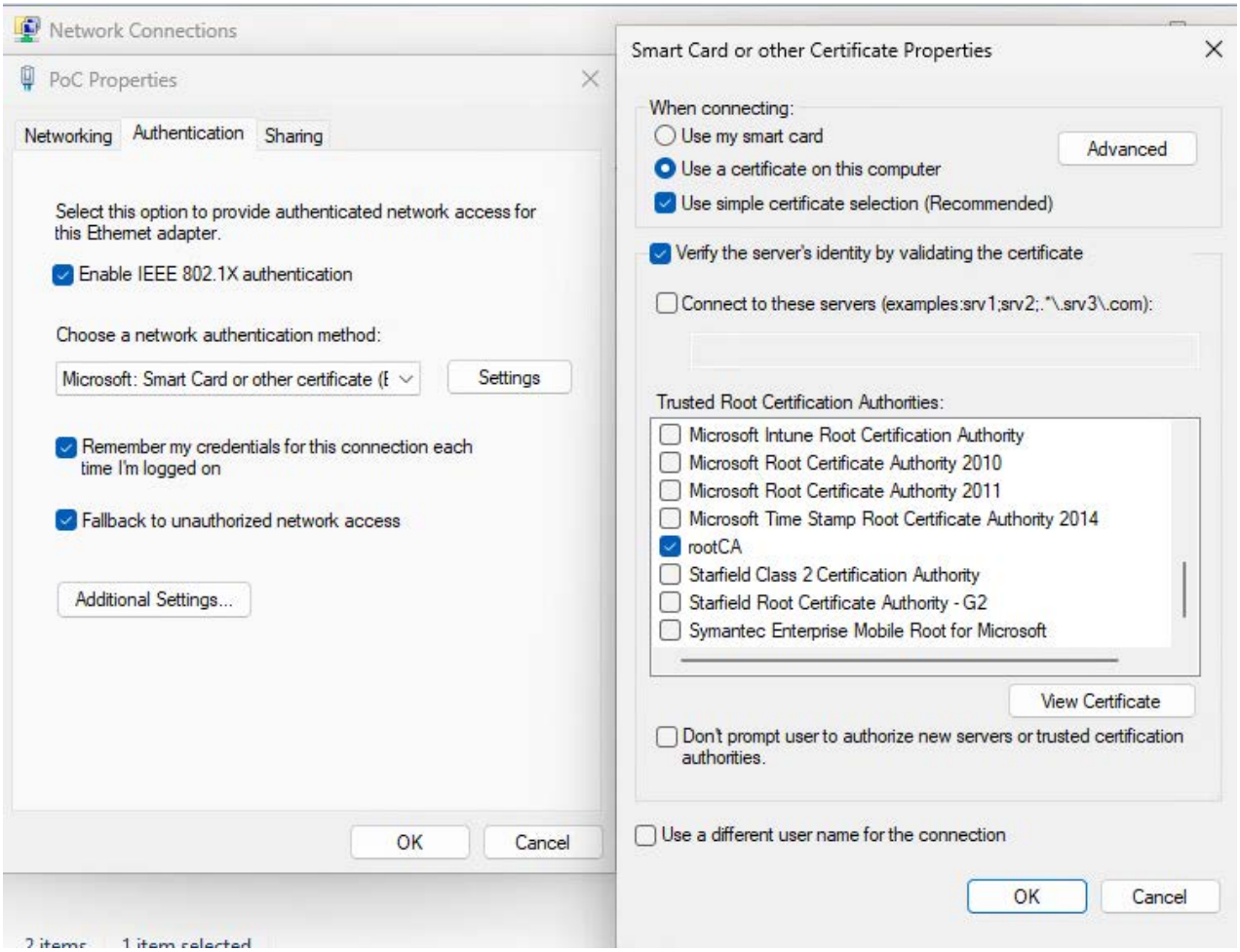
Configure 802.1X on the End-System

You must configure the end-system to use IEEE 802.1X authenticated network access. The following example uses a Windows 11 client.

After you configure the AAA rules, user groups, and Access Control rules, configure 802.1X on the end-system:

1. In Windows 11 search, type **view network connections**, and then select **Open**.
2. Right-click the network connection that you need to configure, and then select **Properties**.
3. Select the **Authentication** tab.
4. Verify that the **Enable IEEE 802.1X authentication** check box is selected.
5. For **Choose a network authentication method**, select **Microsoft: Smart Card or other certificate (EAP TLS)**.
6. Select **Settings**.

7. In the **Trusted Root Certification Authorities** area, select the CA-issued certificate for your Access Control Engines.



8. Select **OK**, and then select **OK** again.

- How to Update ExtremeControl Engine Server Certificates
- Manage Certificates

How to Implement Keycloak Registration with OpenID

This topic describes how to implement authenticated registration using OAuth 2.0 OpenID Connect with Keycloak as the identity provider.

A common use case for this configuration is to apply different network authorizations to different users based on their Keycloak group membership and realm roles. After a user authenticates at Keycloak, ExtremeControl retrieves the groups and realm roles for that user from the Keycloak Admin REST API and matches them against your User Groups and Access Control rules.

This topic includes the following information and instructions:

- Requirements for Keycloak Registration
- Prepare the Keycloak Realm, Roles, Groups, and Users
- Create a Keycloak Client
- Configure the Captive Portal
- Configure User Groups
- Configure Access Control Rules
- Verify the Configuration
- Configure a Multiple NIC Environment
- Deployment Considerations

Requirements for Keycloak Registration

Keycloak registration has the following requirements:

- The Keycloak server must be reachable over HTTPS from the Access Control engine and from ExtremeCloud IQ Site Engine. HTTP is not supported.
- The Access Control engine and ExtremeCloud IQ Site Engine accept the Keycloak server certificate based on the Server Trust Mode setting. The default trust mode accepts any certificate, including a self-signed certificate. LOCKED mode accepts only a Keycloak server certificate that matches the recorded certificate. Importing only the CA certificate is not sufficient.
- Use a Keycloak server certificate that end-user devices trust to prevent browser security warnings, since end-user browsers open the Keycloak sign-in page.

- The ExtremeControl Unregistered access policy must allow access to the Keycloak server (either allow all SSL or make allowances for the Keycloak server). Unregistered end systems must also be able to resolve the Keycloak host name.
- Create a Keycloak client in the realm that contains your users, with **Client authentication** and **Service account roles** enabled (see Create a Keycloak Client).
- Assign the **view-users**, **query-users**, and **query-groups** roles from the **realm-management** client to the service account of the client (see Create a Keycloak Client).
- The Portal Configuration must have OpenID Registration enabled, with **Group Source** set to **Keycloak** and the Keycloak Client ID and Client Secret entered (see Configure the Captive Portal).
- **Username Resolution** and **Registration Username Resolution** must be selected in the engine settings (**Control > Access Control > Configuration > Global & Engine Settings > Engine Settings >** *your settings profile* **> Username Resolution** tab). **Registration Username Resolution** is available only after you select **Username Resolution**. If you clear them, the user name falls back to the MAC address and no OpenID group rule can match.
- MAC-to-IP resolution must work for the end system (for example, DHCP snooping, RADIUS accounting, or SNMP ARP polling).

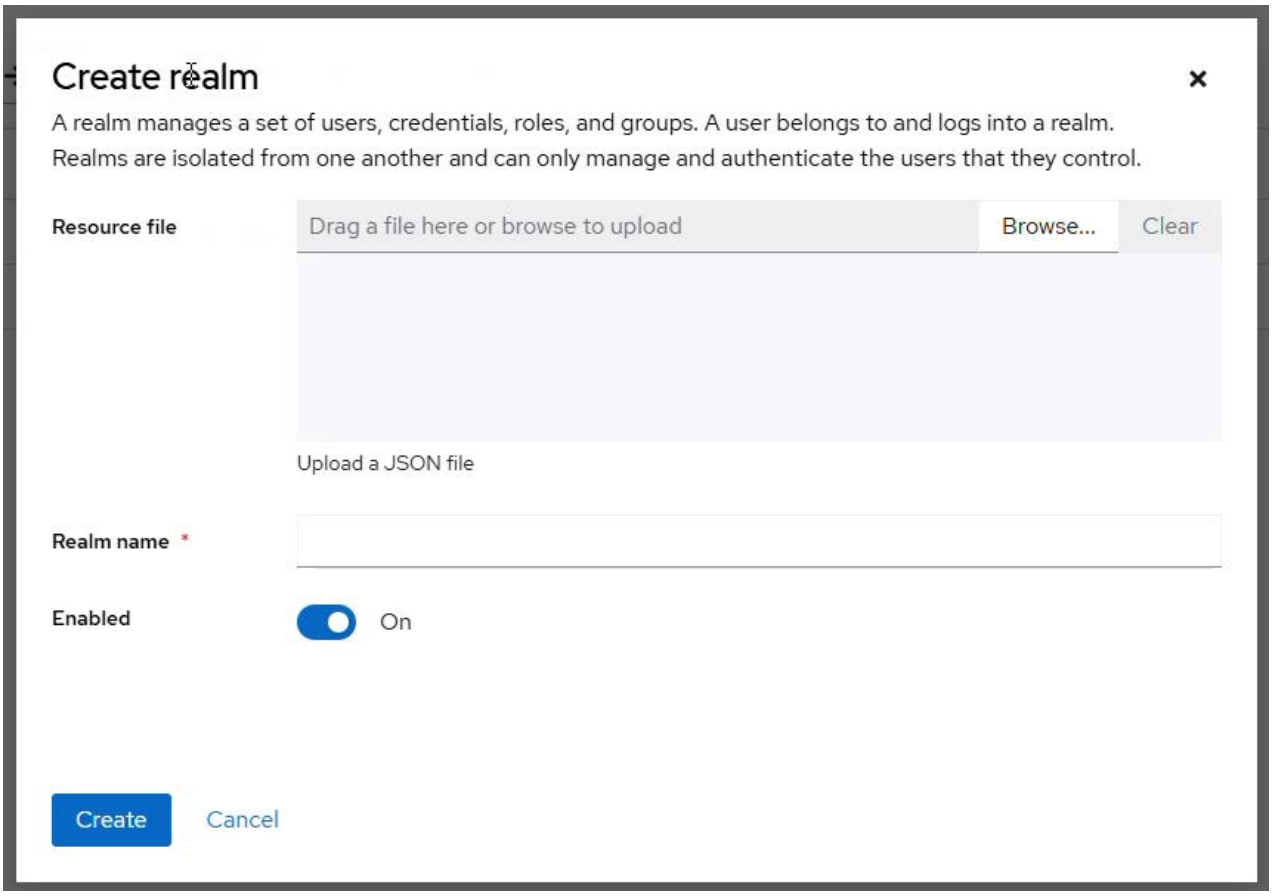
NOTE: You must copy and paste some text values between applications during the registration and configuration.
The Keycloak steps and labels in this topic reflect the Keycloak 26 Admin Console. Labels can differ in other Keycloak versions.

Prepare the Keycloak Realm, Roles, Groups, and Users

If your Keycloak realm already contains the users, groups, and realm roles that you want to use for authorization, see Create a Keycloak Client. Otherwise, use the following steps to prepare the realm.

1. Sign in to the Keycloak Admin Console with your administrator credentials at `https://<keycloak-host>:<port>/admin`.
2. To create a realm, select **Manage realms > Create realm**, enter a **Realm name**, keep **Enabled** set to **On**, and select **Create**.

Make a note of the realm name. It is part of the Discovery URI and Token Endpoint values.



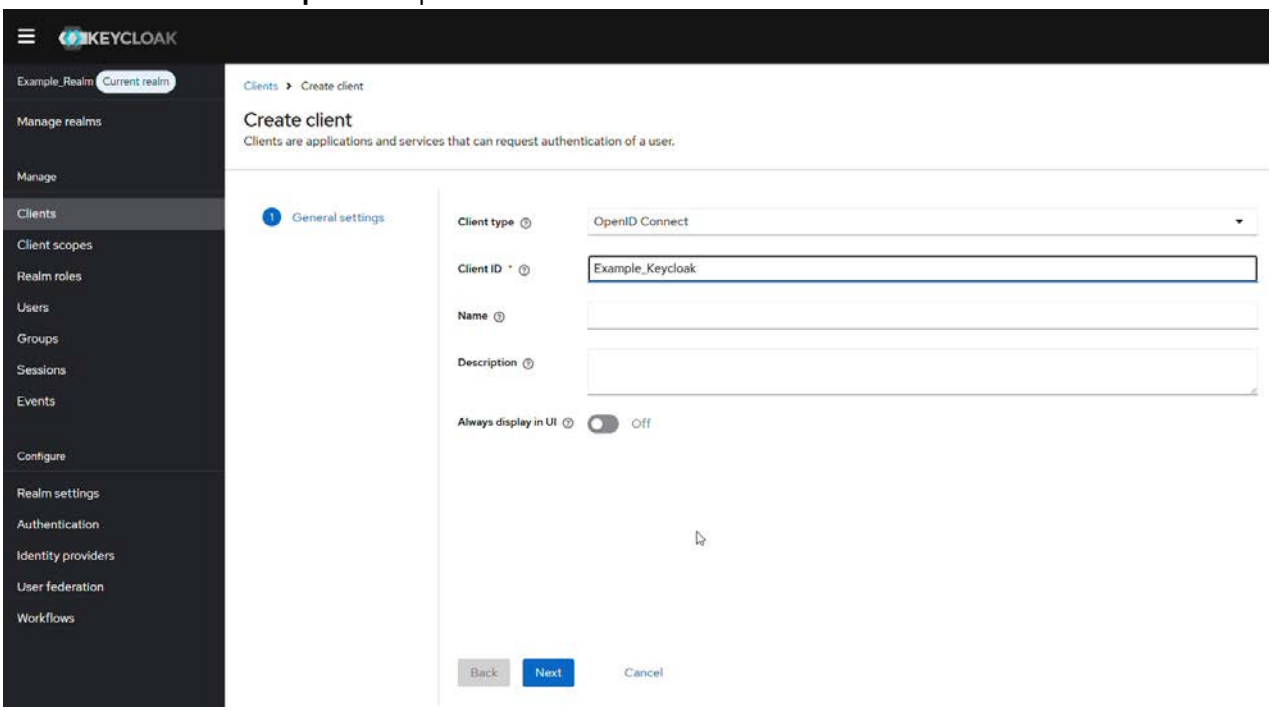
3. To create a realm role, select **Realm roles > Create role**, enter a **Role name**, and select **Save**.
4. To create a group, select **Groups > Create group**, enter a **Name**, and select **Create**.
   To create a child group, next to the parent group, select the ⋮ menu, and then select **Create child group**.
5. To create a user, select **Users > Add user**, enter the **Username**, **Email**, **First name**, and **Last name**, and select **Create**.
6. On the **Credentials** tab for the user, select **Set password**, enter and confirm the password, and select **Save > Save password**.
   If you set **Temporary** to **On**, the user must change the password the first time they sign in at the captive portal.
7. On the **Role mapping** tab for the user, select **Assign role > Realm roles**, select the realm roles for the user, and select **Assign**.
   Assign realm roles directly to each user. A role that a user receives only through group membership is not returned to ExtremeControl.
8. On the **Groups** tab for the user, select **Join Group**, select the groups for the user, and select **Join**.

NOTE: ExtremeControl receives only the groups that a user is a direct member of and the realm roles assigned directly to the user. Parent groups, composite role expansion, and Keycloak client roles are not returned. Use wildcards in your User Groups to match a group hierarchy (see Configure User Groups).

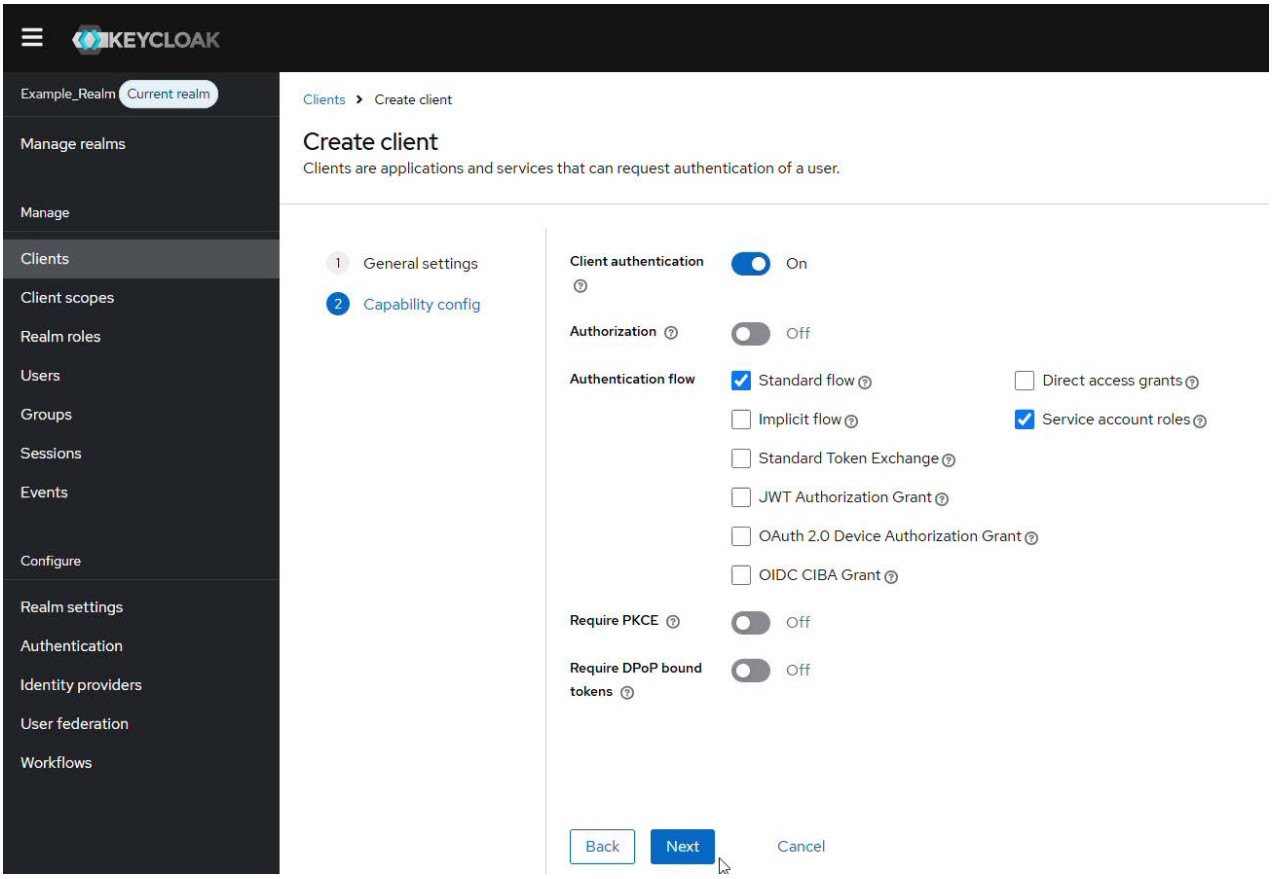
Create a Keycloak Client

To implement authenticated registration using Keycloak and OpenID Connect, you must create a Keycloak client in the realm. ExtremeCloud IQ Site Engine requires the Client ID and Client Secret in the Portal Configuration. ExtremeControl also uses the service account of the client to read the groups and realm roles of each user. To create and configure a Keycloak client:

1. Sign in to the Keycloak Admin Console with your administrator credentials, and select the realm that contains your users.
2. Select **Clients > Create client**.
3. On the **General settings** page, enter the following information, and select **Next**:
   - **Client type** - Select OpenID Connect
   - **Client ID** - Enter a name for the client. Save this value for your App ID.
   - **Name** and **Description** - Optional

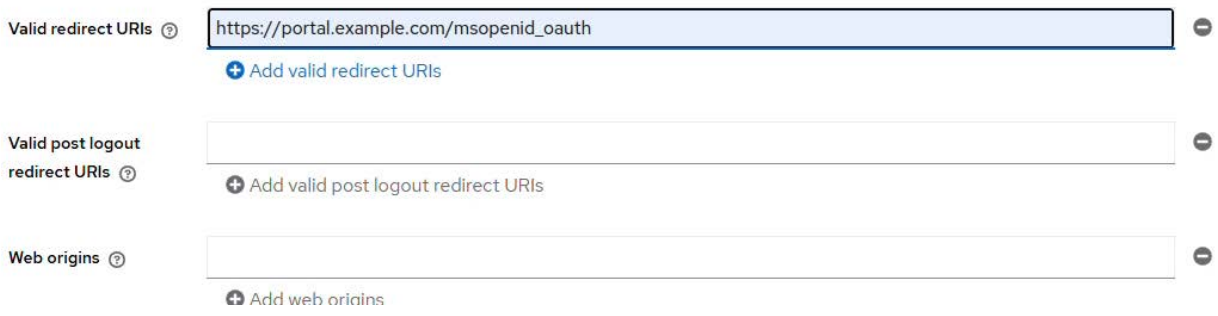


4. On the **Capability config** page, enter the following information, and select **Next**:
    - **Client authentication** – Set to On
    - **Authentication flow** – Keep **Standard flow** selected, and select **Service account roles**



- **NOTE:** **Service account roles** is required. Keycloak controls the client credentials grant separately from the standard sign-in flow. Without it, users can authenticate, but ExtremeControl cannot retrieve their groups and roles.

5. On the **Login settings** page, in **Valid redirect URIs**, enter a URI that uses HTTPS with the FQDN of the captive portal followed by /msopenid_oauth. For example, `https://portal.example.com/msopenid_oauth`.

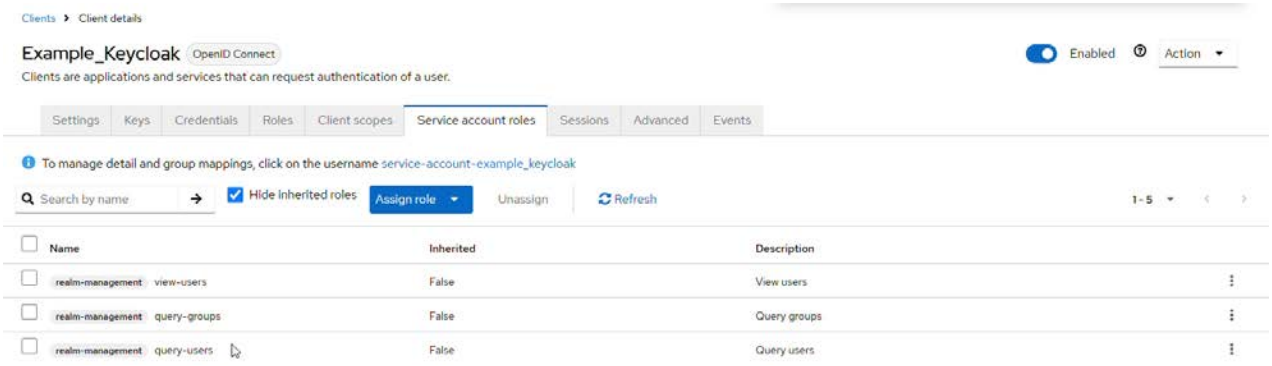


- **NOTE:** The redirect URI must match the **Redirect URI** shown in the Portal Configuration (`https://%CaptivePortalFQDN%/msopenid_oauth`), resolved to the FQDN or IP address of the Access Control Engine captive portal interface. If end systems reach the captive portal on more than one FQDN, add a redirect URI for each.

  The best practice is to use HTTPS and install a trusted certificate as the Captive Portal Server Certificate on the Access Control Engine.

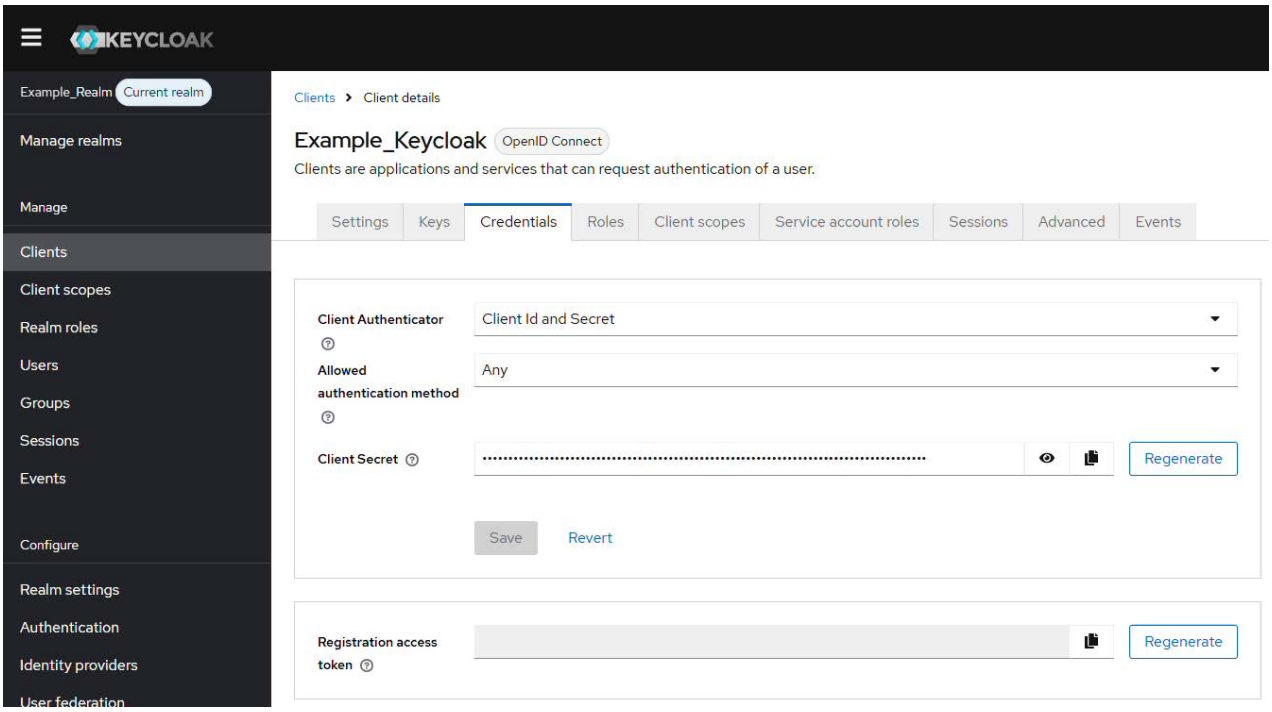
6. Select **Save**.
7. On the **Service account roles** tab, select **Assign role > Client roles**.
8. Select the following roles from the **realm-management** client, and select **Assign**:
   - **query-groups**
   - **query-users**
   - **view-users**

   With the roles, ExtremeControl can query users, groups, and realm roles through the Keycloak Admin REST API. All three roles are required.



9. On the **Credentials** tab, verify that **Client Authenticator** is set to **Client Id and Secret**.
10. Copy the **Client Secret** value. Save this value for your App Secret.
    Unlike Entra ID, you can view the client secret again on this tab. If you select **Regenerate**, you

must update the App Secret in the Portal Configuration.



11. Build and save the following values from your Keycloak host, port, and realm name:

    - **Discovery URI** - `https://<keycloak-host>:<port>/realms/<realm>/.well-known/openid-configuration`
    - **Token Endpoint** - `https://<keycloak-host>:<port>/realms/<realm>/protocol/openid-connect/token`

    For Keycloak versions earlier than 17, include `/auth` before `/realms`. You can also open the discovery document from **Realm settings > General > Endpoints > OpenID Endpoint Configuration** and copy the `token_endpoint` value from the discovery document.

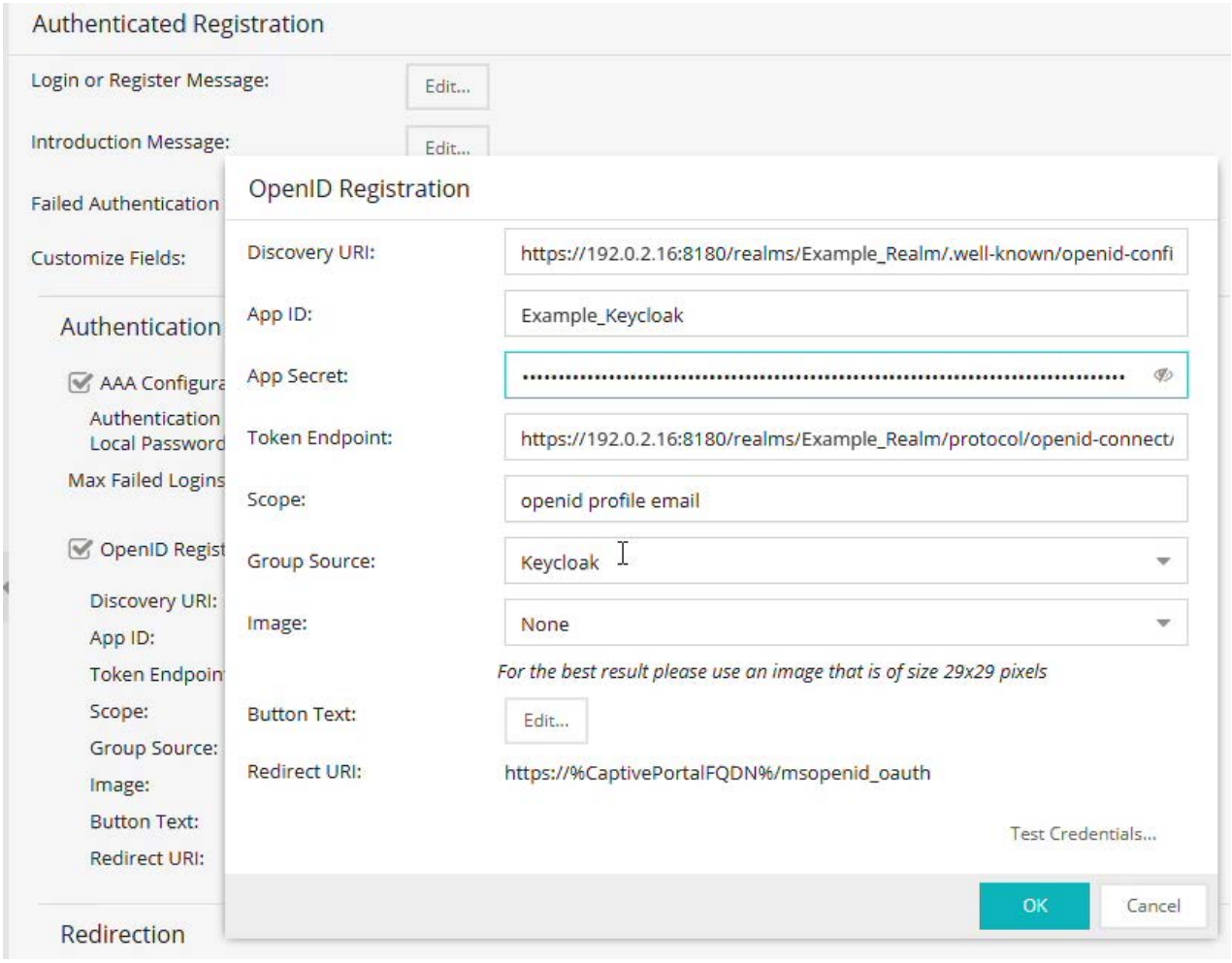
    - **NOTE:** Use the same Keycloak host name in the Discovery URI and the Token Endpoint. Keycloak builds the sign-in address in the discovery document from the host name in the Discovery URI, unless you configure Keycloak with a fixed host name. ExtremeControl redirects end-user browsers to the sign-in address, so use a host name that end-user devices can resolve and reach.

Configure the Captive Portal

In the Portal Configuration, enter the values that you saved when you created the Keycloak client.

To configure authenticated registration using OpenID in the captive portal:

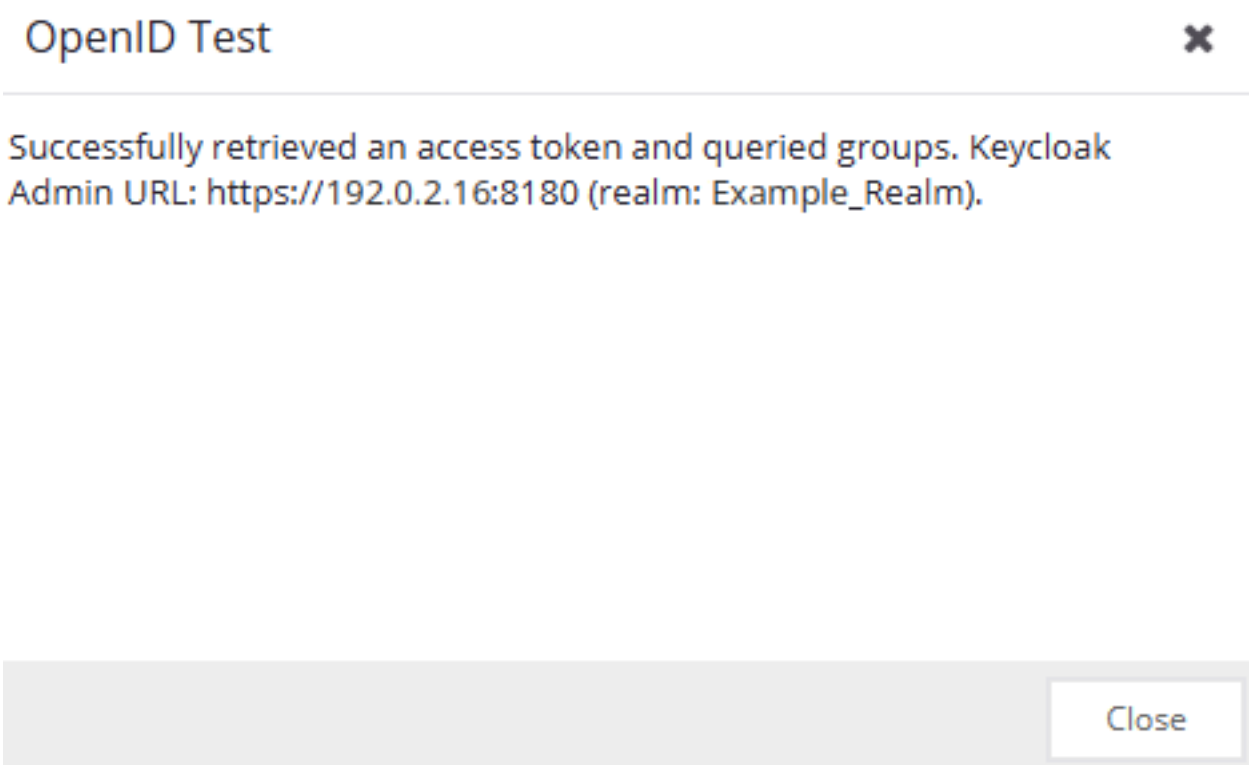
1. In ExtremeCloud IQ Site Engine, go to the **Control** > **Access Control** tab.
2. In the left-panel tree, go to **Configuration > Captive Portals >** *your portal* **> Website Configuration**.
   To create a new portal, select **Captive Portals**, select **Add**, enter a **Name**, select **Base Portal Configuration** as the **Type**, and select **Create**.
3. Select **Authentication Settings**.
4. Select **Authenticated Registration**, and then select **Save**.
5. In the left-panel tree, go to **Website Configuration > Authenticated Registration**.
6. Select the **OpenID Registration** check box.
7. Select **Edit**.



8. Enter the following information in the required fields:
   - Discovery URI – enter the Discovery URI value that you saved.
   - App ID – enter the value copied as "Client ID".

- **App Secret** – enter the value copied as "Client Secret".
- **Token Endpoint** – enter the Token Endpoint value that you saved.
- **Scope** – keep the default value, "openid profile email".
- **Group Source** – select **Keycloak**. The default value is Entra ID.
- **Image** – optional picture to display to the user at the captive portal. For the best result, use an image that is 29 × 29 pixels.
- **Button Text** – text presented on the button. When **Group Source** is Keycloak, the default text is "Sign in with Keycloak". Select **Edit** to change it. To define the text in different languages, use **Website Configuration > Look & Feel > Launch Message String Editor**.
- **Redirect URI** – information only, not configurable. Indicates where the OpenID process redirects the user after the authentication is successful. Register this value as a valid redirect URI in the Keycloak client.

9. Select **Test Credentials...** to verify the connectivity, App ID, App Secret, and Token Endpoint. When **Group Source** is Keycloak, the OpenID Test window also verifies the admin permissions of the service account. A successful test shows that ExtremeControl retrieved an access token and queried groups, and displays the Keycloak Admin URL (the base URL of the Keycloak server) and the realm that ExtremeControl derives from the Discovery URI.



If the test fails, verify that **Service account roles** is enabled on the Keycloak client and that the service account has the **view-users**, **query-users**, and **query-groups** roles.

10. Select **OK**.
11. In **Registration Settings**, clear the **Check Session Validity in Entra ID** check box.

    - **NOTE:** If you do not clear the check box, ExtremeControl attempts to validate sessions through Microsoft services. The validation fails for Keycloak users, but normal operation is not affected.

    - **NOTE:** If Keycloak user names are email addresses, keep **Keep Email Domain Names** selected in **Registration Settings**. If you clear **Keep Email Domain Names**, ExtremeControl removes the domain from the registered user name and cannot find the user in Keycloak. As a result, the Keycloak User Groups do not match the user.

12. Select **Save**.
13. If the portal is not already assigned to your Access Control configuration, go to **Configuration > Configurations >** *your configuration* **> Portal**, for **Portal Configuration**, select the portal, and then select **Save**.
14. Select **Enforce** to enforce the new configuration on your engines.

Configure User Groups

After you configure the captive portal for OpenID registration, use the following steps to configure a user group:

1. In ExtremeCloud IQ Site Engine, go to **Control** > **Access Control** > **Group Editor** > **User Groups**.
2. Select **Add**.
3. For **Name**, enter a name for the user group.
4. (Optional) For **Description**, enter a description for the user group.
5. For **Type**, select **User: OpenID User Group**.
6. For **Mode**, select Match Any or Match All to specify whether a user must match any or all of the attributes to be added to the group.
7. In the Create Group area, select **Add**.
8. For **Attribute Name**, enter one of the following:
    - **groups** to check Keycloak group membership
    - **roles** to check Keycloak realm roles

9. For **Attribute Value**, enter the Keycloak group path without the leading slash (for groups) or the realm role name (for roles). You can use the wildcard character (*).

   Examples:

   - `Engineering` - matches direct members of the Engineering group
   - `Engineering/XIQSE` - matches members of the XIQSE subgroup of Engineering
   - `Engineering/*` - matches members of any subgroup of Engineering, but not direct members of Engineering
   - `Engineering*` - matches members of Engineering, members of any subgroup of Engineering, and members of any other group whose name starts with Engineering
   - `*XIQSE` - matches members of any group whose name ends in XIQSE
   - `Developer` - matches users with the Developer realm role (with Attribute Name **roles**)

   NOTE:

   Keycloak displays group paths with a leading slash (for example, `/Engineering/XIQSE`). ExtremeControl removes the leading slash before matching, so enter group paths without the slash. A value that starts with a slash (/) never matches.

   Keycloak reports direct group membership only. Use a wildcard, such as `Engineering*`, to match the Engineering group and all Engineering subgroups.

   Matching is not case-sensitive. ExtremeControl does not validate values against Keycloak, so a typo in a group path or role name never matches.

   Use **groups** and **roles** for Keycloak. The **memberOf** and **extensionAttribute** attribute names apply only to Entra ID.

10. Select **Save**.

Configure Access Control Rules

After you configure the captive portal and user groups, use the following steps to configure an Access Control rule:

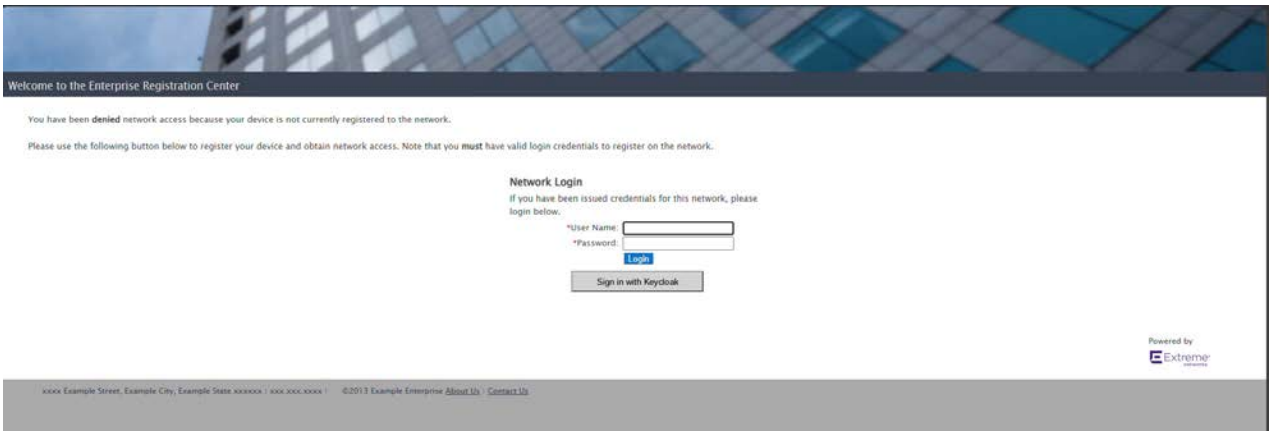
1. In ExtremeCloud IQ Site Engine, go to **Control** > **Access Control** > **Configuration** > *your configuration* > **Rules**.
2. Select **Add**.
3. For **Name**, enter a name for the rule.
4. Select the **Rule Enabled** check box.
5. For **Description**, enter a description for the rule.

6. For **User Group**, select the user group that you created in Configure User Groups.
7. For **End System Group**, select **Web Authenticated Users**.
8. In the **Actions** area, for **Access Control Profile**, select the profile to apply to users who match the rule.
9. Select **Save**.
10. Repeat these steps for each group or role that requires a different authorization, and order the rules so that ExtremeControl evaluates the most specific rules first. Users who do not match any group or role rule receive the profile of the next matching rule, such as a catch-all rule for Web Authenticated Users.
11. Select **Enforce** to enforce the new configuration on your engines.

Verify the Configuration

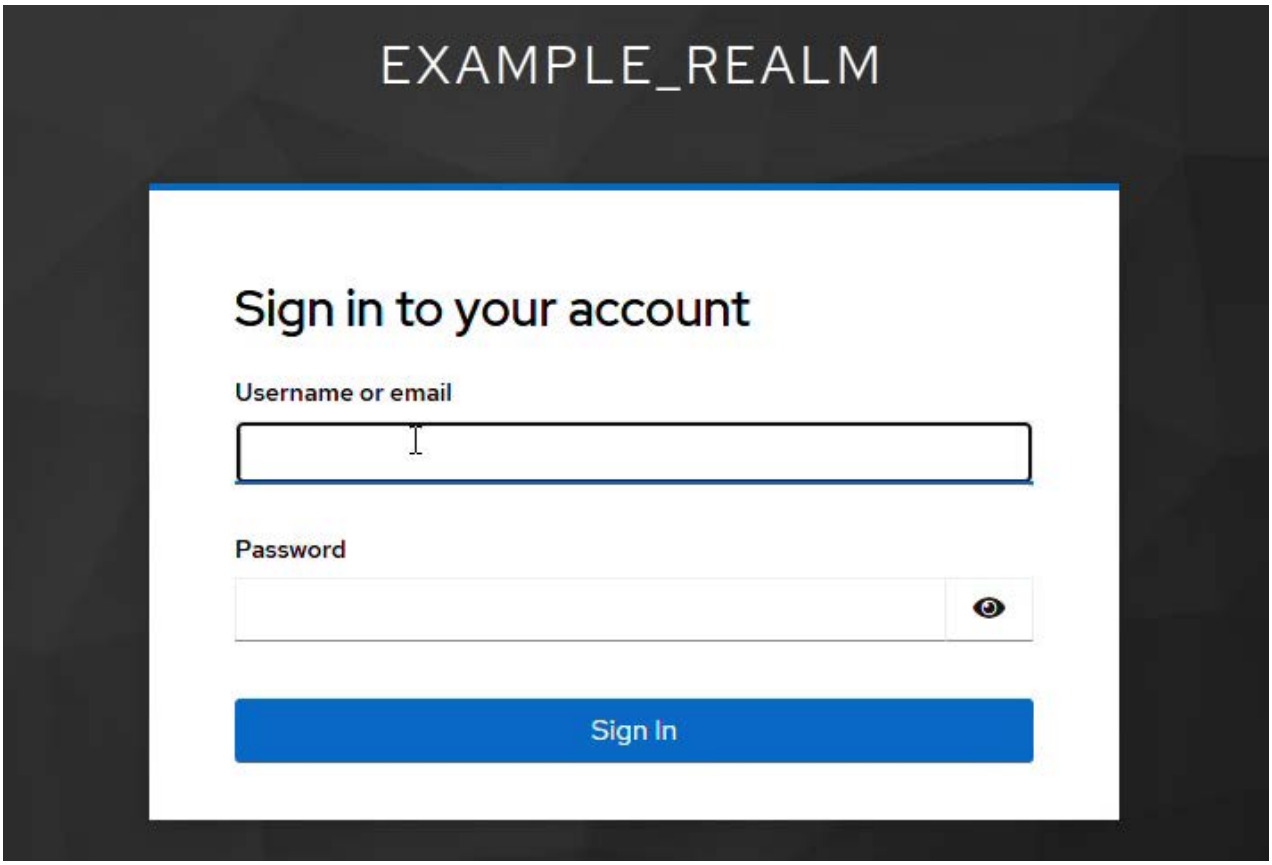
To verify that users authenticate at Keycloak and receive the expected authorization:

1. Connect an unregistered end system to the network and open a web browser. The system redirects the browser to the captive portal.
2. On the captive portal page, select the OpenID button (by default, **Sign in with Keycloak**). The captive portal redirects the browser to the Keycloak sign-in page for your realm.



3. Enter the Keycloak user name and password, and select **Sign In**. The browser returns to the captive portal, which displays a registration progress page while ExtremeControl registers the

end system.



4. In ExtremeCloud IQ Site Engine, go to **Control** > **Access Control** > **Engines**, select your engine, and then select the **End-Systems** tab.
   Verify that the end system shows the Keycloak user name, Authenticated Registration as the **Registration Type**, and the Access Control profile of the rule that matches the group or role of the user.

Configure a Multiple NIC Environment

As a best practice for security, keep Management and Control traffic separate from user traffic.

After you configure the captive portal, user groups, and Access Control rules, you can configure a multiple NIC environment:

1. In ExtremeCloud IQ Site Engine, go to **Control** > **Access Control** > **Engines** > **Engine Groups** > *your group* > *your engine*.
2. Select **Details**, and then in the Interface Summary area, select **Edit**.
3. In the eth0 area, for **Mode**, select **Management Only**.
   The eth0 NIC is now configured for Management, Monitoring Services, Network Services, AAA Servers, Device, Portal: Management, and Traffic Snooping.

4. In the eth1 area, for **Mode**, select **Registration & Remediation Only**.
   The eth1 NIC is now configured for communication with End-System and Traffic Snooping.
   IMPORTANT: The engine does not use a specific NIC for its calls to Keycloak. The operating system of the engine routes these calls like any other outbound traffic, usually through the default gateway interface unless a more specific route exists. Make sure that the engine has a route to the Keycloak server.
5. In the eth1 area, for **Host Name**, enter the FQDN of the Redirect URI.
6. Select **Save**.
7. Select **Enforce** to enforce the new configuration on your engines.

Deployment Considerations

Read the following deployment considerations before you implement a Keycloak authenticated registration configuration:

- The best practice for the captive portal configuration is to use HTTPS and an FQDN.
- You can configure a High Availability Captive Portal by using multiple DNS records for the same FQDN.
- After a successful authentication at Keycloak, the web browser is redirected to the NIC of the Access Control Engine where the captive portal is enabled. If multiple NICs are configured, the lowest-numbered NIC that has Registration & Remediation enabled is used.
- ExtremeControl caches group membership and realm roles for approximately 10 minutes. A change in Keycloak takes effect at the first re-authorization after the cache expires, without the user signing in again. The first sign-in after an engine restart is slower because the caches are empty.
- A user who is not a member of any group still registers successfully and receives the profile of the next matching rule, such as a catch-all rule.
- For an end system that registers through the captive portal, ExtremeControl matches Keycloak groups and realm roles when the end system re-authenticates (for example, with MAC authentication). Matching at re-authentication requires the **Username Resolution** and **Registration Username Resolution** settings (see Requirements for Keycloak Registration).
- Keycloak group-based authorization supports only users who register through the captive portal. ExtremeControl does not support Keycloak group-based authorization for users who authenticate only with 802.1X.
- Each Portal Configuration supports a single Keycloak realm. ExtremeControl derives the realm from the Discovery URI and supports realm roles only, not Keycloak client roles.

- If the AAA configuration also includes Entra ID, ExtremeControl looks up a user name that ends in an Entra ID realm domain in Entra ID instead of Keycloak. The Keycloak User Groups then do not match the user. Make sure that Keycloak user names do not end in a realm domain that the AAA configuration uses for Entra ID.
- Configure switch ports for a single authentication method (web authentication or MAC authentication, not 802.1X and MAC authentication). A port that runs both creates two sessions with different usernames, and rules can appear to match intermittently.
- The **Check Session Validity in Entra ID** option (**Website Configuration > Authenticated Registration > Registration Settings**) applies only to Entra ID. Session revalidation is not supported for Keycloak. The option is selected by default, so clear it for a portal that uses Keycloak (see Configure the Captive Portal).
- If the Access Control Engine is configured as a proxy, you must update the Allowed Web Sites.

- How to Implement Microsoft Entra ID Registration with OpenID
- How to Update ExtremeControl Engine Server Certificates
- Manage Certificates

How to Integrate and Configure Microsoft MDM Intune/Defender

This Help topic describes the steps to integrate and configure the Intune Compliance Module with 802.1X EAP-TLS authentication with Microsoft Intune.

A common use case for this configuration is to apply different network authorizations to devices reported as non-compliant by Microsoft Intune.

This topic includes information and instructions on:

- Solution Overview
- Requirements for Intune Compliance Module
- Creating an Entra ID Application
- Intune Compliance Module Configuration
- End-System 802.1X Configuration
- Example of an End-System's Certificate

Solution Overview

- The device connects to the network and authenticates through 802.1X EAP-TLS.
- The Access Control Engine extracts Intune ID from the user/computer certificate.
- ExtremeCloud IQ Site Engine periodically downloads the list of non-compliant devices from Microsoft and compares Intune IDs.
- MAC addresses of all non-compliant devices are added to the defined end-system group.
- MAC addresses of devices that are not reported as non-compliant are removed from the defined end-system group.
- Change of the compliance status triggers a reauthentication and the network access authorization is updated based on NAC rules.

Requirements

These are the configuration requirements for the Intune Compliance Module.

- The ExtremeCloud IQ Site Engine must have Internet access in order to retrieve compliance information from Microsoft.

- The Intune ID must be part of 802.1X EAP-TLS authentication in Subject Alternative Name (SAN) URI attribute.
- Create a unique Microsoft Entra ID application on the Microsoft Entra ID page (see instructions below).
- The Intune Compliance Module must be enabled and configured (see instructions below).

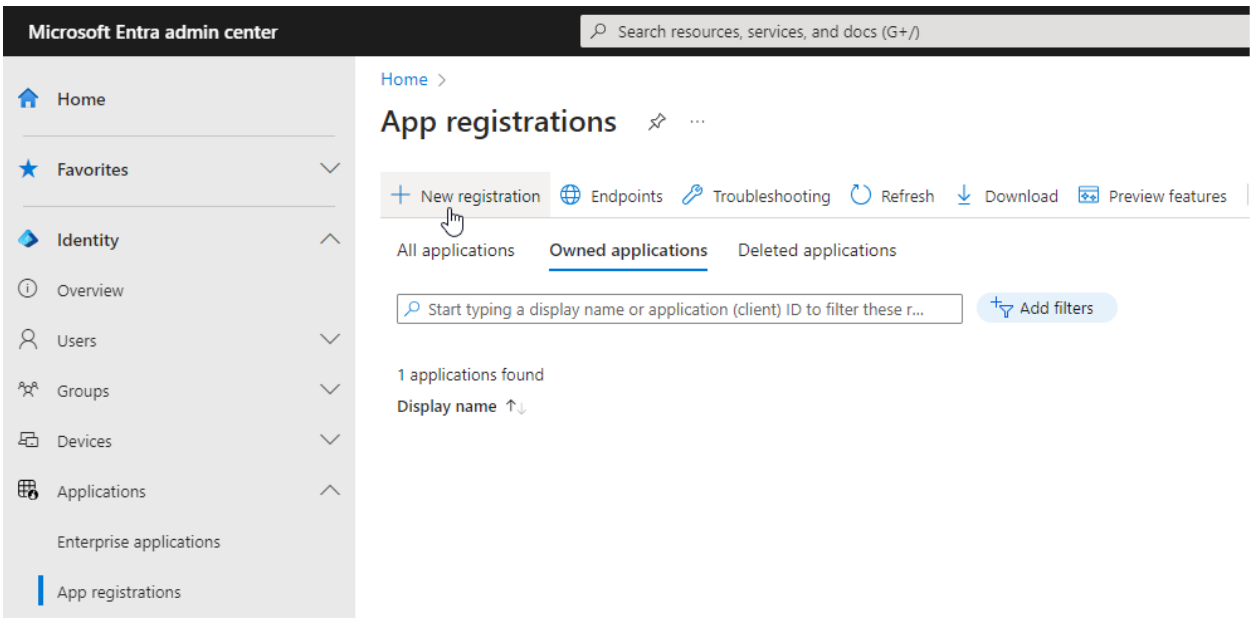
NOTE: You must copy and paste some text values between applications during the registration and configuration.
Ensure you copy and save the required values when instructed, as some are unique secret values that cannot be viewed or received again.

Creating an Entra ID Application

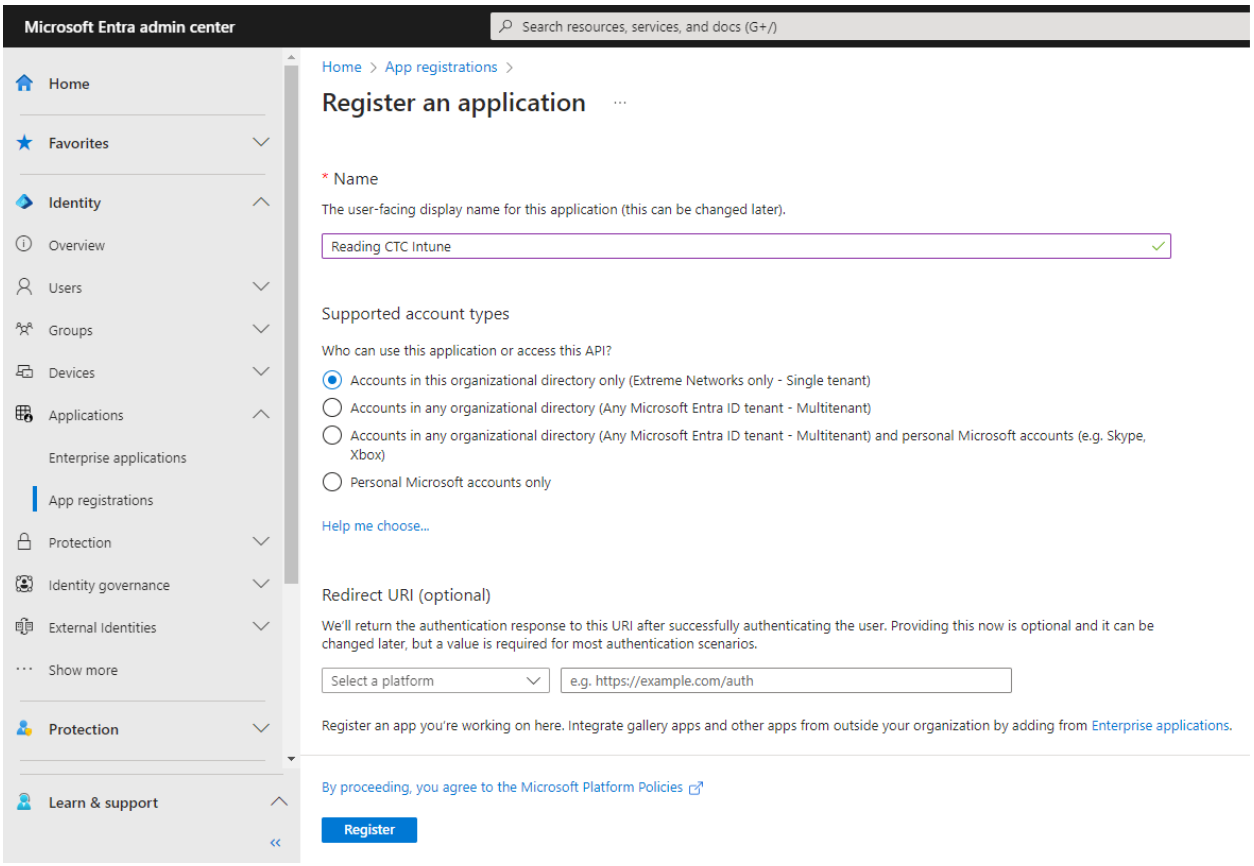
When configuring the compliance check by Intune Compliance Module, you must first create an Entra ID application. This generates an Application ID and Application Secret that are required as part of the ExtremeCloud IQ Site Engine. Use the following steps to create and register an Entra ID application.

1. Access the Microsoft Entra ID page with your Admin credentials at https://portal.azure.com or https://entra.microsoft.com.
2. Select **Manage Microsoft Entra ID > View**.
3. Select **App registrations > New registration**

.

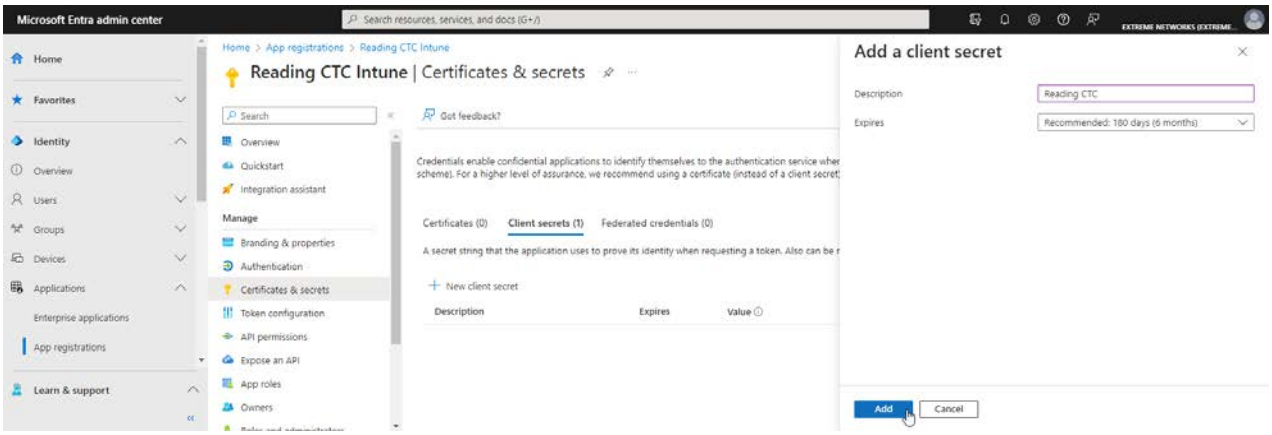


4. Enter the following information into the required fields:
    - **Name** - Enter a name for the Entra ID registered application
    - **Supported account types** - Select Accounts in this organization directory only - (Single tenant)
5. Select **Register**.

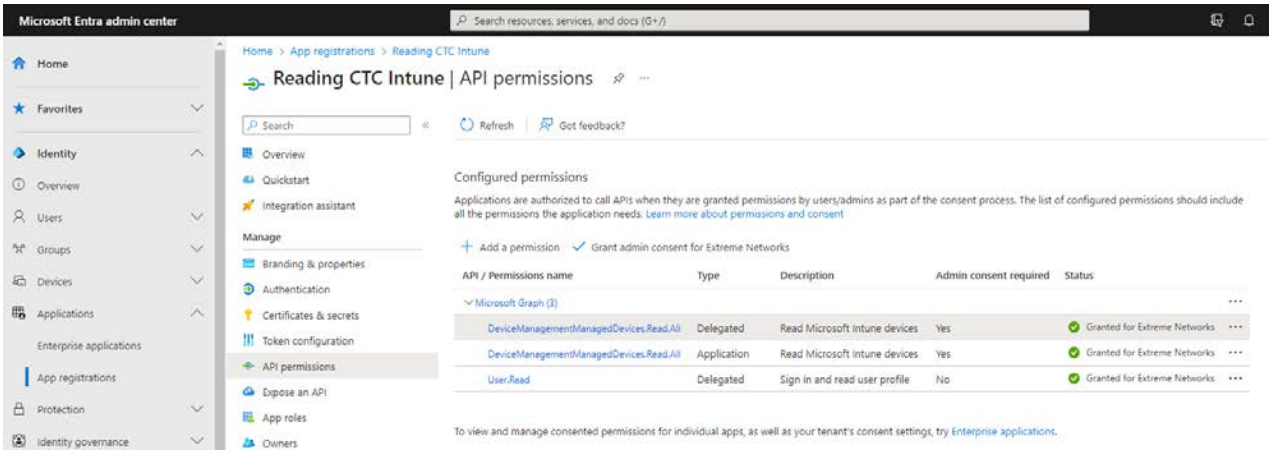


6. Select **Add a certificate or secret**, OR you can navigate to **Certificates & secrets** in the left menu.
7. Select **New client secret**.
8. Enter the following information into the required fields:
    - **Description** - your description of the new credentials
    - **Expires** - define how long the client secret is valid, when the client secret expires the non-compliant list cannot be received.
        - **NOTE:** The expiration of the client secret cannot be modified in Entra ID. The best practice is to create a new client secret before the existing one expires and update the value in ExtremeControl settings.

9. Select **Add**.

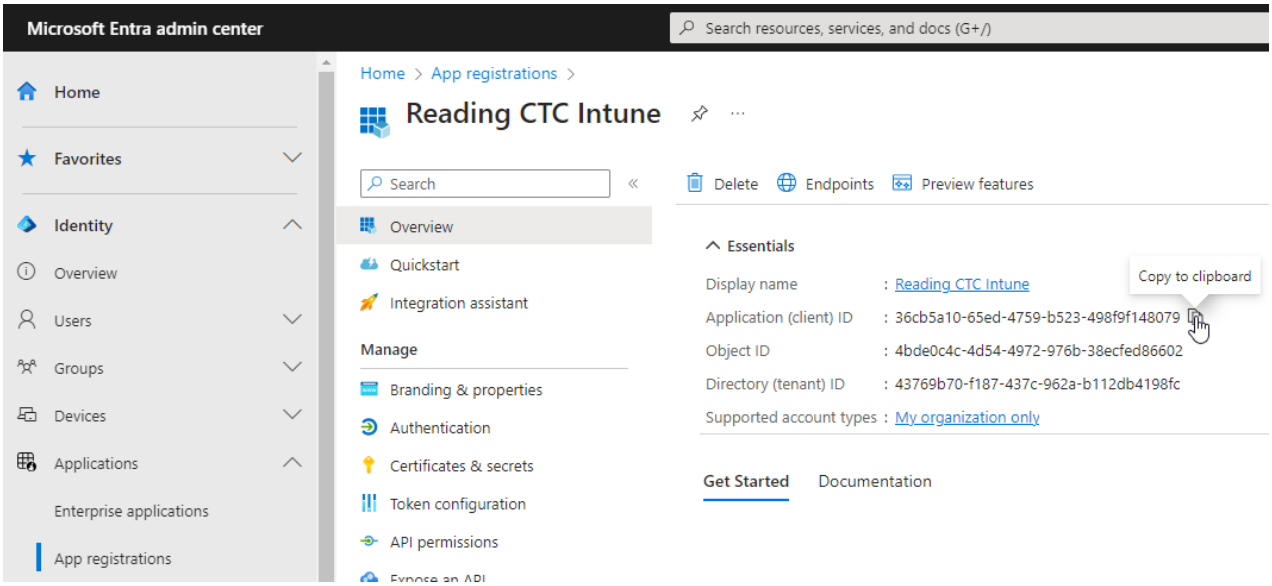


10. Copy the secret value to the clipboard. This is the only time the client secret is displayed. Save the secret value for your Client Secret.
11. Select **API permissions > Add a permission**.
12. Select **Microsoft Graph > Delegated permissions**
13. Select the following delegated permissions:
    - In the **DeviceManagementManagedDevices** select:
      - **DeviceManagementManagedDevices.Read.All**
14. Select Application permissions and add the following additional application permissions:
    - In the DeviceManagementManagedDevices select:
      - DeviceManagementManagedDevices.Read.All
15. Select **Add permissions**.
16. Select **Grant admin consent for <your company domain>**, and select **Yes** to confirm.

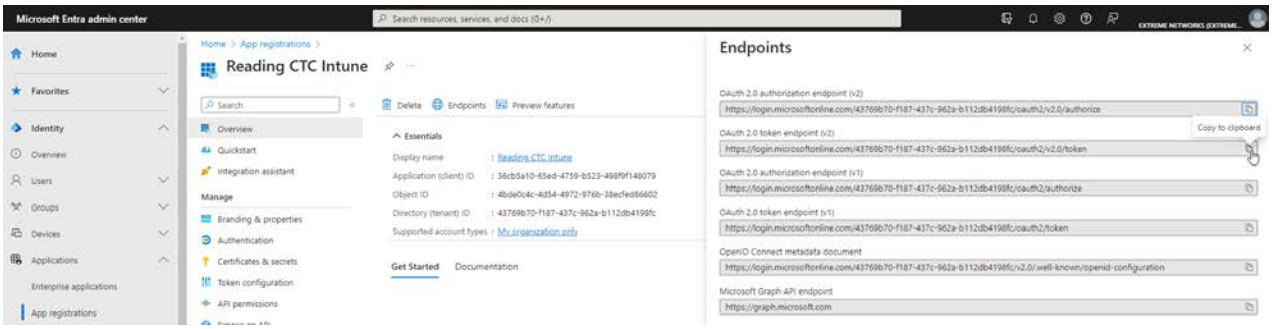


17. Select **Overview**.

18. Copy the displayed **Application (client) ID** value. Save this value for your Client ID.



19. Select **Endpoints**.
20. Copy the displayed **OAuth 2.0 token endpoint (v2)** value. Save this value for your Token Endpoint.



Intune Compliance Module Configuration

You must provide the values you saved during the creation and registration of the Entra ID application in the Administration > Options > Access Control > Intune Compliance Check.

Use the following steps to configure the Intune Compliance Check behavior:

1. From ExtremeCloud IQ Site Engine, open **Adminstration > Options**.
2. In the left-panel tree, navigate to **Access Control > Intune Compliance Check.**

3. Enter the following information into the required fields:
    - Enable Compliance Check - select to check
    - Check Interval - defines how often ExtremeCloud IQ Site Engine downloads the list of non-compliant Intune IDs from Microsoft. If the number of non-compliant devices is high, do not configure a short check interval.
    - Client ID - enter the value copied as "Application (client) ID"
    - Client Secret - enter the value copied as "Client Secret"
    - Token Endpoint - enter the value copied as "OAuth 2.0 token endpoint (v2)"
4. Select **Save**.

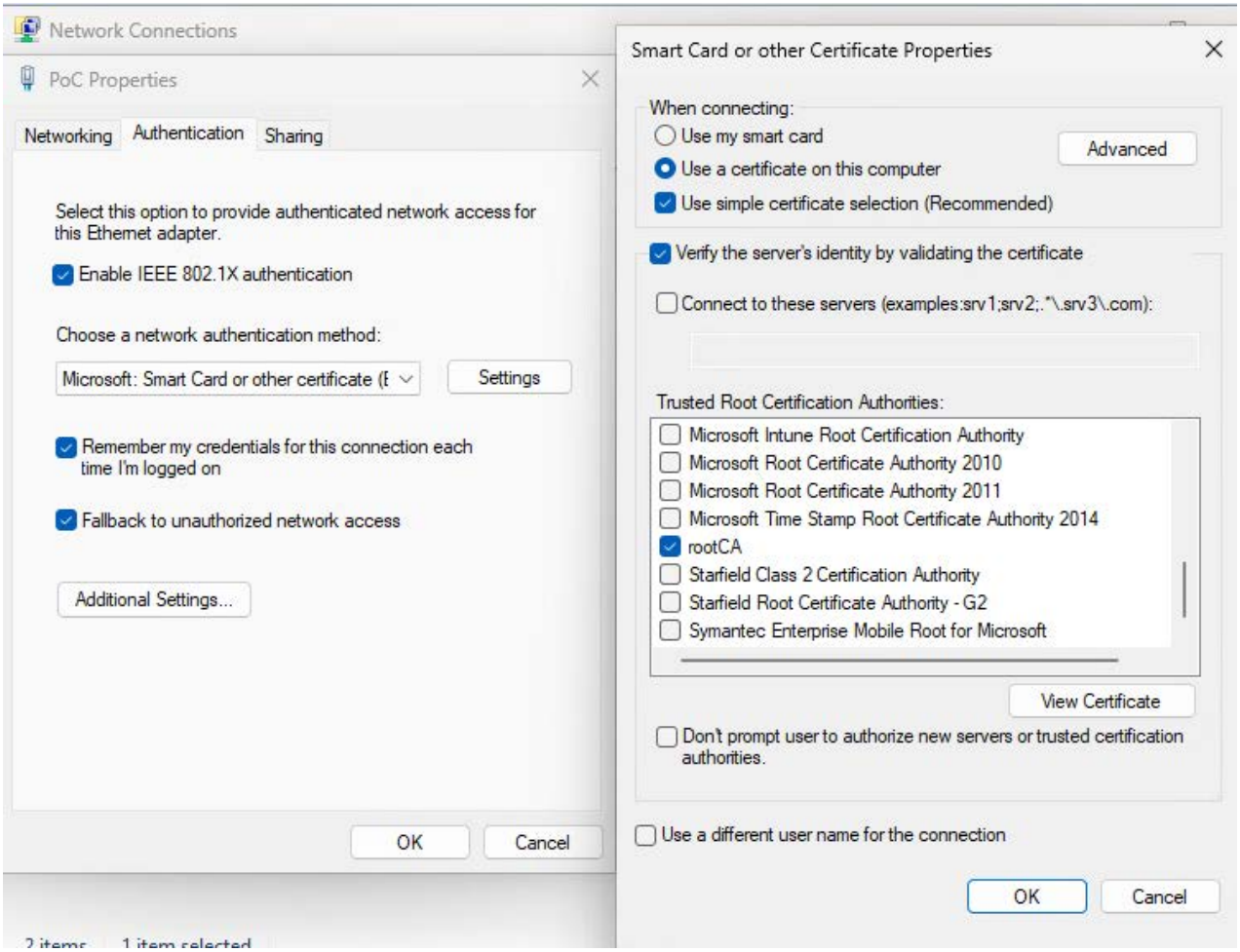
End-System 802.1X Configuration

You must configure the end-system to use IEEE 802.1X authenticated network access. The following is an example using a Windows 11 client.

After you have configured the AAA rules, the User Groups configuration, and the Access Control Rule configuration using the steps above, you must configure 802.1X on the end-system:

1. From Windows 11 search, type **view network connections,** then select **Open**.
2. Right-click on the network connection you need to configure, and select **Properties**.
3. Select the **Authentication** tab.
4. Ensure **Enable IEEE 802.1X authentication** is checked.
5. In the **Choose a network authentication method**, select **Microsoft: Smart Card or other certificate (EAP TLS)**.
6. Select **Settings**.

7. In the **Trusted Root Certification Authorities** area, select the CA issued certificate for your Access Control Engines.

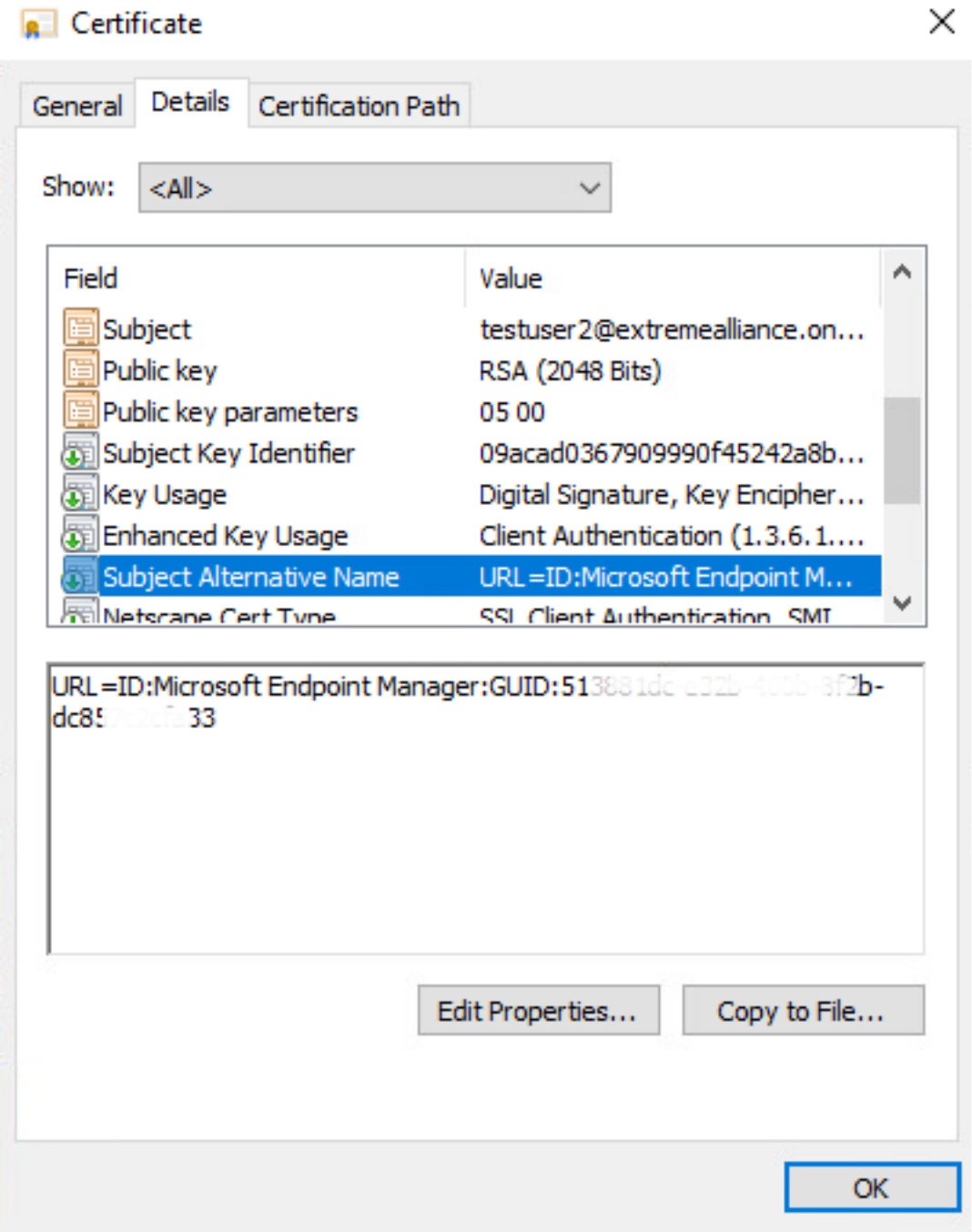


8. Select **OK**, then select **OK** again.

Example of an End-System's Certificate

You must ensure that the Intune ID is part of the Subject Alternative Name URI in the certificate. Example of the industry standard format is: URL=IntuneDeviceId:Microsoft Endpoint Manager:GUID:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx. If Microsoft SCEP is used, see Use SCEP

certificate profiles with Microsoft Intune.



- Access Control Options
- How to Update ExtremeControl Engine Server Certificates
- Manage Certificates

How to Integrate and Configure VMware Workspace ONE UEM

This Help topic describes the steps for integrating ExtremeControl with VMware Workspace ONE UEM (formerly AirWatch) to allow device compliance, posture, and ownership state from Workspace ONE UEM to influence Access Control policy decisions.

A common use case for this configuration is to apply different network authorizations to devices based on their MDM compliance status, ownership type, or compromised state as reported by Workspace ONE UEM. For example, granting full access only to compliant corporate-owned devices, placing non-compliant devices in a restricted VLAN, or applying a BYOD policy to personally-owned devices.

This topic includes information and instructions on:

- Solution Overview
- Requirements for Workspace ONE UEM
- Workspace ONE UEM Compliance Module Configuration
- End-System Groups
- End-System Table Columns
- Creating NAC Rules Based on Workspace ONE UEM Attributes
- Fallback Behavior

Solution Overview

ExtremeControl integrates natively with Workspace ONE UEM REST API. A monitor periodically retrieves device attributes from Workspace ONE UEM and uses the attributes to populate end-system groups and end-system table columns. Administrators can create ExtremeControl rules that reference the end-system groups to enforce network access policies based on device compliance, ownership, and security posture.

The integration functions similarly to the Microsoft MDM Intune/Defender integration. Device attributes are cached locally, lookups at authentication time do not introduce latency or consume API rate limits.

Requirements

These are the configuration requirements for the Workspace ONE UEM Integration.

- A Workspace ONE UEM tenant with API access enabled.
- A Workspace ONE UEM administrator account with API credentials.

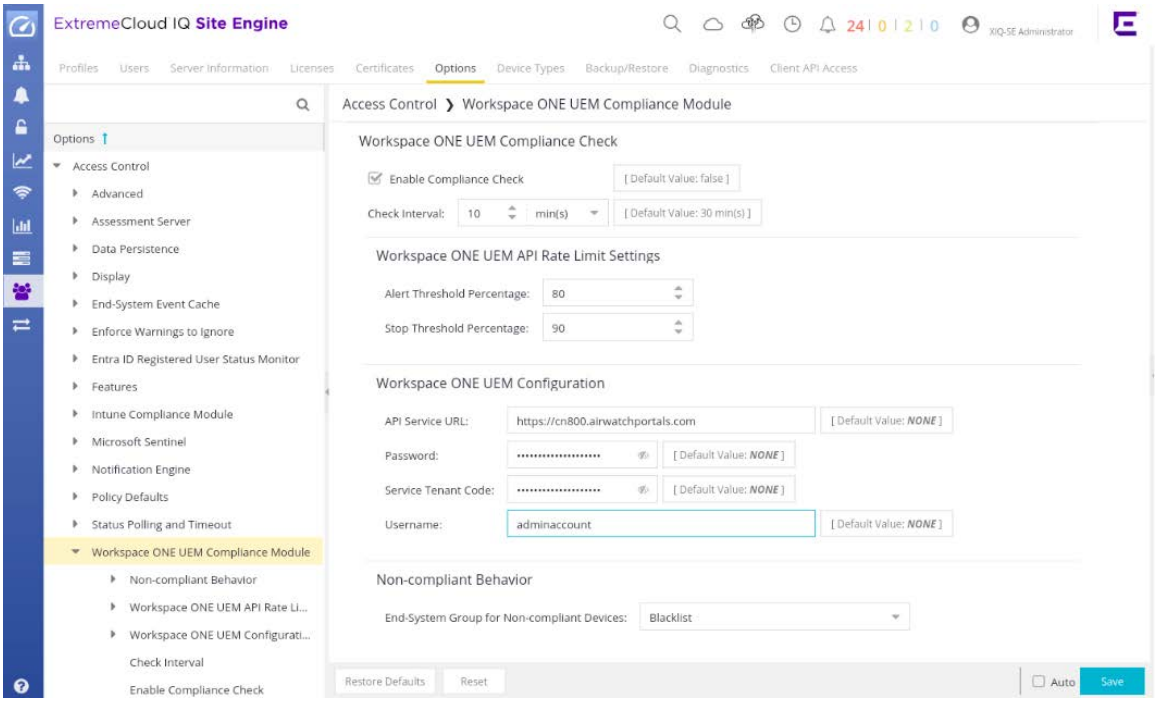
- The Workspace ONE UEM tenant URL (for example, `https://cn800.airwatchportals.com`) and API key (tenant code).
- ExtremeCloud IQ Site Engine must have network connectivity to the Workspace ONE UEM API endpoint.

NOTE: You must copy and paste the Workspace ONE UEM API key (tenant code) and tenant URL from your registration and configuration when configuring the integration in ExtremeCloud IQ Site Engine.

Workspace ONE UEM Compliance Module Configuration

Use the following steps to configure the Workspace ONE UEM integration in ExtremeCloud IQ Site Engine.

1. From ExtremeCloud IQ Site Engine, select **Administration > Options**.
2. In the left-panel navigation tree, expand **Access Control** and select **Workspace ONE UEM Compliance Module**.
3. Configure the following settings:
    - **Enable Compliance Check** — Select to enable the Workspace ONE UEM integration. When enabled, the Access Control engine periodically queries the Workspace ONE UEM API for device attribute updates.
    - **Check Interval** — Specify the frequency (in minutes) at which the integration queries the Workspace ONE UEM API for device attribute updates. Default: 30 minutes.
    - **Alert Threshold Percentage** — Configure alert threshold for generating event logs when API call rate limits are approached.
    - **Stop Threshold Percentage** — Configure stop threshold for generating event logs when API call rate limits are approached. If stop threshold is reached, the system suppresses processing until the Workspace ONE UEM API call limits are reset daily.
    - **API Service URL** — Enter the URL of the Workspace ONE UEM API endpoint (for example, `https://cn800.airwatchportals.com`).
    - **Password** — Enter the Workspace ONE UEM API administrator password.
    - **Tenant Code** — Enter the API key provided by Workspace ONE UEM for your tenant.
    - **Username** — Enter the Workspace ONE UEM API administrator username.
    - **End-System Group for Non-compliant Devices** — Select the existing end-system group to which non-compliant devices are added. Default: Blacklist. You can select any existing end-system group.
4. Select **Save**.



End-System Groups

When enabled, the integration automatically populates the following end-system groups. You can view the populated end-system groups in **Control > Access Control > Configuration > Group Editor > End-System Groups**.

System-Generated Ownership Groups

The following groups are created automatically by the system and populated based on the device ownership type reported by Workspace ONE UEM:

- MDM Corporate Owned — Devices reported by Workspace ONE UEM as corporate-owned
- MDM Personal Owned — Devices reported by Workspace ONE UEM as personally owned bring your own device (BYOD)
- MDM Shared Ownership — Devices reported by Workspace ONE UEM as shared-ownership

Non-Compliant Group

Non-compliant devices are added to the end-system group selected in the Non-Compliant Group setting from your Workspace ONE UEM Compliance Module Configuration. The default group is Blacklist, but you can select any existing end-system group.

NOTE: Changes in group membership can trigger reauthentication of affected end-systems. Reauthentication enables dynamic policy enforcement when device compliance or ownership status changes in Workspace ONE UEM. The existing ExtremeControl function for triggering reauthentication on group membership changes is used.

The Workspace ONE UEM integration does not create a separate end-system group for compromised devices. Compromised devices are expected to be reported as non-compliant and are covered by the non-compliant group.

End-System Table Columns

The following columns are added to the End-Systems table when the integration is active. You can view the columns by selecting **Control > End-Systems**.

- MDM Compliant — Indicates the compliance status of the device as reported by Workspace ONE UEM (Compliant / Non-Compliant).
- MDM Ownership — Indicates the ownership type (Corporate / Personal / Shared).
- MDM Compromised — Indicates if the device has been reported as compromised (true / false).

Creating NAC Rules Based on Workspace ONE UEM Attributes

Use the end-system groups populated by the integration as conditions in your ExtremeControl rules.

1. From ExtremeCloud IQ Site Engine, open the **Control > Access Control** tab.
2. In the left-panel tree, navigate to **Configuration** and select your configuration.
3. Select **Rules**.
4. Select **Add**.
5. In the **Name** field, enter a name for the rule.
6. Select the **Rule Enabled** checkbox.
7. In the **Description** field, enter a description for the rule.
8. In the **End-System Group** field, select one of the MDM groups (for example, MDM Corporate Owned).
9. Configure the appropriate **ExtremeControl Profile** for matching end-systems.
10. Select **Save**.
11. Enforce the configuration to your **Access Control engines**.

Example Policies:

- If a device is non-compliant, assign a Quarantine access policy
- If a device is corporate-owned, assign a Corporate access policy. If personally-owned, assign a BYOD access policy

Fallback Behavior

If the Workspace ONE UEM API becomes unreachable, ExtremeControl uses cached device attribute data from the last successful synchronization. Event logs are generated to alert administrators of connectivity issues.

Logging

Sync operations are logged in the server logs when diagnostic verbosity is enabled. Log entries report the number of MAC addresses added to or removed from MDM groups during each sync cycle, rather than individual end-system events for each.

NOTE: Sync operations are designed not to degrade ExtremeControl performance in large deployments. API rate limits are monitored and event logs are generated when thresholds are approached. Review the Alert Threshold setting in the Workspace ONE UEM Compliance Module configuration.

- How to Integrate and Configure Microsoft MDM Intune/Defender
- Access Control Options

How to Integrate and Configure Microsoft Sentinel Export

This Help topic describes the steps for integrating ExtremeCloud IQ Site Engine with Microsoft Sentinel to export NAC appliance authentication, authorization, and enforcement event data to a customer's Azure Log Analytics Workspace for security analysis, reporting, and alerting.

A use case for this configuration is to provide centralized SOC monitoring of ExtremeControl NAC events alongside endpoint, identity, and cloud telemetry within Microsoft Sentinel. Security teams can build analytics rules, workbooks, and hunting queries using ExtremeControl data as a signal source.

This topic includes information and instructions on:

- Solution Overview
- Requirements for Microsoft Sentinel Export
- Deploying the ARM Template in Microsoft Azure
- Assigning the Monitoring Metrics Publisher Role
- Configuring Microsoft Sentinel Export in ExtremeCloud IQ Site Engine
- Custom Table Schema

Solution Overview

ExtremeCloud IQ Site Engine listens for end-system events sourced from NAC appliances and classifies qualifying events into Authentication, Authorization, or Enforcement categories. When export is enabled, qualifying events are streamed in near real-time to a customer-specified Azure Log Analytics Workspace using the Azure Monitor Logs Ingestion API.

Data lands in a custom Extreme Networks table within the workspace (ExtremeControlEndSystemEventsLog_CL), immediately queryable using Kusto Query Language (KQL). If Microsoft Sentinel is enabled on the same Log Analytics Workspace, the data is automatically available in Sentinel with no additional ingestion steps.

From Microsoft Sentinel, customers can:

- Query ExtremeControl event data directly using KQL
- Create analytics rules to trigger alerts based on NAC event patterns
- Build workbooks for visual dashboards and reporting
- Run hunting queries to investigate authentication or enforcement anomalies

Requirements

These are the configuration requirements for the Microsoft Sentinel Export Integration.

- An active Microsoft Azure subscription.
- An existing Logs Analytics Workspace.
- An existing Azure App Registration (service principal) with a Tenant ID, Client ID, and Client Secret.
- Contributor-level access to the resource group where the Data Collection Rule (DCR) will be deployed.
- Owner or User Access Administrator rights on the resource group (required for the role assignment step).
- ExtremeCloud IQ Site Engine version 26.06.10 or later.
- ExtremeCloud IQ Site Engine network connectivity to the Azure Logs Ingestion API endpoint over HTTPS.
- Extreme Networks ARM Template JSON code to paste into Azure template editor.

NOTE: You must copy and save the Azure App Registration Tenant ID, Client ID, and Client Secret from your registration and configuration in Azure. The values are required when configuring the integration in ExtremeCloud IQ Site Engine.

Extreme Networks ARM template JSON code

```
{
    "$schema": "https://schema.management.azure.com/schemas/2019-04-
01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "dataCollectionRuleName": {
            "defaultValue": "ExtremeControl-DCR",
            "type": "String",
            "minLength": 3,
            "maxLength": 30,
            "metadata": {
                "description": "Name of the Data Collection Rule to create. Must
be 3-30 characters, letters, numbers, and hyphens only. Cannot start or end with
a hyphen."
            }
        },
        "customTableName": {
            "defaultValue": "ExtremeControlEndSystemEventsLog",
            "type": "String",
            "metadata": {
                "description": "Name of the custom table to create in your Log
Analytics Workspace. The '_CL' suffix will be appended automatically."
            }
        },
        "workspaceResourceId": {
            "type": "String",
            "metadata": {
                "description": "The full resource ID of your existing Log
Analytics Workspace. Found under: Workspace > Properties > Resource ID."
            }
        }
    },
    "variables": {
        "tableName": "[concat(parameters('customTableName'), '_CL')]",
        "streamName": "[concat('Custom-', parameters('customTableName'), '_
CL')]",
        "workspaceName": "[last(split(parameters('workspaceResourceId'), '/'))]"
    },
    "resources": [
        {
            "type": "Microsoft.OperationalInsights/workspaces/tables",
            "apiVersion": "2022-10-01",
            "name": "[concat(variables('workspaceName'), '/', variables
('tableName'))]",
            "properties": {
                "schema": {
                    "name": "[variables('tableName')]",
                    "columns": [
                        { "name": "TimeGenerated", "type": "datetime" },
                        { "name": "EventFamily", "type": "string" },
                        { "name": "MacAddress", "type": "string" },
                        { "name": "DeviceFamily", "type": "string" },
```

```
                        { "name": "DeviceType", "type": "string" },
                        { "name": "IpAddress", "type": "string" },
                        { "name": "Ipv6Address", "type": "string" },
                        { "name": "HostName", "type": "string" },
                        { "name": "UserName", "type": "string" },
                        { "name": "State", "type": "string" },
                        { "name": "ExtendedState", "type": "string" },
                        { "name": "Reason", "type": "string" },
                        { "name": "AuthenticationType", "type": "string" },
                        { "name": "Profile", "type": "string" },
                        { "name": "Policy", "type": "string" },
                        { "name": "SwitchIp", "type": "string" },
                        { "name": "SwitchPort", "type": "string" },
                        { "name": "SourceIp", "type": "string" }
                    ]
                }
            }
        },
        {
            "type": "Microsoft.Insights/dataCollectionRules",
            "apiVersion": "2024-03-11",
            "kind": "Direct",
            "name": "[parameters('dataCollectionRuleName')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
                "[resourceId('Microsoft.OperationalInsights/workspaces/tables',
variables('workspaceName'), variables('tableName'))]"
            ],
            "properties": {
                "streamDeclarations": {
                    "[variables('streamName')]": {
                        "columns": [
                            { "name": "TimeGenerated", "type": "datetime" },
                            { "name": "EventFamily", "type": "string" },
                            { "name": "MacAddress", "type": "string" },
                            { "name": "DeviceFamily", "type": "string" },
                            { "name": "DeviceType", "type": "string" },
                            { "name": "IpAddress", "type": "string" },
                            { "name": "Ipv6Address", "type": "string" },
                            { "name": "HostName", "type": "string" },
                            { "name": "UserName", "type": "string" },
                            { "name": "State", "type": "string" },
                            { "name": "ExtendedState", "type": "string" },
                            { "name": "Reason", "type": "string" },
                            { "name": "AuthenticationType", "type": "string" },
                            { "name": "Profile", "type": "string" },
                            { "name": "Policy", "type": "string" },
                            { "name": "SwitchIp", "type": "string" },
                            { "name": "SwitchPort", "type": "string" },
                            { "name": "SourceIp", "type": "string" }
                        ]
                    }
                },
```

```
                "dataSources": {},
                "destinations": {
                    "logAnalytics": [
                        {
                            "workspaceResourceId": "[parameters
('workspaceResourceId')]",
                            "name": "logAnalyticsDestination"
                        }
                    ]
                },
                "dataFlows": [
                    {
                        "streams": [ "[variables('streamName')]" ],
                        "destinations": [ "logAnalyticsDestination" ],
                        "transformKql": "source",
                        "outputStream": "[variables('streamName')]"
                    }
                ]
            }
        }
    ],
    "outputs": {
        "DCR_ImmutableId": {
            "type": "string",
            "value": "[reference(resourceId
('Microsoft.Insights/dataCollectionRules', parameters
('dataCollectionRuleName'))).immutableId]"
        },
        "IngestionEndpoint": {
            "type": "string",
            "value": "[reference(resourceId
('Microsoft.Insights/dataCollectionRules', parameters
('dataCollectionRuleName'))).endpoints.logsIngestion]"
        },
        "StreamName": {
            "type": "string",
            "value": "[variables('streamName')]"
        }
    }
}
```

Deploying the ARM Template in Microsoft Azure

Before configuring the export in Site Engine, you must deploy the required Azure resources. Extreme Networks provides an ARM (Azure Resource Manager) deployment template that automatically creates:

- A Data Collection Rule (DCR) configured for direct log ingestion.
- A custom table in the Log Analytics Workspace with the Extreme Networks event schema.

Use the following steps to deploy the ARM template.

1. In the Azure portal http://portal.azure.com, search for **Deploy a custom template** in the top search bar.
2. Select **Build your own template in the editor**.
3. Select **Quickstart Template**. Clear the contents of the text editor. Paste in the **Extreme Networks ARM template JSON code**, then select **Save**.
4. Fill in the deployment parameters:
    - **Subscription** – The Azure subscription to deploy into.
    - **Resource Group** – The resource group where the DCR is created. Enter the **Log Analytics Workspace resource group**.
    - **Data Collection Rule Name** – The name of the DCR to create. Enter **ExtremeControl-DCR**
    - **Workspace Resource ID** – The full resource ID of the existing Log Analytics Workspace. Find this info in **Workspace > Properties > Resource ID**.
5. Select **Review + Create**. Azure validates the template and parameters.
6. Select **Create** to begin deployment. The deployment typically completes in 1–3 minutes.
7. Once complete, select **Outputs** in the left sidebar of the deployment summary screen. The following three values display, you must copy and save. The values are needed to configure Microsoft Sentinel Export in ExtremeCloud IQ Site Engine:
    - **DCR Immutable ID** – The unique identifier of the created DCR.
    - **Ingestion Endpoint** – The URL to send the log data.
    - **Stream Name** – The name of the stream in the DCR that maps to the custom table.

Assigning the Monitoring Metrics Publisher Role

After deploying the ARM template, the Azure App Registration must be granted permission to write data to the DCR.

Use the following steps to assign the Monitoring Metrics Publisher Role.

1. In the Azure portal, navigate to **Azure Monitor > Data Collection Rules** and open the newly created DCR.
2. Select **Access Control (IAM)** in the left sidebar.
3. Select **Add > Add role assignment**.
4. Search for and select **Monitoring Metrics Publisher**, then select **Next**.
5. From **Assign access to**, select **User, group, or service principal**.

6. Select **Select members**, search for the App Registration being used for this integration, select it, and select **Select**.
7. Select **Review + Assign** to save the role assignment.

NOTE: Allow up to 30 minutes for the role assignment to propagate. If the Test Connection function in ExtremeCloud IQ Site Engine returns a 403 error shortly after setup, wait and try again.

Configuring Microsoft Sentinel Export in ExtremeCloud IQ Site Engine

Use the following steps to configure the Microsoft Sentinel Export in ExtremeCloud IQ Site Engine.

1. From ExtremeCloud IQ Site Engine, select **Administration > Options**.
2. In the left-panel tree, expand **Access Control** and select **Microsoft Sentinel**.
3. Select the **Enable Microsoft Sentinel Export** checkbox.
4. In the **Authentication** section, configure the following fields:
   - **Client ID** – Enter the Azure application (service principal) Client ID.
   - **Client Secret** – Enter the client secret associated with the Azure application.
   - **Tenant ID** – Enter the customers Azure Active Directory Tenant ID.
5. In the Log Analytics Endpoint section, configure the following fields using the values copied from the ARM template deployment Outputs:
   - **DCR Immutable ID** – Enter the DCR Immutable ID.
   - **Logs Ingestion Endpoint Base URL** – Enter the Ingestion Endpoint URL.
   - **Stream Name** – Enter the Stream Name.
6. In the **Events to Export** section, select from the event categories available to export.
   - **Authentication Events** – Exports authentication success and failure events, including method and identity details.
   - **Authorization Events** – Exports authorization decisions, including Role and VLAN assignment and enforcement profile.
   - **Enforcement Events** – Exports enforcement changes, including quarantine, disconnect, and restricted access decisions.
7. Select **Save**.
8. Select **Test Connection** to verify the configuration with an automated two-step validation:

- The first validation step attempts Azure authentication using the Client ID, Client Secret, and Tenant ID.
- After the first validation succeeds, a second validation step sends a probe to request the configured Logs Ingestion Endpoint using the DCR Immutable ID and Street Name.

NOTE: Allow up to 30 minutes for the role assignment to propagate. If the Test Connection function in ExtremeCloud IQ Site Engine returns a 403 error shortly after setup, wait and try again.

Custom Table Schema

The exported data lands in a custom table in the Microsoft Sentinel Log Analytics Workspace. The table name defaults to ExtremeControlEndSystemEventsLog_CL. You can customize the table name during the ARM template deployment. The following lists the exported data table column descriptions:

- **TimeGenerated** – Timestamp of the event.
- **EventFamily** – Event category: Authentication, Authorization, or Enforcement.
- **MACAddress** – MAC address of the device.
- **DeviceFamily** – Device family classification.
- **DeviceType** – Device type classification.
- **IPAddress** – IPv4 address of the device.
- **IPv6Address** – IPv6 address of the device.
- **Hostname** – Hostname of the device.
- **Username** – Username associated with the event.
- **State** – Event state.
- **ExtendedState** – Extended state detail.
- **Reason** – Reason associated with the event outcome.
- **AuthenticationType** – Authentication method used.
- **Profile** – Profile applied.
- **Policy** – Policy applied.
- **SwitchIP** – IP address of the switch.
- **SwitchPort** – Port on the switch.
- **SourceIP** – Source IP address.

Logging and Reliability

Qualifying events are staged in a bounded in-memory queue. Once a minute, the dispatcher drains the staging queue and breaks the events into batches, with each batch capped at 1 MB per API request. If an API request fails, ExtremeCloud IQ Site Engine retries up to two additional times (three attempts total), with a 15-second delay between each retry. If all three attempts fail, the batch is discarded and is not re-queued. Export enable/disable actions and errors encountered during export are recorded in the ExtremeCloud IQ Site Engine server log. Administrators can review the entries for diagnostics.

NOTE: Under normal operating conditions, ExtremeCloud IQ Site Engine performs approximately 10 API calls a minute, well below the Microsoft-documented limit of 12,000 requests a minute for the Logs Ingestion API. The export mechanism is designed not to degrade ExtremeCloud IQ Site Engine performance.

- How to Integrate and Configure Microsoft MDM Intune/Defender
- How to Integrate and Configure VMware Workspace ONE UEM
- Access Control Options

Add/Edit MAC Lock

Use this window to add a new locked MAC address or edit the settings for an existing locked MAC address. MAC Locking lets you lock a MAC address to a specific switch or port on a switch so that the end-system can only access the network from that port or switch. If the end-system tries to authenticate on a different switch/port, it is rejected or assigned a specific policy. You can add or edit MAC locks from the End-Systems tab.

NOTE: MAC Locking to a specific port on a switch is based on the port interface name (e.g. fe.5.1). If a switch board is moved to a different slot in a chassis, or if a stack reorders itself, this name changes and breaks the MAC Locking settings.



MAC Address

Enter the MAC address that you want to lock.

Switch IP

Enter the IP address of the switch on which you want to lock the MAC address.

Lock to Switch and Port

Select this checkbox if you want to lock the MAC address to a specific port on the switch, and enter the port interface name.

Failed Action

Select the action to take when this MAC address tries to authenticate on a different port and/or switch:

- Reject – The authentication request is rejected.
- Use Policy – Use the drop-down list to select the policy that you want applied. This policy must exist in the **Policy** tab and be enforced to the switches in your network.

Getting Started with ExtremeAnalytics

This topic provides information to help you get started using ExtremeAnalytics to view network application data in the ExtremeCloud IQ Site Engine **Analytics** tab. It includes information on ExtremeAnalytics access requirements, configuring the ExtremeAnalytics engine, enabling NetFlow flow collection, and configuring network locations.

ExtremeAnalytics Access Requirements

In order to view the **Analytics** tab, you must be a member of an authorization group assigned the ExtremeCloud IQ Site Engine ExtremeAnalytics Read Access or Read/Write Access capability. The Read Access capability allows the ability to access the **Analytics** tab and view the ExtremeAnalytics reports. The Read/Write capability adds the ability to configure ExtremeAnalytics engines and NetFlow Collecting devices. It also adds the ability to create and modify fingerprints.

ExtremeAnalytics Engine Configuration

The ExtremeAnalytics engine provides the engine to monitor and classify layer 7 application information based on data from CoreFlow switches and reports that information to ExtremeCloud IQ Site Engine, where it is managed and displayed in the **Analytics** tab.

The ExtremeAnalytics engine must be installed and running on your network. For instructions, see the ExtremeAnalytics Engine Installation Guide.

Following installation, the ExtremeAnalytics engine must be added to ExtremeCloud IQ Site Engine and enforced via the **Configuration** tab in the **Analytics** tab.

Enable Flow Collection

Because the **Analytics** tab displays reports based on NetFlow or Application Telemetry (sflow) flow data, you must enable your network devices that act as the flow sensors, and enable flow collection for their device interfaces. You must also configure your flow sensor devices to send their flow information to the ExtremeAnalytics engine. In addition, the device interfaces you enable for flow collection must match the interfaces configured for analysis by the engine.

Enable Jumbo Frames

When configuring a device as an Application Telemetry source for ExtremeAnalytics, jumbo frames must be enabled on the device and any device or virtual machine between the device and the ExtremeAnalytics engine.

For example, to enable jumbo frames on an ExtremeXOS/Switch Engine device, enter the following in the device CLI:

```
enable jumbo-frame ports all
```

- Configuration - Analytics

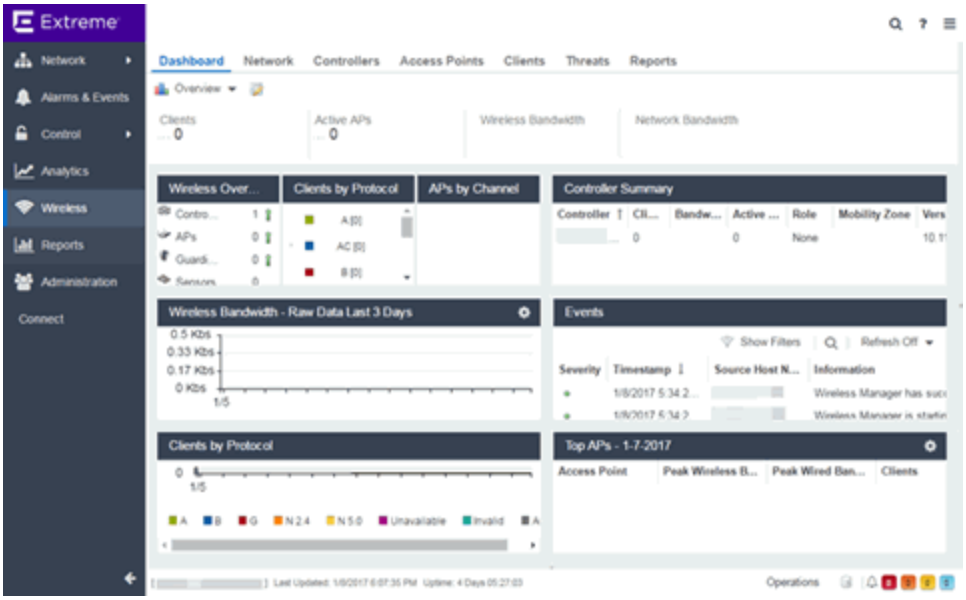
Configuring Enhanced Netflow for Extreme Analytics and Extreme Wireless Controller Version 10.21

When adding a Wireless Controller as a flow source in ExtremeCloud IQ Site Engine, a mirror port is automatically created. Wireless Controllers on which a firmware version of 10.21 or higher is installed use IPFIX, so the mirror port is unnecessary.

NOTE: Wireless Controllers on which a firmware version lower than 10.21 is installed still require the mirror port be configured.

To remove a mirror port on a Wireless Controller running version 10.21:

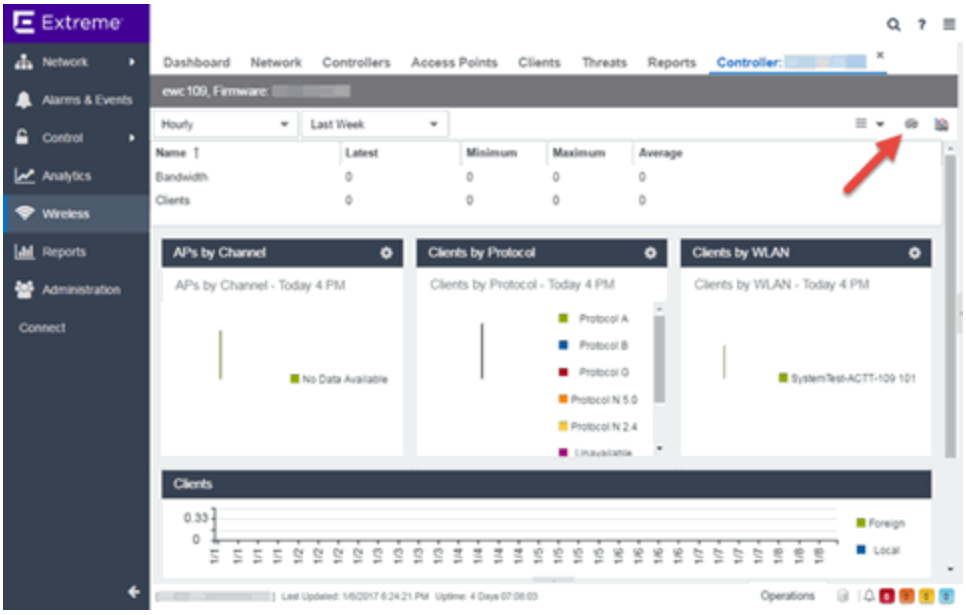
1. Access the **Wireless** tab in ExtremeCloud IQ Site Engine.
   The **Wireless** tab opens.



2. Select the **Controllers** tab.
   The **Controllers** tab opens.

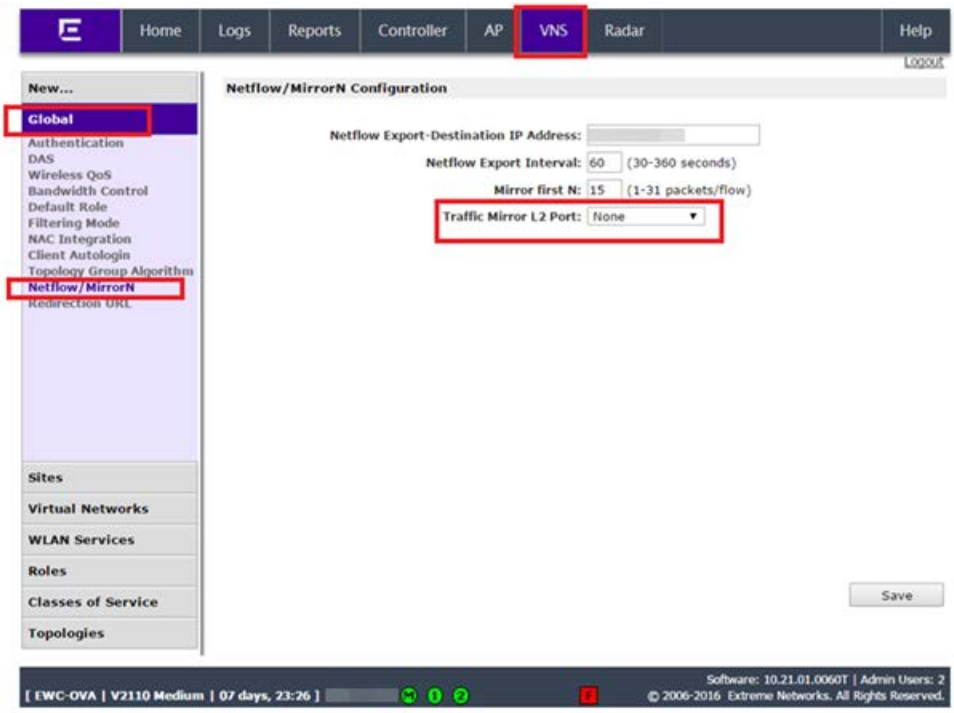


3. Select the **IP address** for the controller, located in the **Controller** column.
   The Wireless Controller Summary page opens.



4. Select the **WebView** icon ( ) at the top right of the Wireless Controller Summary page.
   The WebView opens for the controller.

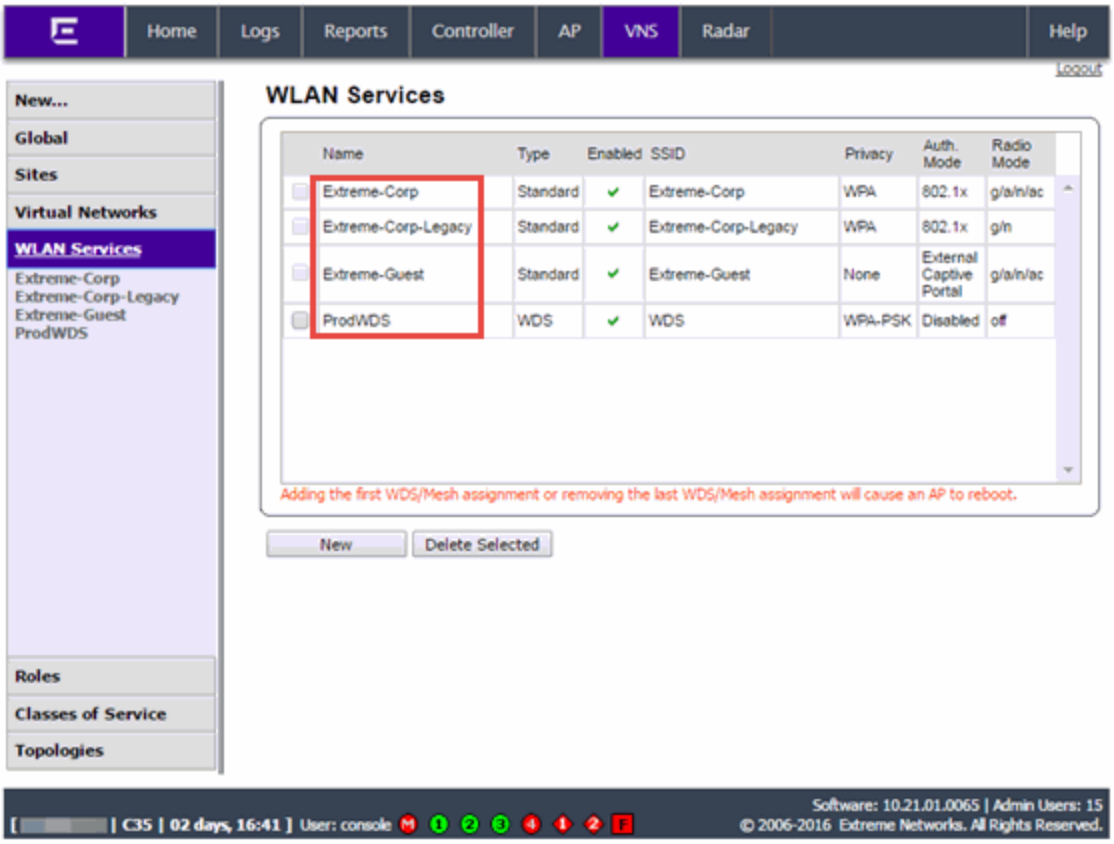
5. Select the **VNS** tab.
   The **VNS** tab opens.



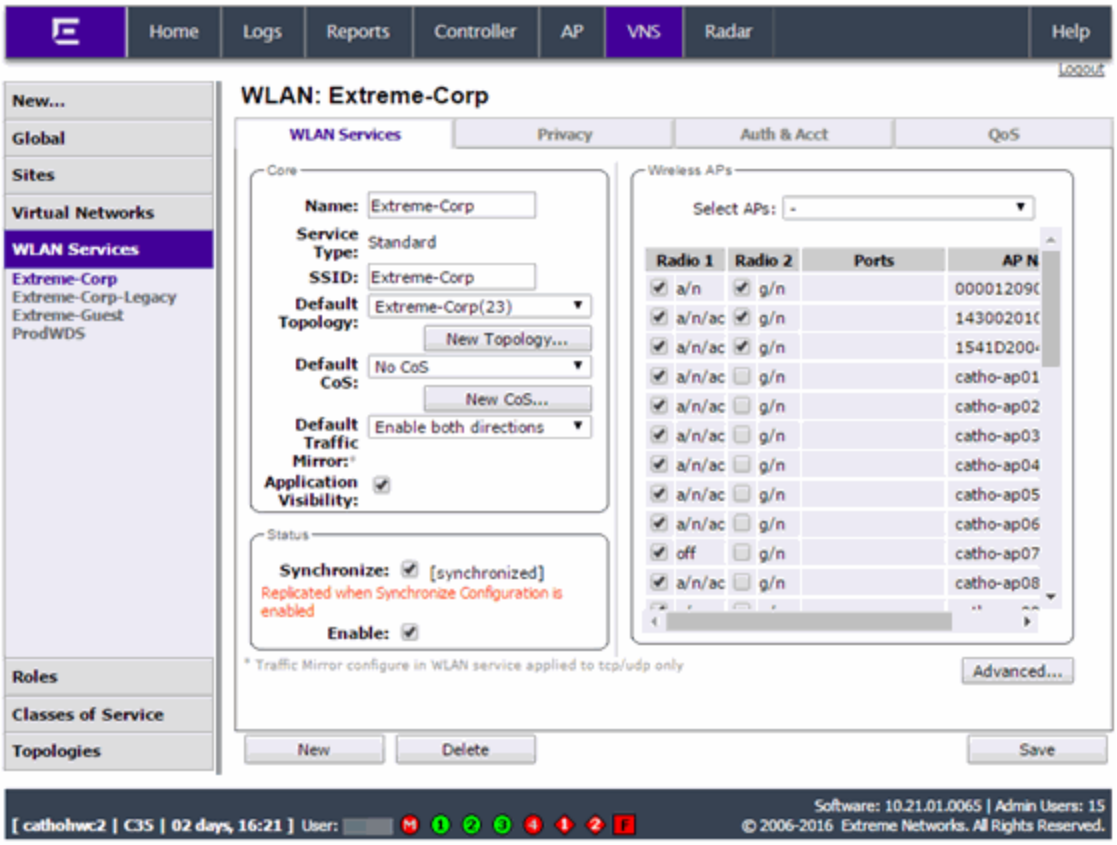
6. Select **Netflow/MirrorN** from the left-panel.
   The Netflow/MirrorN Configuration page opens.
7. Select **None** from the **Traffic Mirror L2 Port** drop-down list.
8. Select the **Save** button.

NOTE: The Mirror Port in the Wireless Control Flow Sources section of the **Analytics** > **Configuration** > **Configuration** tab is not available when the **Traffic Mirror L2 Port** is disabled.

9. Select **WLAN Services** from the left-panel.
   The WLAN Services page opens.

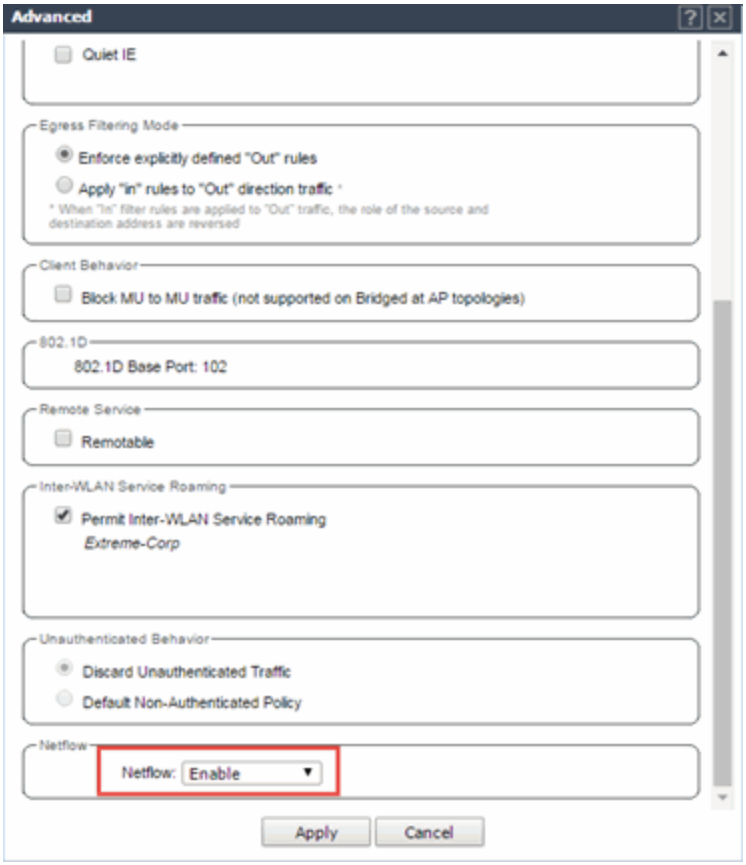

Home
Logs
Reports
Controller
AP
VNS
Radar
Help
Logout
New...
Global
Sites
Virtual Networks
WLAN Services
Extreme-Corp
Extreme-Corp-Legacy
Extreme-Guest
ProdWDS
Roles
Classes of Service
Topologies
WLAN Services
Name
Type
Enabled
SSID
Privacy
Auth. Mode
Radio Mode
Extreme-Corp
Standard
Extreme-Corp
WPA
802.1x
g/a/n/ac
Extreme-Corp-Legacy
Standard
Extreme-Corp-Legacy
WPA
802.1x
g/n
Extreme-Guest
Standard
Extreme-Guest
None
External Captive Portal
g/a/n/ac
ProdWDS
WDS
WDS
WPA-PSK
Disabled
off
Adding the first WDS/Mesh assignment or removing the last WDS/Mesh assignment will cause an AP to reboot.
New
Delete Selected
[| C35 | 02 days, 16:41] User: console
Software: 10.21.01.0065 | Admin Users: 15
© 2006-2016 Extreme Networks. All Rights Reserved.

10. Select a wireless LAN in the table.
    The WLAN page opens for the selected wireless LAN.



11. Select the **Advanced** button.
    The **Advanced** window opens.

12. Scroll to the bottom of the window and ensure the **Netflow** drop-down list is set to **Enable**.



13. Select the **Apply** button.

The wireless controller is now configured.

NOTE: **Rx Packets** and **Rx Bytes** can incorrectly be **0** when flow data is gathered via a wireless controller running version 10.21 or higher. Additionally, application response times and some meta data can be blank. This is a known issue and will be addressed in a future release.

How to Deploy ExtremeAnalytics in an MSP or MSSP Environment

This Help topic presents instructions for deploying ExtremeAnalytics within an MSP (Managed Service Provider) or MSSP (Managed Security Service Provider) environment.

Configuring ExtremeCloud IQ Site Engine Behind a NAT Router

If the ExtremeCloud IQ Site Engine server is located behind a NAT (Network Address Translation) router, use the following steps to add an entry to the nat_config.txt file that defines the real IP address for the ExtremeCloud IQ Site Engine server. This allows the ExtremeCloud IQ Site Engine server to convert the NAT IP address received in the ExtremeAnalytics engine response to the real IP address used by the ExtremeCloud IQ Site Engine server. Not adding the real IP address for the ExtremeCloud IQ Site Engine server to the nat_config.txt file results in the ExtremeAnalytics engine incorrectly displaying a state of **IMPAIRED** (orange) rather than **UP** (green).

NOTE: The text in the nat_config.text file refers to a remote IP address and a local IP address. For this configuration, the NAT IP address is the remote IP address and the real IP address is the local IP address.

1. On the ExtremeCloud IQ Site Engine server, add the following entry to the `<install directory>/appdata/nat_config.txt` file.
   `<NAT IP address>=<real IP address>`
2. Save the file.
3. If the ExtremeCloud IQ Site Engine Management server IP address is not configured to use the NAT IP address of the ExtremeCloud IQ Site Engine server, perform the following steps:
   a. Enter the following command at the engine CLI:
      `/opt/appid/configMgmtIP <IP address>`
      Where *<IP address>* is the NAT IP address of the ExtremeCloud IQ Site Engine server.
      Press **Enter**.
   b. Restart the appidserver when the new IP address is configured by typing:
      `appidctl restart`
      Press **Enter**.
4. On the ExtremeCloud IQ Site Engine server, add the following text to the `<install directory>/appdata/NSJBoss.properties` file. In the second to last line, specify the hostname of the ExtremeCloud IQ Site Engine server.

NOTE: The ExtremeAnalytics engine functions as a client computer independent of the server. Both engines and clients must be able to resolve the hostname you specify.

```
# In order to connect to a ExtremeCloud IQ Site
Engine server behind a NAT firewall or a
# ExtremeCloud IQ Site
Engine server with multiple interfaces you must define these two
# variables on the ExtremeCloud IQ Site Engine
server. The java.rmi.server.hostname
# should be the hostname (not the IP) if multiple IPs are being used
# so that each client can resolve the hostname to the correct IP that
# they want to use as the IP to connect to.
java.rmi.server.hostname=<hostname of the server>
java.rmi.server.useLocalHostname=true
```

5. Save the file.
6. Add the ExtremeCloud IQ Site Engine server hostname to your DNS server, if necessary.

NOTE: ExtremeAnalytics engines, remote ExtremeCloud IQ Site Engine clients, and any ExtremeControl engines must be able to connect to ExtremeCloud IQ Site Engine using this hostname.

Wireless

The **Wireless** tab in ExtremeCloud IQ Site Engine provides dashboards, Top N information, and detailed charts to help you monitor the overall status of your wireless network. Reports are flexible and interactive, allowing you to configure time ranges and data rollup values to use for each report. Use the report Search and Filter capabilities to narrow down the data shown in the report tables. Select links in the reports to quickly drill down to more detailed information.

The **Menu** icon (☰) at the top of the screen provides links to additional information about your version of ExtremeCloud IQ Site Engine.

To view wireless reporting data, you must enable statistics collection for your wireless controller devices from either **Network** tab (or the legacy Console application in the device tree or **Device Properties** tab). On the **Network** tab, right-click a wireless controller and select **Device** > **Collect Device Statistics**. In the Console device tree or **Device Properties** tab, right-click the controller and select the OneView > **Collect Device Statistics** checkbox. When you enable Wireless Controller statistics collection (which includes Wireless Controller, WLAN, Topology, and AP wired and wireless statistics), you also have the option to collect wireless client statistics. ExtremeCloud IQ Site Engine begins collecting data on the controller device it uses in its Wireless reports.

To view all Wireless reports, you must be a member of an authorization group that has been assigned full read access capabilities to all of the ExtremeCloud IQ Site Engine tabs and reports.

This Help topic provides information on each Wireless report, plus a section on helpful report features and functionality.

- Dashboard
- Network
- Controllers
- Access Points
- Clients
- Threats
- Reports

Dashboard

The Dashboard menu in the upper left corner provides access to the Dashboard report and the Overview report, as well as additional Top N and summary reports on your wireless devices and clients.

Overview Report

The Overview displays a selection of reports that provide highly summarized information about your wireless network. Select the **Gear** button () to open additional fields from which you can configure the information presented in the reports.

Select links to drill down for more information. Use the drop-down menus to select the date, time, and whether to display Daily, Hourly, or Raw Data.

Wireless Network Summary Report

The Wireless Network Summary dashboard displays three reports displaying the wireless client information, wireless and wired bandwidth usage, and the number of active APs in your network.

Use the drop-down menus to select the time displayed and whether to display Daily, Hourly, or Raw Data.

Network

The **Network** tab presents a top-level wireless network summary report along with additional reports on wireless mobility zones, virtual networks, controllers, and AP groups. These context sensitive reports include data-point rollovers and drill-down links to additional detailed reports, as well as the ability to launch local management.

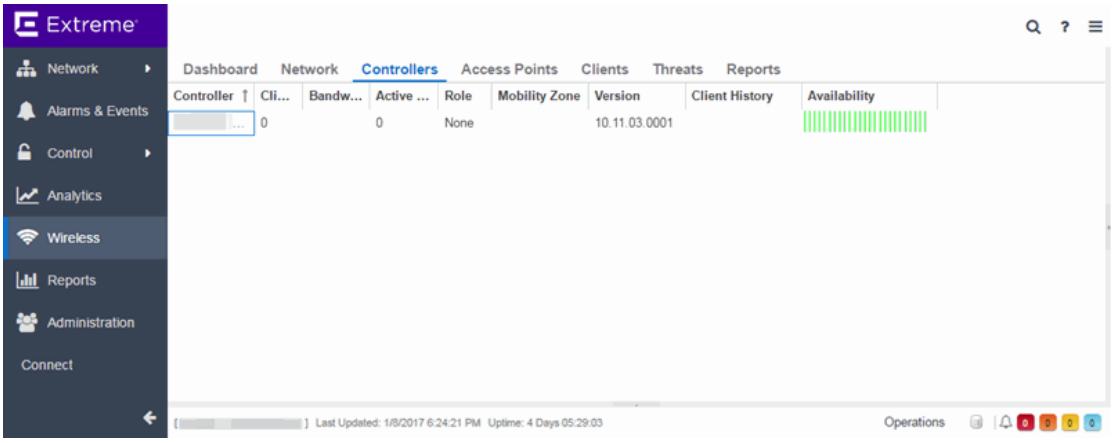
Reports are presented in a familiar wireless component tree structure similar to how components are displayed in Wireless Manager. Selecting any node in the tree provides contextual information for that node.

Select **Discover All Controllers** in the **Tools** menu at the bottom of the tree panel to perform a discover operation that looks for any configuration changes on your wireless controllers with device statistics collection enabled. In addition, you can select **Discover Controller** to rediscover a single controller. Select the controller in the tree, select the down arrow next to the **Discover** button and select **Discover Controller**.

Select **Manage Controllers** in the menu at the bottom of the tree panel to open the ExtremeWireless Assistant where you can remotely manage your wireless controllers.

Controllers

This report displays summary information for each controller. Select the Controller IP address link to open a report that shows APs by channel, clients by protocol, clients by WLAN, clients, and bandwidth usage information for just that controller.



Access Points

This report displays summary information for all the Access Points on your wireless network. Hover over the far left column and select the gray arrow to open the AP Details window that provides controller, bandwidth, and client information. Select a single AP name link to open an in-depth AP Summary view for the selected AP.

Select an AP Status icon to open a table listing the current alarms for the AP. Right-click on a single AP to access a menu of AP reports. Right-click on an AP and select **Search Maps** to open a map with the AP in the center.

Select one or more APs and use the **Menu** icon (☰) in the upper left corner (or right-click on a row) to access various reports and perform various AP actions including:

- Refreshing/rediscovering the selected APs
- Editing AP location
- Setting AP orientation
- Adding selected APs to a specified ExtremeCloud IQ Site Engine map or to maps based on AP location
- Removing selected APs from associated maps
- Searching maps for the selected APs

Additionally, there are two methods of exporting the data in the table:

Export to CSV
: Select to export all of the data in the table to a .CSV file. The exported data displays with any sorting, filtering, and searching applied.

Export Selected to CSV
: Select to export the data in the currently selected row(s) in the table to a .CSV file. The exported data includes all columns in the table (including those not currently displayed).

Clients

The Clients report provides information on wireless network clients and client events. The **Clients** sub-tab displays a list of the currently active clients on the wireless network. The **Client Events** tab shows a historical list of the add, delete, and update events for clients on the wireless network. Events are triggered by:

- Client session start and end
- Inter-AP roaming
- IP address change (including going from no IP address to having one)
- Authentication state change

Events must be collected to display event data in the **Clients** tab. To enable event collection, select the **Enable Event Collection** button at the bottom of the tab.

Select a client or client event in the report tables and use the **Menu** icon (☰) in the upper left corner to access additional reports:

- **Client History** — Opens a report displaying bandwidth, RSS, and packet statistics for the selected client. (You can also access the Client History report by selecting a client's MAC address in the table.) From the Client History window, you can select a button to launch PortView for that client.
- **Client PortView** — Launches a PortView for the client.
- **Search Maps** — If the client is connected to a switch added to an ExtremeCloud IQ Site Engine map, the Maps sub-tab opens with the client centered on the map.
- **AP Summary** — Opens a report displaying summary statistics for the client's AP. From the AP Summary window, you can select a button to launch a Wireless AP Radio Summary report and also launch PortView for the AP device. (You can also access the AP Summary report by selecting the AP Name link in the Client Events table.)

Use the **Search** field to search the reports by specifying an active user name or host name, MAC address, active IP address, or AP name.

Additionally, there are two methods of exporting the data in the table:

Export to CSV
: Select to export all of the data in the table to a .CSV file. The exported data displays with any sorting, filtering, and searching applied.

Export Selected to CSV
: Select to export the data in the currently selected row(s) in the table to a .CSV file. This includes all of the columns in the table.

Client Events Report Options

You can set data collection options for the Client Events report in the Wireless History Settings window accessed from Console OneView Collector options (Tools > Options > Console > OneView Collector > Wireless Collection > Edit Client History and Threat options). These options include setting the maximum number of client changes to store in the history and the maximum number of client events the report can request at one time.

You can also filter client events to include or exclude certain SSIDs using the Console OneView Collector options (Tools > Options > Console > OneView Collector > Wireless Collection > Edit Include/Exclude Filter List). This allows you to filter the history so only events for clients you are particularly interested in are displayed.

Client Location Information

Mouse over the Location column in the report tables to view a tooltip that displays whether the client's location is based on triangulated (Triangulation) or Cell of Origin data. The tooltip also displays whether the client's location is currently being tracked by the controller and if it is on the controller's on-demand list.

To track clients, enable the "Locate Active Sessions" setting in the wireless controller's Location Engine Settings. When this setting is enabled, the controller's location engine automatically tracks the location of all associated clients up to the platform's limit (e.g. 2500 stations for C5210). Even if a client has a session on a controller, if the limit has been reached, the location engine may not be tracking that particular client. Use this tooltip to determine if the client is currently being tracked.

Clients added to the controller's on-demand list are always tracked, regardless of whether tracking is enabled and any platform limits. Place clients that require guaranteed location history on the controller's on-demand list, configured in the controller's Location Engine Settings. Clients on this list also receive better location detection than other tracked clients, minimizing the number of Cell of Origin location results.

For more information on configuring controller Location Engine Settings and on-demand lists, refer to the *Extreme Networks Convergence Software User Guide*. Refer to the section on "Configuring the Location Engine" in the Working with ExtremeWireless Radar chapter.

Event Analyzer

The **Event Analyzer** tab provides information about wireless end-points connecting to your network.

Threats (Legacy)

NOTE: Threats reports provide data only if a compatible Extreme Wireless Controller (EWC) is present. The ExtremeCloud IQ Controller is not compatible with this feature.

These reports show devices detected by the Radar WIDS-WIPS system as sources of threats or interference on the wireless network.

A threat source is a device detected to be performing one or more types of attacks on the wireless network.

An interference source is a device generating a radio signal interfering with the operation of the wireless network. An example of an interference source is a microwave oven, which can interfere with 2.4GHz transmissions.

There are four sub-tabs displaying active and historic data:

- Threats — Lists only currently active threats.
- Threat Events — Lists a historic record of threat events including active threats.
- Interference — Lists only currently active sources of interference.
- Interference Events — Lists a historic record of interference events including active sources of interference.

NOTE: You can set the maximum number of threat events to store in history in Console (Tools > Options > Console > OneView Collector > Wireless Collection > Edit Client History and Threat options).

Following are definitions of the table columns and fields displayed in the sub-tabs.

Status
: The status of the threat or source of interference.

- Active — An active threat or source of interference on the network.
- Inactive — A threat or source of interference no longer active on the network.
- Aged — A threat or source of interference not reported by Radar as having gone away and has not been seen for more than an hour.

Type
: The type of threat or interference detected. Threats with no type display their category.

Categories
: Individual threat types are grouped into the following categories:

- Ad Hoc Device — A device in ad hoc mode can participate in direct device-to-device wireless networks. Devices in ad hoc mode are a security threat because they are prone to leaking information stored on file system shares and bridging to the authorized network.
- Cracking — This refers to attempts to crack a password or network passphrase (such as a WPA-PSK). The Chop-Chop attack on WPA-PSK and WEP is an example of an active password cracking attack.
- Denial of Service (DoS) attacks

- External Honeypot — An AP attempting to make itself a man-in-the-middle by advertising a popular SSID, such as an SSID advertised by a coffee shop or an airport.
- Internal Honeypot — An AP attempting to make itself a man-in-the-middle by advertising an SSID belonging to the authorized network.
- Performance — Performance issues pertain to overload conditions that cause a service impact. Performance issues aren't necessarily security issues, but many types of attacks do generate performance issues.
- Prohibited Device — A MAC address or BSSID is detected that matches an address entered manually into the Radar database.
- Spoofed AP — An AP not part of the authorized network is advertising a BSSID (MAC address) that belongs to an authorized AP on the authorized network.
- Client Spoof — A device using the MAC address of another typically authorized station.
- Surveillance — A device or application probing for information about the presence and services offered by a network.
- Chaff — An attack that overloads a WIDS-WIPS causing it to miss more serious attacks or to go out of service. FakeAP is an example of a chaff attack.
- Unauth Bridge — A device that forwards packets between networks without authorization to do so.
- Injection — The attacker inserts packets into the communication between two devices so the devices believe the packet is coming from an authorized device.

MAC Address
: The MAC address to which this threat event applies. In the case of Spoofed AP, Internal Honeypot, or External Honeypot, it is the advertised BSSID of the threat AP.

Start Time
: The date and time the threat or source of interference is identified.

Stop Time
: The date and time the threat or source of interference stopped.

Countermeasures Applied
: Countermeasures the AP is taking against the threat. These include:

- Prevent authorized stations from roaming to external honeypot APs.
- Prevent any station from using an internal honeypot AP.
- Prevent authorized stations from roaming to friendly APs.
- Prevent any station from using a spoofed AP.
- Drop frames in a controlled fashion during a flood attack.
- Remove network access from clients in ad hoc mode.

- Remove network access from clients originating DoS attacks.
- None

AP Name
Name of the AP reporting the threat or source of interference. Select the link to open the AP Details window that provides controller, bandwidth, and client information.

From the AP History sub-tab, select the **Gear** menu in the upper right corner of the window to access a menu of additional AP reports.

RSS
Receive signal strength (in dBm) of the threat or source of interference.

Additional Details
Additional information including:

- frequency=<channel> or NA
- SSID=<SSID name>
- encryption=<WEP/WPA1/WPA2/WPA12>

Search
Use the **Search** field at the top right of the window to search by threat type, threat category, MAC address, or AP name.

Refresh Interval
Use the **Refresh** drop-down list at the top right of the window to specify an interval (in seconds) at which the threat or interference data is automatically refreshed. To stop auto refresh, select the **Refresh Off** option.

Search Maps
To locate an AP on a map, right-click on a threat and select **Search Maps**. If the AP is added to a map, the map opens with the AP centered on the map.

Reports

The **Reports** tab allows you to view information about the APs, controllers, and wireless traffic on your network. Available reports are accessible via the **Reports** drop-down list at the top of the tab.

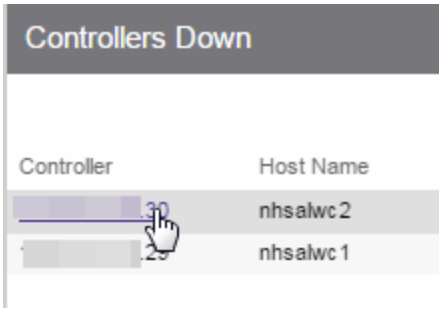
Select the **Export to CSV** button ( ) to export the information contained in the report to your default CSV application, where it can then be manipulated or saved.

Report Features

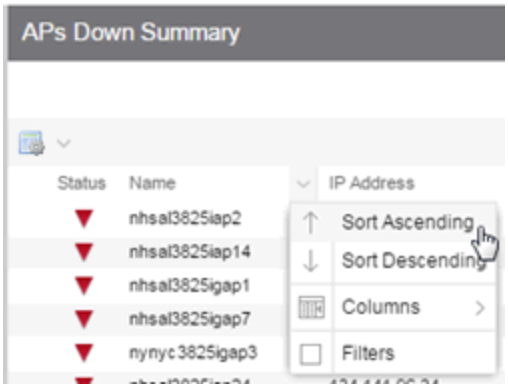
ExtremeCloud IQ Site Engine reports include the following features (depending on the report selected):

- **Drill-down for Details** — Link to summary reports containing more detailed information. For example, in the Controller Summary report, selecting a controller shows a detailed report for

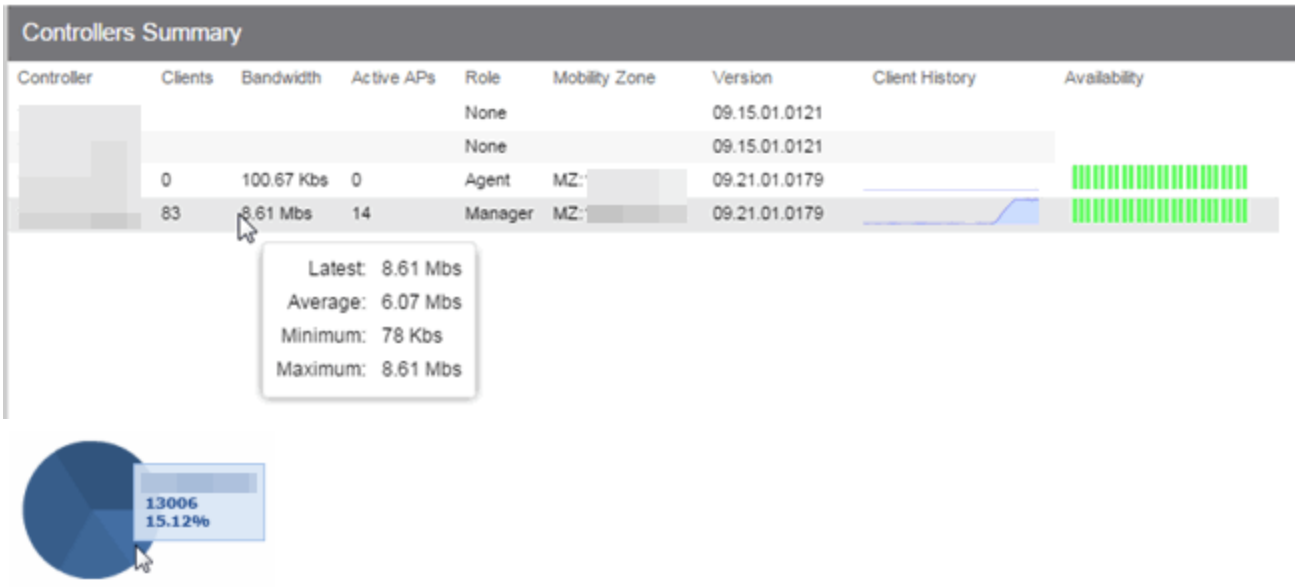
that controller over time.



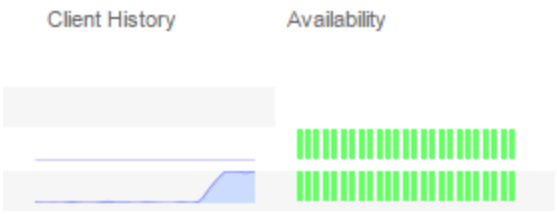
- **Interactive Tables** — Manipulate table data in several ways to customize the view for your own needs:
  - Select the column headings to **perform an ascending or descending sort** on the column data.
  - **Hide or display different columns** by selecting a column heading drop-down arrow and selecting the column options from the menu.
  - **Filter, sort, and search** the data in each column in the table.



- **Interactive Charts** — Use data-point rollovers for quick information on chart data. For example, in the Controller Summary report, rolling over the value reported for Bandwidth provides additional bandwidth statistics over time.



- **Sparkline Charts** — View network trends in dense, succinct charts that present report data in an easy to read, condensed format. This provides you with a quick way to catch possible problem areas that you can investigate further. Rollover charts for additional information.



For information on related ExtremeCloud IQ Site Engine topics:

- Administration
- Network
- Alarms and Events
- Reports
- Search

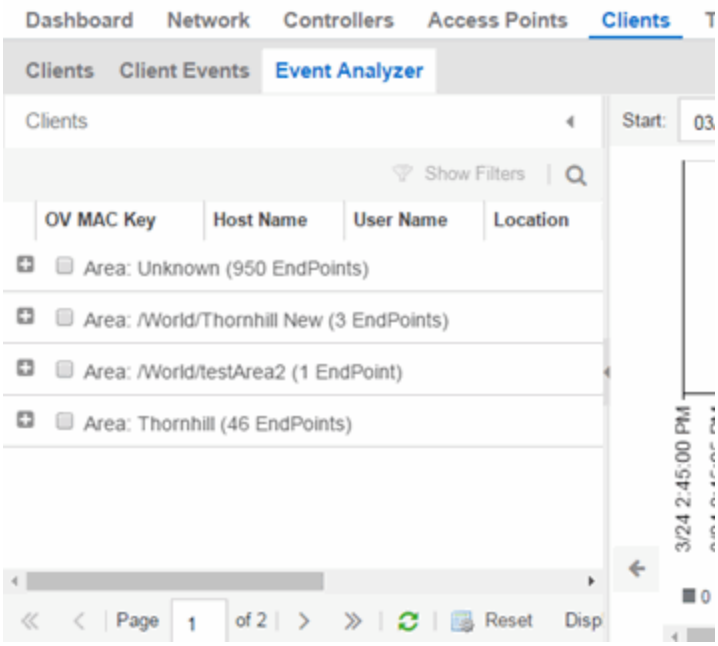
Event Analyzer

The **Event Analyzer** tab provides information about events caused by wireless end-points connecting to your network.

You can access the tab in a number of ways and the information presented changes depending on the method you use:

- Navigating via **Wireless** > **Clients** > **Event Analyzer** shows all end-points.
- Selecting a Location on the **Wireless** > **Clients** tab opens the Event Analyzer for the end-points that occurred for all APs in that Location.
- Selecting a MAC address on the **Wireless** > **Clients** tab opens the Event Analyzer for only that end-point.

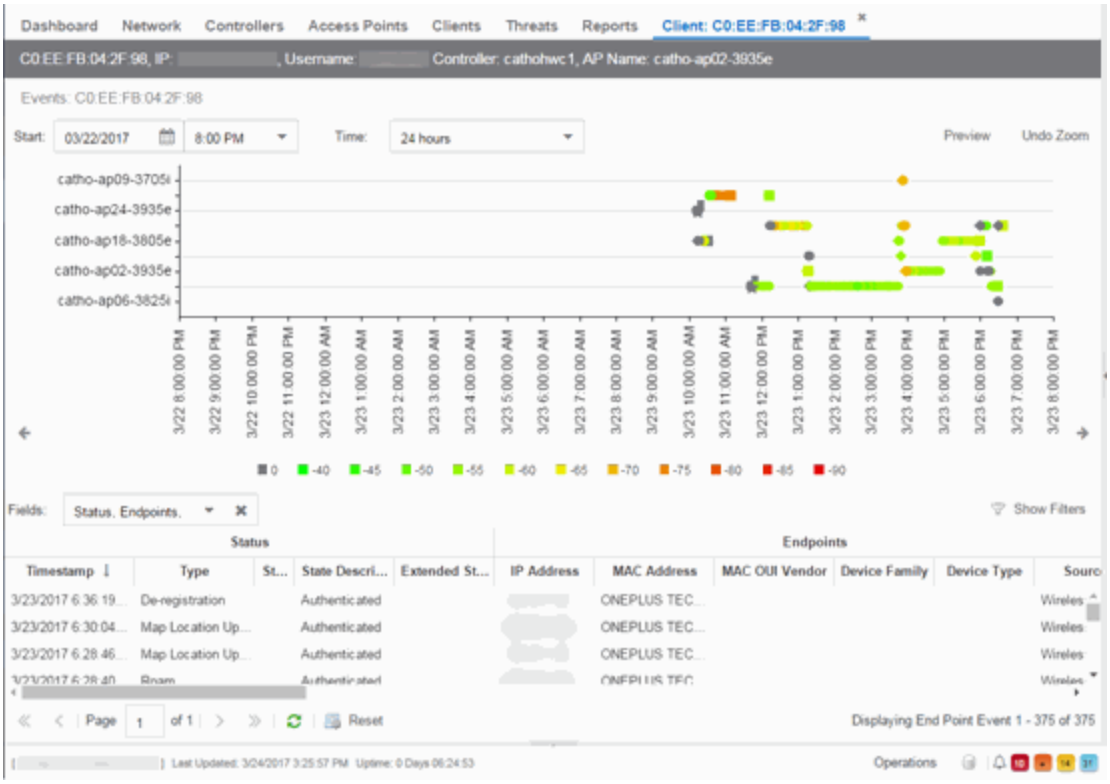
When accessing the tab using the top two methods, a Clients section is available in the left-panel. This section provides you with the ability to display end-point events for specific AP locations.



Once you select the appropriate end-points or areas, this section can be collapsed by selecting the left arrow.

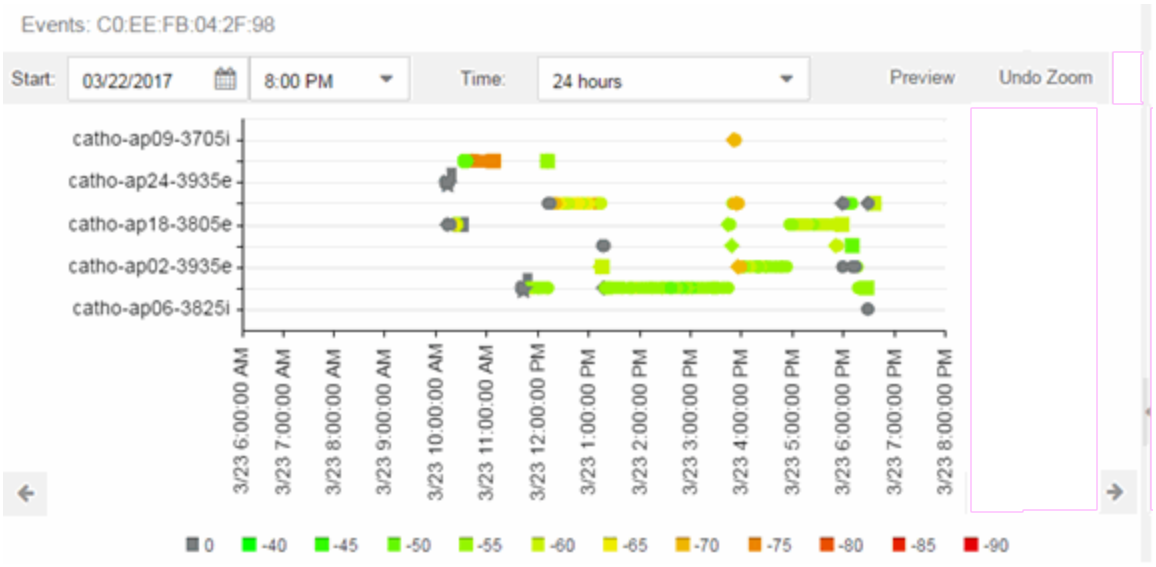
The top of the tab contains a graph displaying the RSS (Received Signal Strength) for the end-point events.

The bottom contains a table showing information about each event.



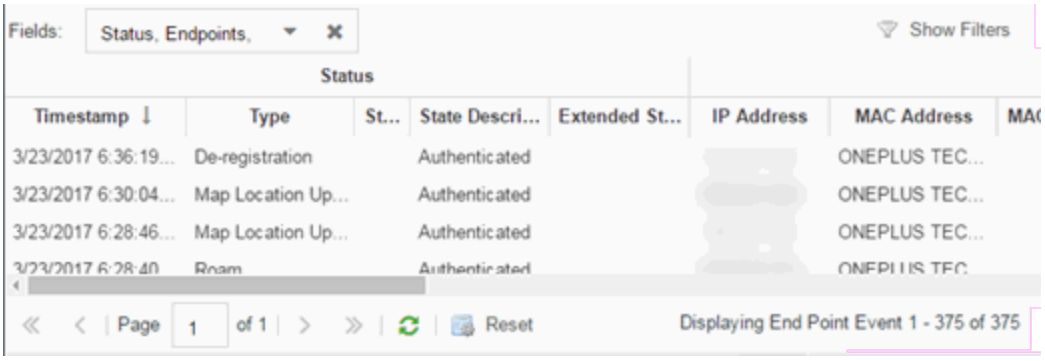
RSS Graph

The RSS graph at the top of the tab shows the signal strength (in dBm) between the end-point and each of the APs to which it connected. The shape of the end-point event indicators in the graph indicate the type of event.



Events Table

The Events table at the bottom of the tab contains details about the end-point events for your network, or for the wireless location or MAC address you selected.



Use the **Fields** drop-down list to select groups of columns to display in the table:

- Select **Status** to display the following columns in the table:
  - Date/Time
  - Type
  - State
  - State Description
  - Extended State
- Select **Endpoints** to display the following columns in the table:
  - IP Address
  - OV MAC Key
  - MAC Address
  - MAC OUI Vendor
  - Host Name
  - Device Family
  - Device Type
  - Source
- Select **User Access** to display the following columns in the table:
  - User Name
  - Policy
  - Authorization

    - Profile
    - Reason
    - Auth Type
    - Registration Type
    - RADIUS Server IP
- Select **Location** to display the following columns in the table:
    - Switch Port
    - Switch Port Index
    - Switch Location
    - AP Name
    - AP Serial #
    - BSSID
    - SSID
    - Protocol
    - Location Type
    - Location
    - Location Details
    - Area Type
    - Area
    - Access Control Engine/Source IP
- Select **Metrics** to display the following columns in the table:
    - RSS
    - SNR
- Select **Threat/Risk** to display the following columns in the table:
    - Categories
    - Start Time
- Select **Network Service** to display the following columns in the table:
    - Switch IP
    - Controller IP

For information on related ExtremeCloud IQ Site Engine topics:

- Wireless

ExtremeCompliance Overview (Legacy)

ExtremeCompliance, contained in the ExtremeCloud IQ Site Engine > **Compliance** tab, provides oversight into the configuration of your devices and wireless threat alerts to ensure you are compliant with industry best practices.

IMPORTANT: The **Compliance** tab is available and supported by Extreme on an ExtremeCloud IQ Site Engine engine running the Linux operating system supplied by Extreme. Other Linux operating systems can support ExtremeCompliance functionality, but python version 2.7 or higher must be installed. Additionally ExtremeCompliance functionality requires the git, python2, python mysql module, python setuptools module, and python "pygtail" module packages be installed and related dependencies managed by the customer for their server's unique operating system and version.

Run an ExtremeCompliance audit against devices on the **Compliance** tab or against device archives on the **Archives** tab.

NOTE: **Compliance** tab functionality requires you to acquire an additional license.

ExtremeCloud IQ Site Engine provides a set of audit tests that enable you to test the configuration of your devices. Groups of audit tests comprise a regime, which tests for a specific regulation or standard. ExtremeCloud IQ Site Engine uses the results to determine a score that indicates compliance with a regulation or standard.

The regimes included in the **Compliance** tab are automatically included in up to ExtremeCloud IQ Site Engine version 24.2 installation on an ExtremeCloud IQ Site Engine engine, but you must import them on a non-ExtremeCloud IQ Site Engine engine by accessing the engine console, navigating to the `<install directory>/GovernanceEngine` directory and entering `./governance-engine.py --db-import-all-tests --governance-type PCI` to import the PCI regime and `./governance-engine.py --db-import-all-tests --governance-type HIPAA` to import the HIPAA regime.

Configure a regime by disabling or editing specific audit tests within the regime. When the regime meets your needs, use it to run an ExtremeCompliance audit against a device or set of devices. You cannot run individual audit tests against a device.

The **Compliance** tab contains the following sub-tabs:

- Dashboard
- Audit Tests

Dashboard

The **Dashboard** tab displays an overview of the audit test results for each regime. Additionally, the tab provides information about how the regime test results changed over time, the performance of each of the devices included in the audit test, and a list of the tests performed as part of the regime.

Audit Tests

The **Audit Tests** tab contains a variety of audit tests organized into the regime or standard of which it is a part. You can also create your own audit tests for the devices on your network via the **Audit Tests** tab.

Audit tests can be run ad-hoc or on a scheduled basis. Use the results to ensure your devices are configured to industry standards and are safe from vulnerabilities.

ExtremeCompliance Integration with Workflows

You can integrate ExtremeCompliance with workflows functionality to automatically remediate devices that fail an audit test. By creating an alarm that is generated when a device fails an audit test, you can configure ExtremeCloud IQ Site Engine to automatically run a workflow when the alarm occurs.

When configured, any time ExtremeCompliance performs an audit test for which a device fails, an alarm occurs that initiates a workflow designed to remediate the reason for the failure. To enable this functionality, configure ExtremeCompliance to send syslog messages by opening the `Installation Directory/GovernanceEngine/logger.conf` file and ensure `enableSyslog=true`.

ExtremeCompliance Overview (Legacy)

ExtremeCompliance, contained in the ExtremeCloud IQ Site Engine > **Compliance** tab, provides oversight into the configuration of your devices and wireless threat alerts to ensure you are compliant with industry best practices.

IMPORTANT: The **Compliance** tab is available and supported by Extreme on an ExtremeCloud IQ Site Engine engine running the Linux operating system supplied by Extreme. Other Linux operating systems can support ExtremeCompliance functionality, but python version 2.7 or higher must be installed. Additionally ExtremeCompliance functionality requires the git, python2, python mysql module, python setuptools module, and python "pygtail" module packages be installed and related dependencies managed by the customer for their server's unique operating system and version.

Run an ExtremeCompliance audit against devices on the **Compliance** tab or against device archives on the **Archives** tab.

NOTE: **Compliance** tab functionality requires you to acquire an additional license.

ExtremeCloud IQ Site Engine provides a set of audit tests that enable you to test the configuration of your devices. Groups of audit tests comprise a regime, which tests for a specific regulation or standard. ExtremeCloud IQ Site Engine uses the results to determine a score that indicates compliance with a regulation or standard.

The regimes included in the **Compliance** tab are automatically included in up to ExtremeCloud IQ Site Engine version 24.2 installation on an ExtremeCloud IQ Site Engine engine, but you must import them on a non-ExtremeCloud IQ Site Engine engine by accessing the engine console, navigating to the `<install directory>/GovernanceEngine` directory and entering `./governance-engine.py --db-import-all-tests --governance-type PCI` to import the PCI regime and `./governance-engine.py --db-import-all-tests --governance-type HIPAA` to import the HIPAA regime.

Configure a regime by disabling or editing specific audit tests within the regime. When the regime meets your needs, use it to run an ExtremeCompliance audit against a device or set of devices. You cannot run individual audit tests against a device.

The **Compliance** tab contains the following sub-tabs:

- Dashboard
- Audit Tests

Dashboard

The **Dashboard** tab displays an overview of the audit test results for each regime. Additionally, the tab provides information about how the regime test results changed over time, the performance of each of the devices included in the audit test, and a list of the tests performed as part of the regime.

Audit Tests

The **Audit Tests** tab contains a variety of audit tests organized into the regime or standard of which it is a part. You can also create your own audit tests for the devices on your network via the **Audit Tests** tab.

Audit tests can be run ad-hoc or on a scheduled basis. Use the results to ensure your devices are configured to industry standards and are safe from vulnerabilities.

ExtremeCompliance Integration with Workflows

You can integrate ExtremeCompliance with workflows functionality to automatically remediate devices that fail an audit test. By creating an alarm that is generated when a device fails an audit test, you can configure ExtremeCloud IQ Site Engine to automatically run a workflow when the alarm occurs.

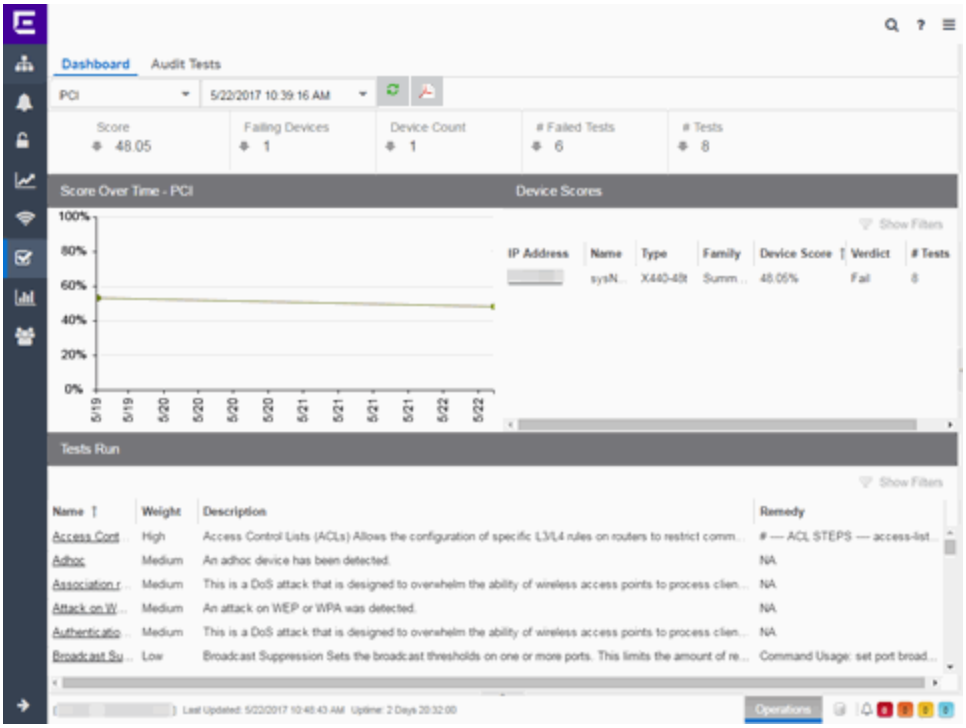
When configured, any time ExtremeCompliance performs an audit test for which a device fails, an alarm occurs that initiates a workflow designed to remediate the reason for the failure. To enable this

functionality, configure ExtremeCompliance to send syslog messages by opening the `Installation Directory/GovernanceEngine/logger.conf` file and ensure `enableSyslog=true`.

Compliance Dashboard (Legacy)

The **Compliance** > **Dashboard** tab provides an overview of your ExtremeCompliance audit test results performed over time on the devices in your network.

Use the drop-down menus at the top of the tab to select the regime and the date and time of the ExtremeCompliance audit to view the results in the tab. Select the **Export to PDF** icon ( ) to produce a PDF report that provides a summary of the regime audit test and a breakdown of the results for each device included in the test.



Test Results

The top of the **Dashboard** tab displays the audit test results for the ExtremeCompliance audit you select using the regime and date in the drop-down list.

Score

The number in this field is an average of the scores on each device included in the audit. Each device earns a score by comparing the percentage of audit tests that ran successfully on the device to the total number of audit tests. Selecting the score opens the **Run Results** tab,

which provides a list of all of the audit tests run on all of the devices included in the audit, including the results.

Failing Devices
The number of devices that failed the ExtremeCompliance audit. Selecting the number of failing devices opens the **Device Scores** tab, which provides a list of the devices that failed the audit test.

Device Count
The total number of devices included in the ExtremeCompliance audit. Selecting the device count opens the **Device Scores** tab, which provides a list of all of the devices included in the audit test.

 # Failed Tests
The number of tests that failed when run against devices included in the ExtremeCompliance audit. Selecting the failed test number opens the **Run Results** tab, which provides a list of the audit tests that failed when run on a device included in the audit.

 # Tests
The total number of tests run against devices included in the ExtremeCompliance audit. Selecting the number of tests opens the **Run Results** tab, which provides a list of all audit tests run on devices included in the audit.

Score Over Time

The Score Over Time graph shows the results of all of the audit tests performed on your devices for the regime selected in the drop-down list at the top of the window. This allows you to determine any trends and map your progress towards compliance with a particular regime.

Device Scores

The Device Scores section of the tab displays a table of the devices included in the audit test, details about those devices, and the results of the ExtremeCompliance audit on each device.

IP Address
The IP address of the device tested.

Selecting an address in the IP Address column opens that device in the **Device Details** tab, which provides ExtremeCompliance audit result information for that device.

Name
The name of the device, configured in the **System Name** field in the **Configure Device** window.

Type
The specific type (model) of the device.

Family
The group of devices to which the device belongs, known as the device family in ExtremeCloud IQ Site Engine.

Device Score
The percentage of audit tests within the regime with which the device passes compliance. For example, if a device complies with 75 out of 100 audit tests in a regime, the **Device Score** is **75%**.

Verdict
The result of the ExtremeCompliance audit (either **Pass** or **Fail**), based on the Device Score. A device with a score of less than 50% is labeled as **Fail** in the Verdict column, while a score of 50% or above is considered a **Pass**.

 # Tests
The number of tests included in the ExtremeCompliance audit run against the device.

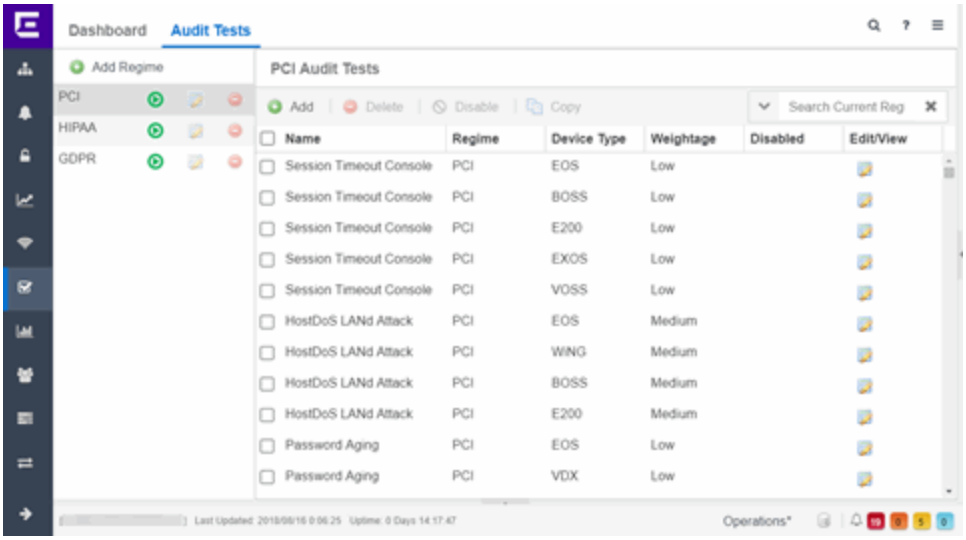
Tests Run

The Tests Run table displays a list of all of the tests included in the regime selected at the top of the window. The section also contains details about each of the audit tests and the action you can take to correct the device in the event that your device fails a test.

Selecting the test name in the Name column opens the Test Details tab, which provides information about the results of the test on all devices both over time and during a particular ExtremeCompliance audit.

Audit Tests (Legacy)

The Audit Tests tab displays your ExtremeCompliance regimes in the left panel, and the audit tests associated with the selected regime that check for vulnerabilities in your devices in the right panel. The tab also allows you to create your own regimes and audit tests you can add to regimes.



The Audit Test list contains a list of all of the audit tests available in ExtremeCloud IQ Site Engine, contained within the regulatory and standards regime of which it is a part. Each individual audit test displays the device types on which the test can be run in the **Device Type** column.

Select a regime, audit test, or device type in the Audit Test list to view the details of any audit tests contained in that folder in the Selected Audit Tests table to the right of the tree. Select **Search Current Reg** and begin typing to search within the regime you selected for a specific audit test.

Disable an audit test by selecting it in the right panel and selecting **Disable**. Delete an audit test by selecting it in the right panel and selecting **Delete**.

NOTE: Only user-created audit tests or audit tests in user-created regimes can be deleted. Additionally, only user-created regimes can be deleted.

Name

This shows the name of the audit test, a test of the configuration of a device to ensure compliance with the best practices of that industry and is nested within the regime to which the test applies. Expand the audit test folder to see the device types to which that test applies.

Regime

This indicates standard or regulation to which you are maintaining compliance. Each regime contains a set of audit tests, specific to a device type. Expand the regime folder to view the tests included as part of the regime.

Selecting a regime opens a list of all of the audit tests in that regime in the selected Audit Tests table to the right of the list. Use the Selected Audit Tests table to select or deselect any of the tests in the regime and then run an audit test using all of the selected tests in the regime on the devices you select to which the tests apply.

Device Type

The device type displays the type of devices on which you can run the expanded audit test and is the lowest level in the Audit Test list, nested within an audit test.

Selecting device type displays that audit test in the Details table to the right of the Audit Test list. Use the Details table to select or deselect the test and then run an audit test on the devices you select to which the test applies.

Additionally, double-clicking the device type from the left-panel opens the Edit Audit Test window from which you can edit the audit test.

Weightage

The value in the **Weightage** column of the Selected Audit Tests table indicates the priority of the audit test:

- **High**
- **Medium**
- **Low**

Disabled

A check mark in this column indicates the test is disabled for the regime. When a test is disabled, it is not run when performing an ExtremeCompliance audit against a device or a group of devices. To disable or enable an audit test, select the test in the left-panel, right-click the audit test, and select **Disable Audit Test** or **Enable Audit Test**, respectively.

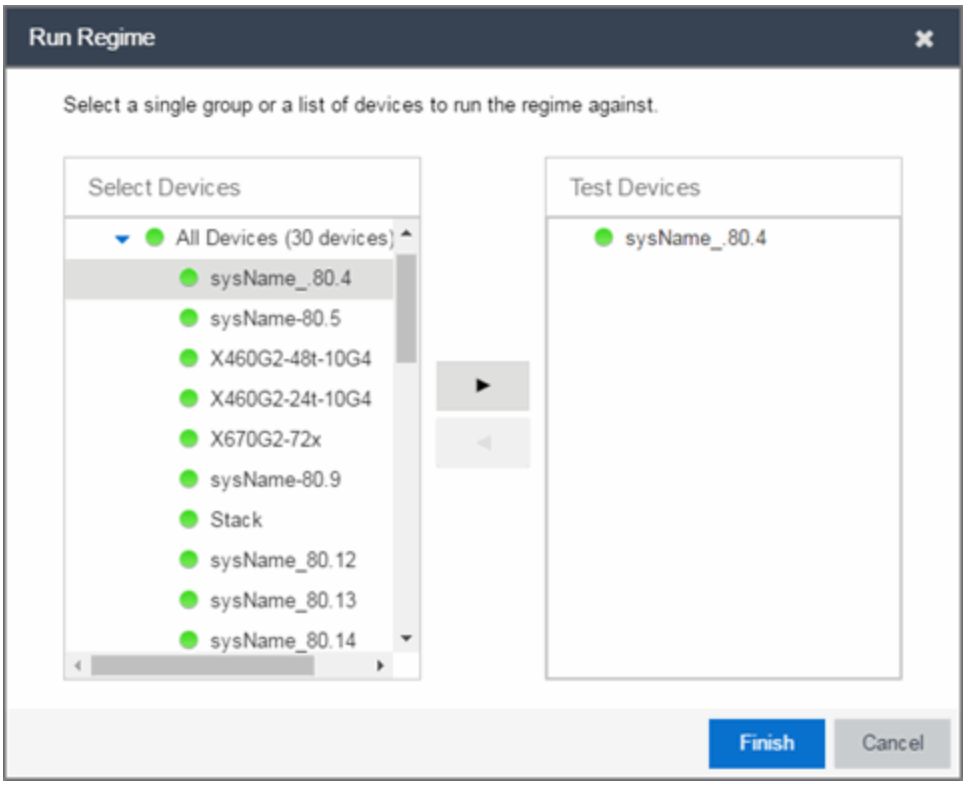
Edit/View

Select the button to open the **Edit Audit Test** window.

Select a regime from the left-panel and select the **Run** icon to open the **Run Regime** window, where you select the device against which to run the audit.

Run Regime (Legacy)

This window allows you to select the device or devices against which to run the selected audit test. The **Run Regime** window contains all of the devices added to ExtremeCloud IQ Site Engine.



Select Devices

Expand the folders and select a single device, multiple devices, or a single device group. Select the right arrow button **›** to move the devices to the Test Devices list.

Test Devices

Lists the device(s) or device group the on which the audit test is performed. To remove a member from the list, select the device or device group and select the left arrow button **‹**.

Right Arrow Button

Select **›** to add the device(s) or device group to the Test Devices list.

Left Arrow Button

Select **‹** to remove the device(s) or device group from the Test Devices list.

Finish Button

Select the **Finish Test** button to run the selected audit test(s) on the devices selected in the Test Devices list. The progress of the ExtremeCompliance audit is displayed in the Operations table.

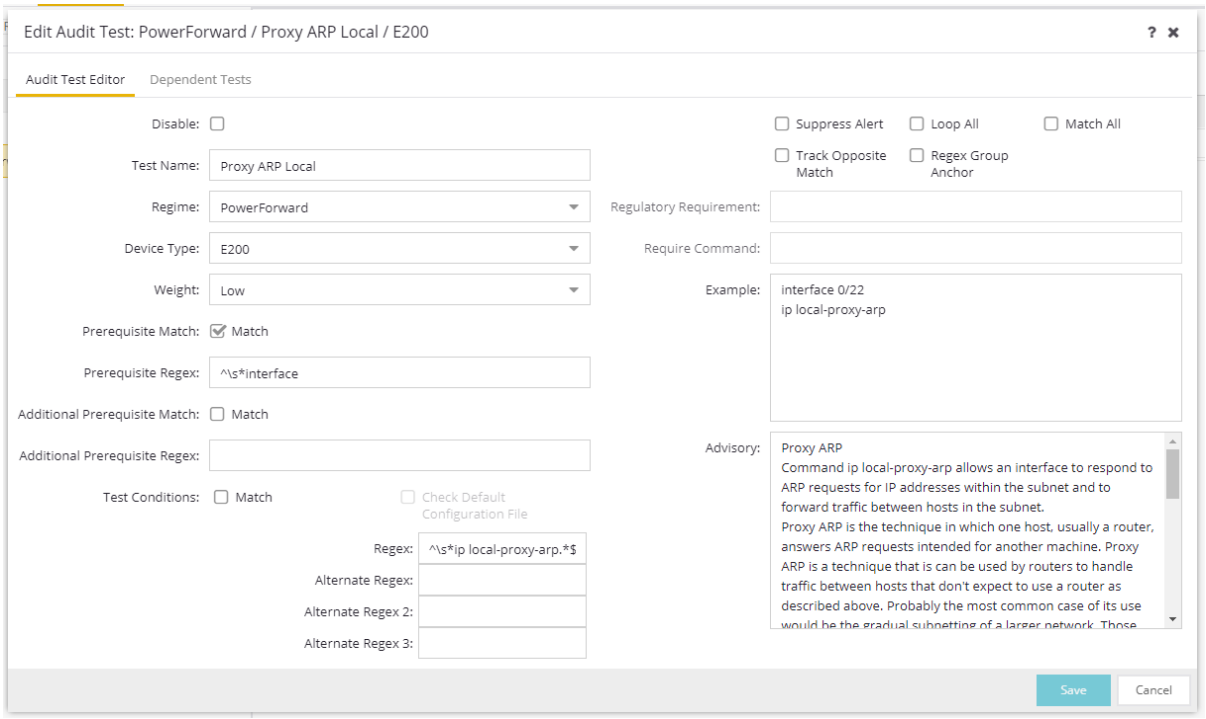
Create/Edit Audit Test (Legacy)

Use the **Audit Test Editor** tab of the **Create/Edit Audit Tests** window to create a new audit test or edit information for an existing audit test. The **Audit Test Editor** tab in the Create/Edit Audit Test window allows you to indicate the name of the audit test, the regime to which it belongs, the device type to which the test applies, and the weight of the test.

Access the Create Audit Test window on the **Compliance** > **Audit Tests** tab by selecting a regime in the left-panel, selecting the **Menu** icon (☰), and selecting **Add** > **Audit Test**.

Access the Edit Audit Test window by selecting an audit test in the left-panel, selecting the **Menu** icon (☰), and selecting **Edit** > **Audit Test**.

NOTE: Only audit tests in user-created regimes can be edited.



Disable

Select the checkbox prevent the audit test from running as part of the regime when an ExtremeCompliance audit is performed on your devices.

Test Name

The name of the audit test. As regimes contain a large number of audit tests, some of which testing similar configurations, ensure the **Test Name** is very specific.

Regime
The set of standards or regulations to which the test applies. ExtremeCloud IQ Site Engine comes with three regimes, PCI, HIPAA, and GDPR. You can create a new regime or edit an existing regime on the **Audit Tests** tab by selecting the **Menu** icon and selecting **Add** or **Edit** > **Regime**.

Device Type
The type of device being tested. In version 26.11.10, ExtremeCloud IQ Site Engine supports multiple Device Types, including **E200**, **Switch Engine**, **EOS**, **BOSS**, Fabric Engine, and **WController**.

Weight
The priority of the audit test. Valid selections are **Low**, **Medium**, or **High**.

Prerequisite Match
Select this checkbox to indicate the regular expression or function audit test must match the configuration file for the audit test to be valid.

Prerequisite Regex
The regular expression that must match the device configuration file for ExtremeCloud IQ Site Engine to consider the audit test valid.

For example, if an audit test is checking if strong ciphers are selected for SSH configuration, use this field to verify that SSH is enabled.

Match
Select this checkbox to indicate the regular expression or function audit test are intended to match the configuration file to be compliant and pass the test. If the checkbox is not selected, any result that does not match the test case is considered compliant and passes the test.

Regex
The regular expression against which ExtremeCloud IQ Site Engine is comparing a device's configuration file.

Alternate Regex
A second regular expression against which ExtremeCloud IQ Site Engine is comparing a device's configuration file, in case the **Regex** test fails.

NOTE: Using multiple Regex fields allows you to run one audit test against multiple configuration file formats (e.g. ExtremeXOS/Switch Engine configuration files use both XML and plain text).

Alternate Regex 2
A third regular expression against which ExtremeCloud IQ Site Engine is comparing a device's configuration file, in case the other **Regex** tests fail.

NOTE: Using multiple Regex fields allows you to run one audit test against multiple configuration file formats (e.g. ExtremeXOS/Switch Engine configuration files use both XML and plain text).

Alternate Regex 3

A fourth regular expression against which ExtremeCloud IQ Site Engine is comparing a device's configuration file, in case the other **Regex** tests fail.

NOTE: Using multiple Regex fields allows you to run one audit test against multiple configuration file formats (e.g. ExtremeXOS/Switch Engine configuration files use both XML and plain text).

Supress Alert

Select this checkbox to indicate the result of the audit test is not factored into the score assigned to the devices included in an ExtremeCompliance audit.

Loop All

Select this checkbox to indicate the audit test is performed repeatedly against the entire device configuration and the match criteria is applied to the end result of the ExtremeCompliance audit. For example, if SSH must be enabled in multiple places on a device, selecting this checkbox requires SSH to be enabled in all places to pass.

Match All

Select this checkbox to indicate all instances of the regular expression you are comparing to the device configuration must match for the audit test to pass.

Track Opposite Match

Select this checkbox if you want the results of the audit test to indicate whether the opposite of the regular expression you are comparing to the device configuration is observed during the ExtremeCompliance audit.

Regex Group Anchor

Select this checkbox to indicate this audit test is the starting point for the regime. Use this checkbox for test chains when collecting data via regex capture groups.

Regulatory Requirement

The requirement from the standard or regulation that serves as the justification for the audit test.

Require Command

The path to a command on the ExtremeCloud IQ Site Engine server, if required for the audit test. For example, enter the path to the `cracklib-check` command for an audit test verifying the strength of cleartext credentials.

Example

A descriptive example of the configuration for which the audit test is checking.

Advisory

The reason the audit test is important to the regulation or standard and the procedure to improve the audit test results.

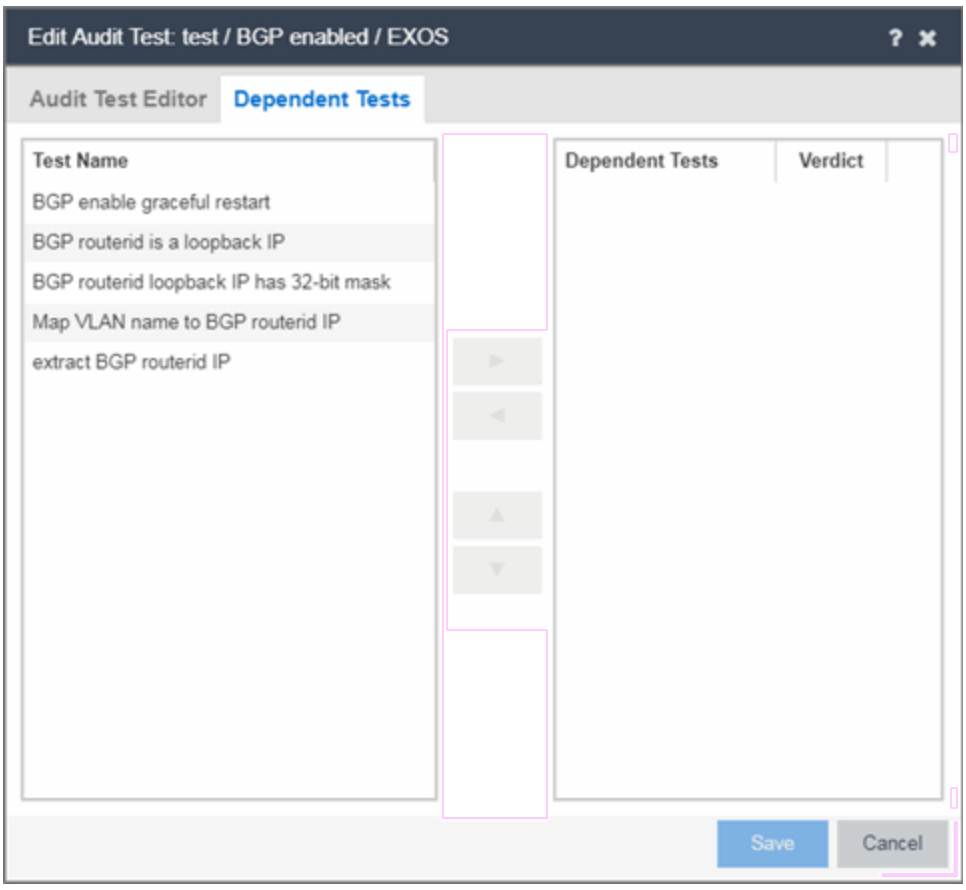
Dependent Tests

The **Dependent Tests** tab of the **Create/Edit Audit Test** window allows you to select audit tests that must run before the selected audit test runs. To be available as a dependent test, an audit test must be in the same regime and match the device type of the selected audit test.

Access the Create Audit Test window on the **Compliance** > **Audit Tests** tab by selecting a regime in the left-panel, selecting the **Menu** icon (☰), and selecting **Add** > **Audit Test**.

Access the Edit Audit Test window by selecting an audit test in the left-panel, selecting the **Menu** icon (☰), and selecting **Edit** > **Audit Test**.

NOTE: Only audit tests in user-created regimes can be edited.



Test Name

The **Test Name** column displays the audit tests in the same regime that also match the device type of the selected audit test.

Dependent Tests
The audit tests that must run before the selected audit test runs.

Verdict
Select this checkbox if the dependent audit test must PASS for the selected audit test to run. If the checkbox is not selected, the dependent audit test must FAIL for the selected audit test to run.

Right Arrow (▸)

Select an audit test from the **Test Name** column and select ▸ to add it to the **Dependent Tests** list.

Left Arrow (◂)

Select an audit test from the **Dependent Tests** column and select ◂ to remove it from the **Dependent Tests** list.

Up Arrow (▲)

If you added multiple audit tests to the **Dependent Tests** column, select an audit test and select ▲ to move the audit test up in the order in which the audit tests are run.

Down Arrow (▼)

If you added multiple audit tests to the **Dependent Tests** column, select an audit test and select ▼ to move the audit test down in the order in which the audit tests are run.

- Audit Test Editor
- Audit Tests

Add a New Regime in ExtremeCloud IQ Site Engine (Legacy)

The **Compliance** tab provides you with regimes that include predefined audit tests. You can also create your own regimes, composed of audit tests you can copy from existing regimes, or configure yourself.

To create a new regime:

1. Open the **Compliance** > **Audit Tests** tab.
2. Select the **Menu** icon (☰) and select **Add** > **Regime**.

   The Create Regime window displays.

3. Enter a **Regime Name**, describing the overarching standard or regulation against which you are testing compliance.
4. Enter a **Description** for the regime, if necessary.
5. Select **Test Wireless Events** to include wireless events in the ExtremeCompliance audit.

NOTE: Because of the number of wireless events potentially stored by ExtremeCloud IQ Site Engine, wireless events are not included in an ExtremeCompliance audit the first time it is run. When the audit is run the first time, older wireless events are moved, so older events are not included in the results.

---

6. Select **Save**.
7. Copy existing audit tests to the new regime, if necessary.
   a. Right-click the audit test in left-panel and selecting **Copy Audit Test**.

      The **Copy Audit Test** window displays.
   b. Enter a new name for the audit test, if necessary.
   c. Select the new regime in the **Regime** drop-down list.
   d. Select the device type to which the audit test applies in the **Device Type** drop-down list.
   e. Select **Copy**.
8. Create your own audit tests.
   a. Select the **Menu** icon (☰) and select **Add** > **Audit Test**.
   b. Complete the fields in the **Audit Test Editor** tab to test for a device configuration.
   c. Complete the fields in the **Dependent Tests** tab, if necessary.
   d. Select **Save**.

Third Party Device Support in ExtremeCompliance (Legacy)

Introduction

ExtremeCompliance now provides the framework required to enable writing the audit tests for the non-Extreme devices that can be discovered in ExtremeCloud IQ Site Engine and Inventory Manager. With this capability you can define your own audit tests for non-Extreme devices.

Prerequisite

Third party devices are identified by their SysOIDs. The user must know the System Object ID (SysOID) of the third-party devices in the network. "1.3.6.1.4.1.9.1.1745" is a sample SysOID display.

Steps

1. Login to ExtremeCloud IQ Site Engine server as a user with write permissions on the installation.
2. Edit the following file: `<Installation_ Directory>/GovernanceEngine/thirdPartyDevices.properties`
3. Follow the instructions given in the file to add SysOIDs. Multiple SysOIDs can be mapped to one user-defined Device Type (for example, 1.3.6.1.4.1.9.1.1745=XYZ, where 1.3.6.1.4.1.9.1.1745 is the SysOID and XYZ is the device type).
4. After defining all the mappings, run the script- "operationsOnThirdparty-properties.sh" present in the same directory. This imports the user defined SysOIDs and Device types into ExtremeCompliance. T\Use the same script to perform operations like read, delete and reimport. Instructions and examples of various available arguments display after running the script.
5. Log into ExtremeCloud IQ Site Engine, create new audit tests or copy and edit existing audit tests into a newly created custom regime or an existing regime. When creating/editing audit tests, you are able to select the device types defined above in the Device Type drop-down list, thereby defining audit tests for the third-party device. Look at the next section for details on how to create new audit tests.
6. Run the required regime in the location in which you added the audit tests.

   All the audit tests applicable to the 3rd party device run and score displays in the dashboard.

Adding a new audit test and verifying that the ExtremeCompliance audit was run successfully

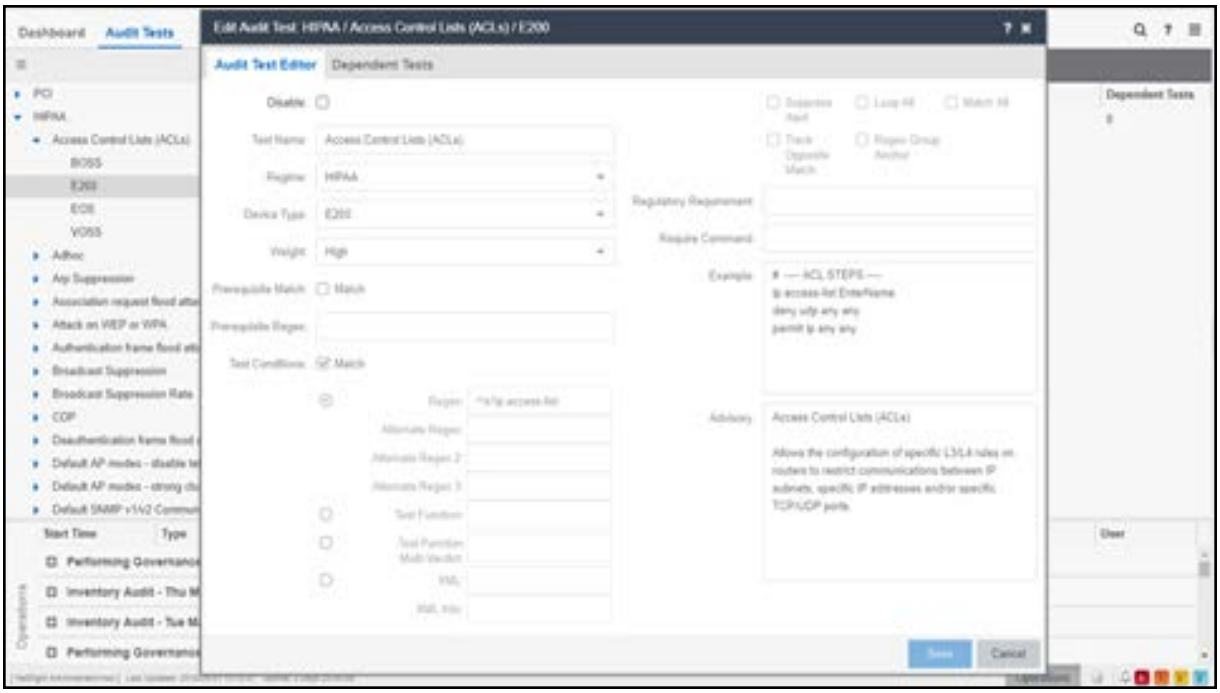
1. Add a new device and verify it is discovered (skip this step if you already have a 3rd party device discovered in ExtremeCloud IQ Site Engine).
   a. Connect to the ExtremeCloud IQ Site Engine server: https://<Server_IP>:8443.
   b. Enter your credentials to logi n to the server.
   c. Access the **Network** > **Devices** tab.
   d. Select **Site** in the left-panel drop-down list.
   e. Select the **World** site.

f. In the right-panel, right-click and select **Device** > **Add Device**.

g. Enter the IP Address of the device, select a profile based on the SNMP profile configured on the device, enter a device nickname, and select **OK**

h. Select on the **Operations** tab at the bottom of the window, which indicates the status of the discovery.

2. Copy an existing audit test or adding a new audit test in a custom Regime.



a. Select the **Compliance** > **Audit Tests** tab.

b. Right-click the regime and select **Add Regime...**.

The **Create Regime** window displays.

c. Enter a **Regime Name** (e.g. Third party), a description of the new regime, and select whether to **Test Wireless Events**.

d. Select **Save**.

e. Select one the existing regimes (e.g. PCI, HIPPA, or GDPR).

f. Select **Access Control Lists (ACLs)**.

g. Right-click a device type (e.g. BOSS, E200, EOS, and Fabric Engine) and select **Copy Audit Test**.

The **Copy Audit Test** window displays.

h. Select the **Regime** from the drop-down list and select **Copy**.

i. Open the regime to which you copied the test to verify the audit test displays.

j. Expand the new regime.

k. Select the Arrow icon to expand the Audit test (e.g., **Access Control Lists (ACLs)**).

l. Right-click the device type and select **Edit Audit Test**.

The **Edit Audit Test** window displays.

m. Change the **Device Type** to the device type the new regime is testing (e.g., **Aruba**, **Cisco**).

n. Change the **Regex** depending on the device type the new regime is testing (Aruba or Cisco).

3. Run the Regime

a. Right-click your regime and select **Run Regime**.

The **Run Regime** window displays.

b. Select the devices on which you are running the regime.

A window displays to indicate the regime is running.

c. Open the **Operations** panel.

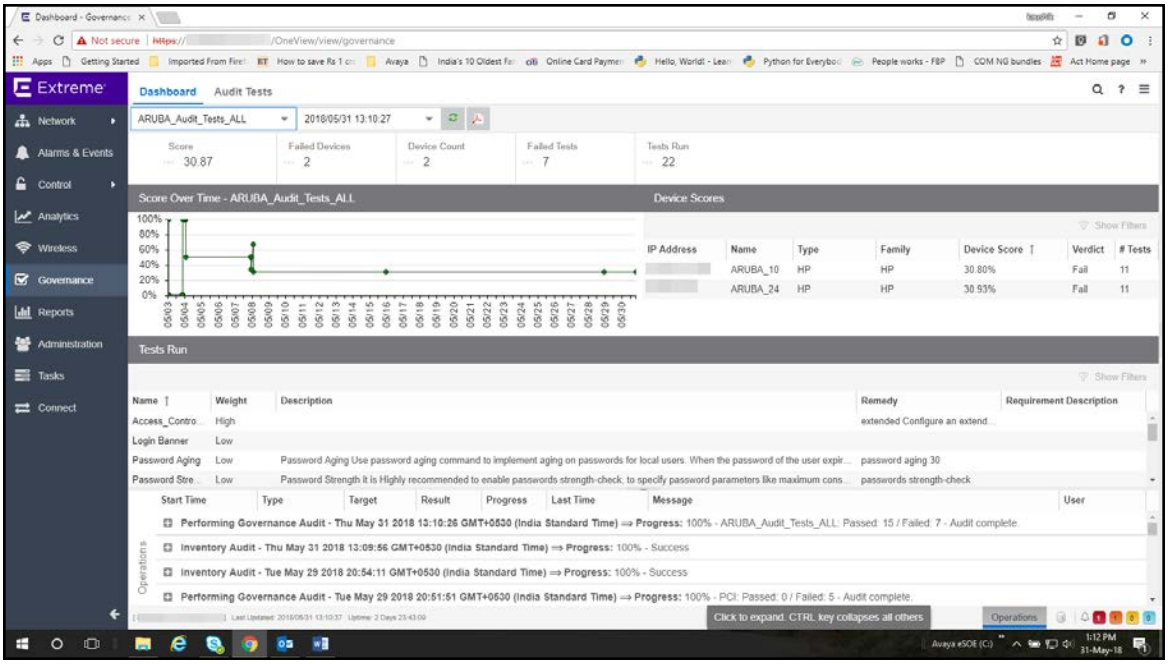
d. Verify the panel displays an **Inventory Audit** entry.

e. Expand the **Inventory Audit** and verify the devices you selected display.

ExtremeCloud IQ Site Engine is performing an archive and save on each device.

The event looks similar to the following:

Governance_$REGIME_$TIMESTAMP - Configuration Retrieved



See Sample regex for audit tests for Aruba devices.

See Sample regex for audit tests for Cisco devices.

Sample regex for audit tests for Aruba devices (Legacy)

The following devices have been tested:

- Aruba 2530 8 PoE+ Switch
- Aruba 2930M 24G PoE

#	Audit tests	Regex
1	Access_Control_Lists_ACLs	^\s*ip access-list
2	Login_Banner	^\s*banner motd .*
3	PasswordStrength	^\s*password complexity
4	Password_Aging	^\s*password configuration aging*
5	Secure_Shell_SSH	^\s*no ip ssh*
6	Simple_Network_Time_Protocol_ SNTP	^\s*sntp

7	SNMPv	^\s*snmp-server community.*
8	SNMP_V_V_Disabled	<snmp-server enable>
9	Syslog_Event_Logging	^\s*logging\s\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}
10	Telnet_Access_Control	^\s*no telnet-server*
11	Web Based Configuration	^\s*no web-management*

Sample regex for audit tests for Cisco devices (Legacy)

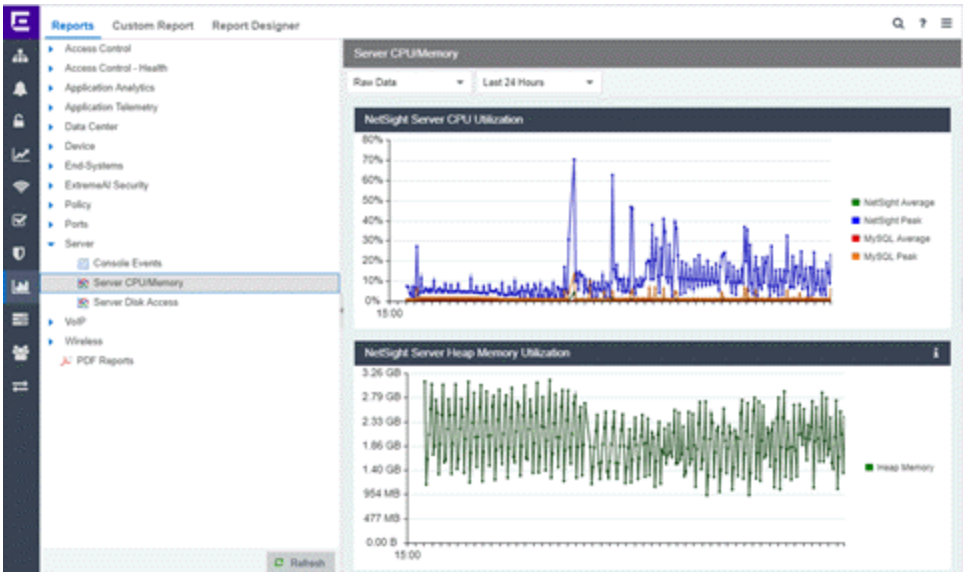
Extreme Networks tested the following devices:

- Cisco IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22) EA2
- Cisco IOS Software, C3750 Software (C3750-IPBASE-M), Version 12.2(35) SE5

#	Audit tests	Regex
1	AuditTest_CISCO_Access Control Lists (ACLs)	^\s*ip access-list
2	AuditTest_CISCO_Broadcast Suppression	^\s*storm-control broadcast
3	AuditTest_CISCO_Web Based Configuration	^\s*ip http server
4	AuditTest_CISCO_Enable password	^\s*enable password
5	AuditTest_CISCO_Exec Timeout	^\s*exec-timeout
6	AuditTest_CISCO_Login Banner	^\s*banner login
7	AuditTest_CISCO_Multicast Suppression	^\s*storm-control multicast
8	AuditTest_CISCO_SNMP v1/v2 Disabled	^\s*snmp-server community\s.* RW
9	AuditTest_CISCO_SNMPv3_No_Auth_No_Priv	^\s*snmp-server group\s.*\sv3\sauth
10	AuditTest_CISCO_Unicast Suppression	^\s*storm-control unicast
11	AuditTest_CISCO_Password Encryption	^\s*service password-encryption
12	AuditTest_CISCO_Port Security	^\s*switchport port-security
13	AuditTest_CISCO_OSPF Router Authentication	^\s*ip ospf authentication

Reports Tab Overview

Use the **ExtremeCloud IQ Site Engine > Reports** tab to view historical and real-time reporting, including high-level network summary information and detailed reports and drill-downs.



The **ExtremeCloud IQ Site Engine > Reports** tab includes three tabs:

- **Reports** tab — Select from the left-panel catalog of reports, many of which are interactive and are adjustable for data and time on which to report. Many include additional report features and functionality. Use the **Info** button at the top-right of the tab to access detailed information about many of the reports.
- **Custom Report tab** — Create your own custom report by selecting a specific target type (such as Interface, Wireless AP, or Identity and Access end-system) and a statistic based on the selected target. Use the display options to show the report as a table or a chart, specify a chart type (column or line), add table titles and chart/axis titles, and assign custom colors to data series inside a chart. Select the **Info** button at the top-right of the tab to access detailed information about custom report options.
- **Report Designer tab** — Create a custom dashboard report, which is accessible from the **Reports** tab.

Additionally, use the **Menu** icon (☰) at the top of the tab to access links to additional information about your version of ExtremeCloud IQ Site Engine.

Requirements

To view all reports on the **Reports** tab, you must be a member of an authorization group assigned full read access capabilities to all of the ExtremeCloud IQ Site Engine tabs and reports.

To collect data in your ExtremeCloud IQ Site Engine reports, you must enable statistics and flow collection for your network devices, interfaces, and wireless clients. For instructions, see How to Enable Data Collection.

Custom Report

Use the **Custom Report** tab to help diagnose a target/statistic pair collection problem as well as view specific ranges of data for a known target. It is a historical report with fully selectable parameters including targets, statistics, category, date range, and display options. Choose the report target such as APs, controllers, or interfaces, as well as the statistics to report on, time frames, and more. Display reports either as a chart or table. You can bookmark the reports you create to view at a later time or to allow you to share the report with others. Report data can also be exported to a file in CSV format. For more information, select the **Info** button at the top-right of the **Reports** tab.

Report Designer

The Report Designer lets you create custom dashboard reports by selecting from a list of available ExtremeAnalytics, IAM, Console, and Wireless dashboards, and customizing report components to meet your specific needs.

Once a report is created, it is available from the **Reports** tab.

Report Features

ExtremeCloud IQ Site Engine reports include the following features (depending on the report selected):

- **Hover Over for Info** — Hover over a pie section to display the name of the segment, the percentage represented by the segment and the number of elements. For some reports, selecting on a pie section opens a filtered end-systems grid for more detailed information.
- **Drill-down for Details** — Link to summary reports containing more detailed information. For example, in the Controller Summary report, selecting on a controller shows a detailed report for that controller over time.
- **Interactive Tables** — Manipulate table data in several ways to customize the view for your own needs.
- **Interactive Charts** — Use data-point rollovers for quick information on chart data. For example, in the Controller Summary report, rolling over the value reported for Bandwidth provides additional bandwidth statistics over time.

- **Sparkline Charts** — View network trends in dense, succinct charts that present report data in an easy to read, condensed format. This provides you with a quick way to catch possible problem areas that you can investigate further. Rollover charts for additional information.
- **CSV Export** — Save report data to a file in CSV format to provide report data in table form.

- Report Designer

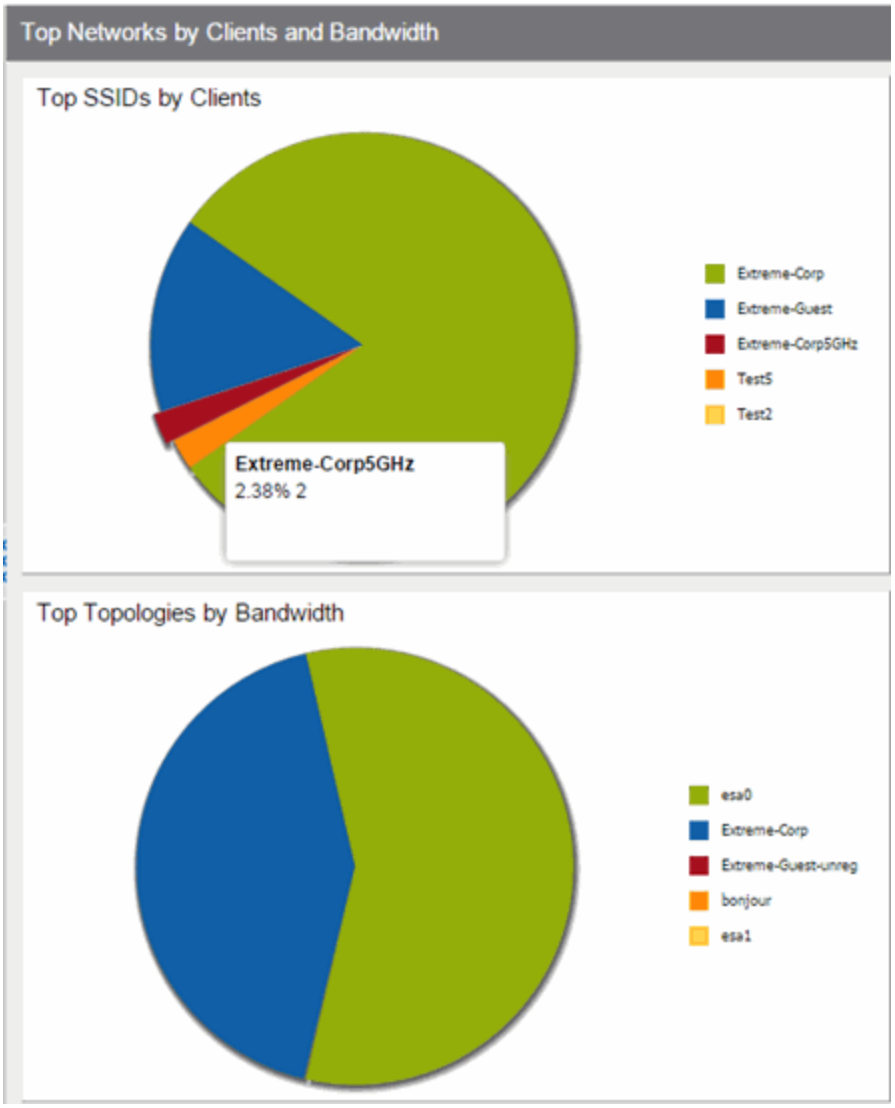
Reports Features

ExtremeCloud IQ Site Engine Reports provide historical and real-time reporting, offering high-level network summary information as well as detailed reports and drill-downs.

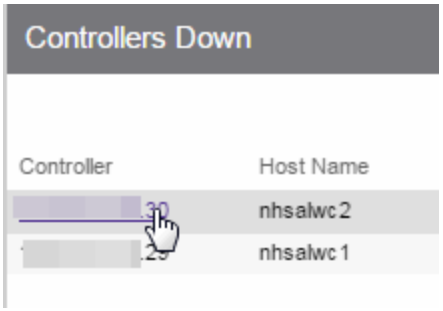
Reports Features

ExtremeCloud IQ Site Engine reports include the following features (depending on the report selected):

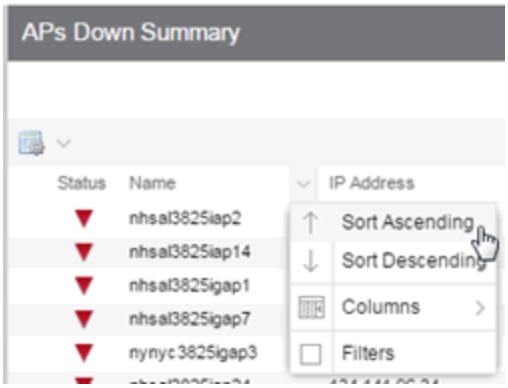
- **Hover Over for Info** — Hover over a pie section to display the name of the segment, the percentage represented by the segment and the number of elements. for some reports, selecting a pie section opens a filtered end-systems grid for more detailed information.



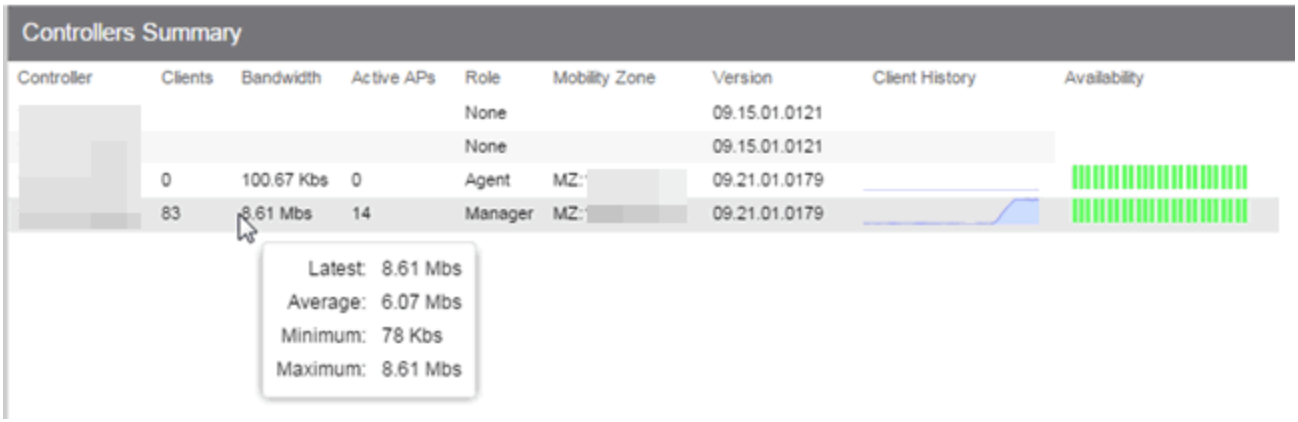
- **Drill-down for Details** — Link to summary reports containing more detailed information. For example, in the Controller Summary report, selecting a controller shows a detailed report for that controller over time.



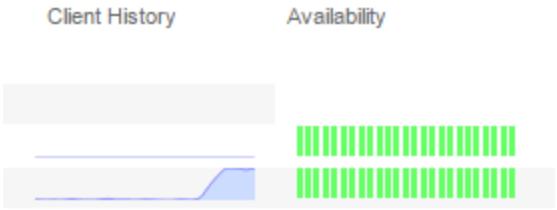
- **Interactive Tables** — Manipulate table data in several ways to customize the view for your own needs:
  - Select the column headings to **perform an ascending or descending sort** on the column data.
  - **Hide or display different columns** by selecting a column heading drop-down arrow and selecting the column options from the menu.
  - **Filter, sort, and search** the data in each column in the table.



- **Interactive Charts** — Use data-point rollovers for quick information on chart data. For example, in the Controller Summary report, rolling over the value reported for Bandwidth provides additional bandwidth statistics over time.



- **Sparkline Charts** — View network trends in dense, succinct charts that present report data in an easy to read, condensed format. This provides you with a quick way to catch possible problem areas that you can investigate further. Rollover charts for additional information.

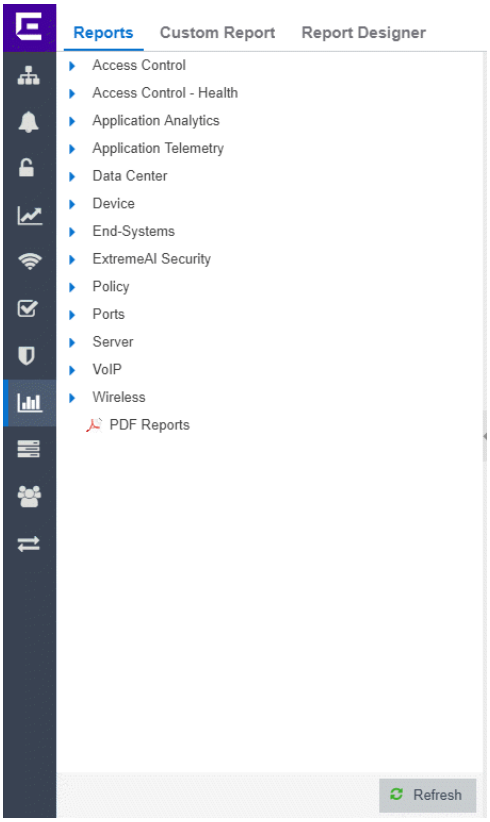


- **CSV Export** — Save report data to a file in CSV format to provide report data in table form.

Reports Catalog

ExtremeCloud IQ Site Engine Reports provide historical and real-time reporting, offering high-level network summary information as well as detailed reports and drill-downs.

Select from a catalog of reports, many of which are interactive, allowing you to adjust the data and time on which to report. See below for a description of each report and a section on helpful report features and functionality. Use the **Info** button at the top-right of the ExtremeCloud IQ Site Engine page to access detailed information about many of the reports.



Reports Catalog

The Reports catalog lets you select a report from the following report types:

- **Access Control** — Provides an overview of end-system connection information. You can also see these reports and others on the **Control** tab.
- **Access Control Health** — Provides reports on end-system assessment and state information. In the Risk Level pie chart, select a pie section to open a filtered end-system grid for more detailed information about end-systems at that risk level.

- **Application Analytics** — These reports provide visibility into the applications on your network and who's using those applications.
- **Application Telemetry** — Provides reports on interfaces, clients, and applications.
- **Data Center** — These reports provide an overview of all virtual machines on the network broken down into VM distribution per ExtremeControl profile, Operating System, Switch, and Hypervisor technology. They also provide table reports with detailed information on all VMs. For each supported Hypervisor technology, sub-reports provide more in-depth data.
- **Device** — The Device reports provide information on device alarms, device archives (archive events and details), device availability, potential duplicate devices, down devices, port usage and details, devices removed from service, top devices by IP traffic, top hosts by resource (memory, CPU, and disk usage), top switches by power (percent usage and consumption in watts), and top switches by resource (CPU and physical memory).
- **End-Systems** — These reports present information on the end-systems connecting to your network.
- **Network** - Includes the Impact Analysis and Network Status Summary reports.
- **Policy** — Provides a Policy Rule Hit Summary report showing top services and roles by rule hits.

NOTE: The Policy Rule Hit Summary report only supports legacy EOS devices, and requires manual configuration of the syslog receiver on UDP port 514. The best practice is to configure the device to only send Rule Hit syslog messages on port 8514 and other Syslog messages on the default port used for alarms.

For Switch Engine devices, you can use the ExtremeCloud IQ Site Engine Control > Policy > Devices & Port Groups > Device > Rule Hit Counts panel for displaying the hit counts when the domain is configured in ACL Rule mode.

- **Ports** — Provides information about the most utilized ports on your network by bandwidth, flows, PoE usage, as well as those that are least available.
- **Server** — These reports provide data on the ExtremeCloud IQ Site Engine server, including the Event Log, CPU and heap memory utilization, and disk access information. The information in the Console Event Log report is the same as the Alarms and Events tab. For more information on using this report, see the "Alarms and Events" Help topic.
- **VoIP** — Provides a report about calls made via Skype for Business.
- **Wireless** — A collection of summary reports providing information on your wireless network components, including reports for AP groups, APs, clients, controllers, and mobility zones.

  Wireless reports also provide data on wireless components ranked by bandwidth and clients, such as top APs by bandwidth, top clients by bandwidth, and top controllers by clients, as well as reports on APs and controllers that are down. In addition, the FloorPlans Summary report, which displays wireless information for selected ExtremeCloud IQ Site Engine floorplans, is included in the collection of summary reports.

For convenience, you can also view some of these reports from the **Wireless** tab.

- **PDF Reports** — Generate summary reports of your current network configuration in PDF format including a Console Report, Network Status Summary, Inventory Report, Identity and Access Summary, and Wireless Configuration Report. You can save these reports or send them to other users in the organization.

Report Designer Overview

The Report Designer lets you create and modify custom reports by selecting from a list of available Analytics, Control, Console, and Wireless dashboards (system reports), and customizing the report component panels to meet your specific needs. The Report Designer also lets you create a new report based on individually selected components, or delete a customized report. When a report is created, it is available from the report catalog in the **Reports** tab.

The Report Designer can be accessed from the **Reports** tab. In order to use the Report Designer, you must be a member of an authorization group that is assigned the **XIQ-SE OneView > Access OneView** and **XIQ-SE OneView > Access OneView Administration** capabilities.

Creating a Report

There are two ways to create a report. You can create a report by customizing an existing system report or by creating a new report based on a selection of individual components.

Customize a System Report

When you change a system report, the new, customized report replaces the original report in the **Reports** tab and all other places in ExtremeCloud IQ Site Engine where that report is used.

Create a New Report

You can create new reports and add them to your system reports and customized reports on the **Reports** tab. Use the tools in the Report Designer to choose the design and layout, as well as which components are included.

Modifying a Report

You can change a report's components and delete panels, but you cannot add new panels. If you want to add new panels, you must create a new report.

Deleting a Report

You can delete a customized system report from the My Reports section in the Report Designer. This also deletes the customized report from the **Reports** tab, and replaces it with the original system report. The original report is available again from the System Reports section in the Report Designer.

You can delete a new report from the My Reports section in the Report Designer. This also deletes the new report from the **Reports** tab.

Custom Components

When you create an Advanced Browser report in the ExtremeAnalytics Browser, you can save it to the Report Designer to use as a custom component. The custom component uses the target, statistic, start time, and search criteria you defined in the Advanced Browser report.

Custom components are listed in the My Components section of the Report Designer. They are available for selection from the **Component** drop-down list in the Applications Browser section when you customize a system report or create a new report.

- ExtremeAnalytics

How to Create a New Report Using the Report Designer

The Report Designer lets you create custom reports by selecting from a list of available Analytics, Control, Console, and Wireless dashboards (system reports), and customizing the report component panels to meet your specific needs. The Report Designer can be accessed from the **Reports** tab. The Report Designer also lets you create a new report based on individually selected components. When a report is created, it is available from the report catalog in the **Reports** tab.

In order to use the Report Designer, you must be a member of an authorization group that is assigned the **XIQ-SE OneView > Access OneView** and **XIQ-SE OneView > Access OneView Administration** capabilities.

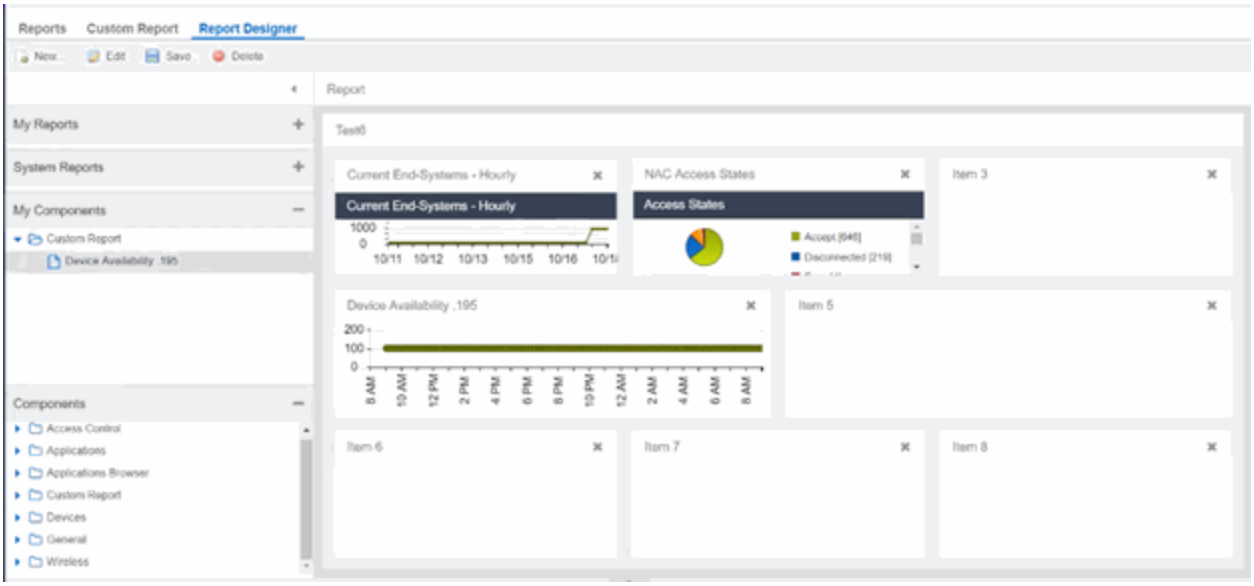
Creating a New Report

Use the following steps to create a new report. The new report is added to the **Reports** tab.

1. Select the **Reports > Report Designer** tab.
2. Select the **New** button . The New Report window opens. Use this window to define the report characteristics.



3. Enter a **Report Name**. Use an easy to recognize name in the **Reports** tab.
4. Select a **Category** for the report from the drop-down list or enter a category in the Category box. This allows you to group your report within an existing report category (in the **Reports** tab) or create a new category.
5. Select from the **Layout** options to determine the number of reports that are displayed in each row and column of your dashboard.
6. Select the **Minimum Panel Height** from the drop-down list.
7. Select the **Include Toolbar** box to add the tool bar to your dashboard.
8. Select the **OK** button. The empty layout format displays in a new tab.
9. Drag and drop the components from the left panel that you want displayed in the dashboard.
10. When in place, the components are a live preview of the data.



11. Select **Save**. The new report is now listed in the **Reports** tab under the appropriate category.

- ExtremeAnalytics tab

How to Modify a Report Using the Report Designer

You can change a report's components and delete panels, but you cannot add new panels. If you want to add new panels, you must create a new report.

1. Select the **Reports** tab and then select the **Report Designer**.
2. In the My Reports section, select the report you want to modify. The report displays in the right panel for editing.
3. Use the **Component** drop-down list to change a component in a panel, or select the **Delete** button to delete a panel.
4. Select the **Save** button. The report populates with data and displays in a new tab. This allows you to preview how the customized report looks.

The new report is now listed in the **Reports** tab under the appropriate category.

For information on related topics:

- Report Designer
- Reports

How to Customize a Report Using the Report Designer

The Report Designer lets you create custom reports by selecting from a list of available Analytics, Control, Console, and Wireless dashboards (system reports), and customizing the report component panels to meet your specific needs. The **Report Designer** also lets you create a new report based on individually selected components. When a report is created, it is available from the report catalog in the **Reports** tab.

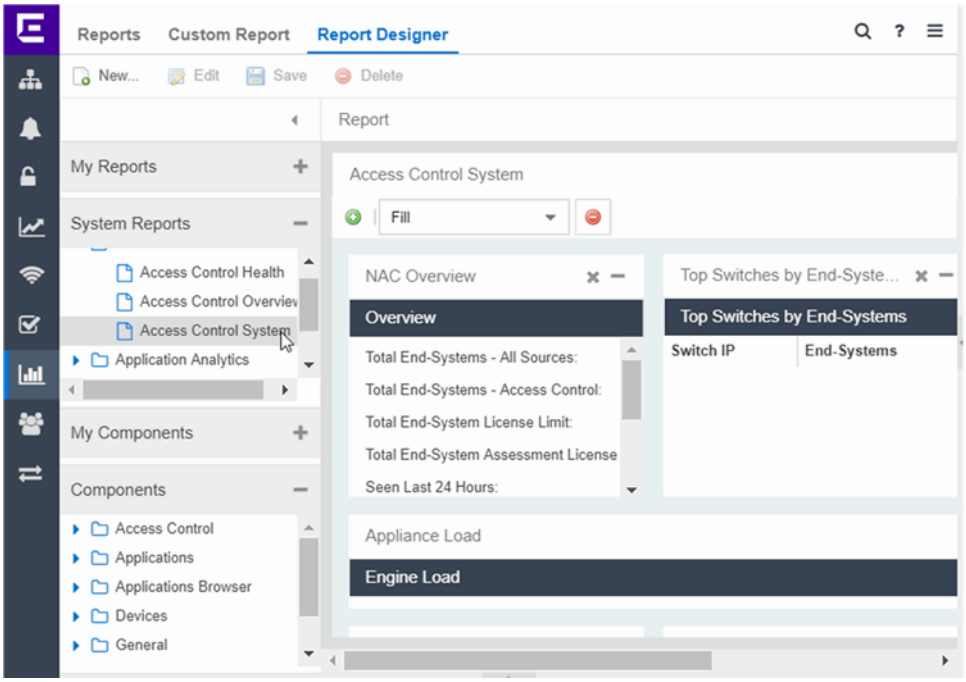
The Report Designer can be accessed from the **Reports** tab. In order to use the Report Designer, you must be a member of an authorization group that is assigned the **XIQ-SE OneView > Access OneView** and **XIQ-SE OneView > Access OneView Administration** capabilities.

Customizing a System Report

Use the following steps to customize an existing system report. The customized report replaces the original report in the **Reports** tab and all other places in ExtremeCloud IQ Site Engine where that report is used.

For example, you want to delete some of the dashboard panels and change some of the dashboard components in the Access Control System report.

1. Select the **Reports** tab in ExtremeCloud IQ Site Engine and then select the **Report Designer**.
2. Select the system report you want to customize in the System Reports section. In the example below, Access Control > Access Control System report is selected. (Use the scroll bar to view the complete list of available reports.) The report becomes available to edit in the right panel.



3. Change the report:
    a. Drag and drop the components that you want displayed in the dashboard.
    b. When in place, the components are a live preview of the data.
4. When you have finished making changes to the report, select the **Save** button. The report is populated with data and displayed in a new tab as a way to preview the report. The name of the customized report is added to the My Reports section.

The custom system report is available in the Reports catalog and replaces the original system report. If you delete the customized system report, the report changes back to the original system report.

Custom Components in Report Designer

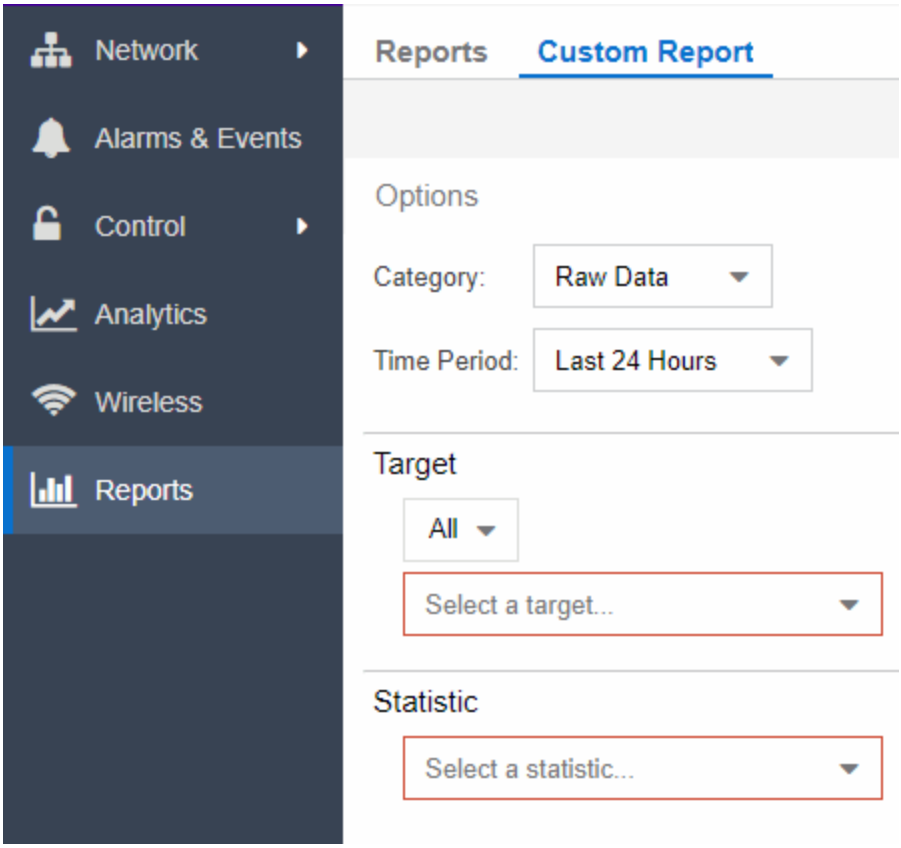
When you create an Advanced Browser report in the ExtremeAnalytics Browser, you can save it to the **Report Designer** to use as a custom component. The custom component uses the target, statistic, start time, and search criteria you defined in the Advanced Browser report.

Custom components are listed in the My Components section in the left-panel of the Report Designer. They are available for selection from the **Component** drop-down list in the Applications Browser section when you customize a system report or create a new report.

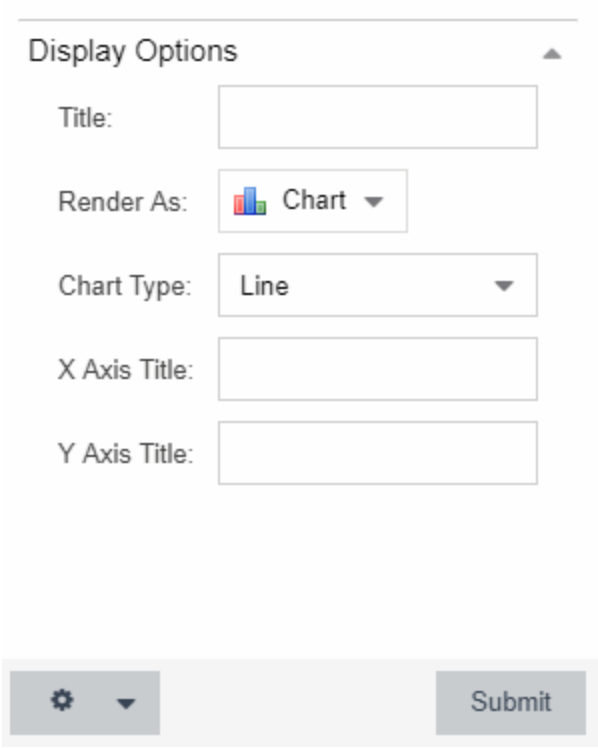
Create a New Component

You can create new components from the **Reports > Custom Reports** tab.

The left-panel options allow you to choose the category and duration of the data captured in the component. You can also choose the target for which the data will be displayed, and which statistical data will be displayed.



1. Select a **Category** from the drop-down list. Options include **Raw Data**, **Hourly**, **Daily**, **Weekly**, and **Monthly**.
2. Choose the **Time Period** for the data to be displayed. Options include **Last 24 Hours**, **Yesterday**, **Last 3 Days**, **Last Week**, **Last 2 Weeks**, **Last Month**, **Last 3 Months**, **Last 6 Months**, **Last Year**, or **Custom**. If you select a custom time period, you can choose your start and end times for the duration of the data.
3. Select the **Target** type from the drop-down list. Then select the specific target from the **Select a target** drop-down list.
4. Select the **Statistic** you want to display from the drop-down list.
5. Enter your **Display Options** to design your chart. You can choose to render the data as a chart or grid.



6. Select **Submit.**
7. Select the **Gear** button ( ) in the bottom left corner and choose from the drop-down list:
    a. (Save) Save to Report Designer - If you choose this option, you can use the component in a new or custom report.
    b. ( ) Export to CSV
    c. ( ) Bookmark
8. Enter a name for your component.

For information on related topics:

- Reports

Administration

ExtremeCloud IQ Site Engine's **Administration** tab provides diagnostic reports and tools to monitor, maintain, and troubleshoot the application and its components.

The **Menu** icon (☰) at the top of the screen provides links to additional information about your version of ExtremeCloud IQ Site Engine.

To view the diagnostic reports and schedules in the **Administration** tab, you must be a member of an authorization group assigned the OneView > Access OneView and OneView > Access OneView Administration capabilities. For additional information about configuring user capabilities, see Users.

This Help topic provides information on the following sub-tabs:

- Profiles
- Users
- Server Information
- Licenses
- Certificates
- Options
- Device Types
- Backup/Restore
- Diagnostics
- Vendor Profiles
- Client API Access

Profiles

The **Profiles** tab enables you to establish access to the devices on your network by creating identities used for authentication when performing SNMP queries and sets. ExtremeCloud IQ Site Engine supports authentication to devices using SNMPv1, SNMPv2 and SNMPv3. When device models are created in the database, you can accept the default profile or assign a specific Profile to describe a set of access Credentials used for authentication at each level of access in the device. (When first installed, ExtremeCloud IQ Site Engine's default profile uses an SNMPv1 credential that provides Read, Write and Max Access privileges.) The specific profile used depends on the protocol that is supported in a device and the credentials required to gain access.

Users

The **Users** tab enables you to create the authorization groups that define the access privileges (called Capabilities) assigned to authenticated users. When a user successfully authenticates, they are assigned membership in an authorization group that grants specific capabilities in the application.

The **Users** tab is also where you define the method used to authenticate users who are attempting to launch ExtremeCloud IQ Site Engine. There are four authentication methods available: OS Authentication (the default), LDAP Authentication, RADIUS Authentication (RadSec is not supported), TACACS+ Authentication, and OKTA SSO Authentication.

Server Information

The **Server Information** tab enables you to view and manage current client connections and ExtremeCloud IQ Site Engine locks.

Licenses

To view license details or to add a new license, select the **Licenses** tab.

There are tiers of licenses for ExtremeCloud IQ Site Engine and devices:

- No License - Status-Only devices
- Extreme Platform ONE Tier 3rd Party - 3rd party devices, Extreme Campus Controller, ExtremeCloud IQ Controller, WiNG wireless devices, and devices not natively supported by ExtremeCloud IQ Site Engine
- Navigator - 3rd party devices, Extreme Campus Controller, ExtremeCloud IQ Controller, WiNG wireless devices, and devices not natively supported by ExtremeCloud IQ Site Engine
- Extreme Platform ONE Tier A - Natively supported Extreme devices of tier A
- Extreme Platform ONE Tier B - Natively supported Extreme devices of tier B
- Extreme Platform ONE Tier C - Natively supported Extreme devices of tier C
- Extreme Platform ONE Tier D - Natively supported Extreme devices of tier D
- Pilot - Natively supported Extreme devices of any tier

As you begin to onboard ExtremeCloud IQ Site Engine and your devices, ExtremeCloud IQ will determine if you meet or exceed the license limits for each license type.

Additionally, the NAC license provides licenses for end-systems connecting to your network.

The table at the top of the **Licenses** tab shows the total number of units (devices/end-systems) used against each type of license.

- Total Entitlements - the licensed quantity purchased
- Active in Cloud - the used licenses in the ExtremeCloud IQ or Extreme Platform ONE (this column is only present in connected deployment)
- Active Locally - the used licenses in this ExtremeCloud IQ Site Engine
- Available - the number of license units available to be used
- % Remaining - what percentage of the total is available to be used

NOTE:

- If you need to add a license using a license entitlement file or add a license key manually, see Updating a License.
- If you need to revoke your Air Gap Licenses, see Revoke Air Gap License.
- In Air Gap mode deployment, the **Realign License Assignment** button triggers the process of automatic realignment of licenses to devices. The device is assigned the best-fit available Tier.
  In Connected mode deployment, use Unmanage/Manage in Extreme Platform ONE Networking or ExtremeCloud IQ to realign licenses.
- Support for Extreme Platform ONE Networking Tier 3rd Party licenses is added in ExtremeCloud IQ Site Engine version 26.06 and later. For ExtremeCloud IQ Site Engine versions 26.02 and older, the Cloud management translates the 3rd party to Navigator license. In Connected Mode deployment with ExtremeCloud IQ Site Engine versions 26.02 and older, you can utilize Tier 3rd party licenses but the value for Navigator shown in the Active Locally column combines both Navigator and Tier 3rd Party.

Source

The origin of the license. Licenses can be managed in ExtremeCloud IQ or in Management Center, when added manually.

Entitlement

The following table shows the mapping of entitlement to a human-friendly licensing name:

Entitlement	License
XIQ-PIL-S-C	Pilot
XIQ-NAV-S-C	Navigator
NetSightEval	Access Control Evaluation
XIQ-NAC-S	Access Control
EP1-STD-T3RD-S-C	Standard 3rd Party
EP1-STD-TA-S-C	Standard Tier A
EP1-STD-TB-S-C	Standard Tier B

Entitlement	License
EP1-STD-TC-S-C	Standard Tier C
EP1-STD-TD-S-C	Standard Tier D
EP1-ADV-TA-S-C	Advanced Tier A
EP1-ADV-TB-S-C	Advanced Tier B
EP1-ADV-TC-S-C	Advanced Tier C
EP1-ADV-TD-S-C	Advanced Tier D

Type
The type of license - either Subscription or Perpetual.

Quantity
The total number of devices included for the license.

For NAC licenses, the value in this column displays two numbers separated by a "/". For example, 100/50. The first number (100) represents the number of end-systems available for the license and the second number (50) represents the number of Guest and IoT (GIM) licenses available for the license.

Start Date
The date the license subscription begins.

End Date
The date the license subscription expires.

Description
Any additional details about the license.

Certificates

The Certificates tab provides a central location for managing the ExtremeCloud IQ Site Engine server certificate.

From this tab you can:

- Update the ExtremeCloud IQ Site Engine Server Certificate by replacing the server private key and certificate.
- Update the Fabric Manager Server Certificate by replacing the server private key and certificate.
- View and change the Server Trust Mode that specifies how servers handle certificates from other servers.
- View and change the Legacy Client Trust Mode that specifies how ExtremeCloud IQ Site Engine clients handle a server certificate.

Options

ExtremeCloud IQ Site Engine options enable you to configure the behavior of ExtremeCloud IQ Site Engine. These options apply across all ExtremeCloud IQ Site Engine applications. In **Options** (**Administration > Options**), the right-panel view changes depending on what you select in the left-panel tree.

Information on the following options:

- Access Control
- Alarm
- Alarm/Event Logs and Table
- Compass
- Compliance
- Customer Experience
- Database Backup
- Device Terminal
- Event Analyzer
- ExtremeCloud IQ Connection
- ExtremeNetworks.com Updates
- FlexView
- Impact Analysis
- Inventory Manager
- Legacy Clients
- Name Resolution
- NetFlow Collector
- Network Monitor Cache
- Policy
- SBI
- SMTP Email
- SNMP
- Site
- Site Engine - Collector
- Site Engine - Engine
- Site Engine - General

- Site Engine - Server Health
- Status Polling
- Syslog
- Tasks
- TopN Collector
- Trap
- Web Server
- Wireless Manager
- ZTP+

Device Types

Configure end-system device identification in ExtremeCloud IQ Site Engine using the **Device Types** tab.

End-systems that connect to your network are identified by ExtremeCloud IQ Site Engine in two ways:

- Using DHCP Fingerprints
- Using MAC OUIs

Detection and Profiling

The **Detection and Profiling** table displays DHCP fingerprints and the device types with which they are associated. ExtremeControl examines the DHCP packet from an end-system as it accesses the network and uses the information in this table to associate it to a device type.

Right-click on a fingerprint in the table to open a drop-down list that enables you to edit the device type profile, delete the fingerprint, or view the Fingerprint Definition for the device.

NOTE:	As of ExtremeCloud IQ Site Engine Version 8.5, DHCP fingerprints are applied to all ExtremeControl engines and are no longer engine-specific

Table Functions

Columns

Select a the arrow at the right of a column heading in the table to expand a column function drop-down list. This column heading drop-down list includes Sort, Columns, and Filter column functions, as well as the following functions:

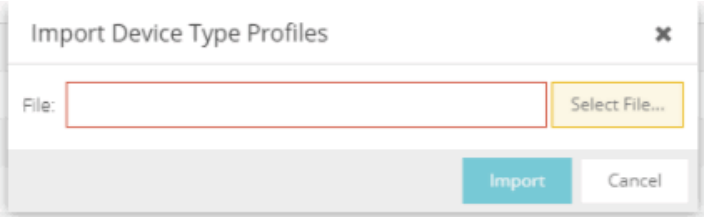
- **Group by this Field** - Select this option to group the data in the table by the selected column heading.

- **Show in Groups** – When you select **Group by this Field** option for a column heading, the **Show in Groups** check box is enabled. The group name displays above the table data at the top left corner of the table. Select the Show in Groups check box to disable this option.

Buttons

You can perform the following functions using the buttons in the table:

- **Add** – Select the **Add** icon to open the **Add Device Type Profile** window, from which you can create or modify a device type identifier for a selected fingerprint in the table.
- **Edit** – Select the **Edit** icon to open the **Edit Device Type Profile** window, from which you can modify a device type identifier for a selected fingerprint in the table. If the fingerprint is a system fingerprint, a custom fingerprint is created that overrides the system fingerprint.
- **Delete/Reset** – Select the **Delete/Reset** icon to remove a fingerprint from the table. If the fingerprint is a custom fingerprint that was overriding a system fingerprint, the system fingerprint becomes active.
- **Import** – Select to apply a custom DHCP fingerprint xml definitions file to ExtremeCloud IQ Site Engine. The Import Device Type Profiles window opens.



NOTE: You can import a fingerprint from another system that uses an .xml file that matches ExtremeCloud IQ Site Engine's fingerprint .xml file.

MAC OUI Vendors

Use the **MAC OUI Vendors** tab to view and configure MAC OUI (organizational unique identifier) values and associate them with a device vendor. ExtremeCloud IQ Site Engine is configured with a number of system-defined MAC OUIs. You can also add your own by selecting the **Add** icon.

Select the **Update** icon to open the **Update OUI Vendor List** window, from which you can update the list of MAC OUI vendors from the internet or from a saved file.

Backup/Restore

The **Backup/Restore** tab enables you to perform database backups and a restore operation for legacy backups as well as configure the URL and password for the database.

Diagnostics

The **Diagnostics** tab provides three levels of information: Basic, Advanced, and Diagnostic.

IMPORTANT: Accessing Server and Server Utilities features on the **Diagnostics** tab require ExtremeCloud IQ Site Engine Administrator access. Attempting to access these features without Administrator access results in being redirected to a window informing you of this requirement.

Use the **Level** menu at the top-left of the page to select the desired report level.

NOTES: All three diagnostic levels enable you to launch the NBI Explorer from the **Server > Server Utilities** menu. You can use the NBI Explorer to access the Northbound Interface.

- **Basic Level** — This level provides basic administrative reports to help you monitor and troubleshoot your network. An option to export the end-system events for a particular date range is available. The export is limited to 250,000 records.
- **Advanced Level** — This level includes all Basic administrative reports as well as additional Advanced reports with more detailed information for debugging problems.
- **Diagnostic Level** — This level includes all Basic and Advanced reports. Additionally, Diagnostic provides access to the following diagnostic actions:
    - **Save Diagnostic Information** — Saves the administrative report data to log files, and the statistic and target information to CSV files, so that you can save and review the information for debugging purposes. The information is saved to <install directory>/appdata/OneView/RptStatus/ as a ZIP file, with the date as part of the file name. Unzip the file to view the log files and CSV files. You can view the save operation progress in the Server Log report (located on the Administration tab under the Server section). When the Save operation is complete, an event is sent to the Console Event log with the full path to the diagnostic zip file.
    - **Diagnostic Levels** — Lets you enable different levels of logging for specific ExtremeCloud IQ Site Engine functionality, and view the debug information in the Server Log report (located on the **Administration** tab under the Server section) or in the <install directory>/appdata/logs/server.log file on the ExtremeCloud IQ Site Engine Server. By default, error and informational data is logged to the log file, with a new file created each day. You can set the diagnostic level to Verbose to collect additional data that is presented in an easy-to-read format. Note that the Informational and Verbose settings create large log files and can impact system performance.

      Off — Turns off all diagnostic logging.

      Default emc.xml Value — Sets the level to the level specified in the emc.xml file.

Critical — Records only Error events.

Warning — Records Warning and Error events.

Informational — Records Warning, Error, and Info events.

Verbose — Records debug information in addition to Warning, Error, and Info events.

- **Clean OneView Data Tables** — Cleans all aggregated report data from the ExtremeCloud IQ Site Engine reporting database. This enables you to restart your database, if required for problem resolution. The operation removes all data from the following database tables:

  rpt_default_raw

  rpt_default_hour

  rpt_default_day

  rpt_default_week

  rpt_default_month

Vendor Profiles

The Vendor Profiles tab enables you to edit configurations for device types. You can enter additional information about the device type to help identify it in ExtremeCloud IQ Site Engine.

Vendor Profiles are a beta feature and are only available by selecting **Enable Beta Features** on the **Administration** > Diagnostics tab.

Client API Access

The Client API Access tab enables you to add access to the ExtremeCloud IQ Site Engine Northbound Interface API from third-party applications.

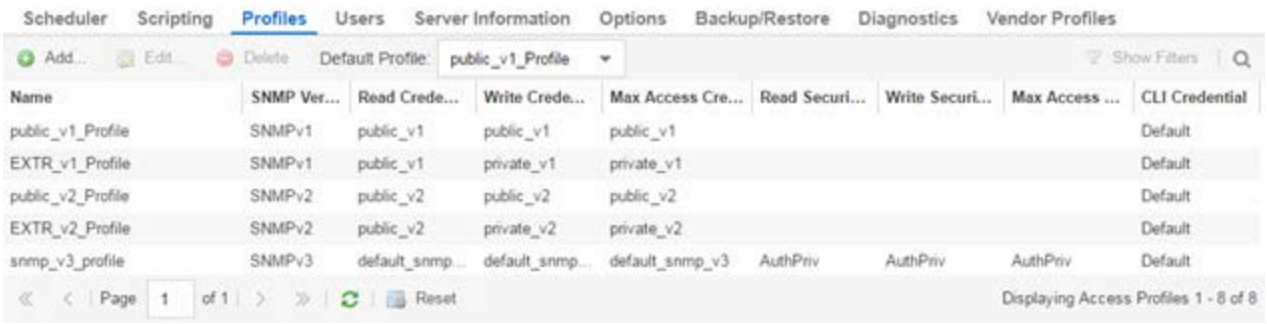
Profiles

ExtremeCloud IQ Site Engine applications access devices in order to control certain device functions and retrieve information for device properties views, FlexViews and periodic polling. Use this tab to create the authentication *credentials* used to manage access to your devices through SNMP and CLI (command line interface), and the *profiles* that use those credentials for various access levels. Profiles are then mapped to specific devices on your network.

- Credentials — Credentials define the authentication values (for example, user names and passwords) used to access your network devices.
  - SNMP Credentials provide support for device management using SNMP.
  - CLI Credentials provide support for device management using the CLI.
- Profiles — Profiles are assigned to device models in the ExtremeCloud IQ Site Engine database. They identify the credentials used for the various access levels when communicating with the device.
- Device Mapping — Allows you to map the profiles you create to Authorization Groups on devices.

Managing device access using credentials and profiles consists of creating your credentials, creating the profiles that uses those credentials, and then mapping the profiles to Authorization Groups on devices.

Profiles Section



Default Profile
: This drop-down list lets you specify a profile used by default to access a device.

ID
: This column, hidden by default, displays a unique numeric identifier for the profile.

Name
: This is the name assigned when the profile is created. The public_v1_Profile is automatically created during ExtremeCloud IQ Site Engine installation and cannot be deleted.

SNMP Version
: This is the SNMP protocol version for the profile. Profiles can be configured for SNMPv1, SNMPv2c, or as SNMPv3.

Read, Write, Max Access Credential
: When the Version is SNMPv1 or SNMPv2c, the Read, Write, and Max Access columns in the table contain the Community Name for each access level. When the Version is SNMPv3, the Read, Write, and Max Access columns in the table contain the credential specified for each access level.

Read, Write, Max Access Security Level
: When the Version is SNMPv3, these columns contain the security level specified for each access credential. When the Version is SNMPv1 or SNMPv2c, these columns do not apply.

CLI Credential
: The CLI credential specified for the profile.

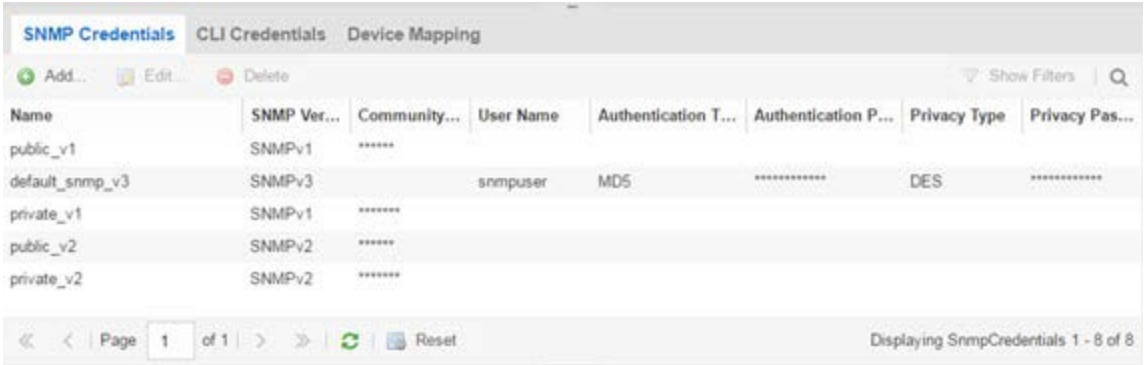
Add Button
: Opens the Add/Edit Profile window where you can select the SNMP version and define the profile name and passwords/community names used by the profile.

Edit Button
: Opens the Add/Edit Profile window where you can modify the SNMP version and passwords/community names used by a selected profile.

Delete Button
: Removes the selected Profile from the Device Access Profiles table. You cannot delete the profile currently selected to be the Default Profile.

SNMP Credentials Subtab

This tab lists all of the SNMP credentials created in the ExtremeCloud IQ Site Engine database. The public_v1 credential is automatically created during installation and cannot be deleted.



ID
: This column, hidden by default, displays a unique numeric identifier for the SNMP credentials.

Name
: This column lists names assigned to credentials created in the ExtremeCloud IQ Site Engine database.

SNMP Version
: This is the SNMP protocol version for the credential. Credentials can be configured for SNMPv1, SNMPv2c, or as SNMPv3.

Community Name
: For SNMPv1 or SNMPv2c credentials, this is the Community Name used for device access.

User Name
: For SNMPv3 credentials, this is the User Name used for device access.

Authentication Password/Authentication Type, Privacy Password/Privacy Type
: For SNMPv3 credentials, these columns show the authentication protocol (None, MD5, or SHA) and privacy protocol (None, DES, or AES) and passwords used by the credential.

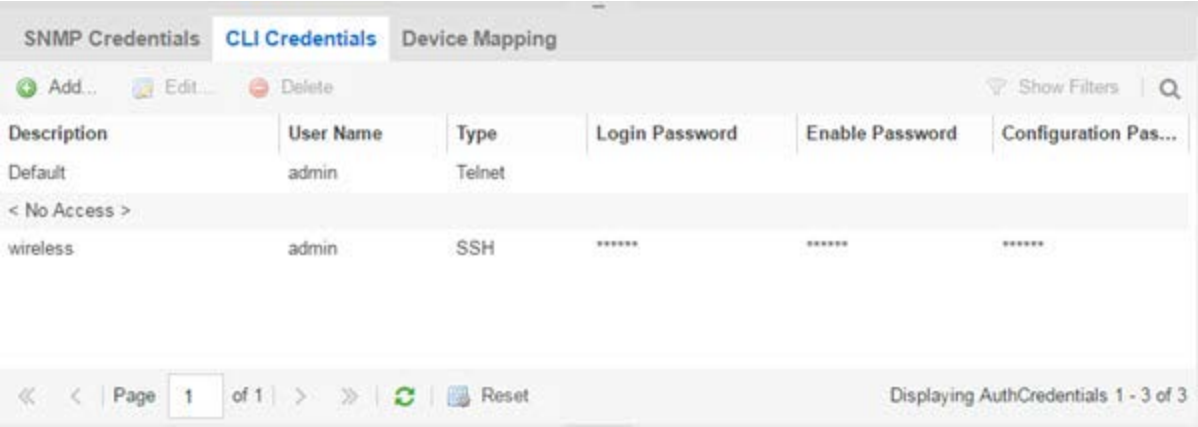
Add Button
: Opens the Add/Edit SNMP Credential window where you can define new SNMP credentials.

Edit Button
: Opens the Add/Edit Credential window where you can modify a credential selected from the SNMP Credentials table.

Delete Button
: Removes a selected credential from the SNMP Credentials table.

CLI Credentials Subtab

This tab lists all of the CLI credentials created in the ExtremeCloud IQ Site Engine database. The Default and <No Access> credentials are created automatically during installation and cannot be deleted.



Description
: A description of the CLI credential.

User Name
: The Username used for device access.

Type
: The communication protocol used for the connection (SSH or Telnet).

Login Password
: The password required to start a CLI session.

Enable Password
: The password required to enter Enable mode in a CLI session.

Configuration Password
: The password required to enter Configure mode in a CLI session.

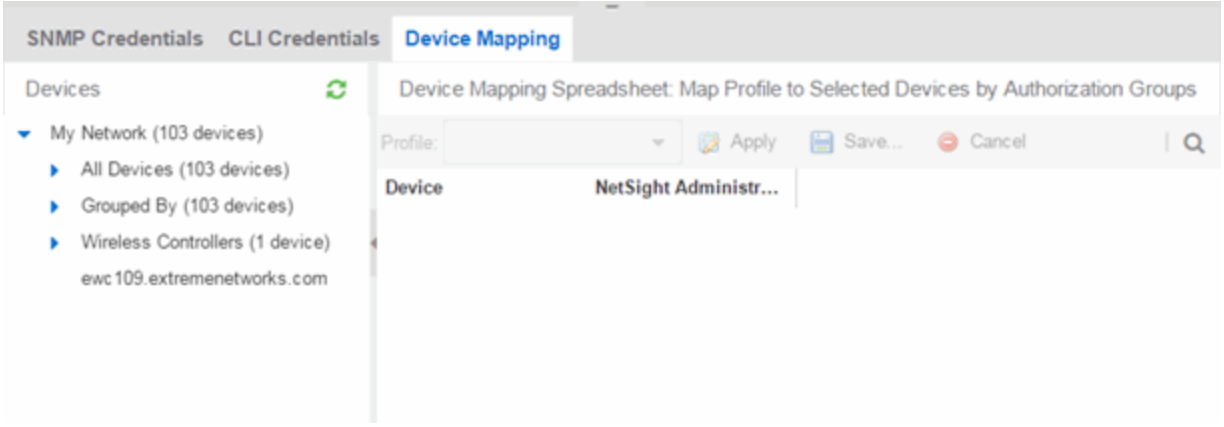
Add Button
: Opens the Add/Edit CLI Credential window where you can define a new CLI credential.

Edit Button
: Opens the Add/Edit CLI Credential window where you can modify a CLI credential selected from the CLI Credentials table.

Delete Button
: Removes a selected credential from the CLI Credentials table.

Device Mapping Subtab

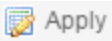
This tab lets you define the specific Profiles to apply to users in each Authorization Group when communicating with network devices. The tab contains a device tree in the left panel where you select devices, and a table in the right panel that lists the current device profile assignments.



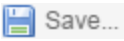
Device Tree
: The left panel contains a device tree, where you select a device or device group to view or configure.

Profile/Device Mapping Table
: This table lists all of the selected devices and shows a column for the Netsight Administrator Group and each *Authorization Group* you defined. The *NetSight Administrator* column shows the profile used by the Netsight Administrator group. The Profile listed/selected for each Authorization Group column used by that group when communicating with the associated device and, as a result, defines the level of access granted to users that are members of that Authorization Group. A <*> in the table indicates that no profile is specified and the Netsight Administrator profile is used.

  Select a Profile from the drop-down list, select the authorization groups to which you want to apply the profile, and select Apply.

Apply Button 

: Sets the profile selected in the Profile drop-down list as the profile for the Authorization Groups selected in the table.

Save Button 

: Saves your changes on the device or devices selected.

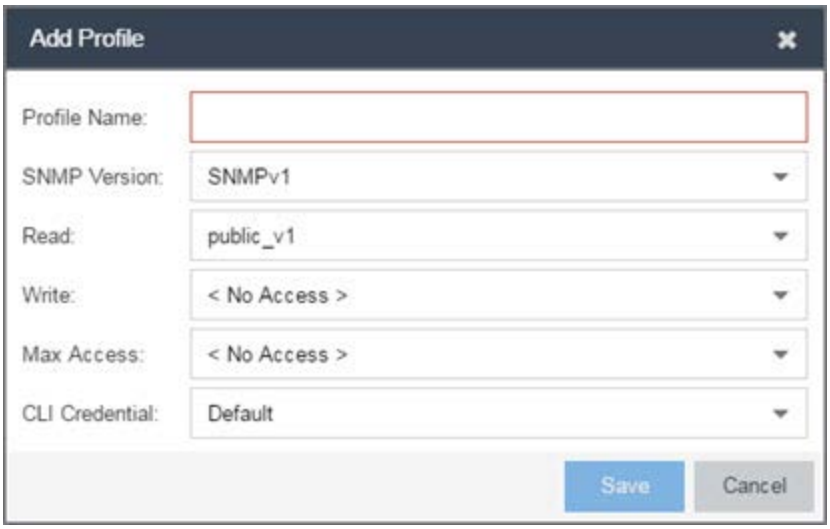
Cancel Button 

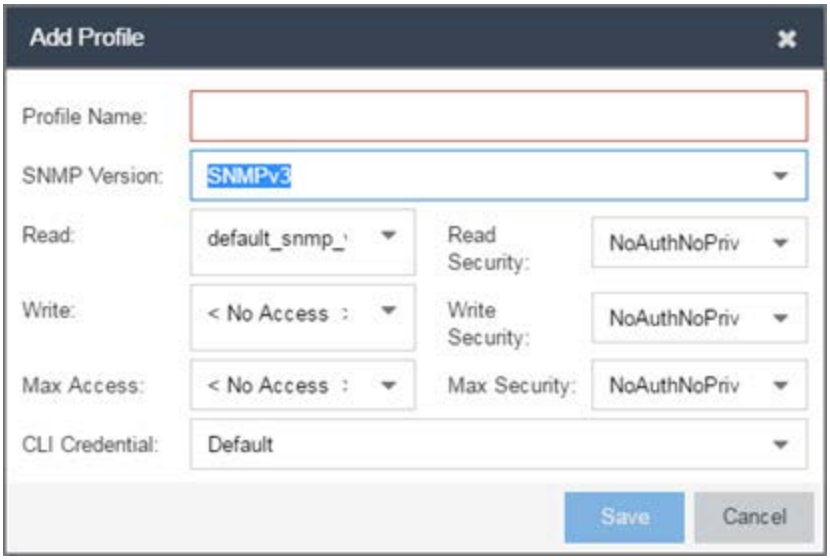
: Discards your unsaved changes.

Add/Edit Profile Window

This window lets you select the SNMP and CLI Credentials for a new profile or modify the credentials for an existing profile.

NOTE: When configuring profiles for ExtremeWireless Controllers, ensure the controllers are discovered using an SNMPv2c or SNMPv3 profile. This profile must also be associated with a SSH-based CLI credential profile with the Login Password and Configuration Password fields configured with the SSH account password. Wireless Manager uses the controller's CLI to retrieve required information and to configure managed controllers.





Profile Name

A unique name (up to 32 characters) assigned to this profile.

When editing an existing profile, you can select a profile from the table to modify its settings. However, you cannot change the name of an existing profile.

SNMP Version

This is the SNMP protocol version for the profile. Profiles can be configured for SNMPv1, SNMPv2c, or as SNMPv3. When either SNMPv1 or SNMPv2c is selected, the editor provides fields where you can configure access levels using Community Names. With SNMPv3 selected, you can configure access levels using Credentials and Security Levels.

Read, Write, Max Access

SNMPv1, SNMPv2c
: Select the SNMP Credential used for the Read, Write, Max Access. These fields define the community names used for these levels of access. You can also select New to open the Add/Edit SNMP Credential window.

  - Read — This Community Name is used for *get* operations.
  - Write — This Community Name is used for *set* operations.
  - Max Access — This Community Name is used for *set* operations that require administrative access, such as changing community names.

SNMPv3
: Select the SNMP Credential used for the Read, Write, Max Access levels, defined by Credentials and Security Level:

  Credentials
  \
  : Credential Names are assigned to each of the three SNMPv3 access levels used for the Read, Write and Max Access operations. You can also select New to open the Add/Edit SNMP Credential window.

    - Read — used for read operations (*gets*).
    - Write — used for write operations (*sets*).
    - Max Access — used for write operations (*set*) that require administrative access.

  Security Level
  : Each access level can be assigned a security level:

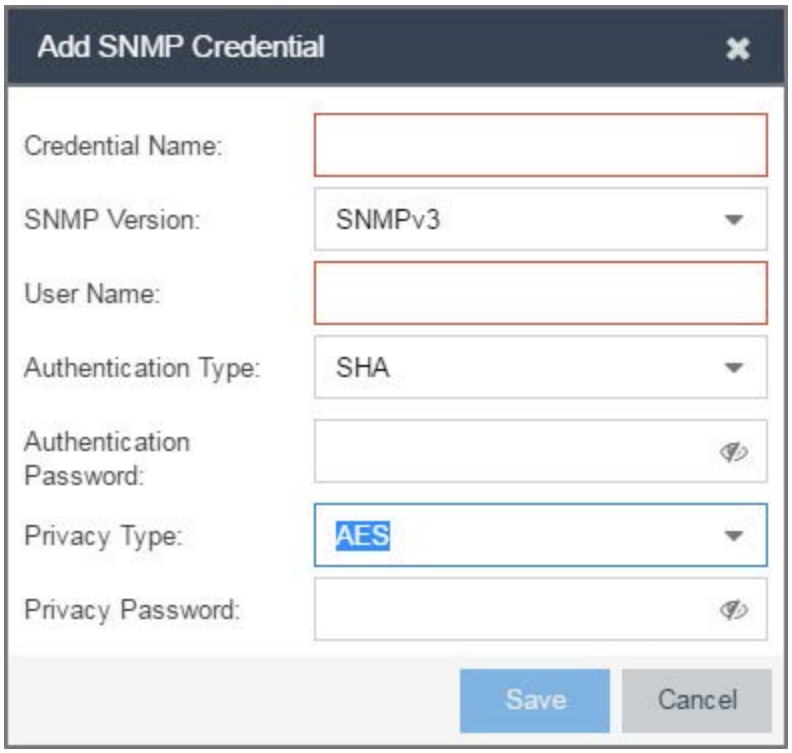
    - AuthPriv — Highest security level requiring authentication and privacy (encrypted information).
    - AuthNoPriv — Requires authentication, but unencrypted information.
    - NoAuthNoPriv — Neither authentication nor privacy required.

CLI Credential
: Use the drop-down list to select the CLI Credential for this profile. CLI credentials provide support for device management using the command line interface (CLI). You can also select New to open the Add/Edit CLI Credential window.

Add/Edit SNMP Credential Window

This window lets you define or edit the names and community names/passwords for SNMP credentials.





Credential Name

A unique name (up to 32 characters) assigned to this access credential. You can define a new credential or select a name from the table to modify settings for an existing credential. You cannot edit the name of an existing credential.

SNMP Version

This is the SNMP protocol version for the credential. Credentials can be configured for SNMPv1, SNMPv2, or as SNMPv3. When either SNMPv1 or SNMPv2 is selected, the window provides fields where you can configure access levels using Community Names. With SNMPv3 selected, you can configure access levels using Authentication and Privacy Types.

Community Name
: For SNMPv1 or SNMPv2 credentials, this is the Community Name used for device access.

User Name
: For SNMPv3 credentials, this is the User Name used for device access.

Authentication Type
: For SNMPv3 credentials, select MD5, SHA1, or None, from this drop-down list.

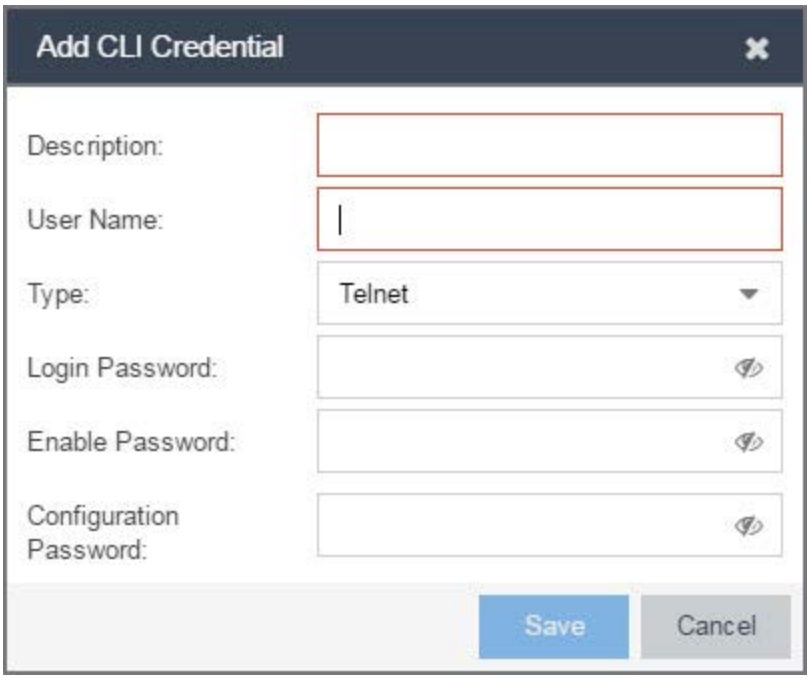
Authentication Password
: This is the password (between 1 and 64 characters in length) used to determine Authentication. If an existing password is changed and the credential is currently used with a profile applied to one or more devices, a confirmation dialog is opened to determine how the changes are handled. You are asked if you want to change the password on the device(s). You can then select the devices where the password is changed and, if this user is a valid user on the device(s), then the new password is set on the device. Select the Eye icon to display your password.

Privacy Type
: For SNMPv3 credentials, select AES, DES, or None from this drop-down list.

Privacy Password
: This is the password (between 1 and 64 characters in length) used to determine Privacy. If an existing password is changed and the credential is currently used with a profile applied to one or more devices, a confirmation dialog is opened to determine how the changes are handled. You are asked if you want to change the password on the device(s). You can then select the devices where the password is changed and, if this user is a valid user on the device(s), then the new password is set on the device. Select the Eye icon to display your password.

Add/Edit CLI Credential Window

This window lets you define or edit the user name and passwords for a CLI credential.



Description
: A description of the credential.

User Name
: The User name used for device access.

Type
: The communication protocol used for the connection (SSH or Telnet).

Passwords
: The passwords used to determine different levels of access to the device:

- Login — The password required to start a CLI session. Select the Eye icon to display your password.
- Enable — The password for entering Enable mode. Select the Eye icon to display your password.
- Configuration — The password for entering Configure mode. Select the Eye icon to display your password.

NOTE: When configuring CLI Credentials for ExtremeWireless Controllers, you must add the username and password Login credentials for the controller to this Add/Edit Credential window in order for Wireless Manager to properly connect (SSH) to the controller and read device configuration data. However, the same Login password must be added to the Configuration password field in addition to the Login password field. The username, Login and Configuration password specified here must match the username and Login password configured on the controller.

Vendor Profiles

Use the **Vendor Profiles** tab to add new device families to ExtremeCloud IQ Site Engine, which includes any element of the device family: Company, Vendor, Subfamily, and Device Types. With the addition of properties for the new device family, the elements determine the reports available for the device in its Device View, the FlexView filters available for the device, and the scripts that apply to the device.

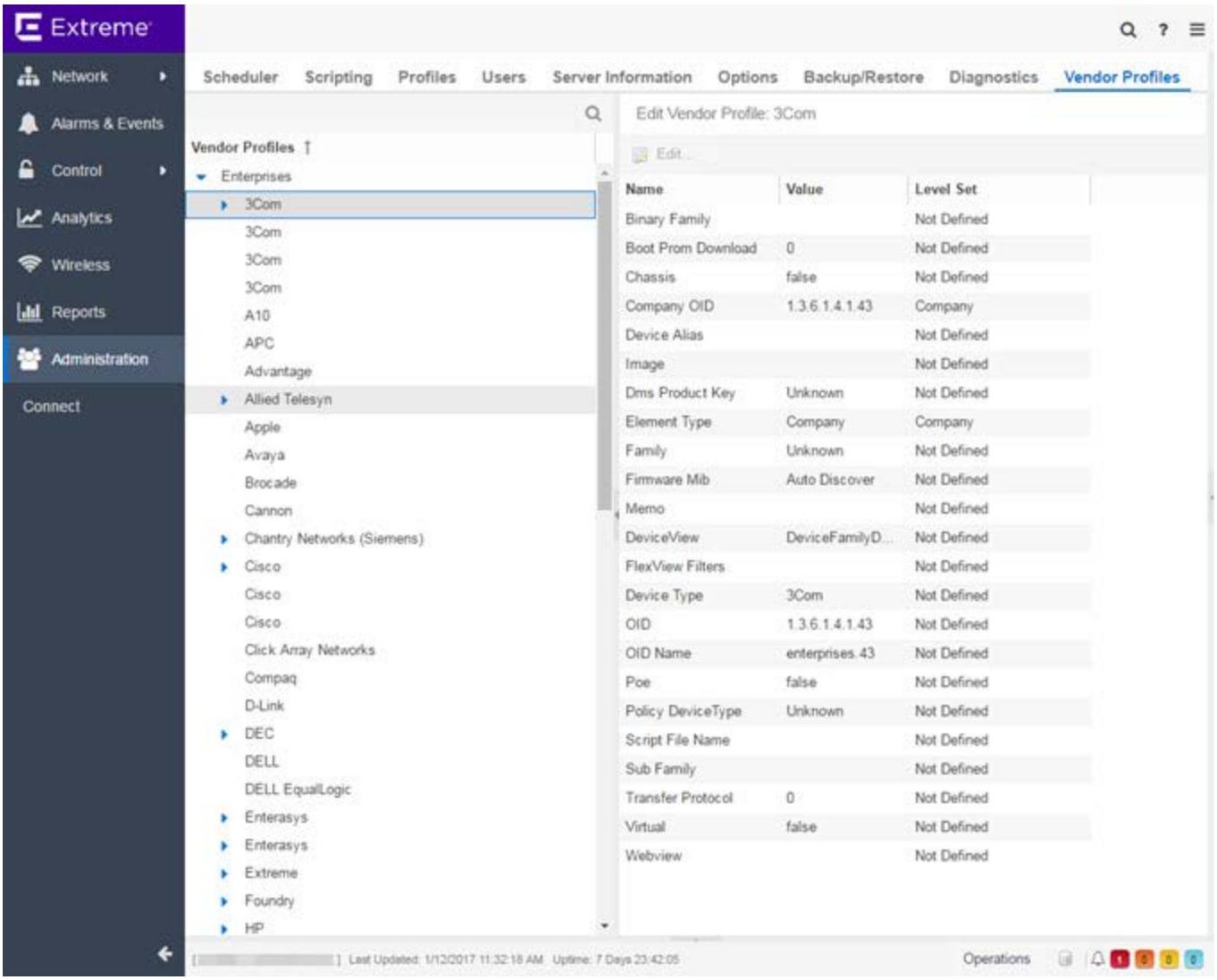
Vendor Profiles are a beta feature. To enable vendor profile functionality, contact Extreme Networks' Global Technical Assistance Center (GTAC).

IMPORTANT: Only make changes to this tab if you are an expert user. Incorrectly configuring this tab causes significant adverse effects in ExtremeCloud IQ Site Engine and can require you to reinstall.

To remove all user-defined Vendor Profile configurations and restore the default system configurations, select the **Restore to Defaults** button on the **Administration** > **Diagnostics** > **System** > **Vendor Profile Cache** tab.

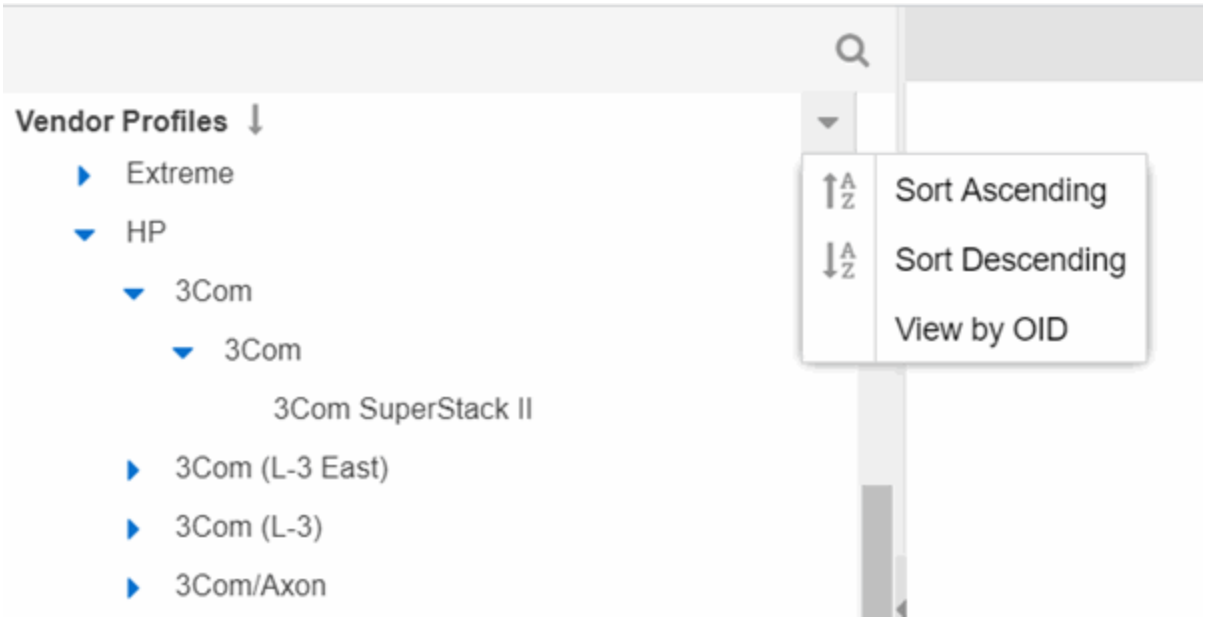
The **Vendor Profiles** tab is organized into two panels. The left panel contains a list of vendors and companies that manufacture networking devices. Nested within the company folder, if a device is part of a series of devices (known in ExtremeCloud IQ Site Engine as a device family), are folders for each device family. Within the device family folder are the individual device types that are a part of that device family. The device family is further defined by device subfamily. Any properties defined at the company or device family level also apply to the devices within that folder, however you can overwrite the default configurations by changing a device family or individual device.

The right panel contains the vendor profile for the vendor, company, device family, or device type you select in the left panel.



Vendor Profiles List

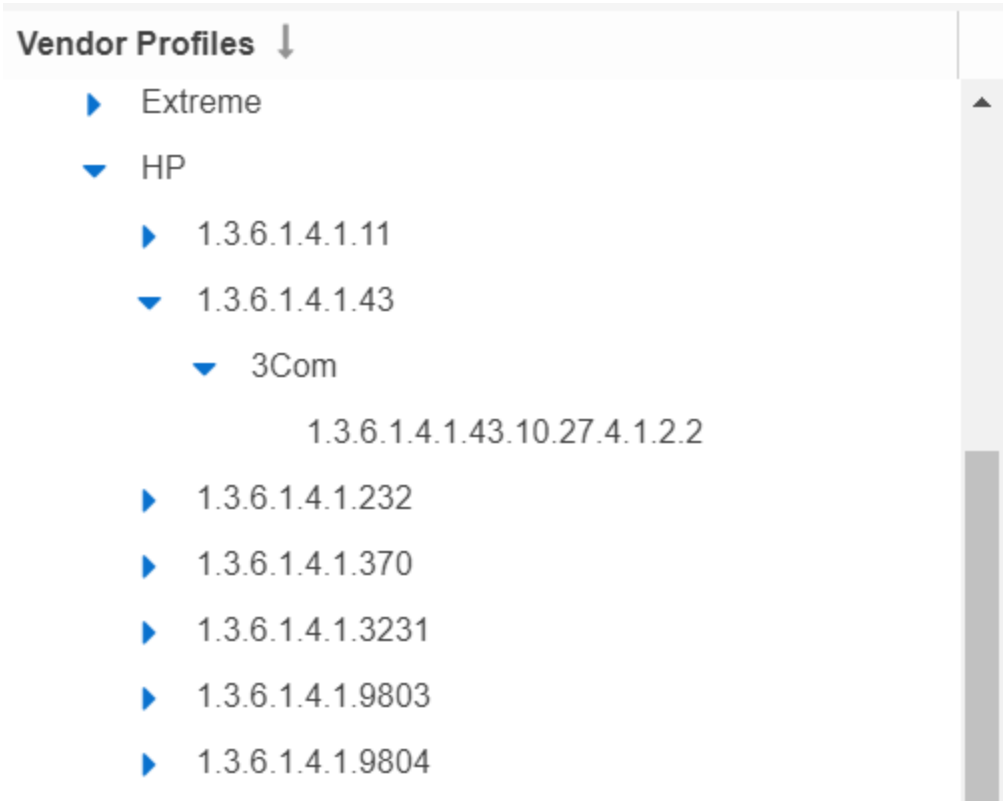
The left-panel of the **Vendor Profiles** tab contains a list of device vendors, displayed in alphabetical order. Select the drop-down list in the left-panel Vendor Profiles field to display the following options:



- **Sort Ascending**
  Displays the vendors in alphabetical order, from A to Z. This is the default sort option.
- **Sort Descending**
  Displays the vendors in reverse alphabetical order, from Z to A.
- **View by OID / View by text**
  Toggles between company Object Identifier and text in the left-panel

For those vendors with multiple products listed in ExtremeCloud IQ Site Engine, select the arrow icon beside the vendor name, company, or subfamily to display additional options related to that vendor. If the vendor's products are organized into product "families" or groups of products of the same type, the product family displays when expanding a vendor. Expanding the product family or a vendor with no product family displays individual devices for that vendor.

Selecting the **View by OID** option in the Vendor Profiles field drop-down list displays the vendor Object Identifier for the companies and devices in the left-panel tree:



Selecting the **View by text** option in the Vendor Profiles field drop-down list displays the companies and devices as text in the left-panel tree.

Select a vendor, product family, or product to open the vendor profile details in the right-panel.

Vendor Profile Details

The right-panel of the **Vendor Profiles** tab displays properties related to the vendor, device family, or device selected in the left-panel Vendor Profiles list. The right-panel only shows the Properties which have specific settings. Properties not displayed for the Device Type are either not applicable, or the Vendor Profile could be using the setting from the Device Type's Subfamily, Family, Company or Vendor.

The configuration of these fields determines how ExtremeCloud IQ Site Engine displays the element selected in the left-panel. Additionally, ExtremeCloud IQ Site Engine uses this information to determine the reports, filters, and scripts that apply to a device. It can be necessary to add a Property to a certain Device Type to configure it in ExtremeCloud IQ Site Engine.

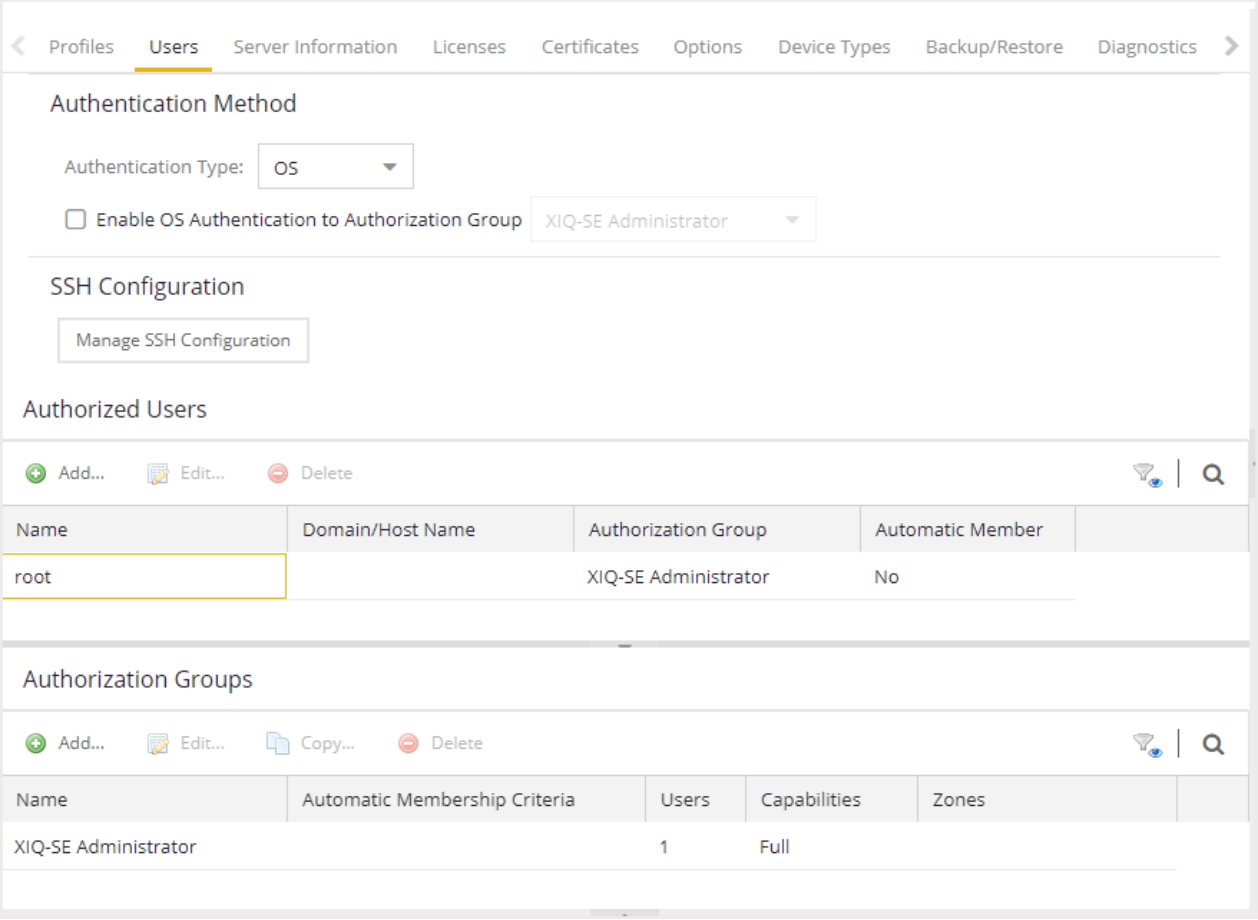
Users

Use the **Users** tab to create the authorization groups that define the access privileges (called *Capabilities*) to specific ExtremeCloud IQ Site Engine application features. When a user successfully authenticates, they are assigned membership in an authorization group. Based on their membership in a particular group, users are granted specific capabilities in the application. For example, create an authorization group called "IT Staff" that grants access to a wide range of capabilities and another authorization group called "Guest" grants a very limited range of capabilities.

The tab is also where you define the method used to authenticate users using ExtremeCloud IQ Site Engine. There are five authentication methods available: OS Authentication (the default), LDAP Authentication, RADIUS Authentication, TACACS+ Authentication, and Okta SSO Authentication.

NOTE: When changes to authentication and authorization configurations are made, clients must restart in order to be subject to the new configuration. Disconnect those clients affected by the changes made to your authentication and authorization configurations. Use the Client Connections tab in the Server Information window to help identify which clients are affected by the changes, and disconnect those clients.

For instructions about how to add authorized users in ExtremeCloud IQ Site Engine, see How to Add Users in ExtremeCloud IQ Site Engine.



Users/Groups Access

Select the **Acquire Lock** button to make changes to the **Users** tab. Only one user can make changes to the fields on this tab at one time, so selecting this button restricts access to other users.

Once you are finished making changes, select the button again to release the lock.

Authentication Method

Use this section to configure the method used to authenticate users who are attempting to launch an ExtremeCloud IQ Site Engine client or access the ExtremeCloud IQ Site Engine database using the ExtremeCloud IQ Site Engine Server Administration web page.

The following authentication methods are available:

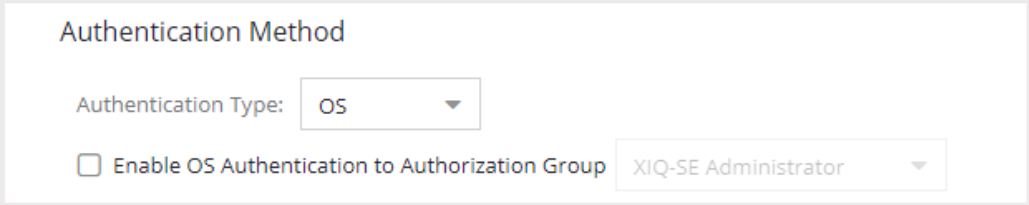
- OS Authentication *(the default)*
- LDAP Authentication
- RADIUS Authentication

- TACACS+ Authentication
- Okta SSO Authentication

WARNING: Changes to the **Authentication Type** are automatically saved to the server, which can prevent access to users.

OS Authentication (Default)

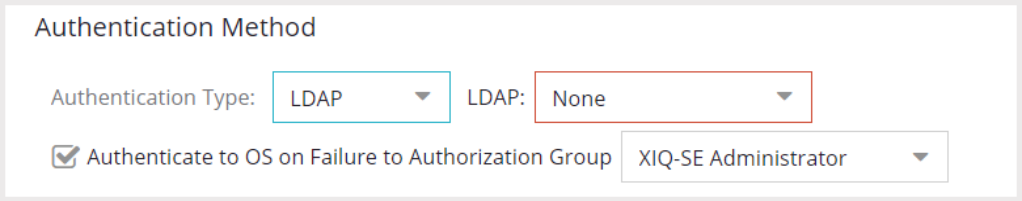
With this authentication method, the ExtremeCloud IQ Site Engine Server uses the underlying host operating system to authenticate users. Use the Authorized Users table to create a list of users allowed access and define their access capabilities.



If desired, enable Automatic Membership and specify an authorization group. The Automatic Membership feature allows the operating system to authenticate a user who is not manually added to the Authorized Users table, dynamically add that user to the table, and assign that user to the specified authorization group the first time they log in. These users are indicated by a **true** in the Automatic Member column of the Authorized Users table.

LDAP Authentication

With this authentication method, the ExtremeCloud IQ Site Engine Server uses the specified LDAP configuration to authenticate users.



Use the drop-down list to select the LDAP configuration for the LDAP server on your network that you want to use to authenticate users. Use the **New** menu option to add a new LDAP configuration or select the **Manage** option to manage your LDAP configurations.

With LDAP Authentication, configure dynamic assignment of users to authorization groups based on the attributes associated with a user in Active Directory. For example, create an authorization group that matches everyone in a particular organization, department, or location. When a user authenticates, the attributes associated with that user are matched against a list of criteria specified as part of each

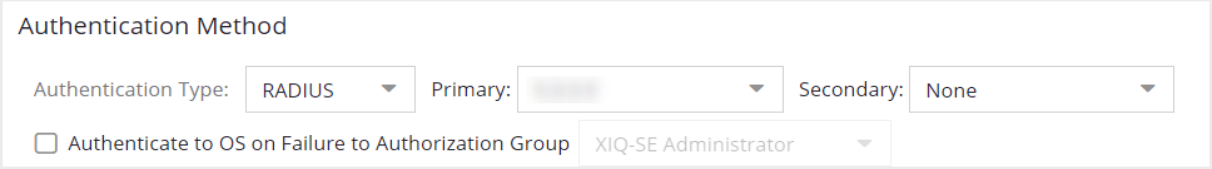
authorization group. The first group with criteria met by the user's attributes becomes the authorization group for that user. The user is then added to the Authorized Users table as an automatic member, with that authorization group.

The **Authenticate to OS on Failure To Authorization Group** feature provides the option to use OS Authentication automatic membership if the LDAP authentication fails. Users authenticated by the operating system are dynamically assigned to the specified authorization group when they log in, and are automatically added to the Authorized Users table. These users are indicated by a **true** in the Automatic Member column of the table.

RADIUS Authentication

With this authentication method, the ExtremeCloud IQ Site Engine Server uses the specified RADIUS servers to authenticate users.

NOTE: The RADIUS Authentication mode supports the PAP authentication type. RadSec is not supported.



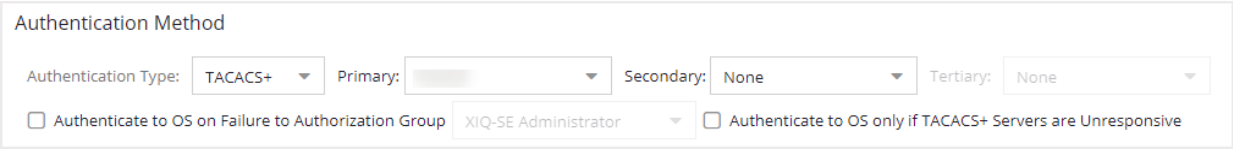
Use the drop-down list to select the primary RADIUS server and backup RADIUS server (optional) on your network that you want to use to authenticate users. Use the **New** menu option to add a RADIUS server, or select **Manage** to manage your RADIUS servers.

With RADIUS Authentication, configure dynamic assignment of users to authorization groups based on the attributes associated with a user in Active Directory. When a user authenticates, the attributes associated with that user are matched against a list of criteria specified as part of each authorization group. The first group with a criteria met by the user's attributes becomes the authorization group for that user. The user is then added to the Authorized Users table as an automatic member, with that authorization group.

The **Authenticate to OS on Failure to Authorization Group** feature provides the option to use OS Authentication automatic membership if the RADIUS server authentication fails. Users authenticated by the operating system are dynamically assigned to the specified authorization group when they log in, and are automatically added to the Authorized Users table. These users are indicated by a **true** in the Automatic Member column of the table. If selected, the RADIUS packets without Message-Authenticator attribute are dropped.

TACACS+ Authentication

With this authentication method, the ExtremeCloud IQ Site Engine Server uses up to three specified TACACS+ servers to authenticate users.



Use the drop-down list to select the primary server, the secondary server (optional), and the tertiary server (optional) on your network that you want to use to authenticate users. Use the **New** menu option to add a server via the Add TACACS+ Server window, or select **Manage** to manage your servers.

With TACACS+ authentication, users are dynamically assigned to authorization groups based on the attributes associated what that user in TACACS+ server. ExtremeCloud IQ Site Engine looks for the XMC-Authorization-Group attribute / value pair (for example, XMC-Authorization-Group=Domain Admin Group) and if that value matches the authorization group name, the user is associated with the group. If there is no XMC-Authorization-Group attribute being returned by TACACS+ server, other attributes (for examle, ip=ppp) are validated and used to authorize and associate the group to the user.

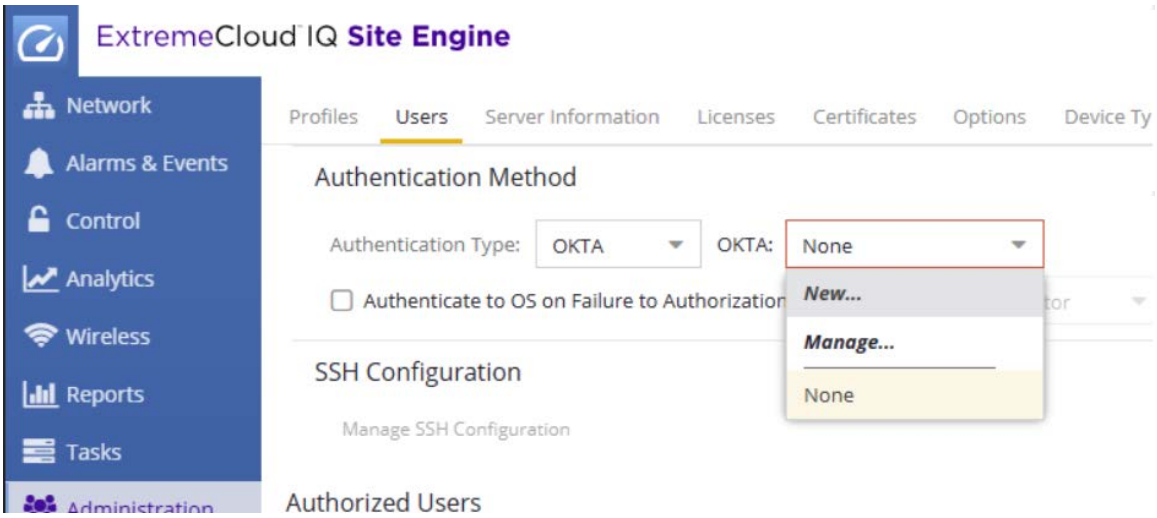
ExtremeCloud IQ Site Engine attempts to authenticate a client from the primary to the secondary and to the tertiary server in the event of communicating to the TACACS+ server. However, if a TACACS+ server responds with any status, the client does not fall through to the next server.

The **Authenticate to OS on Failure to Authorization Group** feature provides the option to use OS Authentication automatic membership if the TACACS+ server authentication fails. Users authenticated by the operating system are dynamically assigned to the specified authorization group when they log in, and are automatically added to the Authorized Users table. These users are indicated by a **true** in the Automatic Member column of the table.

Select the **Authenticate to OS Only if TACACS+ Servers are Unresponsive** checkbox to use OS Authentication only in the event the TACACS+ servers are not responding. If a user attempts to authenticate via a TACACS+ server and is denied when this checkbox is selected, ExtremeCloud IQ Site Engine does not then attempt to authenticate using the host operating system as a fall through.

Okta SSO Authentication

With the Okta Single Sign-On (SSO) authentication method the ExtremeCloud IQ Site Engine server can use the Okta SAML 2.0 standard for SSO.



Use the drop-down list to select the **OKTA** Authentication Type for the Okta service to authenticate users. Use the **New** menu option to add a new OKTA configuration or select the **Manage** option to manage your OKTA configurations.

When adding or editing the OKTA SAML Configuration authentication, configure the IdP SSO URL, IdP Issuer, and X.509 Certificate from the "View SAML setup instructions" in the Okta Admin Console configuration. The SP Entity ID is the "Audience URI" in the Okta Admin Console configuration. Also enter the Roles for Okta authenticated users.

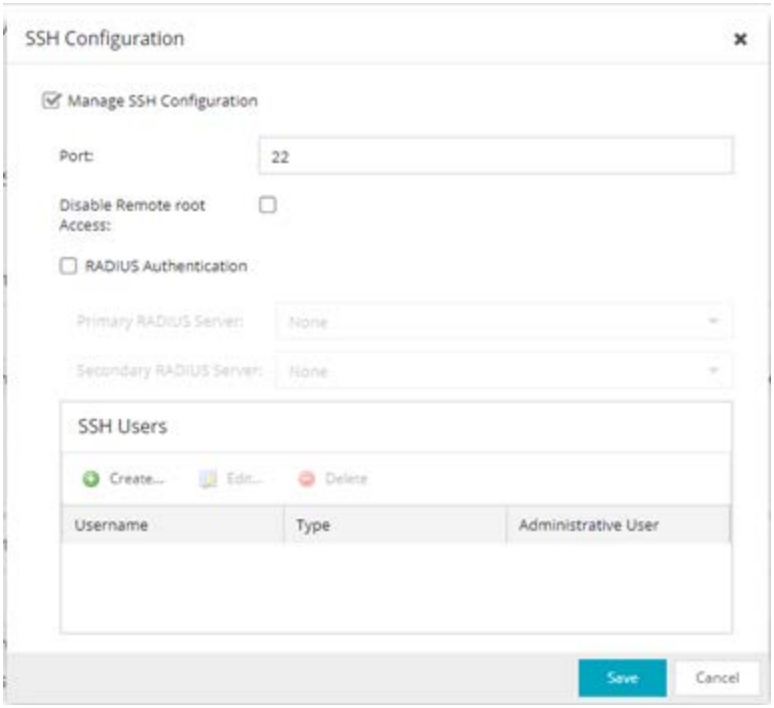
The **Authenticate to OS on Failure To Authorization Group** feature provides the option to use OS Authentication automatic membership if the Okta authentication fails. Users authenticated by the operating system are dynamically assigned to the specified authorization group when they log in, and are automatically added to the Authorized Users table. These users are indicated by a **true** in the Automatic Member column of the table.

For more information, see How to Integrate and Configure Okta SSO Authentication for ExtremeCloud IQ Site Engine Users

Network Settings

SSH configuration provides additional security features for the ExtremeCloud IQ Site Engine engine. Select the **Manage SSH Configuration** button to open the SSH Configuration window.

NOTE: This option requires **root** privileges. If the server is not running with root privileges then the desired configuration changes must be accomplished through the CLI.



Select the **Manage SSH Configuration** check box and provide the following SSH information.

Port

The port field allows you to configure a custom port to be used when launching SSH to the engine. The standard default port number is 22.

Disable Remote root Access

Select this option to disable remote root access via SSH to the engine and force a user to first log in with a real user account and then su to root (or use sudo) to perform an action. When remote root access is allowed, there is no way to determine who is accessing the engine. With remote root access disabled, the /var/log/message file displays users who log in and su to root. The log messages looks like these two examples:

```
sshd[19735]: Accepted password for <username> from 10.20.30.40 port 36777
ssh2
su[19762]: + pts/2 <username>-root
```

Enabling this option does not disable root access via the console. Do not disable root access unless you have configured RADIUS authentication or this disables remote access to the ExtremeCloud IQ Site Engine engine.

RADIUS Authentication

This option lets you specify a centralized RADIUS server to manage user login credentials for users that are authorized to log into the engine using SSH. Select a primary and backup RADIUS server to use, and use the table below to create a list of authorized RADIUS users.

For higher security, select the **Discard RADIUS response without Message-Authenticator attribute**.

You must ensure the Primary and Secondary RADIUS servers are configured to include the Message-Authenticator attribute in every RADIUS packet.

SSH Users Table

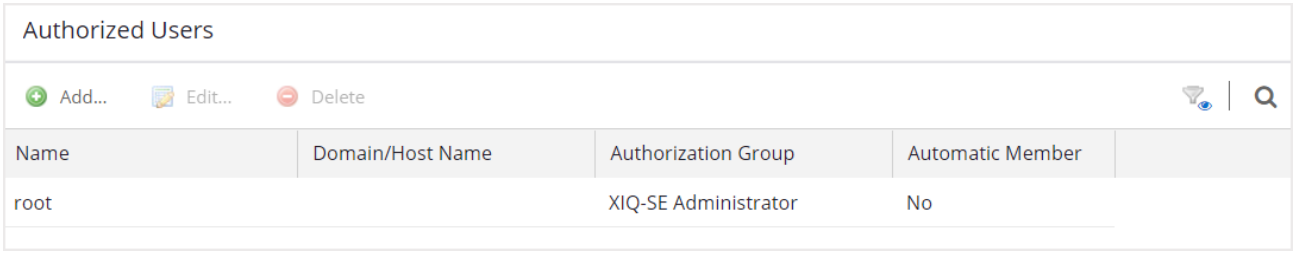
Use the toolbar buttons to create a list of users allowed to log in to the ExtremeCloud IQ Site Engine engine using SSH. You can add Local and RADIUS users and grant the user Administrative privileges, if appropriate. A user that is granted administrative rights can run sudo commands and commands that only a root user would be able to run. For example, some commands that require administrative rights to run would be:

sudo nacctl restart
sudo reboot
sudo nacdb

If a user is not granted administrative rights, they can log in, view files, and run some commands such a ping and ls.

Authorized Users Table

This table lists all of the users who are currently authorized to access the ExtremeCloud IQ Site Engine database and allows you to add, edit, and delete users and define a user's membership in an authorization group. Each entry shows the user name and authorization group for the user and whether the user is an Automatic Member.



For users manually added to the Authorized Users table using this tab, the Automatic Member column is **No**. These users are granted permission to log in, no matter what the authentication setting is set to: OS Authentication, LDAP Authentication, RADIUS authentication, or TACACS+ Authentication. All authentication methods allow the non-automatic users to log in.

User Name

The users added as authorized users. The column may also display the Client ID, a unique, system-defined numeric identifier for the client.

Domain/Host Name

The user's domain/hostname used to authenticate to the ExtremeCloud IQ Site Engine database.

Authorization Group

The authorization group to which the user belongs.

Automatic Member

A value of **Yes** indicates that the user is automatically added to the authorization group of LDAP, RADIUS, TACACS+, OKTA authentication, or the OS Authentication Automatic Membership feature. A value of **No** indicates that the user is an authorized user that was manually added to the table.

Add

Opens the Add/Edit User window, which allows you to define the username, domain, and authorization group for a new authorized user.

Edit

Opens the Add/Edit User window, which allows you to modify the authorization group membership for the selected user.

Delete

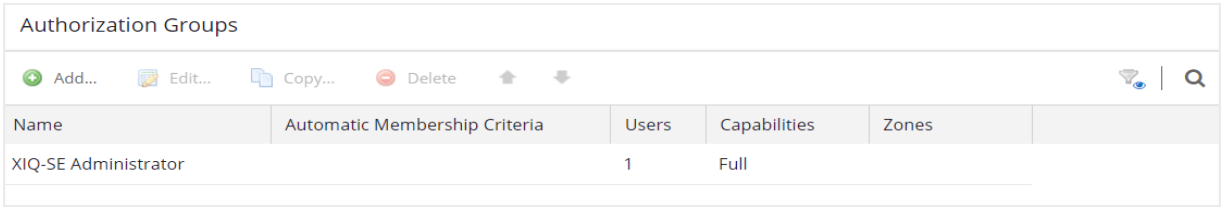
Removes the selected User from the Authorized Users table.

Reset 2FA

Resets the pairing of the two factor authentication app with the user account. The reset 2FA user account is provided the option to pair a new authentication application with the username.

Authorization Groups Table

This table lists all of the authorization groups created. Authorization groups define the access privileges to the ExtremeCloud IQ Site Engine application features. Based on their membership in a particular authorization group, users are granted specific capabilities in the application.



When users are added to the Authorized Users table, they are assigned an authorization group. With LDAP, RADIUS, or TACACS+ authentication, users are dynamically assigned to authorization groups based on the attributes associated with that user in Active Directory (or in TACACS+ Server for TACACS+ Authentication). The attributes are used to match against a list of criteria specified as part of each authorization group. The groups are checked in the order they are displayed in this table, from top to bottom. The first group with criteria matched by the user's attributes becomes the effective authorization group for that user.

Every user must be assigned to a group. A user whose attributes don't match any of the criteria specified for any of the groups are not authenticated and are unable to log in. Create a "catch-all" group (for example, you could use objectClass=person for an LDAP Active Directory), whose criteria is very generic and whose capabilities are highly restricted to allow access to these unauthenticated users.

This helps differentiate between a user who cannot authenticate successfully, and a user who does not belong to any group.

When ExtremeCloud IQ Site Engine is connected to ExtremeCloud IQ, the following Authorization Groups are automatically created. These authorization roles are applied to the user based on Single Sign-On (SSO) authentication from ExtremeCloud IQ:

Name	Role in ExtremeCloud IQ
XIQ-Administrator	Administrator
XIQ-Operator	Operator
XIQ-Monitor	Monitor
XIQ-Help Desk	Help Desk
XIQ-Observer	Observer
XIQ-Installer	Installer

Name

This is the name assigned to the group. The Netsight Administrator group is created during installation and is granted Full capabilities and access. This group cannot be deleted or changed, but its capabilities can be viewed.

Precedence

This column, hidden by default, is available if the **Authentication Method** is **LDAP**, **RADIUS**, or **TACACS+**. This indicates the order of precedence when a user is a member of multiple authorization groups. The authorization group with the higher precedence is the group to which the user is assigned. Use the **Up Arrow** and **Down Arrow** buttons to change the order of precedence for the authorization groups.

Automatic Membership Criteria

This column displays the membership criteria for automatic members defined for the associated group. Members authenticated via LDAP or RADIUS using **Automatic Membership** functionality are validated using the criteria defined here. Users created manually using an Authorization Group are not validated against the criteria defined in this field.

Users

This is the number of current members in the associated group.

Capabilities

This column summarizes the capabilities granted to the associated group: **Full** (all capabilities) or **Customized** (a subset of capabilities).

SNMP Redirect

This column, hidden by default, indicates whether users in the authorization group can edit the setting for Client/Server SNMP Redirect.

Auto Group

This column, hidden by default, indicates whether the group allows users to be automatically

added via LDAP or RADIUS authentication, or the OS Authentication Automatic Membership feature.

Zones
This column displays the end-system zones to which users in the authorization group have access.

Add
Opens the Add/Edit Group window, which allows you to define the capabilities and settings for a new group.

Edit
Opens the Add/Edit Group window, which allows you to modify the capabilities and settings for a selected group.

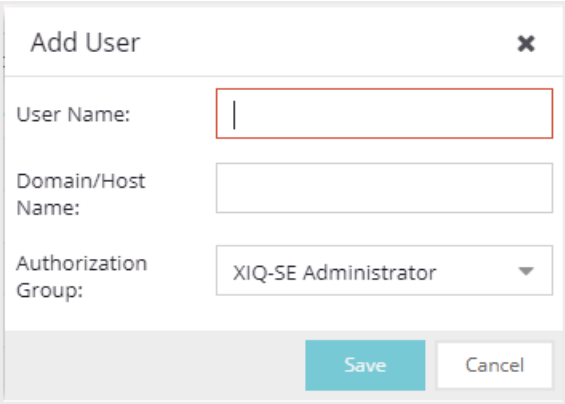
Delete
Removes the selected group from the Groups table.

Copy
Duplicates the selected group from the Groups table and creates a new group with identical capabilities.

Up Arrow and Down Arrow
Changes the order of precedence for the authorization groups.

Add/Edit User Window

This window lets you define a user's user name, domain, and membership in an authorization group. This information is used to authenticate the user to the ExtremeCloud IQ Site Engine database.



User Name
The name or Client ID for the user.

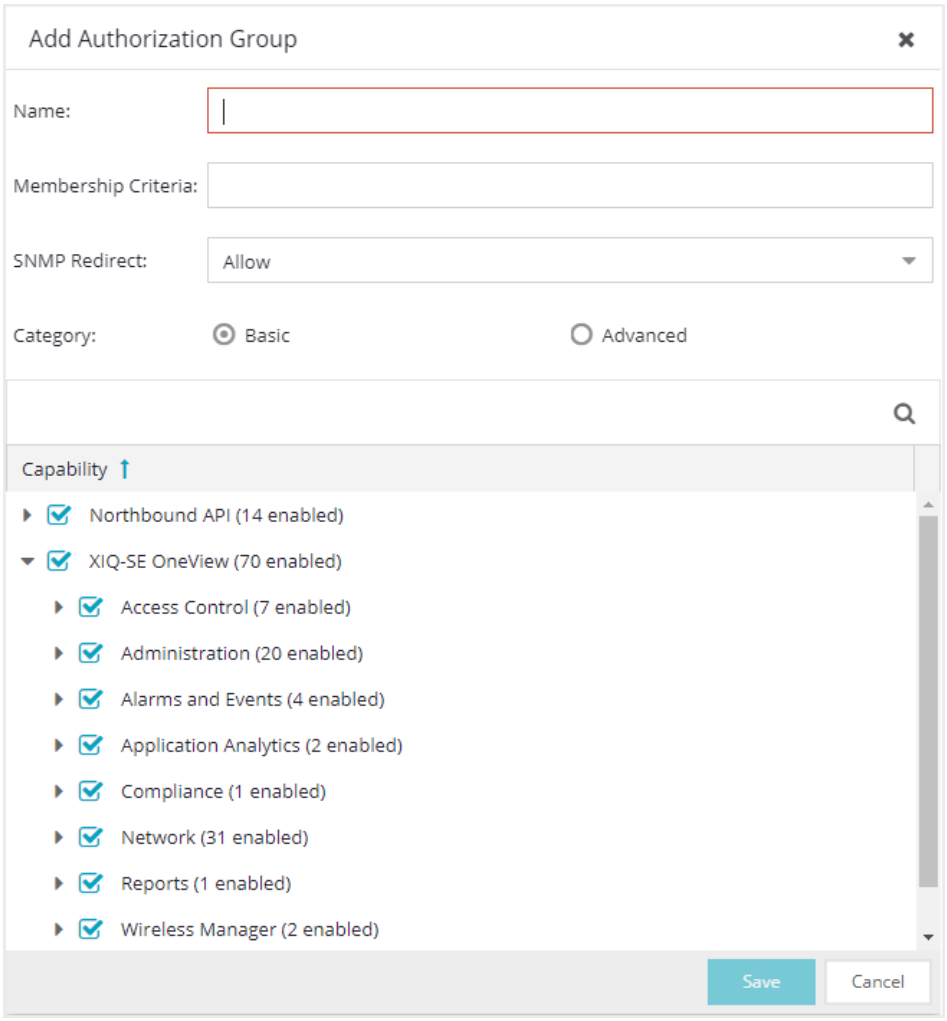
Domain/Host Name
The user's domain/hostname used to authenticate to the ExtremeCloud IQ Site Engine database.

Authorization Group

Use the drop-down list to select the authorization group to which the user is added.

Add/Edit Group Window

This window lets you define a new authorization group or edit an existing group. For additional information, see Authorization Group Capabilities.



Name

This is the name given to the group. When adding a group, enter any text string that is descriptive of the members of this group.

Membership Criteria

When a user is successfully authenticated using LDAP or RADIUS authentication, the Active Directory attributes associated with that user are used to match against this list of criteria to determine membership in the authorization group. The criteria is entered as name=value pairs, for example, department=IT (LDAP) or Service-Type=Framed-User (RADIUS). A user must have

the specified attribute with a value that matches the specified value in order to meet the criteria to belong to this group. Multiple name=value pairs may be listed using a semicolon (";") to separate them. However, a user is considered a member of the group if they match at least one of the specified criteria; they do not need to match all of them.

With a user authenticated using TACACS+ authentication, the TACACS+ server attributes associated with that user are used in the same way as LDAP or RADIUS authentication. However, the criteria is not needed to be entered to associate the authorization group if TACACS+ server returns 'XMC-Authorization-Group' attribute with a value. The value is the name of authorization group to associate to the user. ExtremeCloud IQ Site Engine looks for the XMC-Authorization-Group attribute first and then uses other attributes to match.

NOTE: The Netsight Administrator Group does not allow you to define membership criteria. Membership in the administrator group must be assigned manually using the Authorized Users table.

SNMP Redirect

- ALLOW — Lets users edit the setting for Client/Server SNMP Redirect.
- ALWAYS — Redirects all SNMP requests to the ExtremeCloud IQ Site Engine Server, regardless of the setting for Client/Server SNMP Redirect.
- NEVER — Never redirects SNMP requests to the ExtremeCloud IQ Site Engine Server, regardless of the setting for Client/Server SNMP Redirect.

Enable 2FA

This option enables two factor authentication for this group. An authentication code is required in addition to username and password. The authentication code can be generated in the user's paired authenticator application.

Capability Tab

Expand the Capability tree in this tab and select the specific capabilities granted to users who are members of this group. The capabilities are divided into suite-wide and application-specific capabilities. Access to a particular capability is granted when it is checked in the tree. For a description of each capability, see Authorization Group Capabilities.

Add Users

Users are given access to parts of ExtremeCloud IQ Site Engine based on the authorization group to which they are assigned. Assign a set of capabilities for each authorization group and then add users to each authorization group depending on the capabilities they require.

NOTE: This topic assumes devices are already added to the ExtremeCloud IQ Site Engine database. For additional information on discovering and adding devices, see Discover Devices in ExtremeCloud IQ Site Engine.

For a list of instructions outlining the initial setup of your network in ExtremeCloud IQ Site Engine, see ExtremeCloud IQ Site Engine Initial Configuration Checklist.

When you first log into ExtremeCloud IQ Site Engine the Administrator access through which you are currently logged in is the only set of user credentials.

This topic describes the process for adding users to ExtremeCloud IQ Site Engine, which is accomplished by performing the following steps:

1. Create Authorization Groups
2. Add Users to Authorization Groups
3. Select the Authentication Method

IMPORTANT: ExtremeCloud IQ Site Engine does not save passwords. Users you create are authenticated against the Operating System, the RADIUS server, the LDAP server, the TACACS+ server, or Okta SSO depending on the authentication method you select.

Create Authorization Groups

First, create authorization groups for each group of ExtremeCloud IQ Site Engine users.

1. Access the **Administration** > **Users** tab.
2. Select the **Acquire Lock** button in the Users/Groups Access section at the top of the tab. This button locks access to the tab for all other users and enables you to make changes to the authorization groups and authorized users.
3. Select the **Add** button in the Authorization Groups section at the bottom of the tab.
4. Enter the appropriate information for each authorization group using ExtremeCloud IQ Site Engine.
   The Capability section of the window enables you to expand each capability tree by selecting the arrow to the left of the checkbox to display more specific tasks. Select only those that apply to each user group. Additionally, you can search for a specific capability in the **Search** field above the tree.
5. Select the **Save** button to create the authorization group.
6. Repeat the process to create the necessary authorization groups.

Add Users to Authorization Groups

Next, use of the Administration > Users tab to create the users who require access to ExtremeCloud IQ Site Engine and add them to an authorization group depending on the level of access they require.

1. Select the **Add** button in the Authorized Users section.
2. Enter a User Name, a Domain/Host Name (if necessary), and select the Authorization Group with the appropriate level of access for the user.
3. Select the **Save** button to save the new user.
4. Repeat the process to add all ExtremeCloud IQ Site Engine users for each authorization group.

Select the Authentication Method

Finally, use Administration > Users tab to select the method by which users authenticate when accessing ExtremeCloud IQ Site Engine.

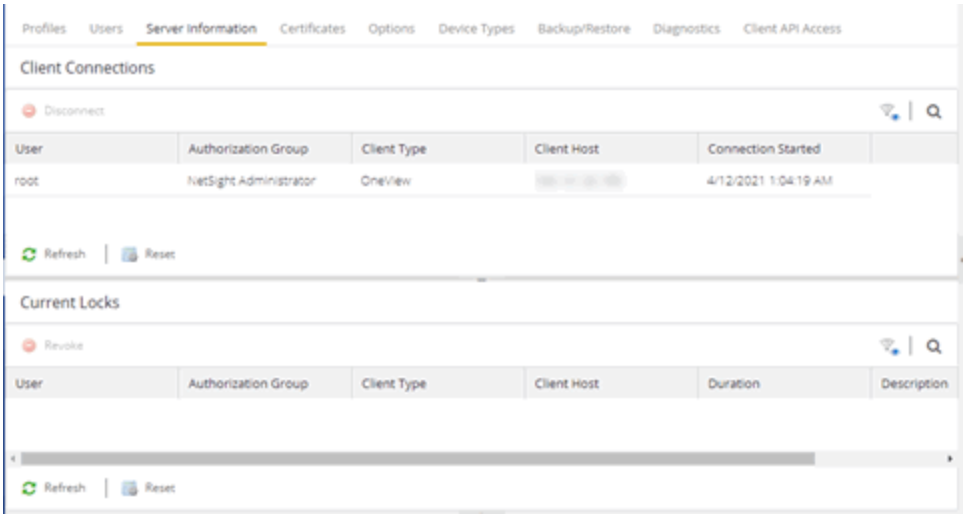
ExtremeCloud IQ Site Engine supports five different authentication methods to authenticate users: using the host Operating System, using an LDAP configuration, using RADIUS servers, using an TACACS+ configuration, or using an Okta SSO configuration.

1. Select the **Authentication Type** using the drop-down list in the Authentication Method section.
   The options change based on the **Authentication Type** selected.
2. Select the supplemental information based on the type selected.
3. Select the **Release Lock** button to enable other users to make changes.

The users you added now have access to the functionality you configured for their respective authorization group.

Server Information

Use the **Server Information** tab to view and manage ExtremeCloud IQ Site Engine client connections and locks. You must be assigned the appropriate user capabilities to access and use this tab.



Client Connections

The Client Connections table lists all of the currently connected clients for this server, with the most recent connection at the top. The list is automatically updated when clients connect or disconnect.

User
The name of the user that has connected to the server as a client.

Authorization Group
The authorization group to which the user belongs.

Client Type
The type of client, Console or another ExtremeCloud IQ Site Engine application.

Client Host
The name of the client host machine.

Connection Started
The date and time the client connection started.

Disconnect Button
This button disconnects the selected client. The client being disconnected receives a message saying that their connection will be terminated in 30 seconds. You must be assigned the appropriate user capability to disconnect clients.

Current Locks

The Current Locks table lets you view a list of currently held operational locks. Operational locks are used to control the concurrency of certain client/server operations. They are used in two ways:

- to lock a device while a critical operation is being performed, such as a firmware download.
- to lock a certain function so that only one user can access it at a time. For example, only one user can make changes to the **Users** tab at a time.

In the Current Locks table you can view information about each lock, such as who owns the lock, the duration of the lock, and a description of the lock. You can cancel a lock by selecting it in the table and selecting the **Revoke** button. When a lock is revoked, a message is displayed on the user's machine informing them that their use of the locked functionality is terminated. When the user acknowledges the message, the function closes. You must be assigned the appropriate user capability to revoke a lock.

User
The name of the user who initiated the lock.

Authorization Group
The authorization group the user belongs to.

Client Type
The type of client: Console or another ExtremeCloud IQ Site Engine application.

Client Host
The client host machine.

Duration
The amount of time the lock has been held.

Description
A description of the lock.

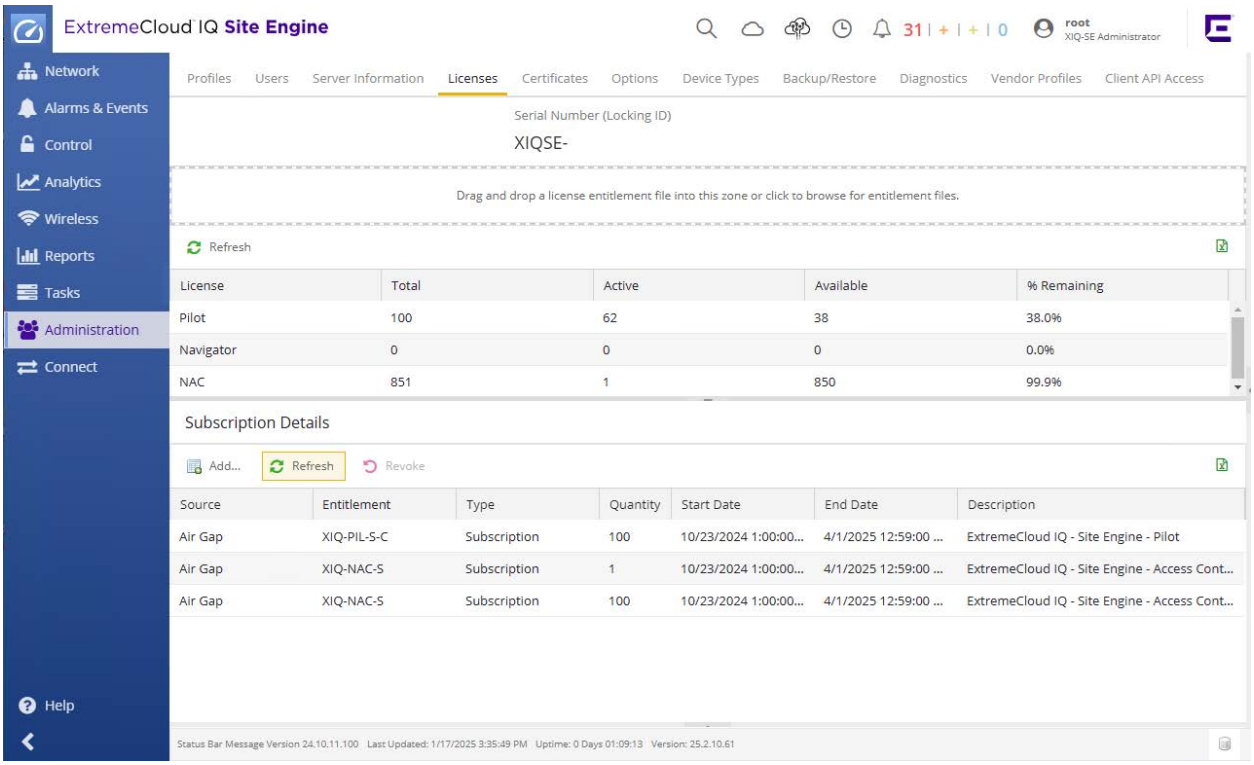
Refresh Button
This button refreshes the table and obtains updated lock information.

Revoke Button
This button removes the selected lock. When a lock is revoked, a message displays on the user's machine informing them their use of the locked functionality is terminated. When the user acknowledges the message, the function closes.

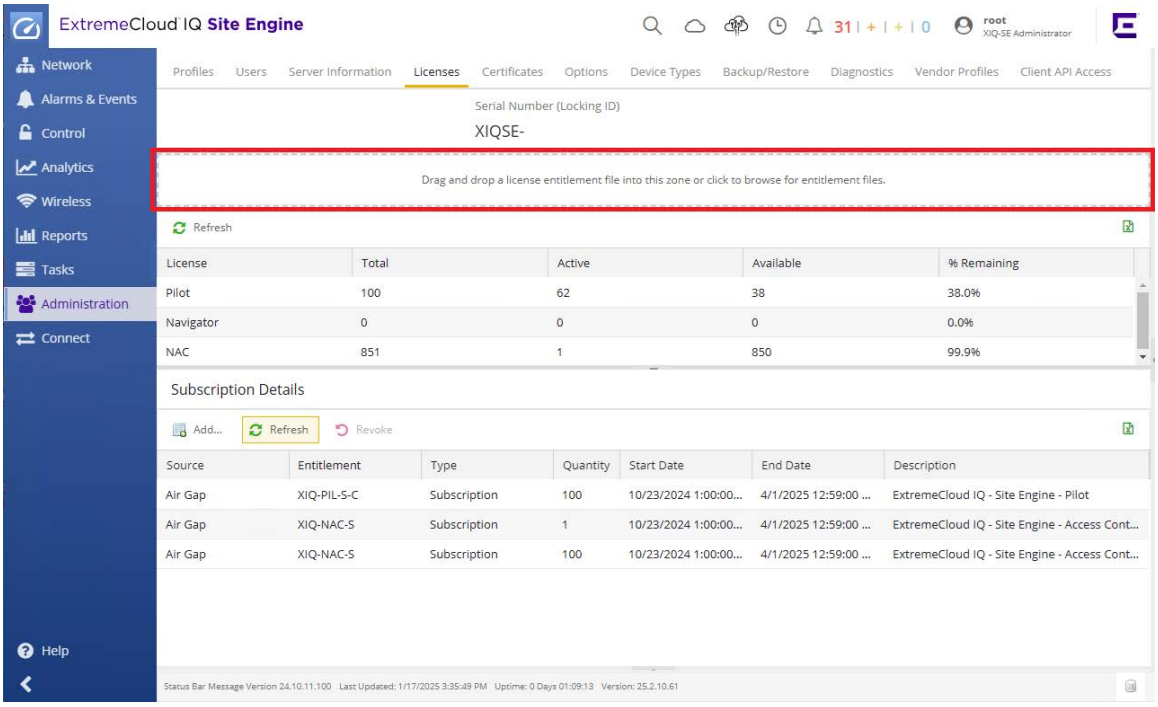
Updating a License

This Help topic provides instructions for updating a license in ExtremeCloud IQ Site Engine.

1. In ExtremeCloud IQ Site Engine, access the **Administration** > Licenses tab.



2. Drag and drop any license entitlement files in the open box above the table.

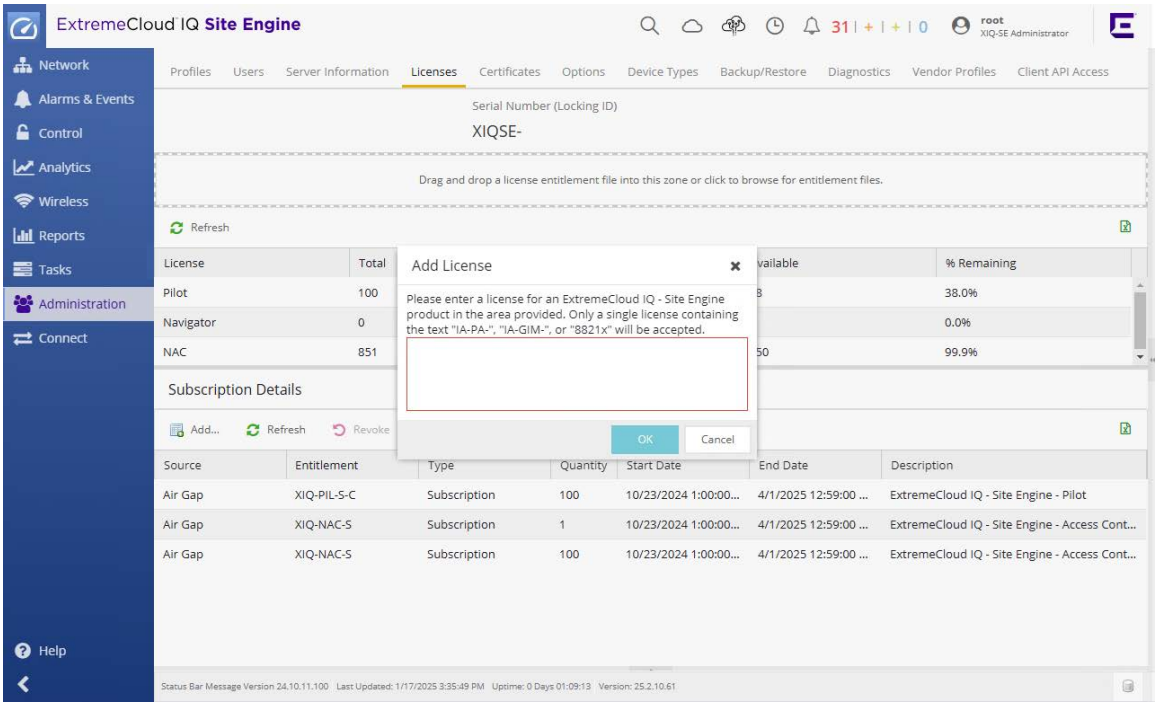


3. In Air Gap mode deployments, select the **Realign License Assignment** button to ensure optimal mapping of license Tier to devices.

Perform the following steps if you have a license key for enabling a specific feature, such as Posture Assessment, Virtual Sensor, or ExtremeCompliance.

1. Select the **Add** button to add additional license keys manually.

   The **Add License** dialog box appears.



2. Enter one license key beginning with "IA-PA-", "851xx", or "8821x".
3. Select **OK**.
4. Select the **Add** button and continue entering additional licenses one at a time.

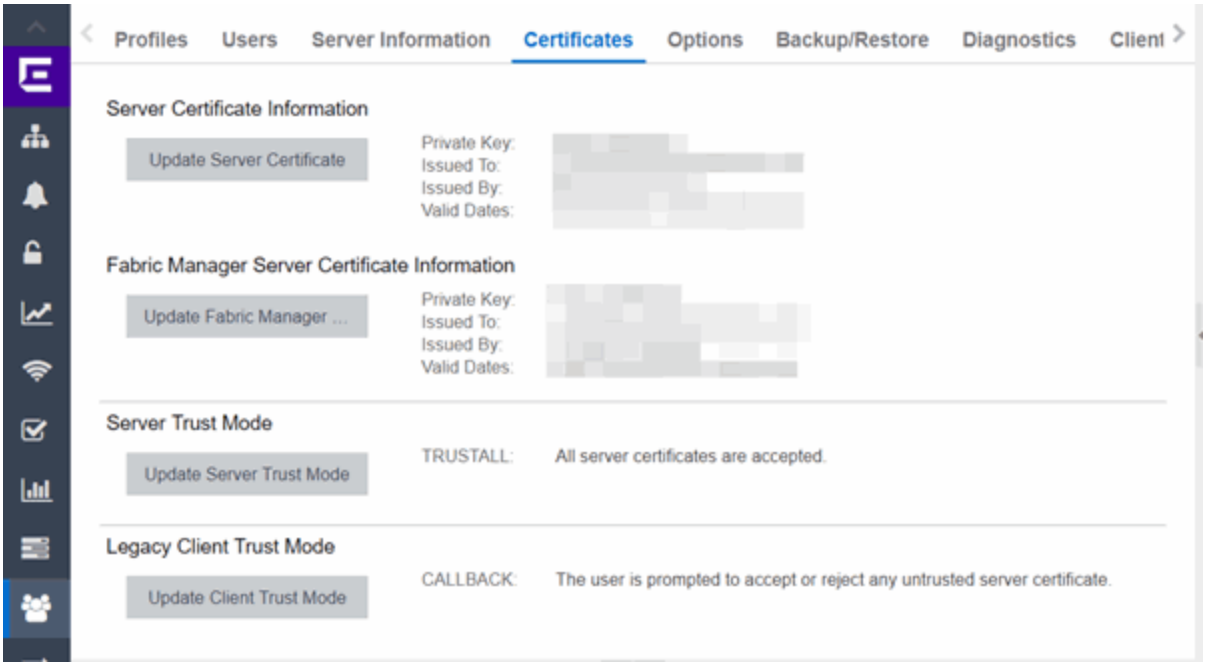
Your licenses are updated.

Certificates

Use the **Certificates** tab to manage certificates in ExtremeCloud IQ Site Engine.

Additionally, use this tab to perform the following:

- Update the ExtremeCloud IQ Site Engine server certificate by replacing the server private key and certificate.
- View and change the server trust mode that specifies how servers in the ExtremeCloud IQ Site Engine deployment handle certificates from other servers.
- View and change the client trust mode that specifies how legacy java application clients handle a server certificate.



Server Certificate Information

Select the **Update Server Certificate** button to open the Update Server Certificate window, where you can view and replace the ExtremeCloud IQ Site Engine server private key and certificate. For information and steps on how to update the certificate, see How to Update the Server Certificate.

Fabric Manager Server Certificate Information

Select the **Update Fabric Manager** button to open the Add Fabric Manager Certificate window, where you can view and replace the Fabric Manager server private key and certificate.

Server Trust Mode

This section displays the current server trust mode that specifies how servers in the ExtremeCloud IQ Site Engine deployment handle certificates from other servers. Select the **Update Server Trust Mode** button to open the Update Server Trust Mode window, where you can change the server trust mode.

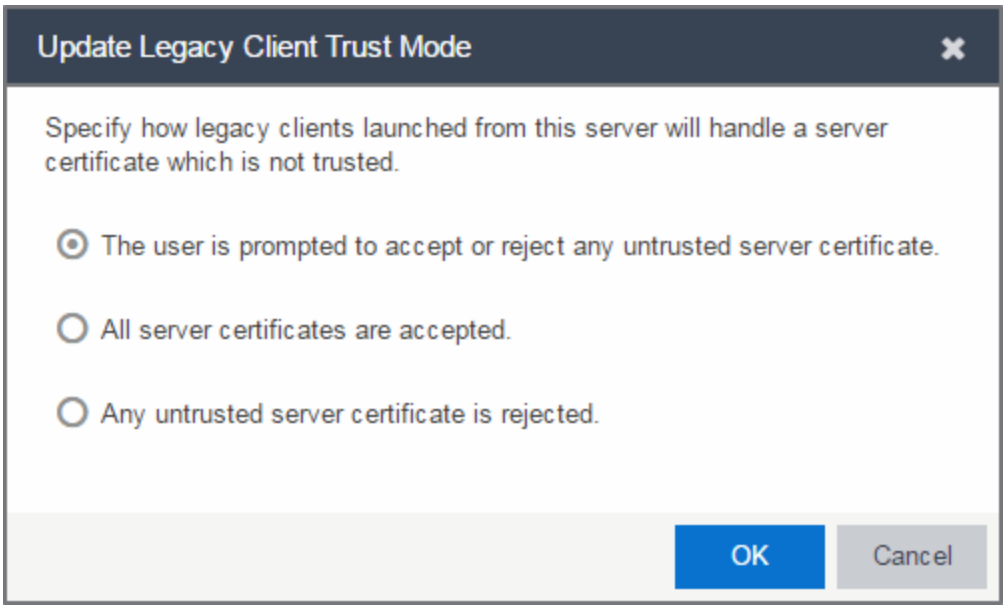
Legacy Client Trust Mode

This section displays the current client trust mode that specifies how legacy java application clients handle a server certificate. Select the **Update Legacy Client Trust Mode** button to open the Update Legacy Client Certificate Trust Mode window, where you can change the client trust mode.

- Update Server Certificate
- Add Fabric Manager Certificate
- Update Server Trust Mode
- Update Client Certificate Trust Mode

Update Legacy Client Trust Mode Window

Use this window to update the client certificate trust mode that specifies how ExtremeCloud IQ Site Engine legacy java application clients handle the server certificates they receive. This option is only applicable if you use legacy java applications. Access this window from the **Administration** > **Certificates** tab.



ExtremeCloud IQ Site Engine use server certificates to provide secure communication between the ExtremeCloud IQ Site Engine server and legacy java application clients. When a server certificate is replaced, ExtremeCloud IQ Site Engine clients must be configured to trust the new certificate. A trust mode is used to determine how all clients handle updated certificates. You can set the client trust mode to one of the following options:

The user is prompted to accept or reject any untrusted server certificate.

If a client encounters a new certificate that is does not trust, the user is prompted to either accept or reject the new certificate. If the server certificate is replaced and the user expects to see the new certificate, then they can accept the certificate if it is correct. If the server certificate is not replaced and the client inadvertently connected to a server that is not trusted, then the user can reject the certificate.

If this option is selected, the Administration > Certificates tab displays the Trust Mode status (for example, CALLBACK) and its definition in the details field to the right of the **Update** button.

All server certificates are accepted.

All server certificates are accepted without a trust check. Use this option if there is no possibility for an untrusted client to connect to a server and the user does not need to be prompted to accept or reject a new certificate.

If this option is selected, the Administration > Certificates tab displays the Trust Mode status (for example, TRUSTALL) and its definition in the details field to the right of the **Update** button.

Any untrusted server certificate is rejected.

If a client encounters a new certificate that is does not trust, the certificate is rejected and the client connection fails. While this option is the most secure, if the server certificate is replaced, the new certificate is rejected. If you are replacing a server certificate, do not use this trust mode until all clients indicate they trust the new certificate.

If this option is selected, the Administration > Certificates tab displays the Trust Mode status (for example, NORMAL) and its definition in the details field to the right of the **Update** button.

For more information on how to use trust modes, see Advanced Security Options in the Secure Communication Help topic.

- Certificates Tab
- Update Server Certificate Trust Mode Window

Update Server Certificate Window

The ExtremeCloud IQ Site Engine server uses a private key and server certificate to provide secure communication for administrative web pages, ExtremeCloud IQ Site Engine and ExtremeControl Dashboard tools, and for internal communication between servers. Use the Update Server Certificate window to replace the ExtremeCloud IQ Site Engine server certificate. Access this window from the **Administration** > **Certificates** tab.

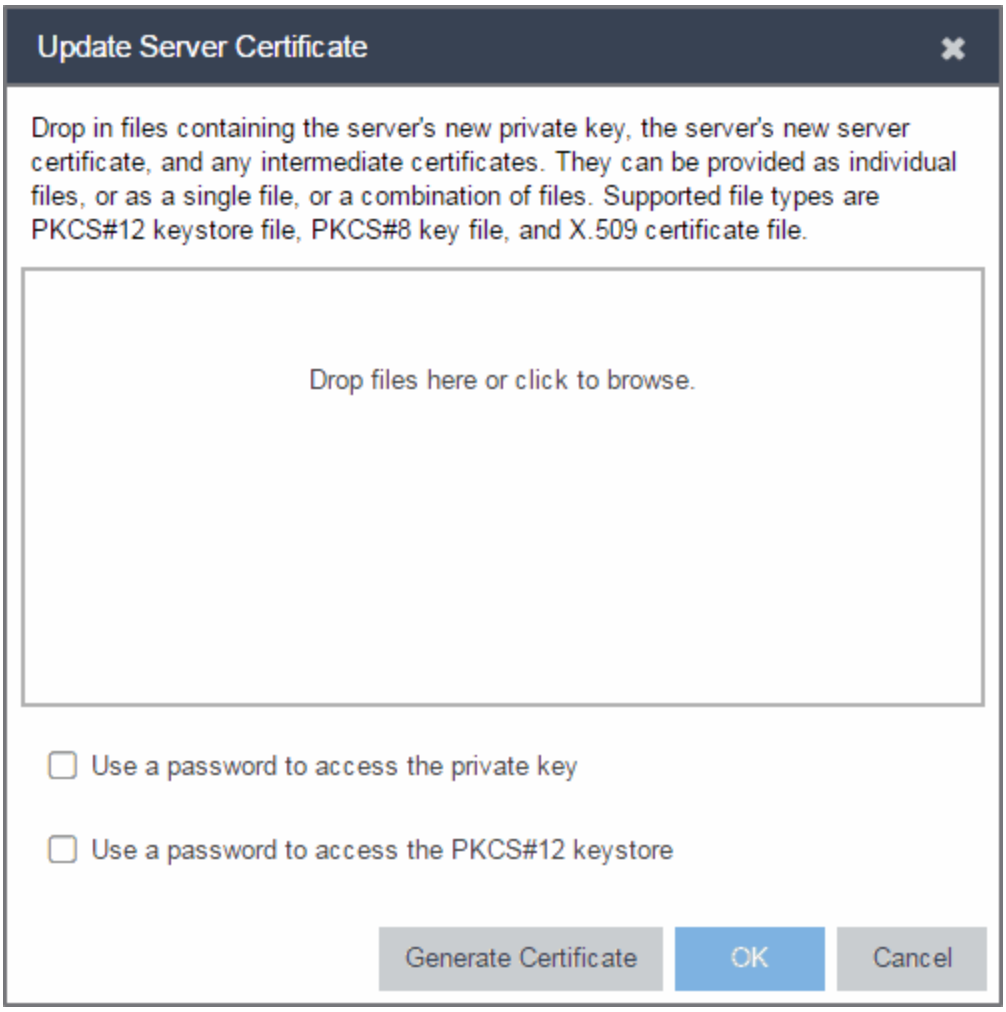
During installation, ExtremeCloud IQ Site Engine generates a unique private server key and server certificate. While these provide secure communication, there can be cases where you want to update the ExtremeCloud IQ Site Engine server certificate to a custom certificate provided from an external certificate authority, or add certificates in order to meet the requirements of external components with which ExtremeCloud IQ Site Engine must communicate. Additionally, you can use a "browser-friendly" certificate so that users don't see browser certificate warnings when they access web pages. For complete instructions on replacing and verifying the certificate, see How to Update the Server Certificate.

After you have updated the certificate, you must restart the ExtremeCloud IQ Site Engine server to deploy the new private key and server certificate.

NOTE: Whenever the ExtremeCloud IQ Site Engine server certificate is changed, other ExtremeCloud IQ Site Engine components can be affected by the change and stop trusting the server. You can specify how ExtremeCloud IQ Site Engine clients and other servers handle updated certificates by configuring the client trust mode and server trust mode settings. Before updating the ExtremeCloud IQ Site Engine server certificate, be sure that the client and server trust modes are configured to trust the new certificate. For more information, see Update Client Certificate Trust Mode window and Update Server Certificate Trust Mode window.

Drag and drop files containing the private key, the server certificate, and any intermediate (chained) certificates provided by the certificate authority. Add the files in any order. For complete instructions on replacing and verifying the certificate using this option, see How to Update the ExtremeCloud IQ Site Engine Server Certificate.

NOTE: Provide certificates for all certificate authorities that need to be trusted. You cannot append to an existing list.



Use a password to access the private key

Select the checkbox and supply the private key password in the field, if the private key is encrypted with a password. If you do not have the private key, refer to the instructions for generating them.

Use a password to access the PKCS#12 keystore

Select the checkbox and supply the keystore password in the field, if the PKCS#12 keystore is protected with a password.

Generate Certificate

Select **Generate Certificate** to automatically generate a new private key and certificate using the same method that occurs when ExtremeCloud IQ Site Engine is installed. Using this method does not require you to provide any files or passwords.

OK

Select **OK** to save your changes. After the ExtremeCloud IQ Site Engine server is restarted, the **Administration > Certificates** tab displays the following updated information:

- Private Key
- Issued To
- Issued By
- Valid Dates

Cancel

Select **Cancel** to close the window and discard your changes.

- Certificates Tab
- Update Server Certificate Trust Mode Window
- Update Client Certificate Trust Mode Window

Add Fabric Manager Certificate (Legacy)

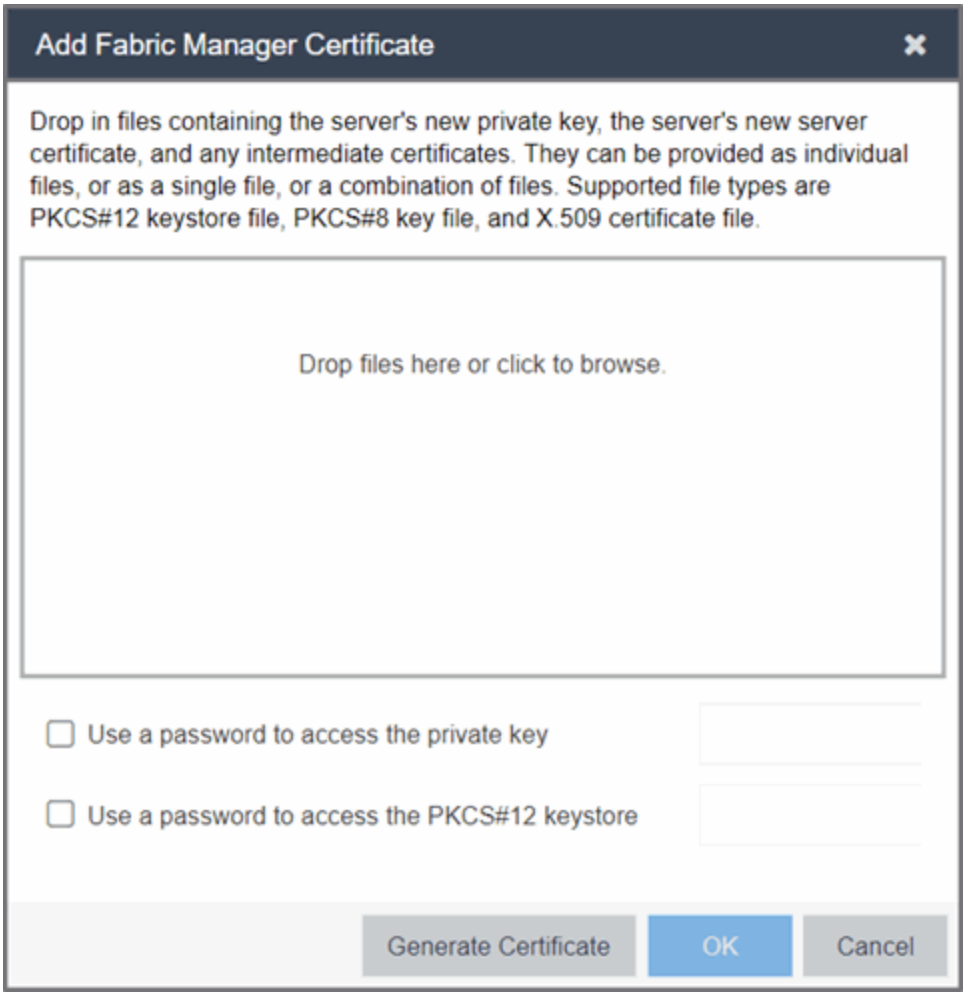
The Fabric Manager server uses a private key and server certificate to provide secure communication for administrative web pages, ExtremeCloud IQ Site Engine Dashboard tools, and for internal communication between servers. Use the Add Fabric Manager Certificate window to replace the Fabric Manager server certificate. Access this window from the **Administration** > **Certificates** tab.

This window is only available when Fabric Manager is installed.

During Fabric Manager installation, the Fabric Manager Certificate Server generates a unique private server key and server certificate for Fabric Manager. While these provide secure communication, there can be cases where you want to update the Fabric Manager server certificate to a custom certificate provided from an external certificate authority, or add certificates to meet the requirements of external components with which Fabric Manager must communicate. Adding or updating Fabric Manager certificates works like adding or updating ExtremeCloud IQ Site Engine certificates except you use the Fabric Manager Certificate window.

After you have updated the certificate, you must restart Fabric Manager to deploy the new private key and server certificate.

Drag and drop files containing the private key, the server certificate, and any intermediate (chained) certificates provided by the certificate authority. Add the files in any order. Provide certificates for all certificate authorities that need to be trusted. You cannot append to an existing list.



Use a password to access the private key

Select the checkbox and supply the private key password in the field, if the private key is encrypted with a password. If you do not have the private key, refer to the instructions for generating them.

Use a password to access the PKCS#12 keystore

Select the checkbox and supply the keystore password in the field, if the PKCS#12 keystore is protected with a password.

Generate Certificate

Select **Generate Certificate** to automatically generate a new private key and certificate using the same method that occurs when Fabric Manager is installed. Using this method does not require you to provide any files or passwords.

OK

Select **OK** to save your changes. After the ExtremeCloud IQ Site Engine server is restarted, the **Administration > Certificates** tab displays the following updated information:

- Private Key
- Issued To
- Issued By
- Valid Dates

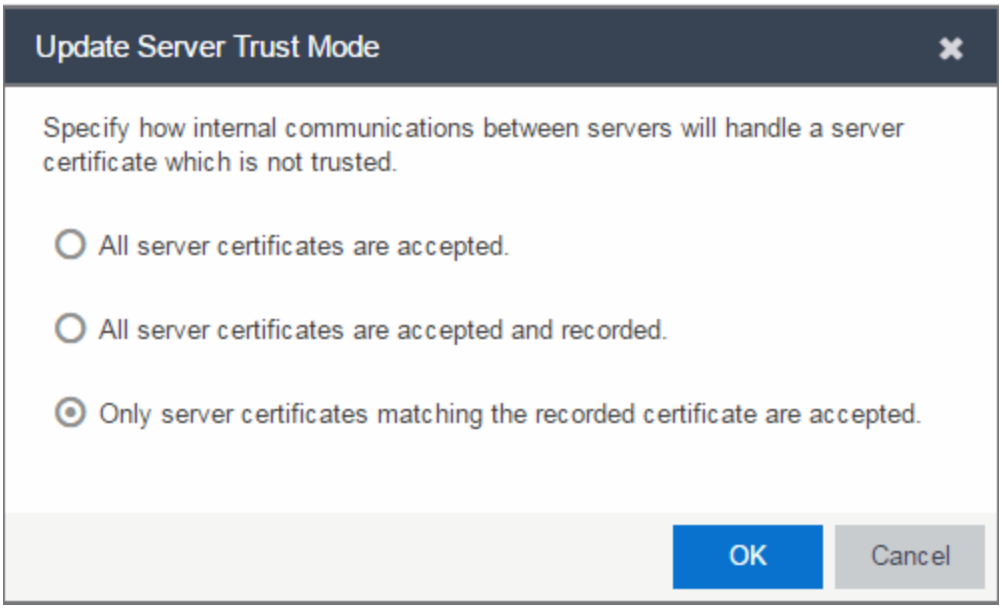
Cancel

Select **Cancel** to close the window and discard your changes.

- Certificates Tab
- Update Server Certificate Trust Mode Window

Update Server Trust Mode Window

Use this window to set the server certificate trust mode that specifies how all the servers in your ExtremeCloud IQ Site Engine deployment handles certificates received from other servers. Access this window from the Administration > **Certificates** tab.



Depending on your deployment, there can potentially be many servers in ExtremeCloud IQ Site Engine and Access Control. For example, there is the ExtremeCloud IQ Site Engine server, the Access Control engine servers, and Access Control assessment servers. In addition, there can be external servers such as LDAP servers with which both ExtremeCloud IQ Site Engine and Access Control can communicate. As these different servers communicate, they use server certificates to determine whether or not they trust each other.

The trust mode is used to specify how the servers handle the certificates they receive from other servers. You can set the trust mode to one of the following options:

All server certificates are accepted.

All certificates from other servers are accepted without a trust check. This mode is primarily used while setting up an ExtremeCloud IQ Site Engine/Access Control deployment, and is also suitable when the network is sufficiently protected from spoofing attacks.

Use this mode when troubleshooting trust problems on the network. It allows the ExtremeCloud IQ Site Engine server to communicate with all Access Control engines, and configure those engines to accept all certificates. This restores any communication broken due to a trust issue and allows you to resolve the problem from Access Control.

If this option is selected, the Administration > Certificates tab displays the Trust Mode status (for example, TRUSTALL) and its definition in the details field to the right of the **Update** button.

All server certificates are accepted and recorded.

All certificates from other servers are accepted without a trust check. Additionally, each server records the certificate that it receives and associates that certificate with the sending server. In this way, each server builds their own set of recorded certificates, creating a list of certificates that they trust.

Use this mode initially until all servers build a complete set of required certificates and then change the mode to **Only server certificates matching the recorded certificate are accepted**. It is important to give this phase enough time so that connections between the various servers can take place and all certificates are recorded. Administrators must ensure that no servers are spoofed during the time this mode is used. When you are confident that all certificates are exchanged and recorded, change the trust mode to **Only server certificates matching the recorded certificate are accepted**.

If this option is selected, the Administration > Certificates tab displays the Trust Mode status (for example, IMPORT) and its definition in the details field to the right of the **Update** button.

Only server certificates matching the recorded certificate are accepted.

Any certificate from another server must match the certificate recorded for that server when the mode is set to **All server certificates are accepted and recorded**. If the server certificate does not match, then the server is not trusted.

This mode provides an extra level of security intended to detect and prevent someone from spoofing a server. If an IP address or hostname is hijacked and connections are routed to another server, that server is not trusted. While this mode is the most secure, if any server certificate is replaced, the new certificate is rejected. Therefore, if you are replacing a server certificate, select **All server certificates are accepted and recorded** until the new certificate is recorded.

If this option is selected, the Administration > Certificates tab displays the Trust Mode status (for example, LOCKED) and its definition in the details field to the right of the **Update** button.

When the trust mode is changed, the ExtremeCloud IQ Site Engine server is immediately changed to use the new mode. Access Control engines begin using the new trust mode when enforced.

For more information on how to use trust modes, see Advanced Security Options in the Secure Communication Help topic.

- Certificates Tab
- Update Client Certificate Trust Mode Window

Update the Server Certificate

Follow these instructions to change the server key and certificate generated during installation in ExtremeCloud IQ Site Engine. While these provide secure communication, you can update to a certificate provided from an external certificate authority, or add certificates in order to meet the requirements of external components with which ExtremeCloud IQ Site Engine must communicate. You can also use a "browser-friendly" certificate so that users don't see browser certificate warnings when they access web pages.

You need a server private key and server certificate to perform the certificate replacement.

Some instructions in this Help topic use OpenSSL software to perform certain tasks. OpenSSL is available on the ExtremeCloud IQ Site Engine engine or can be downloaded from http://www.openssl.org. After downloading and installing OpenSSL, add the OpenSSL tool to your path using the instructions in Add OpenSSL to Your Path in the Secure Communication Help topic. Other software tools can be used to perform these tasks, if desired.

Instructions on:

- Certificate Requirements
- Replacing the Certificate
- Verifying the Certificate
- Generating a Server Private Key and Server Certificate
- Generating a Server Private Key and Server Certificate using CLI

Certificate Requirements

Generate the server certificate using the RSA or DSA server private key (in PKCS #8 format). For "browser-friendly" certificates, the server certificate should identify the ExtremeCloud IQ Site Engine server by its fully qualified host name.

NOTE: Elliptical Curve (EC) and ED25519 private key formats are not supported.

If your certificate authority (CA) provides additional intermediate certificates, provide those as well. Use the intermediate certificates in whatever format the CA provides them: in individual files, in a bundle file, or in the same file as the server certificate. ExtremeCloud IQ Site Engine also accepts PKCS#12 keystore files, which can contain both a private key and certificates. Enter the PKCCS#12 file here.

NOTE: Use the following OpenSSL command where <server.key> is the original non-PKCS #8 formatted key file to convert your key file to a PKCS #8 format. (OpenSSL is available on ExtremeCloud IQ Site Engine and ExtremeControl engines. The server.key file can be copied and converted on either engine.)

```
openssl pkcs8 -provider default -provider legacy -topk8 -in
<server.key> -out server-pkcs8.key -nocrypt
```

Replacing the Certificate

The following steps assume you generated a replacement server private key and server certificate.

NOTE: Whenever the ExtremeCloud IQ Site Engine server certificate is changed, other ExtremeCloud IQ Site Engine components can be affected by the change and stop trusting the server. ExtremeCloud IQ Site Engine clients and other servers must be configured to handle updated certificates using the client certificate trust mode and server certificate trust mode settings. Before updating the ExtremeCloud IQ Site Engine server certificate, be sure that the client and server trust modes are configured to trust the new certificate. For more information, see Update Client Certificate Trust Mode window and Update Server Certificate Trust Mode window.

To replace the server private key and server certificate:

1. Access the **Administration** > **Certificates** tab.
2. Select the **Update Server Certificate** button. The Update Server Certificate window opens.
3. Drag and drop a private key, certificate file, or a keystore file. Select in the box to browse for the file.

   A private key file must be encoded as a PKCS #8 file.

   Use a certificate file as the server certificate and any intermediate or chained certificates.

   Use a PKCS#12 keystore file to provide the private key, or certificates, or both.
4. Select **Use a password to access the private key** if the private key is encrypted in the key file or the keystore file. Enter the password in the field.
5. Select **Use a password to access the PKCS#12 keystore** if the keystore file is protected with a password. Enter the password in the field.
6. Select **OK**.

   A confirmation window listing your file information displays.
7. Confirm that the information you provided is correct.

8. Select **Yes** to proceed with the certificate replacement.

   The private key and server certificate updates on the ExtremeCloud IQ Site Engine server.
9. Restart the ExtremeCloud IQ Site Engine server to deploy the new private key and server certificate.

Verifying the Certificate

When the new server certificate is installed and the server restarts, use one of the following methods to verify the server is now using the proper server certificate.

Use a Browser

1. Access the ExtremeControl Dashboard web page at `https://<Server FQDN>:8443/Monitor/jsp/nac/dashboard.jsp.` or the ExtremeCloud IQ Site Engine web page at `https://<Server FQDN>:8443/Monitor/jsp/reporting/reporting.jsp`.
2. Verify no browser warnings display when you access the web page, if using a "browser-friendly" certificate.
3. Use your browser to view the certificate used:
   - Internet Explorer 7.0 or later: `Select the lock icon to the right of the URL address > View Certificates`
   - Microsoft Edge: `Select the lock icon to the left of the URL address > Connection is secure > certificate icon`
   - Mozilla Firefox 3.5 or later: `Select the lock icon to the left of the URL address > Connection Secure > More information > View Certificate`

Use OpenSSL

1. Use OpenSSL to test the server connection with the following command:
   ```
   openssl s_client -connect <Server IP>:8443
   ```
2. The output from this program includes a section titled "Certificate chain". This enumerates the certificates returned by the server. For each certificate, the Subject and the Issuer are displayed. With multiple certificates, if the certificates are in the proper order, the issuer of each certificate matches the subject of the following certificate. Here is a sample output from

the program:

```
Certificate chain
 0 s:/O=myns.enterprise.com/OU=Domain Control Validated/CN= myns.enterprise.com
   i:/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certificates.godaddy.com/
repository/CN=Go Daddy Secure Certification Authority/serialNumber=07969287
 1 s:/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certificates.godaddy.com/
repository/CN=Go Daddy Secure Certification Authority/serialNumber=07969287
   i:/C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority
 2 s:/C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority
   i:/L=ValiCert Validation Network/O=ValiCert, Inc./OU=ValiCert Class 2 Policy Validation
Authority/CN=http://www.valicert.com//emailAddress=info@valicert.com
 3 s:/L=ValiCert Validation Network/O=ValiCert, Inc./OU=ValiCert Class 2 Policy Validation
Authority/CN=http://www.valicert.com//emailAddress=info@valicert.com
   i:/L=ValiCert Validation Network/O=ValiCert, Inc./OU=ValiCert Class 2 Policy Validation
Authority/CN=http://www.valicert.com//emailAddress=info@valicert.com
```

3. Terminate the program by pressing **[Ctrl]**+**C**.

Generating a Server Private Key and Server Certificate

Generate a server private key and server certificate using the instructions in the sections below.

NOTE: ExtremeCloud IQ Site Engine and ExtremeControl do not support the import of PKCS#8 private keys that are encoded with PKCS#5 v2.0 algorithms. Ensure you import PKCS#5 v1.5 or earlier algorithms.

Perform the following steps:

1. Generate a server private key:
   a. Navigate to **Control > Access Control > Engines >** <select your engine> **> Details > Certificates > Manage... > RADIUS > Server Certificate > Update Certificate...**
   b. Select **Generate a Private Key**, enter the **password** and select the **Key Size**.
   c. Select either **Generate CSR** or **Download Private Key Only**.

      The private key file downloads to your browser regardless of your selection.
2. Create a Certificate Signing Request:
   a. Navigate to **Control > Access Control > Engines >** <select your engine> **> Details > Certificates > Manage... > RADIUS > Server Certificate > Update Certificate... > Generate CSR**.
   (Skip this step if you chose Generate CSR in step 1c.)
   b. Fill in all required fields of the form. Optional fields are marked.

      The Certificate Signing Request file downloads to your browser.
3. Submit the request to a Certificate Authority or generate a self-signed certificate.

   The procedure for submitting a CSR to a Certificate Authority (CA) varies with the service

used. Usually, it is done through a website using a commercial service such as VeriSign. You can also use an in-house CA, which generates certificates used internally by your enterprise. You provide information including the contents of the CSR, and receive back one or more files containing the server certificate and possibly other certificates to be used in a chain.

4. Verify the contents of the server certificate.

   It is important to verify that the new server certificate contains the data you supplied when creating the CSR. In particular, make sure the Common Name (CN) is the fully qualified host name of the ExtremeCloud IQ Site Engine server.

   Use OpenSSL to view the contents of the server certificate file server.crt using the following command:

   ```
   openssl x509 -in server.crt -text -noout
   ```

You can use the following steps regardless of whether you are using a commercial certificate authority or an in-house certificate authority.

Generating a Server Private Key and Server Certificate using CLI

Generate a server private key and server certificate using the instructions in the sections below.

NOTE: ExtremeCloud IQ Site Engine and ExtremeControl do not support the import of PKCS#8 private keys that are encoded with PKCS#5 v2.0 algorithms. Ensure you import PKCS#5 v1.5 or earlier algorithms.

Perform the following steps:

1. Generate a server private key:

   a. Enter the following command to use OpenSSL to generate a password-encrypted PKCS #8 formatted server private key file. Use the key size and output file name you prefer. (If you are unsure of the key size, use 2048.)

   ```
   openssl genrsa <key_size> | openssl pkcs8 -v1 PBE-SHA1-RC4-128 -topk8 -provider default -provider legacy -out <file_name>.key
   ```

   For example:

   ```
   openssl genrsa 2048 | openssl pkcs8 -v1 PBE-SHA1-RC4-128 -topk8 -provider default -provider legacy -out <file.key>
   ```

   b. You are prompted for an Encryption Password. Be sure to make a note of the password that you enter. If the password is lost, you need to generate a new server private key and a new server certificate.

NOTE: If the private key was previously generated without the `-v1` format, convert the PKCS#5 v2.0 encoded key to PKCS#5 v1.5 format using the following command:

```
openssl pkcs8 -v1 PBE-SHA1-RC4-128 -in <original_key_file>
-topk8 -out -provider default -provider legacy <new_key_
file>
```

2. Create a Certificate Signing Request:

   a. Enter the following command to generate a CSR file. Use the output file name you used in step 1 above as the input file, and specify the output file name you prefer:

   ```
   openssl req -new -provider default -provider legacy -key <key_
   name>.key -out <csr_name>.csr
   ```

   For example:

   ```
   openssl req -new -provider default -provider legacy -key
   server.key -out server.csr
   ```

   b. You are prompted for information that displays in the certificate. When you are prompted for a Common Name, specify the fully qualified host name of the ExtremeCloud IQ Site Engine server. For example:

   ```
   Common Name (eg, YOUR name) []:netsight1.mycompany.com
   ```

3. Submit the request to a Certificate Authority or generate a self-signed certificate.

   The procedure for submitting a CSR to a Certificate Authority (CA) varies with the service used. Usually, it is done through a website using a commercial service such as VeriSign. You can also use an in-house CA, which generates certificates used internally by your enterprise. You provide information including the contents of the CSR, and receive back one or more files containing the server certificate and possibly other certificates to be used in a chain.

4. Verify the contents of the server certificate.

   It is important to verify that the new server certificate contains the data you supplied when creating the CSR. In particular, make sure the Common Name (CN) is the fully qualified host name of the ExtremeCloud IQ Site Engine server.

   Use OpenSSL to view the contents of the server certificate file server.crt using the following command:

   ```
   openssl x509 -in server.crt -text -noout
   ```

You can use the following steps regardless of whether you are using a commercial certificate authority or an in-house certificate authority.

Authorization Group Capabilities

As part of configuring Authorization and Device Access, users are assigned to authorization groups that define their access privileges to ExtremeCloud IQ Site Engine application features. These access privileges (called Capabilities) grant specific capabilities in the application. For example, you may have an authorization group called "IT Staff" that grants access to a wide range of capabilities, while another authorization group called "Guest" grants a very limited range of capabilities.

The Enable 2FA option enables two factor authentication for this group. An authentication code is required in addition to username and password. The additional authentication code is generated in the user's paired authenticator application.

Capabilities are defined when you create an authorization group and assign users to the group by selecting the Add button in the Authorization Groups section of the Administration > Users tab. In the Add/Edit Authorization Group window, the Capability list displays all the various capabilities for your selection.

There are two Categories of capabilities : Basic and Advanced.

- **Basic** — Select **Basic** in the **Add Authorization Group** window or in the **Edit Authorization Group** window to enable ExtremeCloud IQ Site Engine to resolve many dependencies automatically (for example, enabling XIQ-SE OneView Administration automatically selects the Initialize Plugin Data capability) and order capabilities based on the product menu structure.
- **Advanced** — Select **Advanced** in the **Add Authorization Group** window or in the **Edit Authorization Group** window to list all capabilities. To ensure capabilities are properly configured for Authorization Groups, enable required dependencies as noted in this help topic.

Selecting a capability grants access to that capability.

The list below includes capabilities that are only available when the Advanced Category is selected.

The following sections provide a description of each capability:

- Event Correlation
- Fabric Manager
- Northbound API
- XIQ-SE Console
- XIQ-SE Mediation Agent
- XIQ-SE NAC Manager
- XIQ-SE OneView
    - Administration
    - Alarms and Events

    - Application Analytics
    - Compliance
    - Network
    - Reports
    - Wireless Manager
    - Workflows/Scripts
- XIQ-SE Suite
    - Authorization/Device Access
    - Common Web Services
    - Device Local Management WebView
    - Web Service Credentials
    - ExtremeCloud IQ Site Engine All User Options
    - ZTP+ Registration

ExtremeCloud IQ Site Engine Event Correlation

Event Correlation Read Access

Allows ExtremeCloud IQ Site Engine to correlate similar events and respond to a perceived threat to the network. This is an experimental feature. Contact GTAC for additional information.

Event Correlation Read/Write Access

Adds the ability to configure ExtremeCloud IQ Site Engine's threat response behavior and event correlation. This is an experimental feature. Contact GTAC for additional information.

ExtremeCloud IQ Site Engine Fabric Manager

Fabric Manager Read Access

Allows the ability to access Fabric Manager and view topologies. Selecting this capability requires you to select the capability for Northbound Interface Read Access.

Fabric Manager Read/Write Access

Adds the ability to access Fabric Manager topologies and provision fabric topologies. Selecting this capability requires you to select the capability for Northbound Interface Read/Write Access.

Northbound API

Northbound API capabilities control *only* the queries and mutations that are not under Access Control and Policy. To use the queries and mutations included in the Northbound Interface but managed by

Access Control or Policy, you must provide access to **both**. For example, to use Access Control queries, you must enable two choices in the Add Authorization Group dialog: **Access Control Northbound Interface Read Access** and **Northbound Interface Read Access**.

Select the capabilities for which the user requires access in ExtremeCloud IQ Site Engine:

Access Control Northbound Interface Read Access
Provides the user with access to the Access Control queries in the Northbound Interface. To use Access Control queries included in the Northbound Interface, you must enable this capability and the Northbound Interface Read Access capability.

Access Control Northbound Interface Read/Write Access
Provides the user with access to the Access Control mutations in the Northbound Interface. To use ExtremeControl mutations, you must enable this capability and the Northbound Interface Read/Write Access capability.

Administration Northbound Interface Read Access
Provides the user with access to the Administrative Northbound Interface queries. To use ExtremeControl mutations, you must enable this capability and the Northbound Interface Read Access capability.

Administration Northbound Interface Read/Write Access
Provides the user with access to the Administrative Northbound Interface queries and mutations. To use ExtremeControl mutations, you must enable this capability and the Northbound Interface Read/Write Access capability.

Inventory Northbound Interface Read Access
Provides the user with access to the Inventory Northbound Interface queries. To use ExtremeControl mutations, you must enable this capability and the Northbound Interface Read Access capability.

Inventory Northbound Interface Read/Write Access
Provides the user with access to the Inventory Northbound Interface queries and mutations. To use ExtremeControl mutations, you must enable this capability and the Northbound Interface Read/Write Access capability.

Network Northbound Interface Read Access
Provides the user with access to the Network Northbound Interface queries. To use ExtremeControl mutations, you must enable this capability and the Northbound Interface Read Access capability.

Network Northbound Interface Read/Write Access
Provides the user with access to the Network Northbound Interface queries and mutations. To use ExtremeControl mutations, you must enable this capability and the Northbound Interface Read/Write Access capability.

Northbound Interface Read Access
Provides the user with access to Northbound Interface queries. This capability is required for

Access Control and Policy NBI queries and to use the NBI tools, accessible via the **Administration** > **Diagnostics** tab.

Northbound Interface Read/Write Access
Provides the user with access to the Northbound Interface mutations. This capability is required for Access Control and Policy NBI mutations. This capability requires the capability for Northbound Interface Read Access.

Policy Northbound Interface Read Access
Provides the user with access to the Policy queries in the Northbound Interface. To use policy queries included in the Northbound Interface, you must enable this capability and the Northbound Interface Read Access capability.

Policy Northbound Interface Read/Write Access
Provides the user with access to the Policy queries and mutations in the Northbound Interface. To use policy mutations, you must enable this capability and the Northbound Interface Read/Write Access capability.

Workflows Northbound Interface Read Access
Provides the user with access to the Workflows queries in the Northbound Interface. To use policy queries included in the Northbound Interface, you must enable this capability and the Northbound Interface Read Access capability.

Workflows Northbound Interface Read/Write Access
Provides the user with access to the Workflows queries and mutations in the Northbound Interface. To use policy mutations, you must enable this capability and the Northbound Interface Read/Write Access capability.

XIQ-SE Console

Configure FlexViews
Allows the ability to create and modify FlexViews.

Device Manager
Allows the ability to configure devices.

Launch a XIQ-SE Console Client
Allows the ability to launch a console client.

MIB Tools
Allows the ability to access the MIB tools.

Modify Compass SNMP MIBs
Allows the ability to select Compass SNMP MIBs.

Modify Device Access
Allows the ability to modify device access information.

Show Passwords in Clear Text
Allows the ability to view passwords in clear text.

TFTP Download
Allows the ability to perform a configuration upload/download or firmware image download on a device.

Topology Manager
Allows the ability to launch and use the Topology Manager options:

- Configure Map Discovery & Overlay Update Options - Allows the ability to configure map discovery and overlay the topology update options.
- Save Maps - Allows the ability to save maps.
- Start - Allows the ability to launch Topology Manager.

VLAN Models
Allows the ability to view or configure VLAN Models using the VLAN Elements Editor, accessed from the **VLAN** tab in Console:

- Configure - Allows the ability to configure VLAN Models.
- View - Allows the ability to view VLAN Models.

XIQ-SE Mediation Agent

Read access to the Mediation Agent Web Services API
Provides the ExtremeAnalytics engine with read access to ExtremeCloud IQ Site Engine (ExtremeCloud IQ Site Engine) via web services API.

Read/Write access to the Mediation Agent Web Services API
Provides the ExtremeAnalytics engine with read/write access to ExtremeCloud IQ Site Engine via web services API.

XIQ-SE NAC Manager

Edit NAC Manager Configuration
Allows the ability to edit all aspects of the NAC Manager configuration including rule components, NAC profiles, assessment, registration, and managing advanced configurations.

Force reauthentication and scan (assess) End-Systems
Allows the ability to force end-systems to be reauthenticated and scanned, but does not allow the ability to edit the NAC Manager configuration.

Launch NAC Manager
Allows the ability to launch the NAC Manager application. Users who do not have this capability see an error message when they attempt to launch NAC Manager.

Read access to Guest and IoT Management
Provides read access to the Guest and IoT management options.

Read access to End-System REST API
Provides read access to the end system web service, which is an external integration point. The web service exposes methods for manipulating end system infrastructure components.

Read access to the NAC System Web Services APIs
Provides read access to the NAC System web services, allowing programmatic access to advanced web services that are not publicly documented.

Read access to the NAC Web Services API
Provides read access to the NAC web service, which is an external integration point. The NAC web service exposes methods for manipulating NAC infrastructure components.

Read/Write access to Guest and IoT Management
Provides read/write access to the Guest and IoT management options.

Read/Write access to End-System REST API
Provides read/write access to the end system web service, which is an external integration point. The web service exposes methods for manipulating end system infrastructure components.

Read/Write access to the NAC System Web Services APIs
Provides read/write access to the NAC System web services, allowing programmatic access to advanced web services that are not publicly documented. Also provides the ability to use the NAC Request Tool.

Read/Write access to the NAC Web Services API
Provides read/write access to the NAC web service, which is an external integration point. The NAC web service exposes methods for manipulating NAC infrastructure components.

XIQ-SE OneView

Access Control
Allows the ability to perform the following ExtremeControl functions:

- Access OneView Access Control Reports - Provides access to the Dashboard view, System view, Health view, and Data Center view from the **Control** tab.
- OneView End-Systems Read Access - Provides access to the End-Systems view from the **Control** tab. Selecting this capability requires you to select the capability for Access OneView.
- OneView End-Systems Read/Write Access - Provides access to the End-Systems view from the **Control** tab, and allows the ability to perform actions such as forcing reauthentication.

- OneView Group Read Access - Allows the ability to launch the Group Editor tool from the **Control** tab > End-Systems view, and view group information.
- OneView Group Read/Write Access - Allows the ability to launch the Group Editor tool from the **Control** tab > End-Systems view, and edit group information, and add, remove, or edit group membership.
- Policy Domain Read Access - Allows the ability to launch the Policy Manager application. Users who do not have this capability see an error message when they attempt to launch Policy Manager.
- Policy Enforce/Verify and Domain Write Access - Allows the ability to manage and enforce policy to network devices using Policy Manager.

Access OneView
Allows the ability to access ExtremeCloud IQ Site Engine (formerly OneView).

Access OneView Search
Adds the ability to use the **Search** tab.

Access Operation Status Log
Adds the ability to access the operation status log.

Administration

Access OneView Administration
Adds the ability to access administration tools and enable data collection.

OneView Certificates Read Access
Allows the user read access to certificates in ExtremeCloud IQ Site Engine.

OneView Certificates Read/Write Access
Allows the user read and write access to certificates in ExtremeCloud IQ Site Engine.

Client API Read Access
Allows the ability to access the **Administration** > **Client API Access** tab.

Client API Read/Write Access
Adds the ability to access and configure API access for external applications via the **Client API Access** tab.

Configure Profiles/Credentials
Allows access to the Profiles tab and the ability to define the SNMP credentials used to access network devices and the profiles that use those credentials.

Configure Users, User Groups, and Capabilities
Allows access to the Users tab and create and edit users and authorization groups.

ExtremeCloud IQ Site Engine Database

Allows the following ExtremeCloud IQ Site Engine database management capabilities:

- Backup Database - Save the currently active database to a file.
- Change Database URL - Change the URL the ExtremeCloud IQ Site Engine Server uses when connecting to the database.
- Initialize Plugin Data - Initialize a specific ExtremeCloud IQ - Site Engine application's components in the ExtremeCloud IQ - Site Engine database by using the **File** > **Database** > **Initialize Components** menu option.
- Restore or Initialize Database - Restore the initial database or restore a saved database.
- View or Change Database Password - View and change the password the ExtremeCloud IQ Site Engine Server uses to access the database.

OneView Device Types Read Access

Allows the user read access to device types in ExtremeCloud IQ Site Engine.

OneView Device Types Read/Write Access

Allows the user read and write access to device types in ExtremeCloud IQ Site Engine.

OneView Options Read Access

Allows the user read access to options in ExtremeCloud IQ Site Engine.

OneView Options Read/Write Access

Allows the user read and write access to options in ExtremeCloud IQ Site Engine.

Configure Server View

Allows the ability to view and configure ExtremeCloud IQ - Site Engine Console client connection options:

- View - Access and view the Client Connections.
- Configure - Configure the type and number of clients that can connect to your server.

Disconnect Clients

Allows the ability to disconnect clients in the Client Connections table on the **Server Information** tab.

Revoke Locks

Allows the ability to revoke operation locks in the Locks table on the **Server Information** tab.

View Server Information

Allows the ability to view, but not to configure the **Server Information** tab. Users who do not have this capability see an error message when they attempt to access the tool.

Vendor Profiles

Allows the ability to view and configure vendor profiles on the **Administration** tab and on the **Vendor Profile** tab in the **Configure Device** window:

- OneView Vendor Profile Read Access - Access and view Vendor Profiles.
- OneView Vendor Profile Read/Write Access - Configure the Vendor Profiles in ExtremeCloud IQ Site Engine.

Alarms and Events

Alarms

Allows the following Alarm configuration capabilities:

- Configure - Configure alarms using the **Alarms Definition** tab.
- OneView Alarms Read Access - Allows the ability to view alarm information on the **Alarms & Events** tab.
- OneView Alarms Read/Write Access - Allows the ability to view and edit information on the **Alarms & Events** tab.
- View - View alarms in the Event Log.

Application Analytics

Application Analytics Read Access

Allows the ability to access the **Analytics** tab and view the ExtremeAnalytics reports. Selecting this capability requires you to select the capability for Access OneView Reports.

Application Analytics Read/Write Access

Adds the ability to view the **Analytics** > **Configuration** tab and configure ExtremeAnalytics engines and NetFlow and Application Telemetry Collecting devices. Also adds the ability to create and modify fingerprints. Selecting this capability requires you to select the capability for Access OneView Reports.

Events

Allows the following Event configuration capabilities:

- Acknowledge Events - Acknowledge events in the event log.
- Clear and Roll Server Log Managers - Clear and roll event logs on the ExtremeCloud IQ Site Engine Server using the button in the lower-right corner of the event log.
- Configure Event Options - Set suite-wide Event Logs options available from the Tools > Options window.
- Configure Server Log Managers - Add, edit, and remove Log Managers using the **Event Configuration** tab.
- View Event Logs - View event logs in all ExtremeCloud IQ Site Engine applications.
- View Events for No Access Devices - If you configured an authorization group with "No Access" to specific devices (in the Profile/Device Mapping tab), this capability allows

members of that group to view events for the No Access devices, even though they cannot access the devices.

Compliance

OneView Compliance Read Access
Allows the ability to view configuration compliance information on the **Compliance** tab.

OneView Compliance Read/Write Access
Allows the ability to view and edit configuration compliance information on the **Compliance** tab.

Network

Archives
Allows the ability to create and configure an archive to save device configuration data and capacity planning data:

- OneView Archives Read Access - View archive data.
- OneView Archive Read/Write Access - View and edit archive data.

Configuration Templates
Allows the ability to create and customize the configuration templates used for grouping product and device families by enabling any of the following options:

- OneView Templates Read Access - View configuration template data.
- OneView Templates Read/Write Access - View and edit configuration template data.

Devices

Access Terminal
The Access Terminal capability controls your access to opening a terminal session from the device menu.

NOTE: If you are upgrading to ExtremeCloud IQ Site Engine Version 8.5.3 (and future versions), the Access Terminal capability is enabled by default for new Authorization Groups, but is DISABLED by default for existing Authorization Groups. After upgrading to version 8.5.3, you must review and modify your Administrative Groups and configure them for Access Terminal individually.

Add, Discover, and Import
Allows the ability to add devices using the **Add Device** window, discover devices using the **Discovered** tab and import devices.

Allow SNMP sets to Devices
Allows the ability to write SNMP sets to network devices.

Authentication Configuration
Allows the ability to configure and change the authentication settings on your devices.

Configure Devices
Allows the ability to configure settings on your devices.

Configure Groups
Allows the ability to create device groups and add and remove devices to and from device groups.

Delete
Allows the ability to delete devices from the ExtremeCloud IQ Site Engine database.

Execute CLI Commands
Allows the ability to execute CLI commands on a device using the command line interface.

FlexView
Allows the ability to perform the following OneView FlexView functions:

- OneView FlexView Read Access - Allows the ability to launch a FlexView from the **Network** tab.
- OneView FlexView Read/Write Access - Allows the ability to launch and edit a FlexView from the **Network** tab.

Configuration Archive Management
Allows the ability to create and configure an archive to save device configuration data and capacity planning data by enabling any of the following options:

- Archive Restore Wizard
- Stamp New Versions
- View/Compare Configurations
- Configuration Templates Download Wizard
- Firmware/Boot PROM Upgrade Wizard
- Restart Device Wizard

Launch WebView
Adds the ability to execute the WebView of a device.

NOTE: If you are upgrading to ExtremeCloud IQ Site Engine Version 8.5.1 (and future versions), the "Launch WebView" capability is enabled by default for new Authorization Groups. For ExtremeCloud IQ Site Engine Versions 8.5.0 or earlier, the "Launch WebView" capability is DISABLED by default. After upgrading to version 8.5.1, you must review and modify your Administrative Groups and configure them for “Launch WebView” individually.

Maps/Sites

Allows the ability to perform the following map functions:

- Maps Write Access -Adds the ability to access the **Map** tab, and view and modify maps. This includes adding devices to the maps, drawing on the maps, changing map scale, and changing map properties (for example, the map name and background image).
- Maps/Sites Read Access - Adds the ability to access the **Map** and **Sites** tab, and view maps and site details.
- Sites Write Access - Adds the ability to access the **Sites** tab, and view and modify sites. This includes adding devices to the sites, changing site properties, and deleting sites.

Overwrite Local Changes

Allows the ability to overwrite local changes made to the **Devices** tab.

RADIUS Configuration

Allows the ability to configure RADIUS Servers and Configurations.

Set Device Profiles

Allows the ability to specify the SNMP profiles each authorization group uses when communicating with each device.

Syslog Configuration

Allows the ability to launch and use the Syslog Receiver Configuration window.

Trap Configuration

Allows the ability to launch and use the Trap Receiver Configuration window.

Firmware

Firmware

Provides the ability to perform the following firmware functions via ExtremeCloud IQ Site Engine:

- OneView Firmware Read Access - Allows the ability to view firmware images.
- OneView Firmware Read/Write Access - Allows the ability to perform a configuration upload/download or firmware image download on a device.

Reports

Access OneView Reports

Adds the ability to view all reports accessed from the Reports tab.

Wireless Manager

Configure

Allows the ability to configure Wireless Manager.

Launch
Allows the ability to launch Wireless Manager from the **Wireless** tab.

Workflows/Scripts

Access Scheduled Tasks
Adds the ability to use the **Scheduled Tasks** tab.

View and Edit Workflows, Scripts, and Saved Tasks
Allows the ability to view, edit, and run workflows, scripts, and saved tasks on the **Tasks** tab in ExtremeCloud IQ Site Engine.

NOTE: Access to some ExtremeCloud IQ Site Engine components is determined by capabilities in other capabilities groups:

XIQ-SE Console > Wireless Manager > Launch
Adds the ability to view the **Wireless** tab.

XIQ-SE Suite > Devices > Add, Discover and Import
Adds the ability to add devices in the **Network** tab.

XIQ-SE Suite > Devices > Delete
Adds the ability to delete devices in the **Network** tab.

Inventory Manager > Configuration Archive Management > View/Compare Configurations
Adds the ability to compare archived device configurations in either the **Network** tab or the Archive Details Report available in the **Reports** tab.

XIQ-SE Suite

Authorization/Device Access

Allow Tools to Use All Profiles
In MIB Tools, this capability allows users to select from all available profiles when using a Console profile to contact the device.

Allow View of No Access Devices
If an authorization group is configured with "No Access" to specific devices (in the Profile/Device Mapping tab), this capability allows members of that group to view the No Access devices in the left-panel tree, even though they cannot access the devices.

Configure LDAP and RADIUS and TACACS Servers
Allows the ability to configure RADIUS Servers and LDAP Configurations in the Users/Groups tab in the Authorization/Device Access tool.

Manage SNMP Passwords
Allows access to the Manage SNMP Passwords tab in the Authorization/Device Access tool and the ability to manage the credentials set on network devices.

View Authorization/Device Access
Allows the ability to view, but not to configure Authorization/Device Access.

Common Web Services

Web Services APIs Read Access
Provides read access to the ExtremeCloud IQ Site Engine Common web service, which is an external integration point. The Common web service exposes methods for manipulating ExtremeCloud IQ Site Engine infrastructure components.

Web Services APIs Read/Write Access
Provides read/write access to the ExtremeCloud IQ Site Engine Common web service, which is an external integration point. The Common web service exposes methods for manipulating ExtremeCloud IQ Site Engine infrastructure components.

Device Local Management WebView

Auto Login to Web Local Management for ExtremeWireless Controllers
Allows the ability to launch local management for wireless controllers without requiring a login for users with the necessary credentials. Users who do not have this capability are required to log in.

Auto Login to Web Local Management for NAC Appliances
Allows the ability to launch local management for ExtremeControlengines without requiring a login for users with the necessary credentials. Users who do not have this capability are required to log in.

Web Service Credentials

Read operations
Provides read access to the ExtremeCloud IQ Site Engine Credentials web service, allowing programmatic access to authentication profiles and credentials used for device access.

Read/write operations
Provides read/write access to the ExtremeCloud IQ Site Engine Credentials web service, allowing programmatic access to authentication profiles and credentials used for device access.

ExtremeCloud IQ Site Engine All User Options

These capabilities provide the ability to set suite-wide options that apply to all users.

Configure SMTP E-mail Options
Allows the ability to specify the SMTP email server used by the ExtremeCloud IQ Site Engine email notification feature.

Configure Services for NetSight (ExtremeCloud IQ Site Engine) Server Options
Allows the ability to specify TFTP settings.

Configure Web Server
Allows the ability to specify the port ID for HTTP web server traffic.

Open GTAC Support Case
Allows the ability to create a GTAC support case or RMA case from the **Network** tab.

Request and Configure ExtremeNetworks.com Support
Allows the ability to request information about the latest ExtremeCloud IQ Site Engine product releases via the **Help > Check for Updates** option from the menu bar in any application and request information about firmware releases via the **Help > Check for Firmware Updates** option in Inventory Manager. It also allows you to configure the check for updates operation (including scheduled updates) in the Suite options. These features tell you when updated versions of ExtremeCloud IQ Site Engine products and firmware are available and allow you to download newer versions to keep your software and firmware current.

ZTP+ Registration

Allows the ability to configure a ZTP+ enabled device and add it to ExtremeCloud IQ Site Engine.

Access Control Options

Selecting Access Control in the left panel of the **Options** tab provides the following view, where you can edit settings associated with the **Control** > **Access Control** tab. The right-panel view changes depending on what you select in the left-panel tree. Expand the Access Control tree to view all the different available options. These settings apply to all users.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.

Select the link for information on the following ExtremeControl options:

- Advanced
- Assessment Agent Adapter Credentials
- Data Persistence
- Display
- End-System Event Cache
- Enforce Warning Settings
- Entra ID Registered User Status Monitor
- Features
- Intune Compliance Module
- Workspace ONE UEM Compliance Module
- Microsoft Sentinel
- Notification Engine
- Policy Defaults
- Status Polling and Timeout

Advanced

Use this view to configure advanced settings for the Access Control tab.

Enable IPv6 Addresses for End-Systems

The **Enable IPv6 Addresses for End-Systems** option enables Access Control to collect, report, and display IPv6 addresses for end-systems in the end-systems table. When this option is changed, you must enforce your engines before the new settings take effect. In addition, end-systems need to rediscover their IP addresses in order to reflect the change in the end-systems table. This can be done by either deleting the end-system or performing a Force Reauth on the end-system.

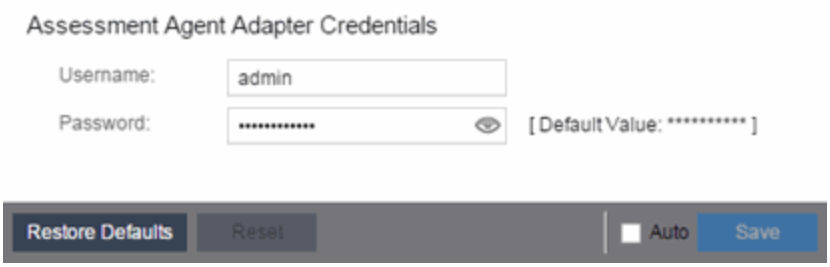
Only end-systems with a valid IPv4 address as well as one or more IPv6 addresses are supported. End-systems with only IPv6 addresses are not supported. End-system functionality support varies for IPv6 end-systems. For complete information, see IPv6 Support in the ExtremeCloud IQ Site Engine Configuration Considerations Help topic.

Resource Allocation Capacity

The **Resource Allocation Capacity** option lets you configure the ExtremeCloud IQ Site Engine resources allocated to end-system and configuration processing services. The greater the number of end-systems and engines in your Access Control deployment, the more resources it requires.

- Low - For low performance shared systems.
- Low-Medium - For medium performance shared systems, or low performance dedicated systems
- Medium - For medium performance shared systems, or medium performance dedicated systems.
- Medium-High - For high performance shared systems, or medium performance dedicated systems.
- High - For high performance dedicated systems.
- Maximum - For extremely high performance dedicated systems.

Assessment Agent Adapter Credentials

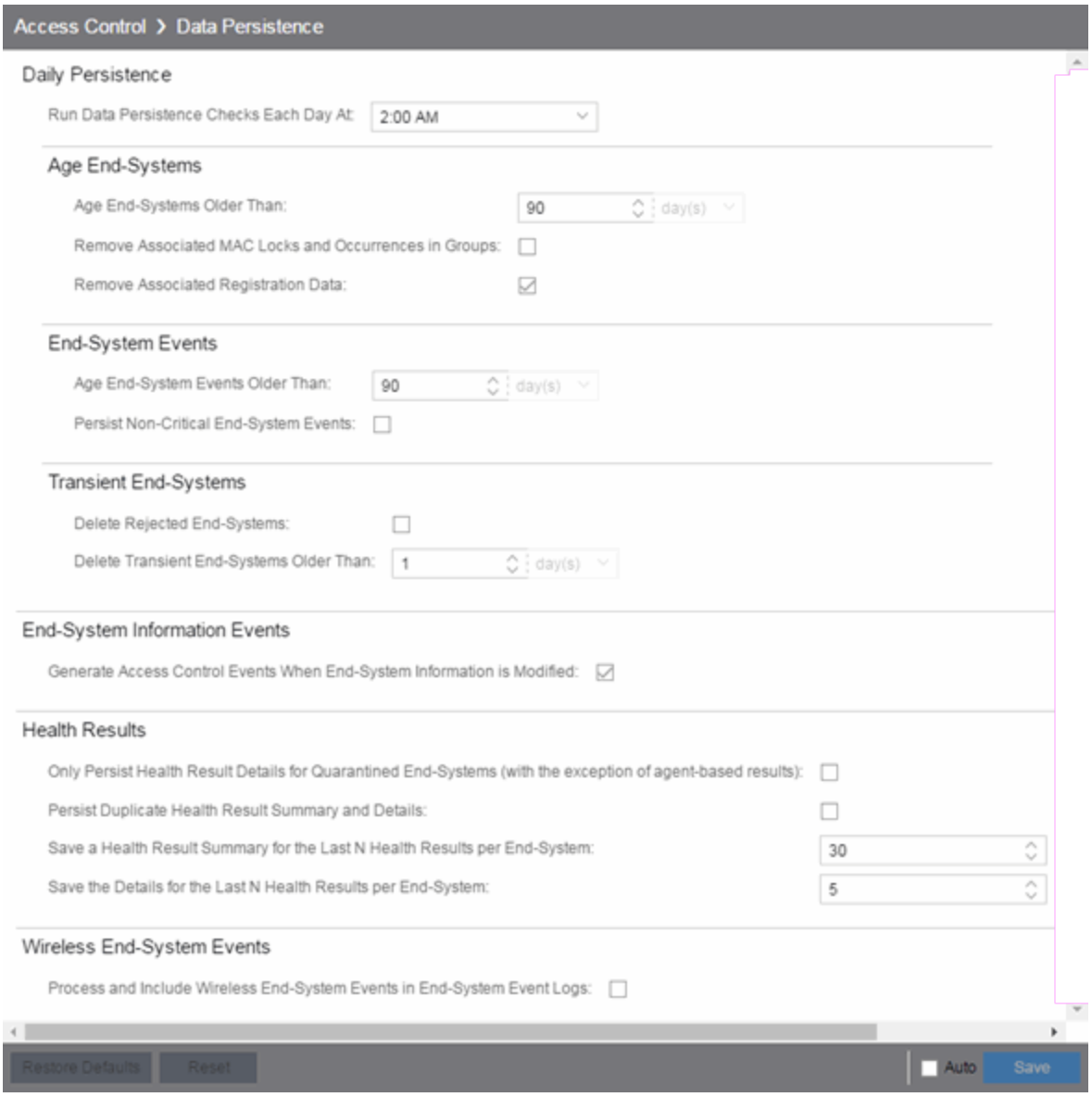


Assessment Agent Adapter Credentials

Specify the username and password the Access Control engine uses when attempting to connect to network assessment servers, including Extreme Networks Agent-less, Nessus, or a third-party assessment server (an assessment server not supplied or supported by ExtremeCloud IQ Site Engine). The password is used by the assessment agent adapter (installed on the assessment server) to authenticate assessment server requests. ExtremeCloud IQ Site Engine provides a default password you can change, if desired. However, if you change the password here, you need to change the password on the assessment agent adapter as well, or connection between the engine and assessment agent adapter is lost and assessments are not performed. For additional information, see How to Change the Assessment Agent Adapter Password.

Data Persistence

Use this panel to customize how ExtremeControl ages-out or deletes end-systems, end-system events, and end-system health (assessment) results from the tables and charts in the End-Systems tab.



Daily Persistence

Run Data Persistence Checks Each Day At

Set the time that the Data Persistence Check is performed each day.

Age End-Systems

Age End-Systems Older Than

Specify the amount of time ExtremeCloud IQ Site Engine keeps end-system information in the database. Each day, when the Data Persistence check runs, it searches the database for end-systems for which Access Control did not receive an event in the number of days specified (90 days by default). It removes those end-systems from the End-System table in the End-Systems tab.

If you select the **Remove Associated MAC Locks and Occurrences in Groups** checkbox, the aging check also removes any MAC locks or group memberships associated with the end-systems being removed.

The **Remove Associated Registration Data** checkbox is selected by default, so that the aging check also removes any registration data associated with the end-systems being removed.

End-System Events

Age End-System Events Older Than

End-system events are stored in the database. Each day, when the Data Persistence check runs, it removes all end-system events which are older than the number of days specified (90 days by default).

Persist Non-Critical End-System Events

Select this checkbox to save non-critical end-system events (e.g. duplicate end-system events, re-authentication events where the end-system's state did not change) to the database.

Transient End-Systems

Delete Rejected End-Systems

Select this checkbox to delete end-systems in the Rejected state as part of the cleanup.

Delete Transient End-Systems Older Than

Specify the amount of time to keep transient end-systems in the database before they are deleted as part of the nightly database cleanup task. The default value is 1 day. A value of 0 disables the deletion of transient end-systems. Transient end-systems are unregistered end-systems not seen for the specified number of days. End-systems are not deleted if they are part of an End-System group or there are MAC locks associated with them.

End-System Information Events

Generate Access Control Events When End-System Information is Modified

Select the checkbox if you want Access Control to generate an event when end-system information is modified.

Health Results

Only Persist Health Result Details for Quarantined End-Systems (with the exception of agent-based results)

Select this checkbox to only save the health result details for quarantined end-systems (with the exception of agent-based health result details, which are always saved for all end-systems).

Persist Duplicate Health Result Summary and Details

Select this checkbox to save duplicate health result summaries and details. By default, duplicate health results obtained during a single scan interval are **not** saved. For example, if the assessment interval is one week, and an end-system is scanned five times during the week with identical assessment results each time, the duplicate health results are not saved (with the exception of administrative scan requests such as Force Reauth and Scan, which are always saved). This reduces the number of health results saved to the database.

Save a Health Result Summary for the Last N Health Results per End-System

Specify how many health (assessment) result summaries are saved and displayed in the End-Systems tab for each end-system. By default, the Data Persistence check saves the last 30 health result summaries for each end-system.

Save the Details for the Last N Health Results per End-System

Specify how many health (assessment) result details are saved and displayed in the End-Systems tab for each end-system. By default, the Data Persistence check saves detailed information for the last five health results per end-system.

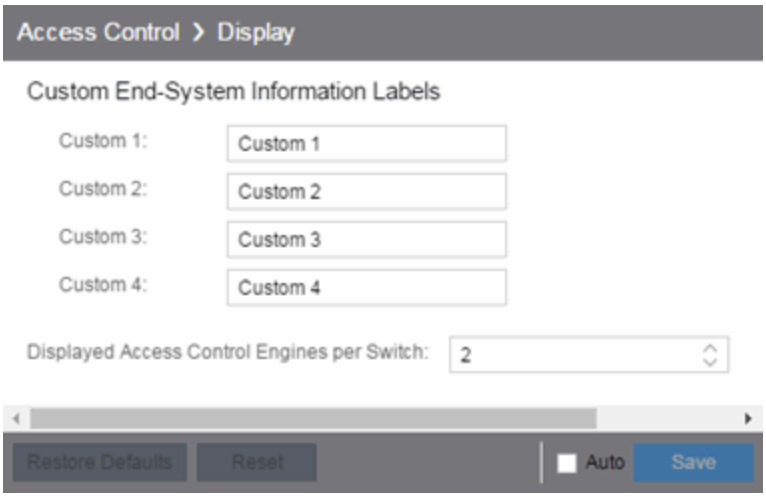
Wireless End-System Events

Process and Include Wireless End-System Events in End-System Event Logs

Select the checkbox if you want ExtremeCloud IQ Site Engine to generate an event when wireless end-system information is modified. This option is disabled by default.

Display

Use this Options view to configure new column names for the **Custom** columns in the End-System table on the **Control** > **End-Systems** tab, as well as the number of redundant Access Control engines you can select when adding or editing a switch in an Access Control Engine group.



Custom End-System Information Labels

This option lets you specify new text for the **Custom** column headings in the End-System table on the **End-Systems** tab.

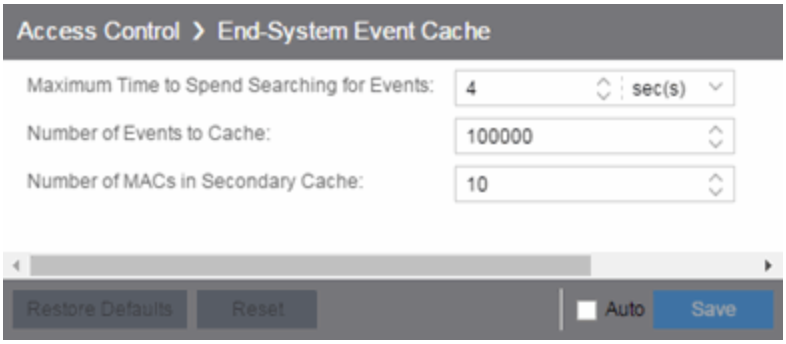
Displayed Access Control Engines per Switch

Select the number of Access Control engines displayed in the Add Switches to Group or Edit Switches in Group windows. By default, these windows enable you to configure two Access Control engines per switch for redundancy, but this option enables you to increase the number up to three or four engines per switch.

End-System Event Cache

End-system events are stored in the database. In addition, the end-system event cache stores the most recent end-system events in memory and displays them in the End-System Events tab. This cache enables ExtremeControl to quickly retrieve and display end-system events without having to search through the database.

Use these options to configure the amount of resources used by the end-system event cache.



Maximum Time to Spend Searching for Events

Specify the time ExtremeCloud IQ Site Engine spends when searching for older events outside of the cache. (The search is initiated by using the **Search for Older Events** button in the **End-System Events** tab.) The search is ended when the number of seconds entered is reached.

Number of Events to Cache

Specify the number of events to cache. The more events you cache, the faster data is returned, but caching uses more memory.

Number of MACs in Secondary Cache

The End-System Event Cache also keeps a secondary cache of events by MAC address. This means that a particular end-system's events can be more quickly accessed in subsequent requests. Use this field to specify the number of MAC addresses kept in the secondary cache. Keep in mind that the more MAC addresses you cache, the more memory used. Also, note that the secondary cache can include events not in the main cache.

Enforce Warnings to Ignore

Select the checkbox next to the warning message you don't want displayed and select **Save**.

When an engine configuration audit is performed during an Enforce operation, warning messages can display in the audit results listed in the Enforce window. If there is a warning associated with an engine, you are given the option to acknowledge the warning and proceed with the enforce anyway.

Use these settings to select specific warning messages you do not want displayed in the audit results. This enables you to proceed with the Enforce without having to acknowledge the warning message. For example, your network always results in one of these warning messages on your Access Control configuration. By selecting that warning here, it is ignored in future audit results and you no longer need to acknowledge it before proceeding with the Enforce.

Entra ID Registered User Status Monitor

The Entra ID Registered User Status Monitor periodically checks the session validity for users registered through Entra ID. If the user session is revoked in Entra ID, then the user registered through authenticated registration will automatically expire.

Check Validity of the user's session in Entra ID

Enable or disable the Entra ID Registered User Status Monitor.

NOTE: This feature must be enabled with the **Check Session Validity in Entra ID** option in the **Registration Settings** of the **Authenticated Registration** section of **Captive Portals** configuration.

Check Interval

Defines how often ExtremeCloud IQ Site Engine starts the process to check the user session validity in Entra ID.

Number of Users per Batch

Defines the burst, how many users are checked in a batch. There are 20 users in each API call.

NOTE: Decrease the number of **Users per Batch** if you experience API throttling from Microsoft.

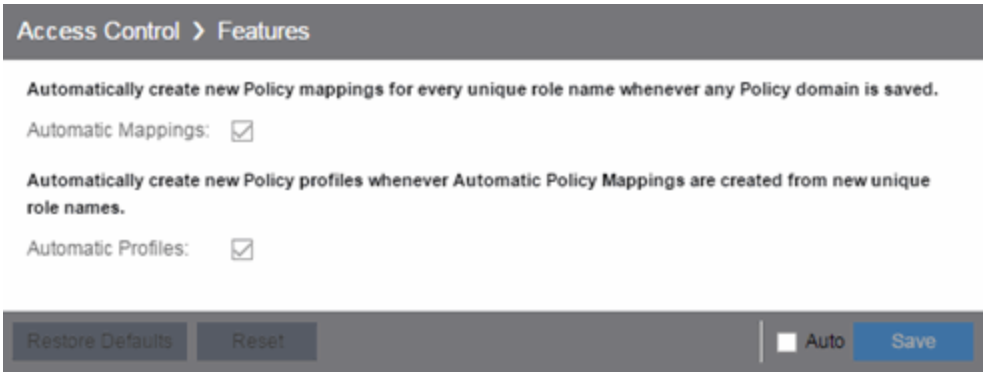
Consider the number of users you have when specifying values to prevent performance degradation.

Batch Processing Interval

Defines how often the batch is generated.

Features

Use this panel to automatically create new Policy mappings and profiles. If you are not using these features, disable them to remove sections that pertain only to those features from certain Access Control windows.



Intune Compliance Module

Use this panel to configure integration with Microsoft Intune and Defender to handle non-compliant end systems. The Site Engine periodically downloads the list of non-compliant Intune IDs through API calls from Microsoft. The Intune ID is a unique identifier of a device enrolled into Microsoft Intune. The entries of the list are compared with the content of end-systems Certificate URI and if the non-compliant end-system is found then the MAC address of such end-system is added to End-System Group for Non-compliant Devices.

Enable Compliance Check

Enable or disable the compliance integration with Microsoft Intune.

Check Interval

Defines how often ExtremeCloud IQ Site Engine downloads the list of non-compliant Intune IDs from Microsoft. If the number of non-compliant devices is high, do not configure a short check interval.

Intune Configuration

Defines how to access the Microsoft Intune API. The mandatory fields are:

Client ID

The application identifier of the registered application in Entra ID. In Entra ID the App ID is the Application (client) ID.

Client Secret

The client secret for the registered application in Entra ID.

Scope

The scope used by API calls.

Token Endpoint

The OAuth 2.0 token endpoint (v2) provided by Entra ID in App registrations.

Non-compliant Behavior

Defines what happens with non-compliant end-systems reported by Microsoft Intune

End-System Group for Non-compliant Devices

Defines a MAC based end-system group where the MAC address of a Non-compliant device is added.

Workspace ONE UEM Compliance Module

Use the Workspace ONE UEM Compliance Module options to configure the integration between ExtremeControl and VMware Workspace ONE UEM. When enabled, the integration periodically retrieves device attributes from Workspace ONE UEM and uses the attributes to populate end-system groups and end-system table columns.

Access the following settings from **Administration > Options > Access Control > Workspace ONE UEM Compliance Module**.

Enable Compliance Check

Enable or disable the compliance integration with VMware Workplace ONE UEM.

Check Interval

Defines how often (in minutes) ExtremeCloud IQ Site Engine queries the Workspace ONE UEM API for device attribute updates. Default: 30.

Alert Threshold Percentage

Defines the threshold for generating event logs when API call rate limits are approached.

Stop Threshold Percentage

Defines the threshold for generating event logs when API call rate limits are approached. If stop threshold is reached, the system suppresses processing until the Workspace ONE UEM API call limits are reset daily.

API Service URL
The Workspace ONE UEM API endpoint URL.

Password
The Workspace ONE UEM API administrator password.

Tenant Code
The Workspace ONE UEM API key for your tenant.

Username
The Workspace ONE UEM API administrator username.

End-System Group for Non-compliant Devices
Defines the end-system group which non-compliant devices are added. Default: Blacklist.

Microsoft Sentinel

Use the Microsoft Sentinel options to configure the export of NAC appliance event data from ExtremeCloud IQ Site Engine to a Microsoft Sentinel Log Analytics Workspace. When enabled, qualifying authentication, authorization, and enforcement events are exported in near real-time to a custom table in the Azure environment.

Access the following settings from **Administration > Options > Access Control > Microsoft Sentinel**.

Enable Microsoft Sentinel Export
Enable or disable the Microsoft Sentinel Export feature. All of the required configuration fields are disabled until you select the Enable Microsoft Sentinel Export checkbox.

Client ID
The Azure application (service principal) Client ID.

Client Secret
The secret associated with the Azure application.

Tenant ID
The Azure Active Directory Tenant ID.

DCR Immutable ID
The unique identifier of the Data Collection Rule, copied from the ARM template deployment Outputs.

Logs Ingestion Endpoint Base URL
The URL to send log data to Azure, copied from the ARM template deployment Outputs.

Stream Name
The stream within the DCR that maps to the custom table, copied from the ARM template deployment Outputs.

Authentication Events
Select to export authentication events to Microsoft Sentinel Logs Analytics Workspace.

Authorization Events
Select to export authorization events to Microsoft Sentinel Logs Analytics Workspace.

Enforcement Events
Select to export enforcement events to Microsoft Sentinel Logs Analytics Workspace.

Test Connection
Validates the configured Azure authentication and the configured Microsoft Sentinel endpoint.

Notification Engine

Use this panel to define the default content contained in Access Control notification action messages. For example, with an email notification action, define the information contained in the email subject line and body. With a syslog or trap notification action, define the information included in the syslog or trap message.



There are certain "keywords" available to use in your email, syslog, and trap messages to provide specific information. Following is a list of the most common keywords used. For additional information, see Keywords.

- $type - the notification type.
- $trigger - the notification trigger.
- $conditions - a list of the conditions specified in the notification action.
- $ipaddress - the IP address of the end-system that is the source of the event.
- $macaddress - the MAC address of the end-system that is the source of the event.
- $switchIP - the IP address of the switch where the end-system connected.
- $switchPort - the port number on the switch where the end-system connected.
- $username - the username provided by the end user upon connection to the network.

Custom Arguments
If the notification action specifies a custom program or script to be run on the ExtremeCloud IQ Site Engine Server, then use this field to enter the "all" option. Using the "all" option returns values for all the Access Control Notification keywords applicable to the notification type. For additional information, see Keywords.

Email Subject
Defines the text and keyword values included in the email subject line.

Email Body
Defines the text and keyword values included in the email body.

Syslog Message
Defines the text and keyword values included in the syslog message.

Syslog Tag
Defines the string used to identify the message issued by the syslog program.

Trap Message
The varbind sent in the trap.

Trap Message OID
The OID of the varbind being sent that represents the message.

Trap OID
The OID that defines the trap.

Event Queue Service Period
Defines how often the queue is checked for events to process. The dispatcher runs one time every service period. So by default, the dispatcher processes events every 5 seconds.

Maximum Event Queue Size
The maximum number of events that can be queued. By default, the dispatcher drops events after 5000 events are queued.

Maximum Events Queuable in Service Period
This limits the rate that events can be added to the queue (not processed from the queue) and

protects the event engine against a large amount of events arriving too quickly. If events arrive at a rate that exceeds this amount, they are discarded.

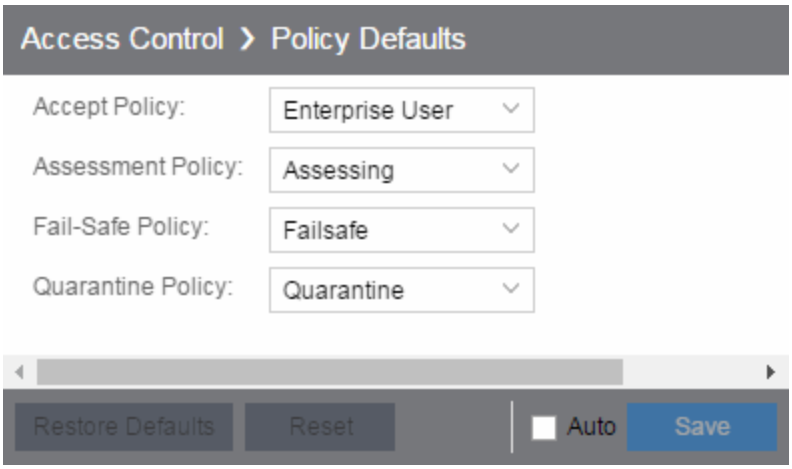
Maximum Events Serviced Each Period

The maximum number of events pulled from the queue for processing each service period. By default, the dispatcher processes 100 events every service period.

Policy Defaults

Use this Options view to specify a default policy for each of the four access policies. These default policies display as the first selection in the drop-down menus when you create an Access Control profile. For example, if you specify an Assessment policy called "New Assessment" as the Policy Default, then "New Assessment" is automatically displayed as the first selection in the Assessment Policy drop-down list in the New ExtremeControl Profile window.

ExtremeCloud IQ Site Engine supplies seven policy names from which you can select. Add more policies in the Edit Policy Mapping window, where you can also define policy to VLAN associations for RFC 3580-enabled switches. After a policy is added, it becomes available for selection in this view.



Accept Policy

Select the default Accept policy. The Accept policy is applied to an end-system when the end-system is authorized locally by the Access Control engine and passed an assessment (if an assessment was required), or the "Replace RADIUS Attributes with Accept Policy" option is used when authenticating the end-system.

Assessment Policy

Select the default Assessment policy. The Assessment policy is applied to an end-system while it is being assessed (scanned).

Fail-Safe Policy

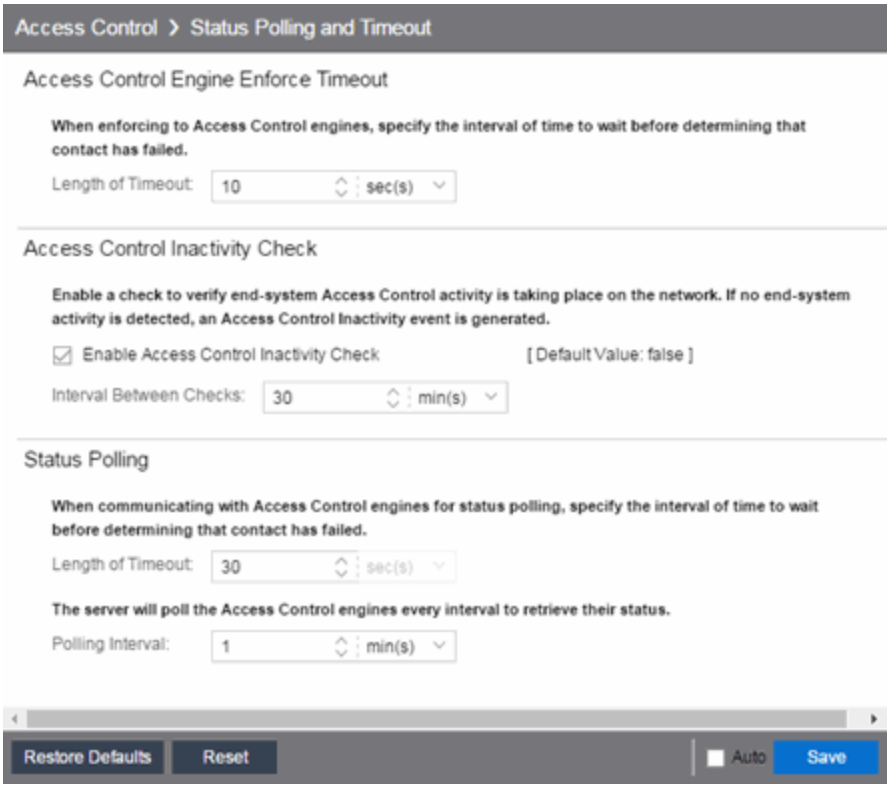
Select the default fail-safe policy. The fail-safe policy is applied to an end-system if the end-system's IP address cannot be determined from its MAC address, or if there is a scanning error and an assessment of the end-system could not take place.

Quarantine Policy

Select the default Quarantine policy. The Quarantine policy is applied to an end-system if the end-system fails an assessment.

Status Polling and Timeout

Use this Options panel to specify the enforce timeout and status polling options for Access Control engines.



Access Control Engine Enforce Timeout

When enforcing to Access Control engines, this value specifies the amount of time ExtremeCloud IQ Site Engine waits for an enforce response from the engine before determining the engine is not responding. During an enforce, an ExtremeControl engine responds every second to report that the enforce operation is either in-progress or complete. Do not increase this timeout value, unless you are experiencing network delays that require a longer timeout value.

Access Control Inactivity Check

Enable a check to verify end-system ExtremeControl activity is taking place on the network. If no end-system activity is detected, an Access Control Inactivity event is sent to the Events view. Use the **Alarms and Events** tab to configure custom alarm criteria based on the Access Control Inactivity event to create an alarm, if desired.

Status Polling

Length of Timeout — When communicating with Access Control engines for status polling, this value specifies the amount of time ExtremeCloud IQ Site Engine waits before determining contact failed. If ExtremeCloud IQ Site Engine does not receive a response from an engine in the defined amount of time, ExtremeCloud IQ Site Engine considers the engine to be "down". The engine status refers to Messaging connectivity, not SNMP connectivity. This means that if the engine is "down," ExtremeCloud IQ Site Engine is not able to enforce a new configuration to it.

Polling Interval — Specifies the frequency ExtremeCloud IQ Site Engine polls the Access Control engines to determine engine status.

Alarm Options

Selecting Alarm in the left panel of the **Options** tab provides the following view, where you can configure alarm settings.

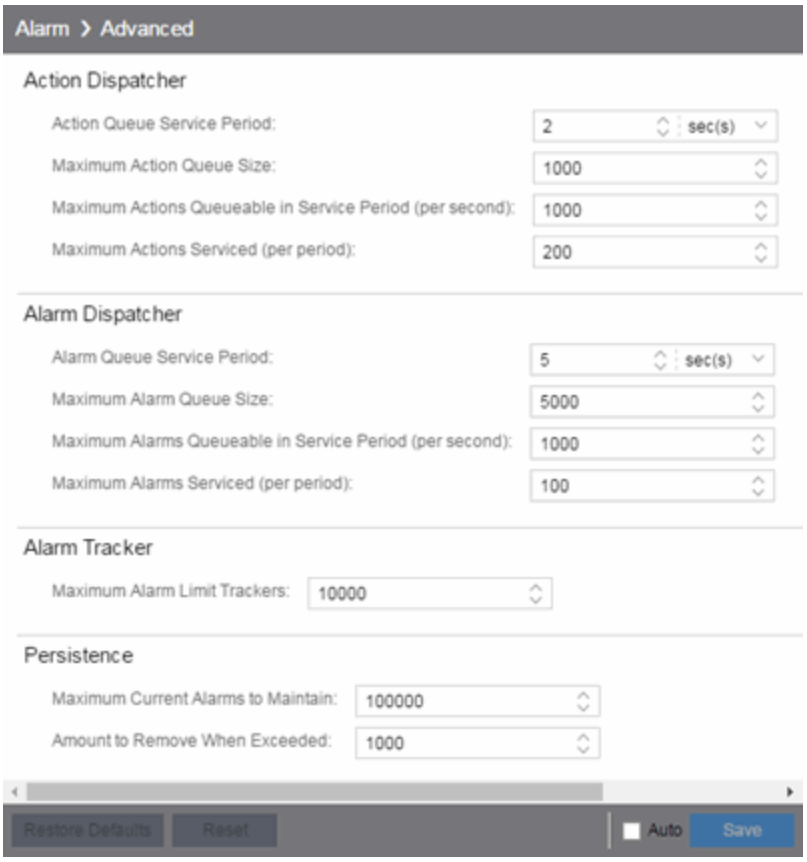
Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.

Select the link for information on the following Alarm options:

- Advanced
- Alarm Action Defaults
- Alarm History
- Consolidate Email
- Override Email

Advanced

Use this view to configure advanced settings for the alarms functionality in ExtremeCloud IQ Site Engine. These settings apply to all users.



Action Dispatcher Options

Use these options to limit resources used by ExtremeCloud IQ Site Engine action handling.

After alarms are processed by the alarm dispatcher, they are checked for an action. If an action is found, the alarm is moved into the action queue for processing by the action dispatcher. A specified number of actions are taken from the queue and processed one time each service period, according to the option values specified below.

Action Queue Service Period

This controls how often the queue is checked for actions to process. The dispatcher runs one time every service period. So by default, the dispatcher processes actions every 2 seconds.

Maximum Action Queue Size

The maximum number of actions that can be queued. By default, the dispatcher drops actions after 1,000 actions are queued.

Maximum Actions Queuable in Service Period (per second)

This limits the rate at which actions can be added to the queue (not processed from the queue) and protects the alarm engine against a large amount of actions arriving too quickly. If actions arrive at a rate that exceeds this amount, they are discarded.

Maximum Actions Serviced (per period)
The maximum number of actions pulled from the queue for processing each service period. By default, the dispatcher processes 200 actions every service period.

Alarm Dispatcher Options

Use these options to limit resources used by ExtremeCloud IQ Site Engine alarm handling.

When alarms are triggered, they are moved into the alarm queue for processing by the alarm dispatcher. A specified number of alarms are taken from the queue and processed one time each service period, according to the option values specified below.

Alarm Queue Service Period
This controls how often the queue is checked for alarms to process. The dispatcher runs one time every service period, so by default, the dispatcher processes alarms every 5 seconds.

Maximum Alarm Queue Size
The maximum number of alarms that can be queued. By default, the dispatcher drops alarms after 5,000 alarms are queued.

Maximum Alarms Queuable in Service Period (per second)
This limits the rate at which alarms can be added to the queue (not processed from the queue) and protects the alarm engine against a large amount of alarms arriving too quickly. If alarms arrive at a rate that exceeds this amount, they are discarded.

Max Alarms Serviced (per period)
The maximum number of alarms pulled from the queue for processing each service period. By default, the dispatcher processes 100 alarms every service period.

Alarm Tracker Options

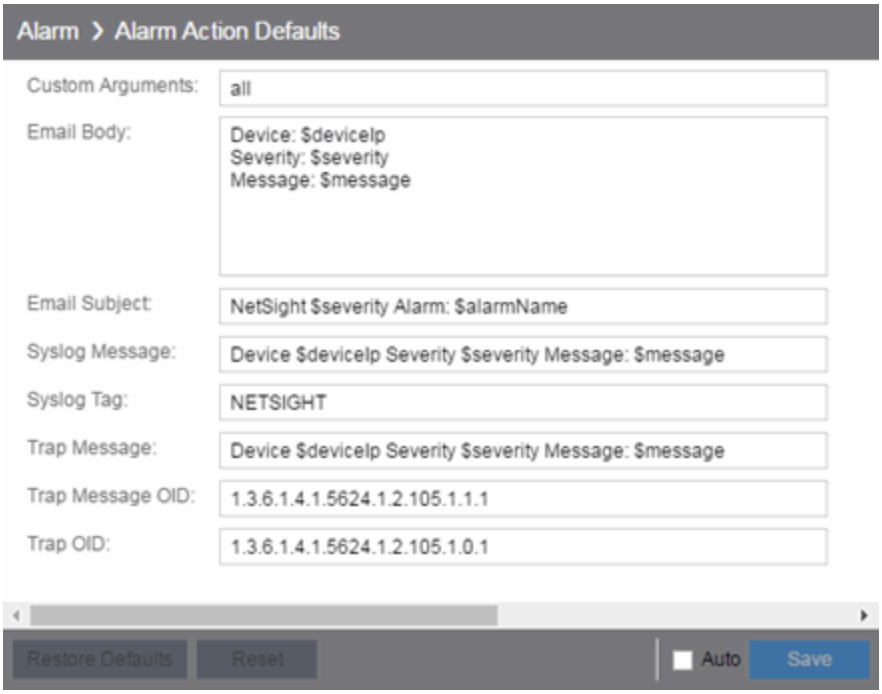
When you define an alarm with a limit, ExtremeCloud IQ Site Engine tracks whether the limit is exceeded and when to reset the count. Use this option to set the maximum number of alarms that ExtremeCloud IQ Site Engine tracks. (An alarm limit specifies the number of times the alarm action performed for an alarm.)

Increase the number if you are sure the system is able to handle the increased load.

Persistence Options

Use these options to prevent or troubleshoot ExtremeCloud IQ Site Engine performance problems caused by the number of current alarms being maintained. If you increase the maximum number of current alarms to maintain, be sure the server system is able to handle the increased load. Only increase the number of alarms to remove if the maximum current alarms number is being exceeded too frequently.

Alarm Action Defaults



Use this panel to define the default content for alarm action messages. For example, with an email action, define the information contained in the email subject line and body. With a syslog or trap action, specify the information you want contained in the syslog or trap message. ExtremeCloud IQ Site Engine uses these values unless they are overridden in an individual alarm.

The message content is configured as a template, with the content passed exactly as typed, except for the variable information which is specified by $keyword. The variable information ($keyword) is replaced with information from the alarm when the alarm action is executed.

Following is a list of the most common keywords used. For additional information, see Keywords.

- $alarmName – the name of the alarm.
- $severity – the severity of the alarm.
- $deviceIP – the IP address of the device that is the source of the alarm.
- $message – the event message.
- $time – the date and time when the event or trap occurred.

Custom Arguments

Specifies the arguments passed to a program. Each argument is delimited by spaces. An argument can be a literal, passed to the program exactly as typed, or a variable, specified as $keyword. A group of literals and variables can be combined into a single argument by using

double quotes. "All" is a special value that tells ExtremeCloud IQ Site Engine to pass all variable values to the program as individual arguments.

Email Body
Defines the text included in the email body.

Email Subject
Defines the text included in the email subject line.

Syslog Message
Defines the text included in the syslog message.

Syslog Tag
Defines the string used to identify the message issued by the syslog program.

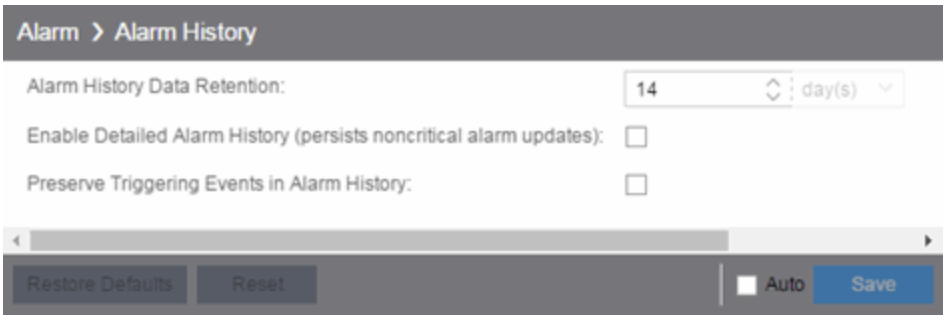
Trap Message
The varbind sent in the trap.

Trap Message OID
The OID of the varbind being sent that represents the message.

Trap OID
The OID that defines the trap.

Alarm History

Use this panel to configure options for how alarms are handled on your network. These settings apply to all users.



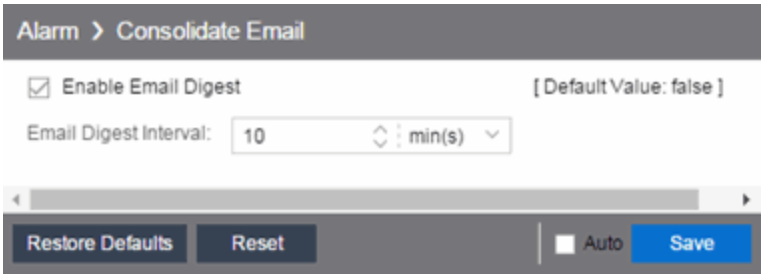
Alarm History Data Retention
Specify (in days) the amount of time Alarm History is retained.

Enable Detailed Alarm History (persists noncritical alarm updates)
Select this checkbox to record repeat occurrences of an alarm being raised. By default, a history record is created the first time an alarm is raised on a device or interface, and also when it is cleared.

Preserve Triggering Events in Alarm History

Select this checkbox to preserve alarm triggering events, so that any triggering events are stored with the alarm history record. This allows you to view the triggering event by selecting the View Trigger button in the Alarm History window.

Consolidate Email



Enable Email Digest

Selecting this option combines alarm action emails into a single email. Email notifications are collected over the specified interval indicated in the **Email Digest Interval** and then delivered as a single consolidated email.

Email Digest Interval

Enter the amount of time ExtremeCloud IQ Site Engine waits before sending an email of alarm actions when **Select Enable Email Digest** is selected.

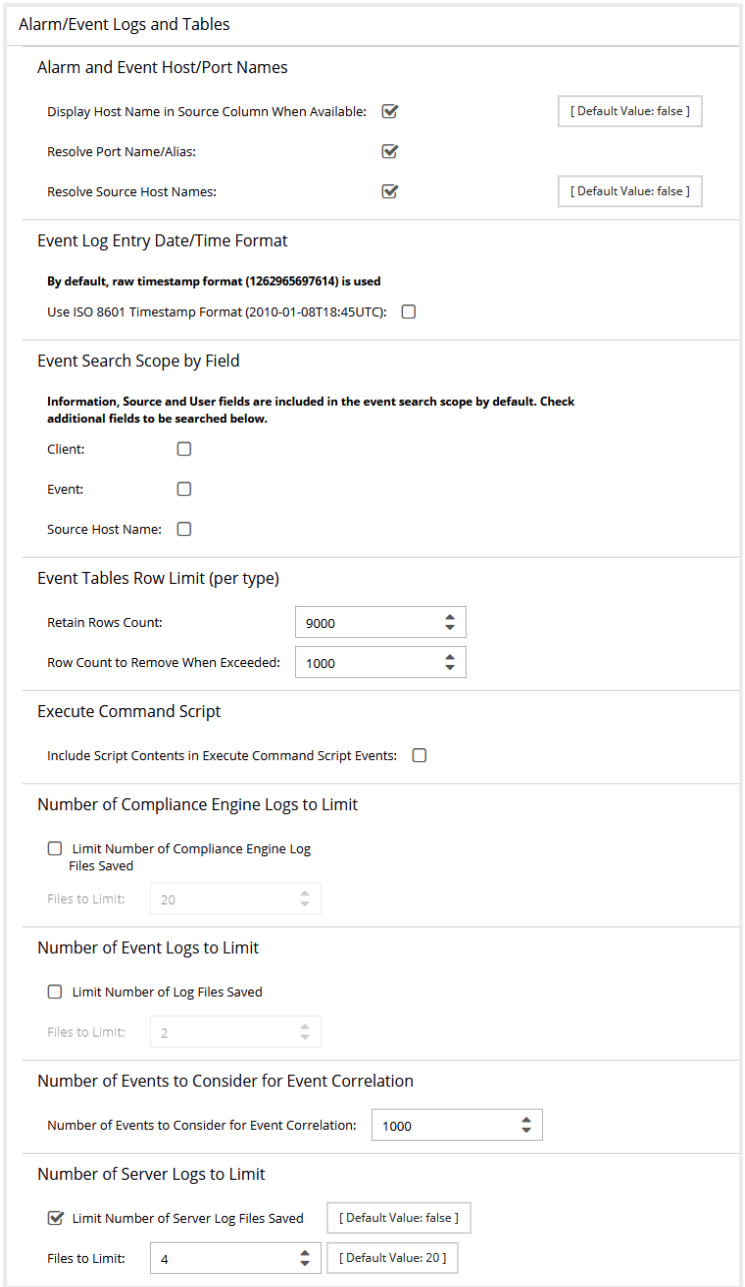
Override Email



Enable this option to override the sender of an email for an alarm email action, including the ability to set the sender's password, if needed. Since alarms are typically sent out as email/text messages, this option allows IT staff to set different ring-tones based on the alarm definition. Doing this on a smartphone typically involves changing the ring-tone for calls from a specific person.

Alarm/Event Logs and Tables Options

Selecting **Alarm/Event Logs and Tables** in the left panel of the **Options** tab provides the following view, where you can specify options for limiting disk usage by alarm and event logs, and ExtremeCloud IQ Site Engine server logs. These settings apply to all users. You must be assigned the appropriate user capability to configure these options.



Alarm and Event Host/Port Names

Use these options to configure host name and port name resolution, and display the device host name in the Source column in alarm and event tables:

- **Display Host Name in Source Column When Available** — Select this option to display the host name in the source column on both the **Alarms** and **Events** tabs of the **Alarms and Events** tab, if it's available in ExtremeCloud IQ Site Engine.
- **Resolve Port Name/Alias** — Select this option to resolve device port indices to port names and port aliases, and device port names and port aliases to port indices, if possible. This option allows you to enable/disable port name resolution for Event and Alarm tables only. (Port name resolution is enabled globally using Enable Name Resolution .)
- **Resolve Source Host Names** — Select this option to resolve host names to IP addresses and IP addresses to host names, if possible. This option allows you to enable/disable host name resolution for the Event and Alarm tables only. (Host name resolution is enabled globally using Enable Name Resolution.)

Event Log Entry Date/Time Format

Use this option to specify the timestamp format used for log entries in the actual application log files. (This option does not affect the log entry format displayed in ExtremeCloud IQ Site Engine client Event Log views.) Selecting **Use ISO 8601 Timestamp Format** displays log entry timestamps in a readable format that makes it easier to view the files in a text file. Not selecting this option uses the raw timestamp format, in which timestamps are displayed in a raw, non-readable format.

Event Search Scope by Field

Use this option to include **Client**, **Event**, or **Source Host Name** in the **Events** search. This setting impacts the duration of the search because you have added additional options. **Source Host Name** is hidden by default and will need to be unhidden to see the search results.

Event Tables Row Limit (per type)

Use these settings to determine the number of table rows displayed in all of the logs on the Events tab of the **Alarms and Events** tab. The table size reaches an absolute limit when the number of rows is equal to the value in the **Retain Rows Count** field. When the number of rows exceeds that value, the number of rows are reduced by the value specified in the **Row Count to Remove When Exceeded** field. Subsequent entries are retained until the **Retain Rows Count** value is exceeded and the row total is again reduced.

Execute Command Script

The Execute Command Script feature includes script contents in logged events, which is not secure if the script includes passwords. If this option is deselected (default), the script is removed from the logged event. Select this option to include script contents in Execute Command Script events.

Number of Compliance Engine Logs to Limit

Use this option to limit the number of ExtremeCompliance engine log files saved to the `<install directory>\appdata\logs` directory. It does not limit the number of Traps or Syslog log files saved.

- **Limit Number of Compliance Engine Log Files Saved** — Selecting the checkbox sets a limit to the number of ExtremeCompliance engine log files saved. Older files are deleted when the maximum number is reached.
- **Files to Limit** — Enter the maximum number of ExtremeCompliance log files saved.

Number of Event Logs to Limit

This option limits the number of application log files saved to the `<install directory>\appdata\logs` directory. It does not limit the number of Traps or Syslog log files saved.

- **Limit Number of Log Files Saved** — Selecting the checkbox sets a limit to the number of application log files saved. Older files are deleted when the maximum number is reached.
- **Files to Limit** — Enter the maximum number of application log files saved.

Number of Events to Consider for Event Correlation

This option allows you to determine the number of events ExtremeCloud IQ Site Engine uses when correlating events. Event Correlation is performed by ExtremeCloud IQ Site Engine to determine trends and allows you to take action on those observations.

Number of Server Logs to Limit

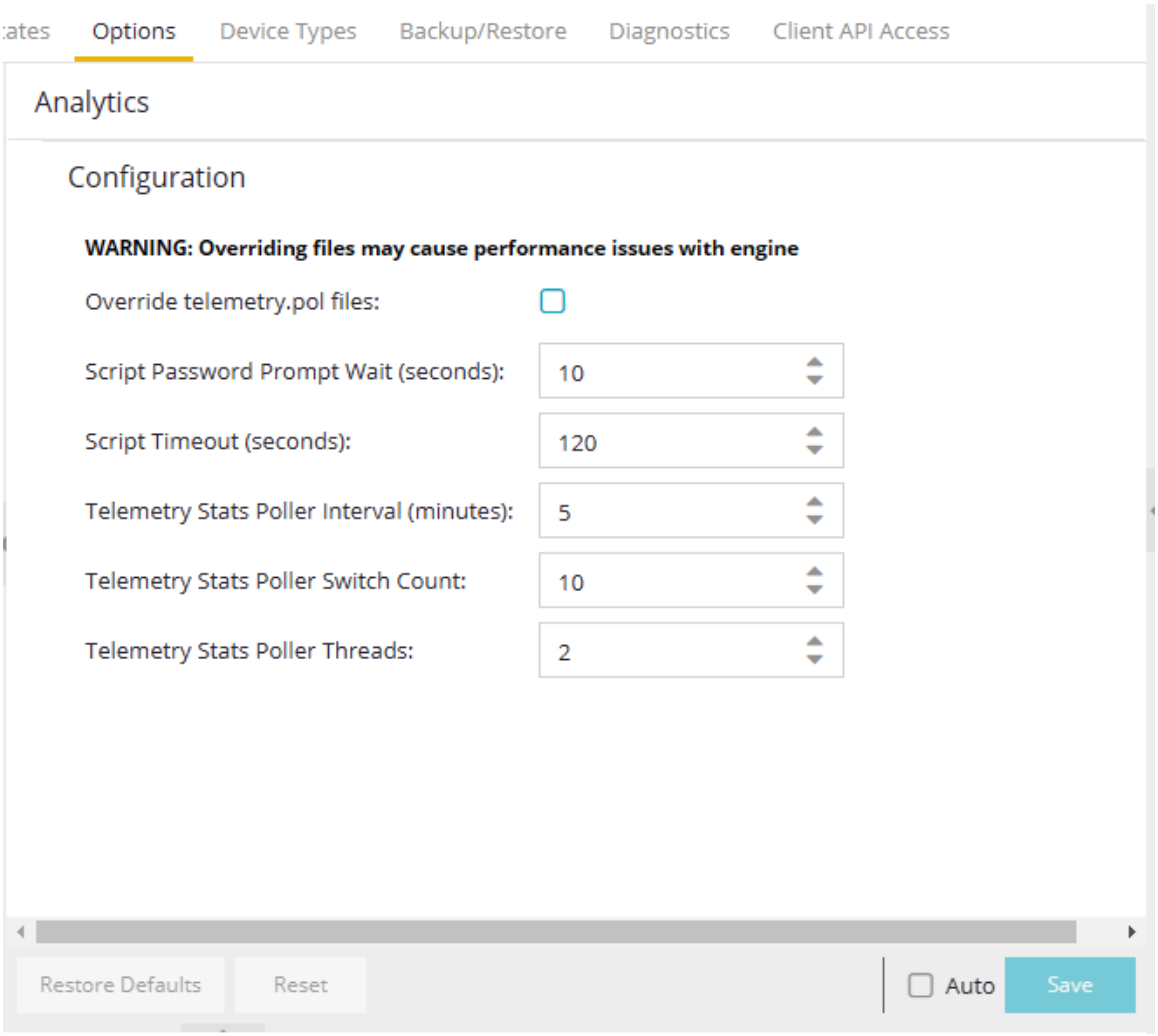
A new server log is created every day. Use this option to limit the number of server log files saved to the `<install directory>\appdata\logs` directory.

- **Limit Number of Server Log Files Saved** — Selecting the checkbox sets a limit to the number of server log files saved. Older files are deleted when the maximum number is reached.
- **Files to Limit** — Enter the maximum number of server log files saved.

Analytics Options

Selecting Analytics in the left panel of the **Options** tab provides the following view.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.



Configuration

Override telemetry.pol files

Select the checkbox to maintain user custom telemetry.pol files in the Inventory Manager paths, not overwritten by the system telemetry.pol files. The default value for this setting is disabled. For additional information, see ExtremeAnalytics Engine Advanced Configuration.

Script Password Prompt Wait

The length of time to wait in seconds for the application telemetry script to receive a password prompt from the application telemetry source.

Script Timeout

The length of time to wait in seconds for the application telemetry script to expect results before terminating.

Telemetry Stats Poller Interval

The periodic frequency in minutes the Application Telemetry polls run. Increasing the value is recommended as the number of application telemetry sources increases.

Telemetry Stats Poller Switch Count

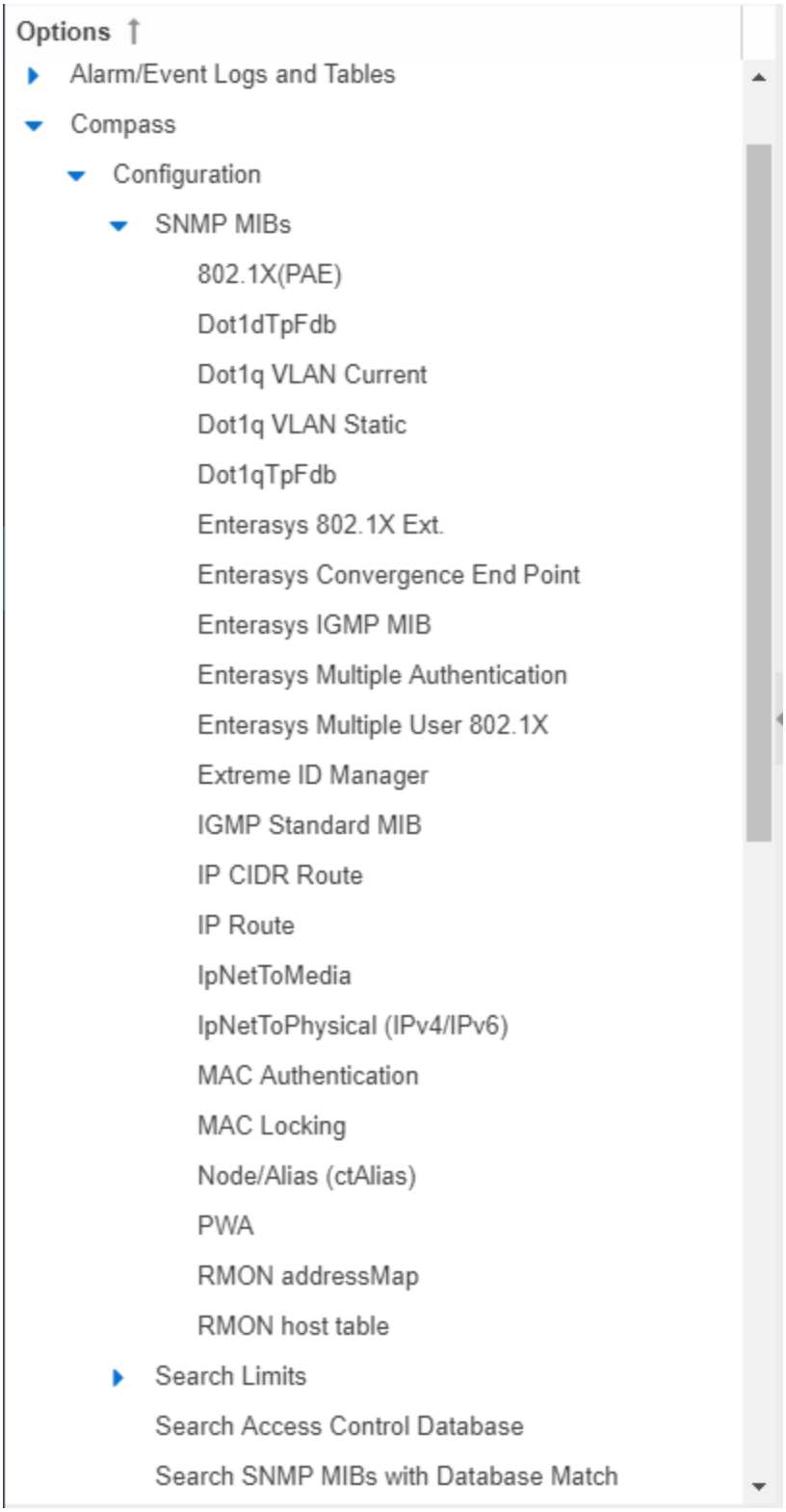
The number of switches polled during a single switch poll cycle.

Telemetry Stats Poller Threads

The number of switch poller threads allowed during poll cycles.

Compass Options

Selecting Compass and expanding Configuration in the left panel of the **Options** tab provides the following view, where you can view Compass SNMP MIBs and Search options.


Options
Alarm/Event Logs and Tables
Compass
Configuration
SNMP MIBs
802.1X(PAE)
Dot1dTpFdb
Dot1q VLAN Current
Dot1q VLAN Static
Dot1qTpFdb
Enterasys 802.1X Ext.
Enterasys Convergence End Point
Enterasys IGMP MIB
Enterasys Multiple Authentication
Enterasys Multiple User 802.1X
Extreme ID Manager
IGMP Standard MIB
IP CIDR Route
IP Route
IpNetToMedia
IpNetToPhysical (IPv4/IPv6)
MAC Authentication
MAC Locking
Node/Alias (ctAlias)
PWA
RMON addressMap
RMON host table
Search Limits
Search Access Control Database
Search SNMP MIBs with Database Match

Double-click **Configuration** in the left-panel to open the **Compass Configuration** window, which allows you to specify and limit your search options. Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.



Search Limits

Use these options to configure the Compass search in ExtremeCloud IQ Site Engine. In addition to search options, they include search limit settings, which are used to help limit the ExtremeCloud IQ Site Engine server resources used for the searches.

- **Number of Devices Allowed for a Search** — The maximum number of devices that can be included in a search.
- **Number of Search Results Allowed** — The maximum number of search results that can be displayed in the table.
- **Number of Searches Allowed at Once** — The maximum number of ExtremeCloud IQ Site Engine Compass searches that can be performed at one time.
- **Time Limit for a Search** — The maximum search time.

Search Access Control Database

Select this checkbox to include Access Control data in Compass searches. The Compass search begins by resolving IP address to MAC address in order to start searching for MAC-IP pairs from the network. When a match is found in the Access Control Database, the SNMP MIBs are **not** searched unless the **Search SNMP MIBs with Database Match** checkbox is also selected. If the **Access Control** checkbox is deselected, then the Access Control Database is not used to resolve IP address to MAC address.

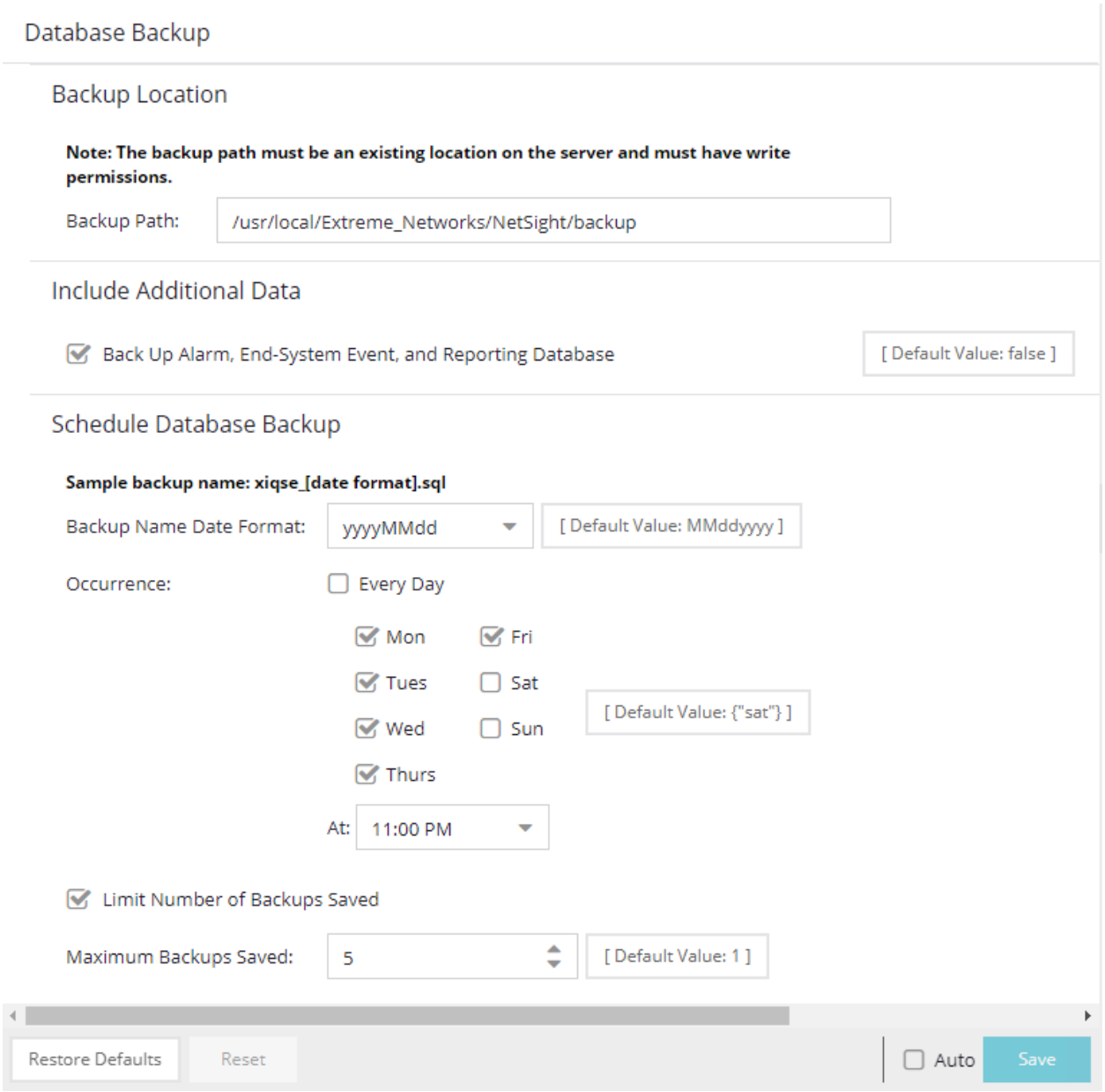
Search SNMP MIBs with Database Match

Select this checkbox to include various SNMP MIB objects when performing searches. When the checkbox is selected, the SNMP MIBs section displays, from which you can select the individual SNMP MIB objects to include in Compass searches. For additional information, see Compass SNMP MIBs Descriptions.

Database Backup Options

Selecting Database Backup in the left panel of the **Options** tab provides the following view, where you can schedule backups of the ExtremeCloud IQ Site Engine database. An up-to-date database backup is an important component to ensuring that critical information pertaining to all ExtremeCloud IQ Site Engine applications is saved and readily available, if needed.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.



Backup Location

Backup Path

The database backup is saved to the directory specified in the **Backup Path** field. Saving backups to a separate location such as a network share ensures that an up-to-date copy of the database is available should a problem such as a server disk failure occur. The backup directory must exist and be writable or it is not accepted. Both the start and stop of the database backup are logged to the Console Event View log for verification and tracking purposes.

The complete backup consists of multiple files and a predefined directory structure. All files must be present for a later full restore. The name of the scheduled backup starts with "xiqse_" followed by the date and ".sql". The name of the on-demand backup can be specified by the user. The complete backup includes files in the following directories: Connect, InventoryMgr, OneView, Purview, Scripting, VendorProfiles, WirelessMgr. There are subdirectories with the backup name, all files in those subdirectories are necessary.

NOTE: Example of the backup name: MyBackup
Example of the directory structure related to the backup:
MyBackup/
Connect/MyBackup/
InventoryMgr/MyBackup/
OneView/MyBackup/
Purview/MyBackup/
Scripting/MyBackup/
VendorProfiles/MyBackup/
WirelessMgr/MyBackup/

Include Additional Data

Back Up Alarm, End-System Event, and Reporting Database

Use this checkbox to enable and disable the automatic backup of alarm data, end-system event data, and ExtremeCloud IQ Site Engine reporting data. Because the alarm, event, and reporting databases can be quite large, this allows you to control the amount of disk space used by the database backup operation.

Schedule Database Backup

Backup Name Date Format

Customize the date and time formats of scheduled backup files by selecting the option that formats the date -- day (DD), month (MM), and year (YYYY) -- according to your personal preference in the drop-down list.

Occurrence

Select one or more days of the week and specify a time for the backup to be performed. The backup takes place at the same time for each selected day.

Limit Number of Backups Saved

Select the checkbox to limit the number of scheduled backup files saved.

Maximum Backups Saved

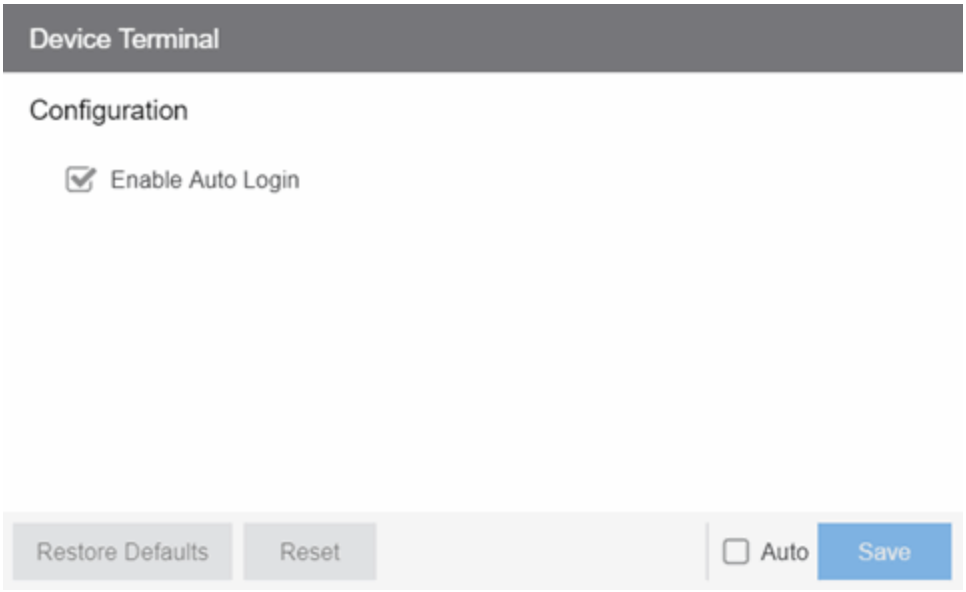
If **Limit Number of Backups Saved** is selected, enter the maximum number of scheduled backup files to save. When the limit is reached, older backups are removed when a new scheduled backup completes.

For additional information, see Tuning Database Backup Storage.

Device Terminal Options

Selecting Device Terminal in the left panel of the **Options** tab provides the following view, where you can configure options related to the **Open Device Terminal** option on the **Devices** tab.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.



Configuration

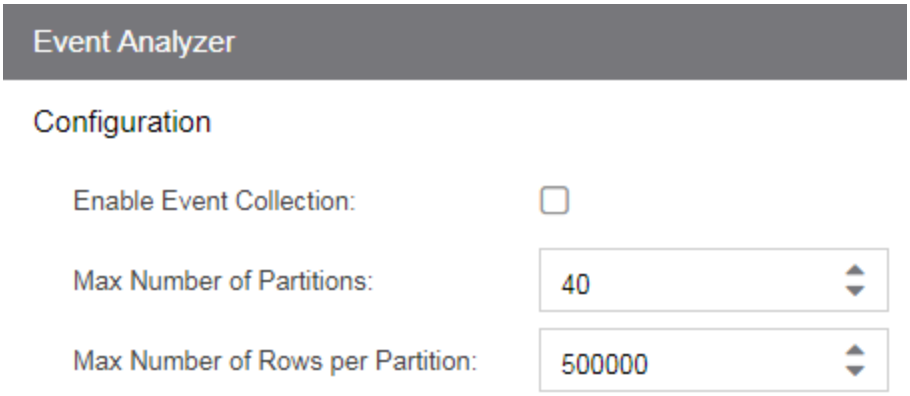
Enable Auto Login

Select the checkbox to automatically log in to a device when selecting the **Open Device Terminal** option from the right-click menu on the **Devices** tab.

Event Analyzer Options

Selecting Event Analyzer in the left panel of the **Options** tab provides the following view, where you can configure the settings related to the Event Analyzer in ExtremeCloud IQ Site Engine.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.



Enable Event Collection

Selecting the **Enable Event Collection** option saves wireless client events and enables **Event Analyzer** tab functionality so that the tab populates with live data.

NOTE: Enabling Event Collection uses a large amount of disk space, so this option is disabled by default.

Max Number of Partitions

Enter the maximum number of partitions used for the Event Analyzer.

NOTE: Only change this value if you are an expert user.

Max Number of Rows per Partition

Enter the maximum number of rows for each partition used for the Event Analyzer.

NOTE: Only change this value if you are an expert user.

Proxy Server

Selecting Proxy Server in the left panel of the Options tab provides the following view, where you can configure options for accessing internet targets. These settings apply to all users. You must be a member of an authorization group that includes the "Request and Configure ExtremeNetworks.com Support" capability in order to configure these options.

Changing a value from the system default causes a Default Value button to appear. Selecting this button changes the field back to the system default value.

HTTP Proxy

If your network is protected by a firewall, select the **Enable Proxy Server** checkbox and enter your proxy server address and port ID. Consult your network administrator for this information. If your proxy server requires authentication, select the **Proxy Authentication** checkbox and enter the proxy username and password credentials. The credentials you add here must match the credentials configured on the proxy server. Proxy credentials are cached when used successfully. If you change them here, restart the ExtremeCloud IQ Site Engine Server to clear the old credentials from the cache.

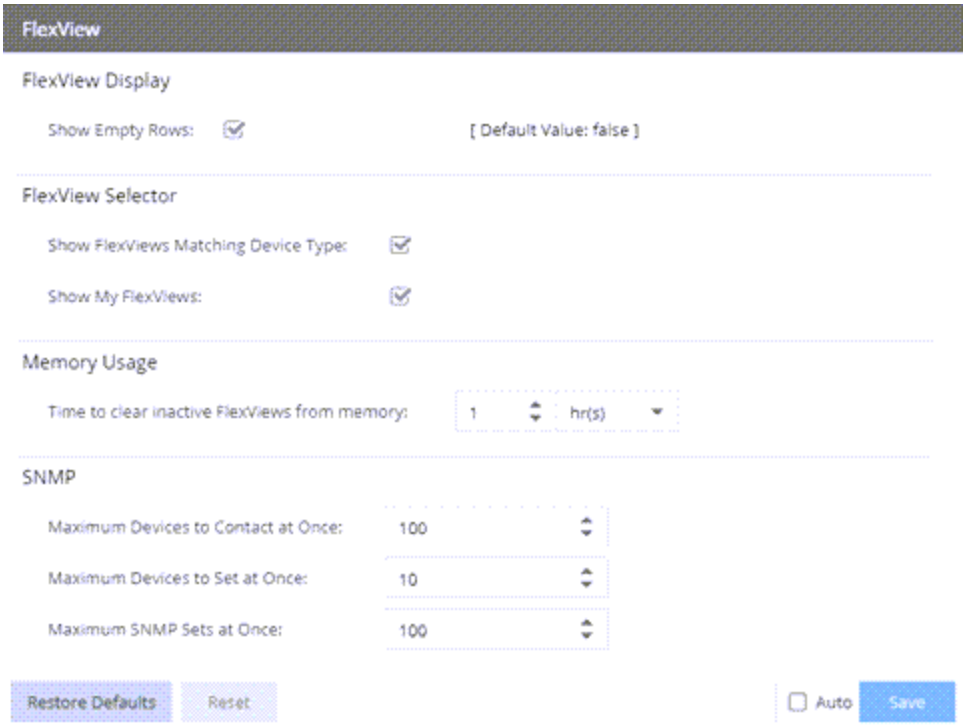
NOTE: The update procedure uses these proxy settings only when necessary; otherwise, the settings are ignored.

FlexView Options

Selecting FlexView in the left panel of the **Options** tab provides the following view, where you can configure the settings related to FlexViews in ExtremeCloud IQ Site Engine. The options enable you to determine which FlexViews are available, how the FlexViews are displayed, and how FlexView information is retrieved and maintained.

NOTE: Bookmarked FlexViews are not affected by these options.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.



FlexView Display

Show Empty Rows

Select this checkbox to display empty rows in FlexViews when there is no response from an IP address.

FlexView Selector

Use this section to determine which FlexViews are displayed and how they are organized.

Show FlexViews Matching Device Type
: Select this box to display only those FlexViews that match the device type you select.

Show My FlexViews
: Select this checkbox to include FlexViews saved in the My FlexViews folder when selecting a FlexView on the **Devices** tab. ExtremeCloud IQ Site Engine saves all FlexViews you create or modify in the My FlexViews folder.

Memory Usage

Time to clear inactive FlexViews from memory
: The amount of time before ExtremeCloud IQ Site Engine removes inactive FlexViews from memory.

SNMP

These options determine FlexView settings for devices whose Poll Type is set to SNMP.

Maximum Devices to Contact at Once
: The maximum number of IP addresses ExtremeCloud IQ Site Engine attempts to contact (read) simultaneously.

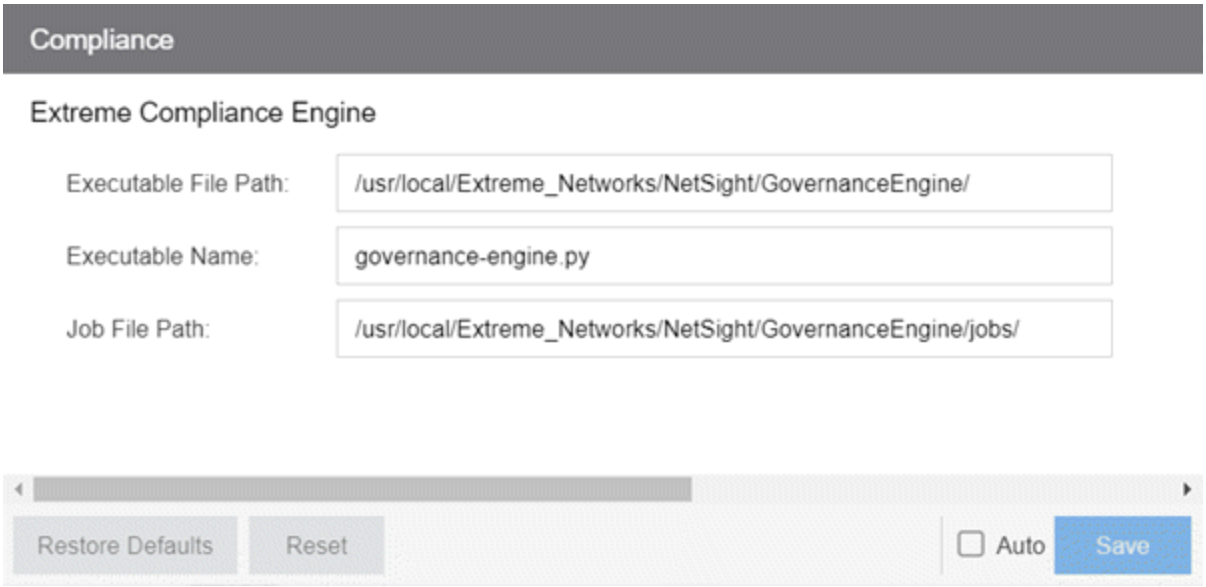
Maximum Devices to Set at Once
: The maximum number of IP addresses ExtremeCloud IQ Site Engine attempts to perform PDU (protocol data unit) sets against simultaneously.

Maximum SNMP Sets at Once
: The maximum number of SNMP PDU sets ExtremeCloud IQ Site Engine attempts to contact simultaneously.

Compliance Options (Legacy)

Selecting Compliance in the left panel of the **Options** tab provides the following view, where you can specify the ExtremeCompliance engine file name used by ExtremeCloud IQ Site Engine, the path to the directory in which the file is located, and the path to the job file directory. These settings apply to all users. You must be assigned the appropriate user capability to configure these options.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.



Executable File Path
The directory in which the ExtremeCompliance engine executable file is located.

Executable Name
The name of the executable file used by the ExtremeCompliance engine.

Job File Path
The path to the directory in which the job files are located. The ExtremeCompliance engine uses job files to test device configurations in order to provide you with vulnerability information.

Impact Analysis Options

Selecting **Impact Analysis** in the left panel of the **Options** tab provides the following view, where you can edit settings associated with the **Impact Analysis** dashboard. The right-panel view changes depending on what you select in the left-panel tree. Expand the Impact Analysis tree to view all the different available options. These settings apply to all users.

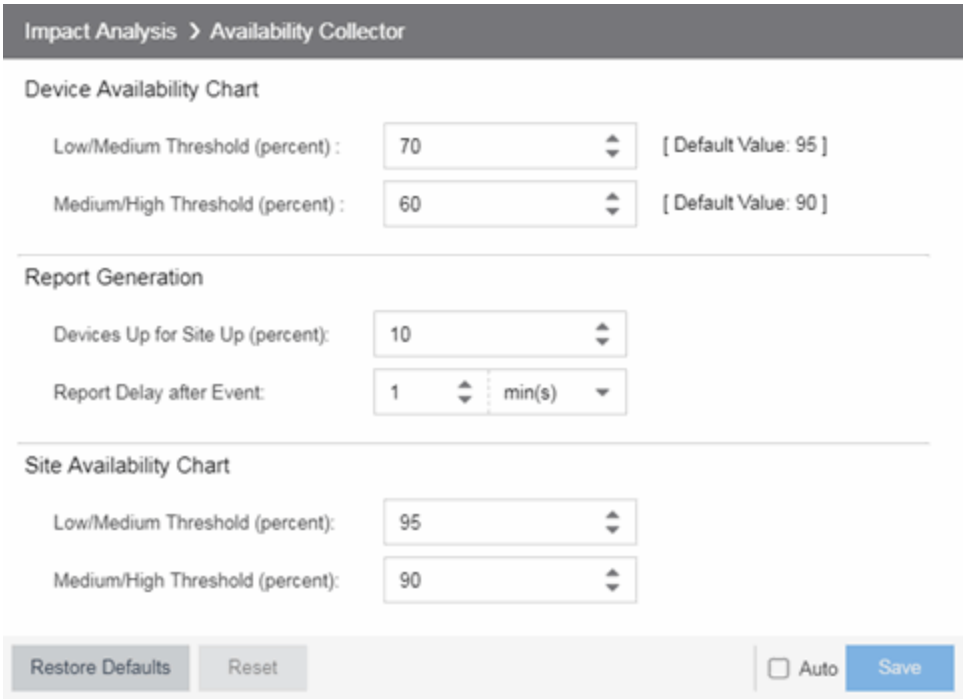
Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.

Select the link for information on the following Impact Analysis options:

- Availability Collector
- Capacity/Health Collector
- Configuration Collector
- Performance Collector

Availability Collector

Use these options to configure the threshold settings for the Site and Device Availability Charts in the Impact Analysis dashboard.



Device Availability Chart

Low/Medium Threshold (percent)
: Indicates the percentage of devices on your network that ExtremeCloud IQ Site Engine can reach. If the value falls below the percentage entered here, the **Impact Status** of the Device Availability chart moves from **Low** to **Medium**. For devices to be included, data collection must be enabled.

Medium/High Threshold (percent)
: Indicates the percentage of devices on your network that ExtremeCloud IQ Site Engine can reach. If the value falls below the percentage entered here, the **Impact Status** of the Device Availability chart moves from **Medium** to **High**. For devices to be included, data collection must be enabled.

Report Generation

Devices Up for Site Up (percent)
: Indicates the percent of devices included in a site that ExtremeCloud IQ Site Engine can reach. If the value falls below the percentage entered here, the ExtremeCloud IQ Site Engine considered the site down.

Report Delay after Event
: Indicates the amount of time ExtremeCloud IQ Site Engine waits before reporting a device is down.

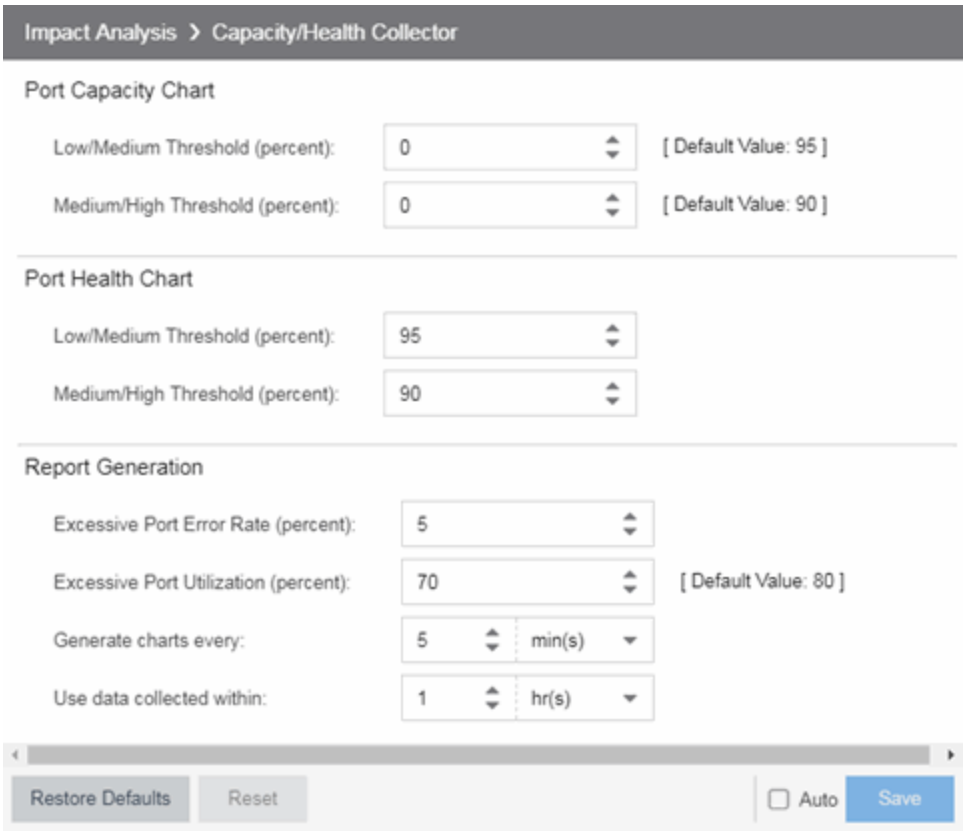
Site Availability Chart

Low/Medium Threshold (percent)
: Indicates the percentage of devices included in a site that ExtremeCloud IQ Site Engine can reach. If the value falls below the percentage entered here, the **Impact Status** of the Site Availability chart moves from **Low** to **Medium**. For devices to be included, data collection must be enabled.

Medium/High Threshold (percent)
: Indicates the percentage of devices included in a site that ExtremeCloud IQ Site Engine can reach. If the value falls below the percentage entered here, the **Impact Status** of the Site Availability chart moves from **Medium** to **High**. For devices to be included, data collection must be enabled.

Capacity/Health Collector

Use these options to configure the thresholds for the Port Capacity and Port Health Charts in the Impact Analysis dashboard.



Port Capacity Chart

Low/Medium Threshold (percent)

Indicates the percentage of ports on your network with an acceptable level of utilization. If the value falls below the percentage entered here, the **Impact Status** on the Port Capacity chart moves from **Low** to **Medium**. For ports to be included, data collection must be enabled.

Medium/High Threshold (percent)

Indicates the percentage of ports on your network with an acceptable level of utilization. If the value falls below the percentage entered here, the **Impact Status** on the Port Capacity chart moves from **Medium** to **High**. For ports to be included, data collection must be enabled.

Port Health Chart

Low/Medium Threshold (percent)

Indicates the percentage of ports on your network with an acceptable error rate. If the value falls below the percentage entered here, the **Impact Status** on the Port Health chart moves from **Low** to **Medium**. For ports to be included, data collection must be enabled.

Medium/High Threshold (percent)
: Indicates the percentage of ports on your network with an acceptable error rate. If the value falls below the percentage entered here, the **Impact Status** on the Port Health chart moves from **Medium** to **High**. For ports to be included, data collection must be enabled.

Report Generation

Excessive Port Error Rate (percent)
: Indicates the port error rate, in percent of total port traffic, above which ExtremeCloud IQ Site Engine considers the port error rate excessive. A port error rate below this percentage is considered acceptable.

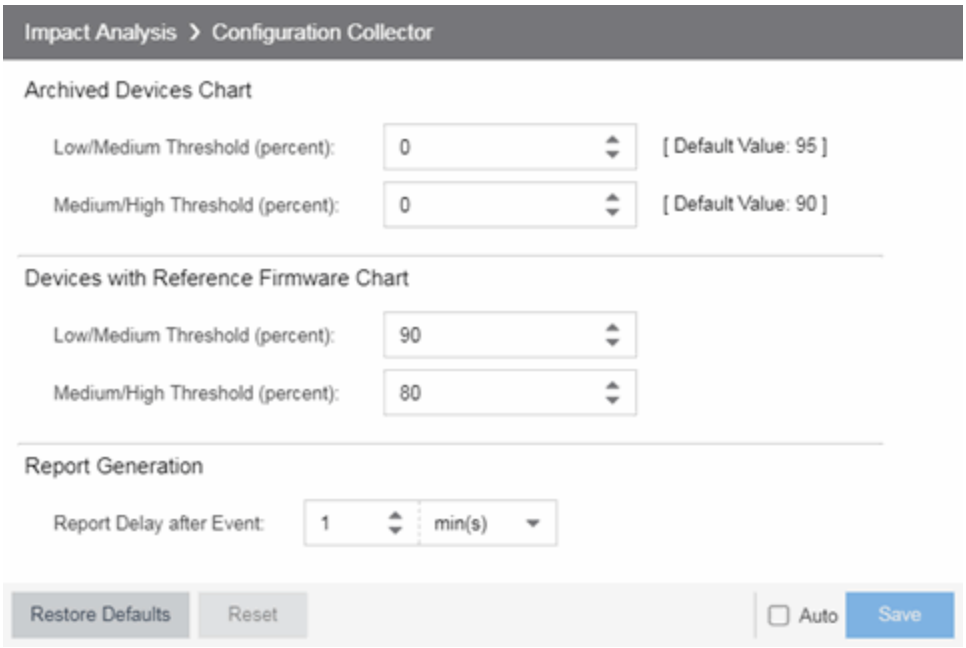
Excessive Port Utilization (percent)
: Indicates the port utilization, in percent of total port traffic, above which ExtremeCloud IQ Site Engine considers the port utilization excessive. A port utilization below the percentage entered here is considered acceptable.

Generate charts every
: Indicates the interval between which ExtremeCloud IQ Site Engine polls ports to generate the Port Capacity and Port Health charts.

Use data collected within
: Indicates the amount of time within which the data collected for a report is valid.

Configuration Collector

Use these options to configure the thresholds of the Archived Devices and the Devices with Reference Firmware charts in the Impact Analysis dashboard.



Archived Devices Chart



Low/Medium Threshold (percent)

Indicates the percentage of devices for which an archive was created within the duration you select in the Past Days field. If the value falls below the percentage entered here, the **Impact Status** on the Archived Devices chart moves from **Low** to **Medium**. For ports to be included, data collection must be enabled.

Medium/High Threshold (percent)
: Indicates the percentage of devices for which an archive was created within the duration you select in the Past Days field. If the value falls below the percentage entered here, the **Impact Status** on the Archived Devices chart moves from **Medium** to **High**. For ports to be included, data collection must be enabled.

Past Days
: Use the **Past Days** field to select the duration within which devices' archive activity is monitored by the Configuration Collector. Set the duration for any value between 1 and 100 days.

Devices with Reference Firmware Chart

Low/Medium Threshold (percent)
: Indicates the percentage of devices on which firmware you define as a reference image is installed. If the value falls below the percentage entered here, the **Impact Status** on the Devices with Reference Firmware chart moves from **Low** to **Medium**. For ports to be included, data collection must be enabled.

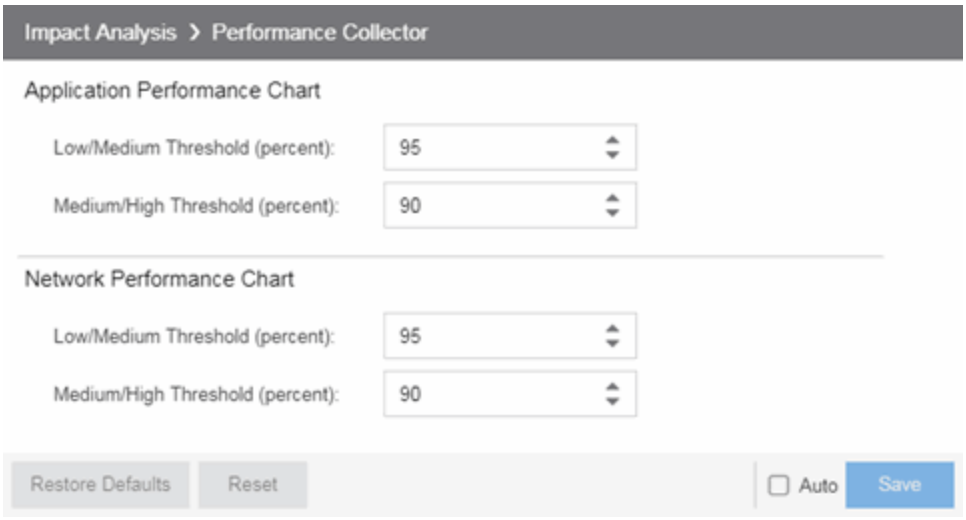
Medium/High Threshold (percent)
: Indicates the percentage of devices on which firmware you define as a reference image is installed. If the value falls below the percentage entered here, the **Impact Status** on the Devices with Reference Firmware chart moves from **Medium** to **High**. For ports to be included, data collection must be enabled.

Report Generation

Report Delay after Event
: Indicates the amount of time ExtremeCloud IQ Site Engine waits before reporting a device does not have an archive created in the last 30 days or does not have a reference firmware image installed.

Performance Collector

Use these options to configure the thresholds of the Application and Network Performance charts in the Impact Analysis dashboard.



Application Performance Chart

Low/Medium Threshold (percent)

Indicates the percentage of tracked applications with a response time in the expected or better than expected range. If the value falls below the percentage entered here, the **Impact Status** on the Application Performance chart moves from **Low** to **Medium**. The expected response time is established using an average of the previously observed response times.

Medium/High Threshold (percent)

Indicates the percentage of tracked applications with a response time in the expected or better than expected range. If the value falls below the percentage entered here, the **Impact Status** on the Application Performance chart moves from **Medium** to **High**. The expected response time is established using an average of the previously observed response times.

Network Performance Chart

Low/Medium Threshold (percent)

Indicates the percentage of network services with a response time in the expected or better than expected range. If the value falls below the percentage entered here, the **Impact Status** on the Network Performance chart moves from **Low** to **Medium**. The expected response time is established using an average of the previously observed response times.

Medium/High Threshold (percent)

Indicates the percentage of network services with a response time in the expected or better than expected range. If the value falls below the percentage entered here, the **Impact Status** on the Network Performance chart moves from **Medium** to **High**. The expected response time is established using an average of the previously observed response times.

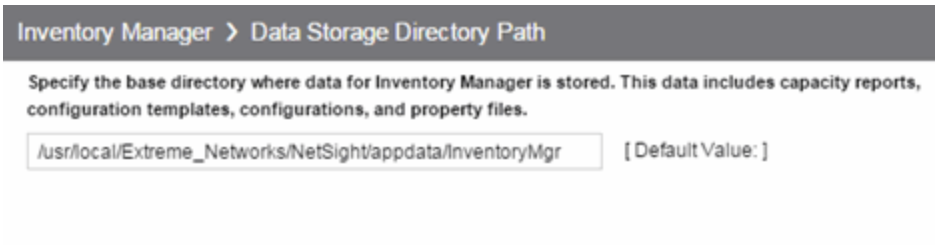
Inventory Manager Options

Selecting Inventory Manager in the left panel of the **Options** tab provides the following view, where you can select the path in which Inventory Manager data is stored as well as configure file transfer settings for firmware upgrades.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.

Data Storage Directory Path Setting

Use this option to specify a different base directory where Inventory Manager data is stored. This data includes capacity planning reports, configuration templates, archived configurations, and property files. If you specify a new data directory, you need to move the data files stored under the old directory to the new directory so ExtremeCloud IQ Site Engine can find them.



File Transfer Settings

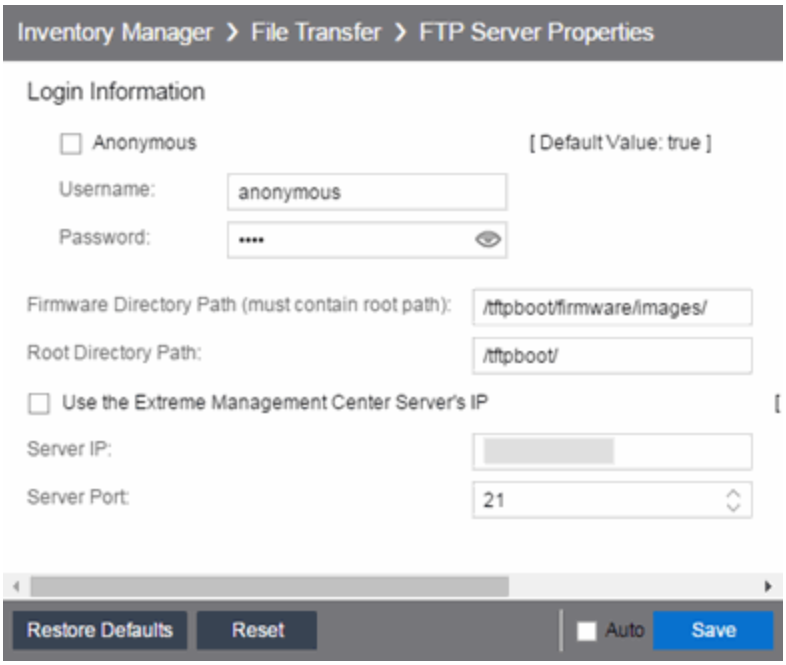
These options specify the FTP, SCP, SFTP, or TFTP file transfer settings used when upgrading firmware.

Select the link for information on the following File Transfer Settings options:

- FTP Server Properties Settings
- SCP Server Properties Settings
- SFTP Server Properties Settings
- TFTP Server Properties Settings

FTP Server Properties Settings

Use these options to set FTP server properties and login information, including specifying the FTP server IP address, setting paths to the root and firmware directories, and setting login information. The FTP server needs access to these directories in order to perform archive operations or firmware/boot PROM upgrades. These settings apply to all users.



Anonymous

Select this checkbox if your FTP server is configured to accept Anonymous logins. Selecting this checkbox disables the **Username** and **Password** fields.

Username/Password

Enter your username and password to access the FTP server. By default, your password is displayed as a series of asterisks. Select the **Eye** icon to display your password.

Firmware Directory Path

The default firmware directory is tftpboot/firmware/images. If you would like to use an alternate firmware directory, enter a path to that directory in this field. The firmware directory must be a subdirectory of the root directory. (For additional information, see How to Upgrade Firmware.) If you are using an FTP server on a remote system, use the UNC standard described in the following Note when specifying the path.

Root Directory Path

The root directory is the base directory to which the FTP server is allowed access. The FTP server is allowed to create files in or read files from this directory and any of its subdirectories. The default root directory is the tftpboot directory ExtremeCloud IQ Site Engine automatically creates when it is installed. To use an alternate root directory, enter a path to that directory in this field.

NOTE: Keep in mind the following requirements when setting the path to your root directory:

- If your FTP server is configured with an FTP root directory, it must match the root directory entered here.
- If your FTP server is **not** configured with an FTP root directory, change the FTP root directory here to the root of the drive.
- **If you are using an FTP server on a remote system,** use the Universal Naming Convention (UNC) when specifying the root directory path. The UNC convention uses two slashes // to indicate the name of the system, and one slash or backslash to indicate the path within the computer.

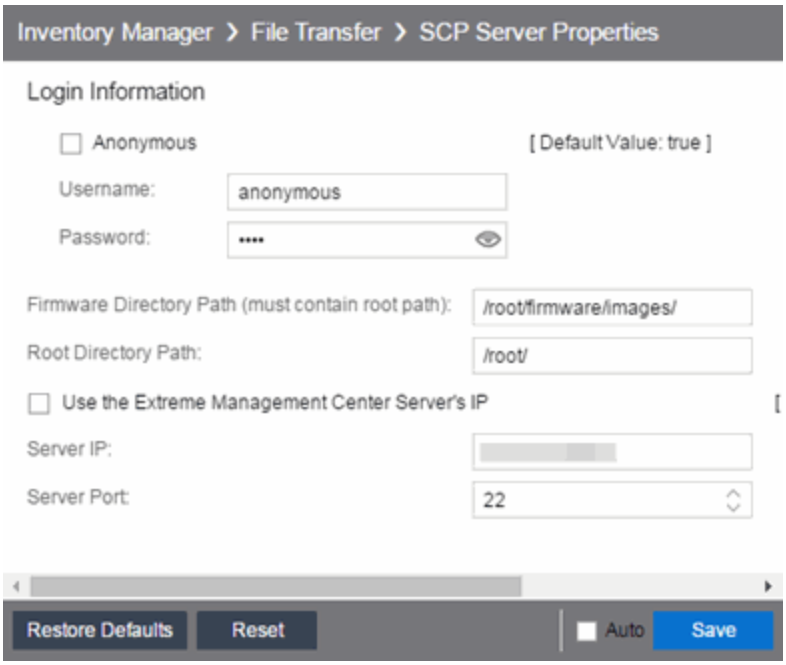
Use the ExtremeCloud IQ Site Engine Server's IP
Select this checkbox if your FTP server is on the same machine as the ExtremeCloud IQ Site Engine Server. Selecting this checkbox disables the **Server IP** field.

Server IP
Enter the IP address of the device where the FTP server resides.

Server Port
Specify the port number on which your FTP server is configured to run.

SCP Server Properties Settings

Use these options to set SCP server properties and login information, including specifying the SCP server IP address, setting paths to the root and firmware directories, and setting login information. The SCP server needs access to these directories in order to perform archive operations or firmware/boot PROM upgrades. These settings apply to all users.



Anonymous

Select this checkbox if your SCP server is configured to accept Anonymous logins. Selecting this checkbox disables the **Username** and **Password** fields.

Username/Password

Enter your username and password to access the SCP server. By default, your password is displayed as a series of asterisks. Select the **Eye** icon to display your password.

Firmware Directory Path

Enter the path to the default firmware directory in this field. The **Firmware Directory Path** must be a subdirectory of the **Root Directory Path**.

Example Scenario	Firmware Directory Path
A sftp user was created for SCP and SFTP purposes during the installation	`/home/sftp/firmware/images/`
A custom user was created for SCP and SFTP purposes during the installation	`/home/<custom>/firmware/images/`
A custom user was not created during the installation, the service is running under netsight	`/home/netsight/firmware/images/`
A custom user was not created during the installation, the service is running under root	`/root/firmware/images/`

NOTE: To ensure this directory is secure, change this path from the `{{tftpboot}}` directory. Using the `{{tftpboot}}` directory may provide access to a third-party.

Root Directory Path

Enter the path to the home directory specified in the Username field. The root directory is the base directory to which the SCP server is allowed access. The SCP server is allowed to create files in or read files from this directory and any of its subdirectories.

Example Scenario	Root Directory Path
A sftp user was created for SCP and SFTP purposes during the installation	`/home/sftp/`
A custom user was created for SCP and SFTP purposes during the installation	`/home/<custom>/`
A custom user was not created during the installation, the service is running under netsight	`/home/netsight/`
A custom user was not created during the installation, the service is running under root	`/root/`

NOTE: Keep in mind the following requirements when setting the path to your root directory:

- If your SCP server is configured with an SCP root directory, it must match the root directory entered here.
- If your SCP server is **not** configured with an SCP root directory, change the SCP root directory here to the root of the drive.
- To ensure this directory is secure, change this path from the `{{tftpboot}}` directory. Using the `{{tftpboot}}` directory may provide access to a third-party.
- **If you are using an SCP server on a remote system,** use the Universal Naming Convention (UNC) when specifying the root directory path. The UNC convention uses two slashes // to indicate the name of the system, and one slash or backslash to indicate the path within the computer.

Use the ExtremeCloud IQ Site Engine Server's IP

Select this checkbox if your SCP server is on the same machine as the ExtremeCloud IQ Site Engine Server. Selecting this checkbox disables the **Server IP** field.

Server IP

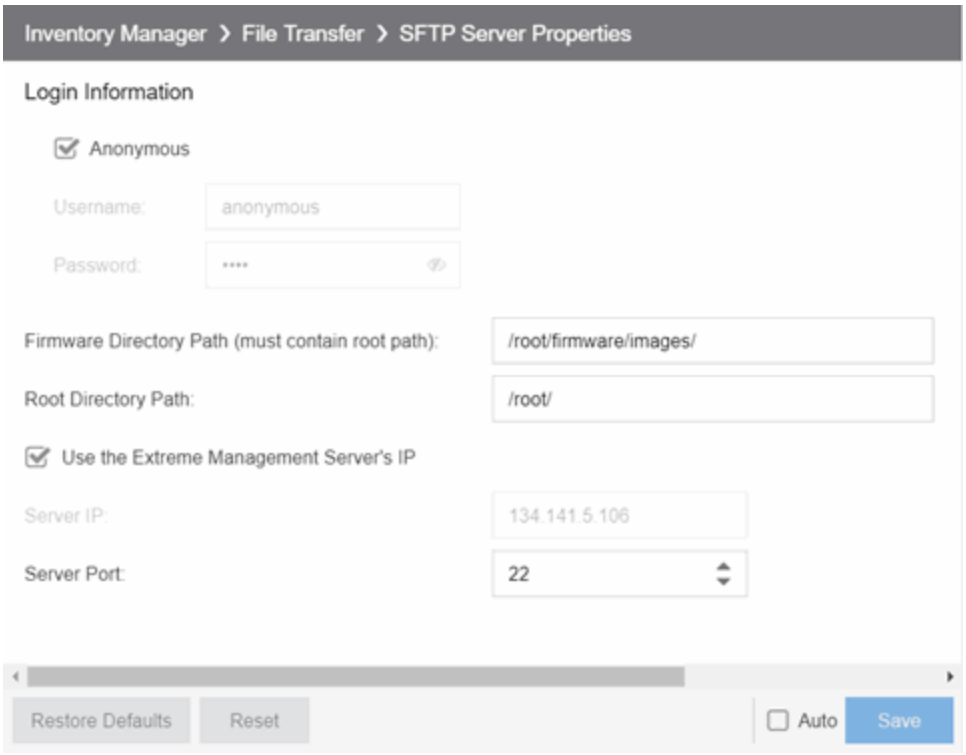
Enter the IP address of the device where the SCP server resides.

Server Port

Specify the port number on which your SCP server is configured to run.

SFTP Server Properties Settings

Use these options to set SFTP server properties and login information, including specifying the SFTP server IP address, setting paths to the root and firmware directories, and setting login information. The SFTP server needs access to these directories in order to perform archive operations or firmware/boot PROM upgrades. These settings apply to all users.



Anonymous

Select this checkbox if your SFTP server is configured to accept Anonymous logins. Selecting this checkbox disables the **Username** and **Password** fields.

Username/Password

Enter your username and password to access the SFTP server. By default, your password is displayed as a series of asterisks. Select the **Eye** icon to display your password.

Firmware Directory Path

Enter the path to the default firmware directory in this field. The **Firmware Directory Path** must be a subdirectory of the **Root Directory Path**.

Example Scenario	Firmware Directory Path
A sftp user was created for SCP and SFTP purposes during the installation	`/home/sftp/firmware/images/`
A custom user was created for SCP and SFTP purposes during the installation	`/home/<custom>/firmware/images/`
A custom user was not created during the installation, the service is running under netsight	`/home/netsight/firmware/images/`
A custom user was not created during the installation, the service is running under root	`/root/firmware/images/`

For additional information, see How to Upgrade Firmware. If you are using an SFTP server on a remote system, use the UNC standard described in the following Note when specifying the path.

NOTE: To ensure this directory is secure, change this path from the `{{tftpboot}}` directory. Using the `{{tftpboot}}` directory may provide access to a third-party.

Root Directory Path

Enter the path to the home directory specified in the username field. The root directory is the base directory to which the SFTP server is allowed access. The SFTP server is allowed to create

files in or read files from this directory and any of its subdirectories.

Example Scenario	Root Directory Path
A sftp user was created for SCP and SFTP purposes during the installation	`/home/sftp/`
A custom user was created for SCP and SFTP purposes during the installation	`/home/<custom>/`
A custom user was not created during the installation, the service is running under netsight	`/home/netsight/`
A custom user was not created during the installation, the service is running under root	`/root/`

NOTE: Keep in mind the following requirements when setting the path to your root directory:

- If your SFTP server is configured with an SFTP root directory, it must match the root directory entered here.
- If your SFTP server is **not** configured with an SFTP root directory, change the SFTP root directory here to the root of the drive.
- To ensure this directory is secure, change this path from the `{{tftpboot}}` directory. Using the `{{tftpboot}}` directory may provide access to a third-party.
- **If you are using an SFTP server on a remote system,** use the Universal Naming Convention (UNC) when specifying the root directory path. The UNC convention uses two slashes // to indicate the name of the system, and one slash or backslash to indicate the path within the computer.

Use the ExtremeCloud IQ Site Engine Server's IP

Select this checkbox if your SFTP server is on the same machine as the ExtremeCloud IQ Site Engine Server. Selecting this checkbox disables the **Server IP** field.

Server IP

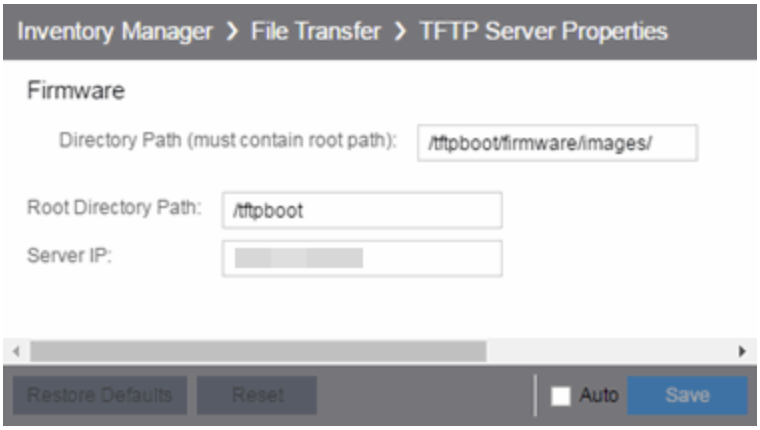
Enter the IP address of the device where the SFTP server resides.

Server Port

Specify the port number on which your SFTP server is configured to run.

TFTP Server Properties Settings

Use these options to set TFTP server properties, including specifying the firmware directory path, setting the TFTP root directory path, and setting server IP address. These settings apply to all users.



Directory Path

The default firmware directory is `tftpboot/firmware/images`. If you would like to use an alternate firmware directory, enter a path to that directory in this field. The firmware directory must be a subdirectory of the root directory. (For additional information, see How to Upgrade Firmware.)

Root Directory Path

The root directory is the base directory to which the TFTP server is allowed access. The TFTP server is allowed to create files in or read files from this directory and any of its subdirectories. The default root directory is the tftpboot directory ExtremeCloud IQ Site Engine automatically creates when it is installed. To use an alternate root directory, enter a path to that directory in this field.

NOTE:

Keep in mind the following requirements when setting the path to your root directory:

- If your TFTP server is configured with a TFTP root directory, it must match the root directory entered here.
- If your TFTP server is **not** configured with a TFTP root directory, change the TFTP root directory here to the root of the drive.
- **If you are using a TFTP server on a remote system,** use the Universal Naming Convention (UNC) when specifying the root directory path. The UNC convention uses two slashes // to indicate the name of the system, and one slash or backslash to indicate the path within the computer.

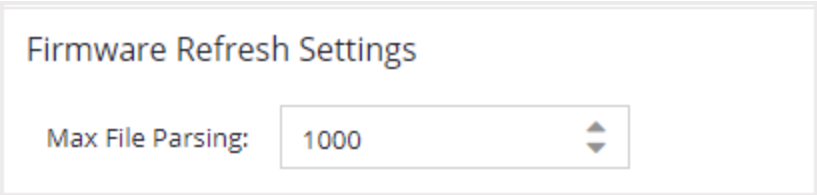
Server IP

Enter the IP address of the device where the TFTP server resides.

Firmware Refresh Settings

Max Files Parsed

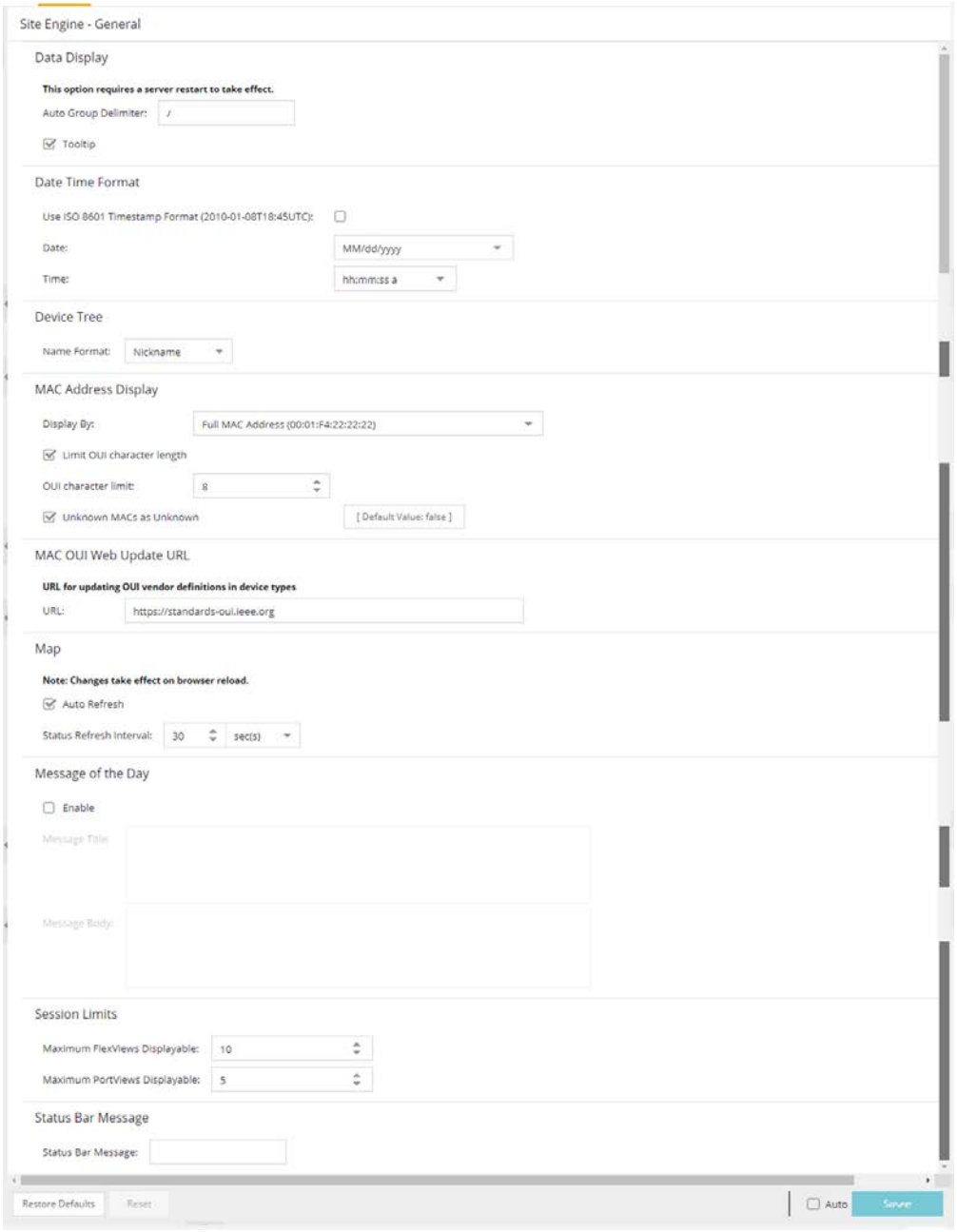
This option controls the maximum number of files to parse when ExtremeCloud IQ Site Engine searches the path for device firmware files. The maximum is 65535, and the default is 1000.



ExtremeCloud IQ Site Engine Options

Selecting Site Engine - General in the left panel of the **Options** tab provides the following view, where you can customize ExtremeCloud IQ Site Engine preferences. These settings apply to the user currently logged-in.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.



Data Display

Auto Group Delimiter

ExtremeCloud IQ Site Engine uses this character to separate the values that define a device's **Contact** and **Location** grouping in the left-panel device tree. Sub-groups in the **Grouped By > Contact** and **Grouped By > Location** folders are automatically created based on the Contact and Location values in the Console Properties Tab (Device). Use this option to define the delimiter that is used to separate those values into groups. For example, using the default delimiter (/), a device's location defined as *NewHampshire/Salem/Closet3* will automatically create a hierarchy of three sub-groups under the **Grouped By > Location** folder.

After changing the Auto Group Delimiter, you must restart the ExtremeCloud IQ Site Engine server.

Date Time Format

Use ISO 8601 Timestamp Format

Select the checkbox to use the ISO 8601 timestamp format (yyyy-mm-ddThh:mm:ssTimeZone) in ExtremeCloud IQ Site Engine. Selecting this checkbox disables the **Date** and **Time** fields.

Date

To determine how the date is formatted in ExtremeCloud IQ Site Engine, expand the drop-down list and select a format.
The options in this field signify the following:

- **MM/dd/yyyy** — Month/Day/Year (for example, 10/19/2020)
- **yyyy/MM/dd** — Year/Month/Day (for example, 2020/10/19)
- **dd/MM/yyyy** — Day/Year/Year (for example, 19/10/2020)
- **MMM dd, yyyy** — Month (abbreviated) Day, Year (for example, Oct. 19, 2020)

Time

Select whether time is formatted as a 12-hour (**hh:mm:ss a**) or 24-hour (**HH:mm:ss**) clock.

The options in this field signify the following:

- **hh:mm:ss a** — Hour:Minute:Second am or pm (for example, 3:30:10 pm).
- **HH:mm:ss** — Hour:Minute:Second (for example, 15:30:10)
- **hh:mm:ss.SSS a** — 12-hour time format with millisecond precision (for example, 2:30:45.123 PM)

- HH:mm:ss.SSS — 24-hour time format with millisecond precision (for example, 14:30:45.123)

NOTE: After upgrading ExtremeControl to version 26.06.10 or later, configure the syslog event log format to ISO 8601. The ISO 8601 timestamp format is required for correct parsing and display of high-precision timestamps in the event log. During a clean install the ISO 8601 timestamp format setting is configured automatically.

Device Tree

Name Format

Select one of the following options to choose how the device name displays in the Device Tree. The Name Format you select will also be used as the Source in the Events Log.

- **IP** — use the device's IP address.
- **System Name** — use the administratively-assigned name of the device taken from the *sysName* MIB object.
- **Nickname** — use the user-defined nickname as defined in the Configure Device window.

MAC Address Display

Display By

Select the format ExtremeCloud IQ Site Engine uses to display MAC addresses: the entire MAC address, or the MAC OUI prefix.

Limit OUI character length

Select the checkbox to configure the length of the MAC OUI displayed in ExtremeCloud IQ Site Engine. After selecting this checkbox, use the **OUI character limit** field to define the number of characters ExtremeCloud IQ Site Engine displays.

OUI character limit

Enter the number of characters ExtremeCloud IQ Site Engine displays for a MAC OUI prefix.

Unknown MACs as Unknown

Select the checkbox to display **Unknown** for MAC addresses ExtremeCloud IQ Site Engine can not determine.

MAC OUI Web Update URL

URL for updating OUI vendor definitions in device types

This field allows you to define the URL used for the MAC OUI Vendor update.

Map

Auto Refresh
: Use this function to refresh maps based on the interval set in **Status Refresh Interval**. It is turned on by default.

Status Refresh Interval
: Select the interval that determines how often maps are automatically refreshed by ExtremeCloud IQ Site Engine.

Message of the Day

Enable
: Select the checkbox to enable the **Message Title** and **Message Body** fields, where you can enter a message that displays to all users accessing ExtremeCloud IQ Site Engine.

Message Title
: Enter a title for the message displayed to all ExtremeCloud IQ Site Engine users when the **Enable** checkbox is selected.

Message Body
: Enter a body for the message displayed to all ExtremeCloud IQ Site Engine users when the **Enable** checkbox is selected.

Session Limits

Maximum FlexViews Displayable
: Allows you to determine the maximum number of FlexViews displayed per session.

Maximum PortViews Displayable
: Allows you to determine the maximum number of PortViews displayed per session.

Status Bar Message

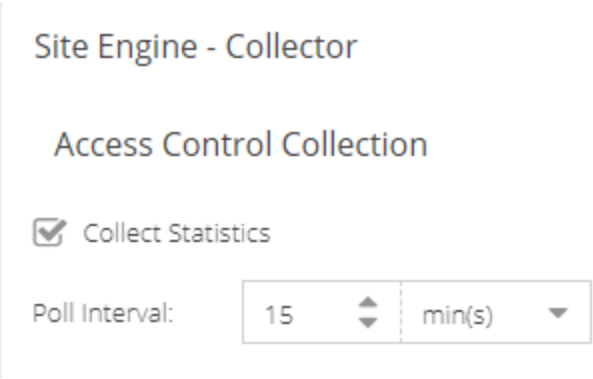
Status Bar Message
: Allows you to add custom information (for example, your organization's name) to the footer of ExtremeCloud IQ Site Engine pages.

ExtremeCloud IQ Site Engine Collector Options

Selecting Site Engine - Collector in the left panel of the **Options** tab provides the following view, where you can configure ExtremeCloud IQ Site Engine Collector tree settings. Use these settings to access advanced device and interface collection settings for the ExtremeCloud IQ Site Engine Collector.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.

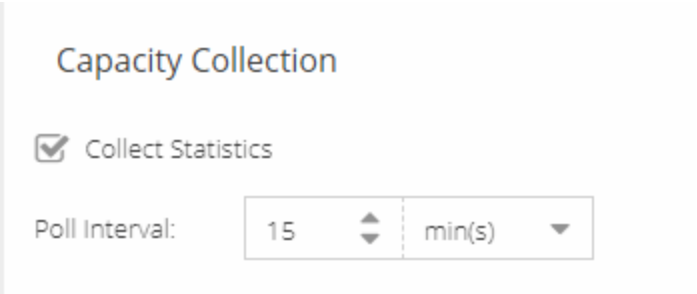
Access Control Collection



Collect Statistics
Select this check box to enable ExtremeControl data collection.

Poll Interval
The amount of time the data collector waits between polling ExtremeControl engines.

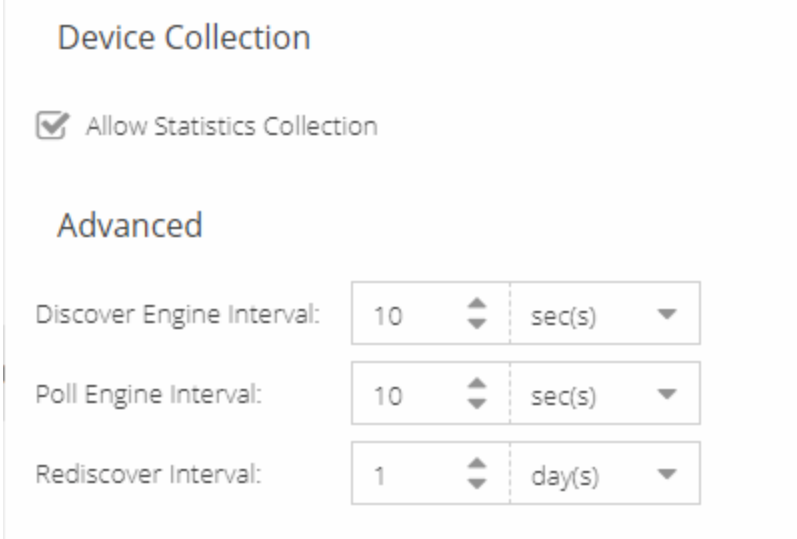
Capacity Collection



Collect Statistics
Enables or disables additional statistics collection.

Poll Interval
The amount of time the data collector waits between polling devices.

Device Collection



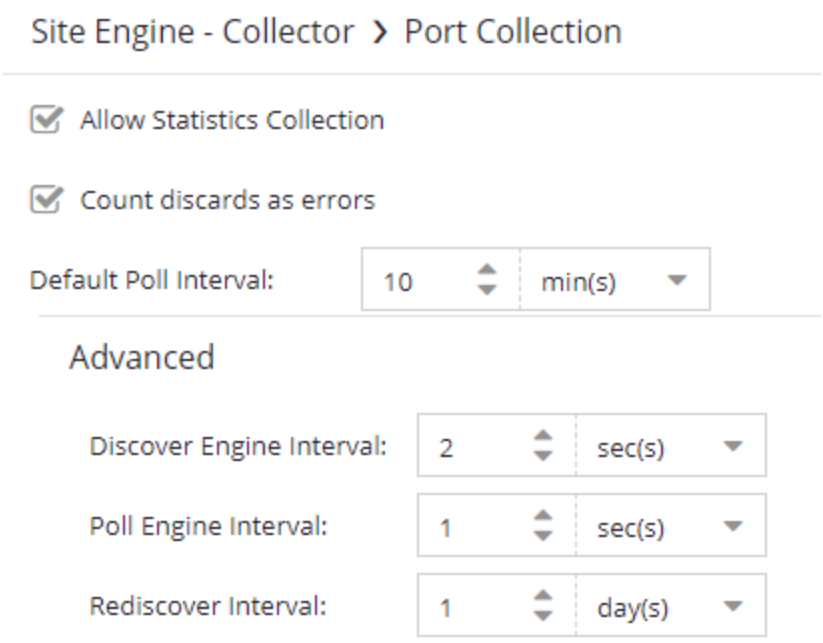
Allow Statistics Collection
Select this check box if you want statistics to be collected when you have enabled statistics collection on the device.

Discover Engine Interval
This interval specifies the frequency with which the data collector performs discover operations on the collection targets. Discover operations are performed in blocks specified by the **Maximum Outstanding SNMP per Collector** value, with a new block scheduled according to the interval specified here.

Poll Engine Interval
The amount of time the data collector waits between polling devices.

Rediscover Interval
This interval specifies the frequency with which the data collector performs a rediscover operation on the collection targets.

Port Collection



Allow Statistics Collection
Disable the check box if you do not want statistics to be collected when you have enabled statistics collection on the port.

Count discards as errors
Disable the check box if you do not want to count ifDiscards and ifOutDiscards as errors.

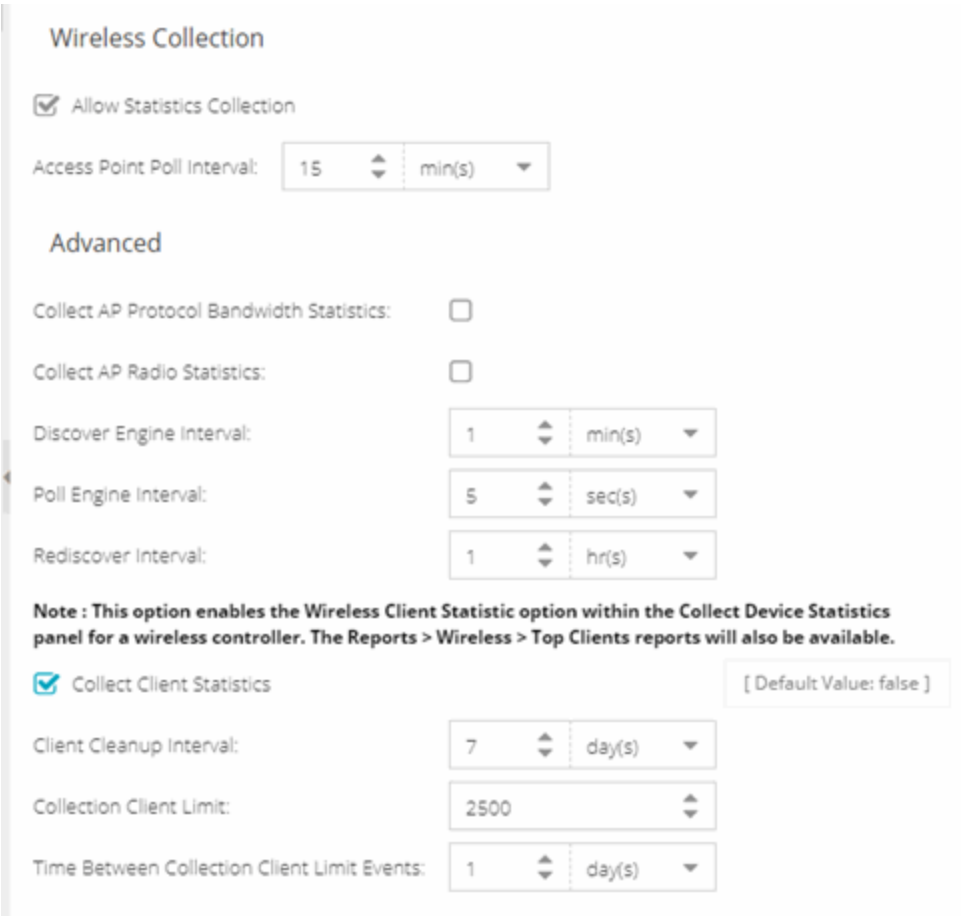
Default Poll Interval
The Poll Interval specifies the frequency with which the data collector polls the collection targets. The default interval of 10 minutes is assigned when the port is configured.

Discover Engine Interval
This interval specifies the frequency with which the data collector performs discover operations on the collection targets. Discover operations are performed in blocks specified by the **Maximum Outstanding SNMP per Collector** value, with a new block scheduled according to the interval specified here.

Poll Engine Interval
This interval specifies the frequency with which the data collector polls the collection targets. Polling is performed in blocks specified by the **Maximum Outstanding SNMP per Collector** value, with a new block scheduled according to the interval specified here.

Rediscover Interval
This interval specifies the frequency with which the data collector performs a rediscover operation on the collection targets.

Wireless Collection



Allow Statistics Collection

Select this check box if you want statistics to be collected when you have enabled statistics collection on the wireless device.

Access Point Poll Interval

The amount of time the data collector waits between polling wireless access points. Valid values are 1-60 minutes.

Collect AP Protocol Bandwidth Statistics

Select the checkbox to collect protocol bandwidth statistics for your access points.

NOTE: The statistics collected in this report are used in the Venue Report. Only enable this option if you use that report.

Collect AP Radio Statistics

Select the checkbox to collect radio statistics for your access points.

NOTE: The statistics collected in this report are used in the Venue Report. Only enable this option if you use that report.

Discover Engine Interval

This interval specifies the frequency the data collector performs discover operations on the collection targets. Discover operations are performed in blocks specified by the **Maximum Outstanding SNMP per Collector** value, with a new block scheduled according to the interval specified here.

Poll Engine Interval

This interval specifies the frequency with which the data collector polls the collection targets. Polling is performed in blocks specified by the **Maximum Outstanding SNMP per Collector** value, with a new block scheduled according to the interval specified here.

Rediscover Interval

This interval specifies the frequency the data collector performs a rediscover operation on the collection targets.

Collect Client Statistics

Use this check box to enable or disable client data collection. Collect Client Statistics is disabled by default.

Client Cleanup Interval

Wireless client statistics stored by the data collector are periodically cleaned up according to this interval. When the **Collection Client Limit** is reached, clients inactive longer than the time specified in the **Time Between Collection Client Limit Events** are aged out.

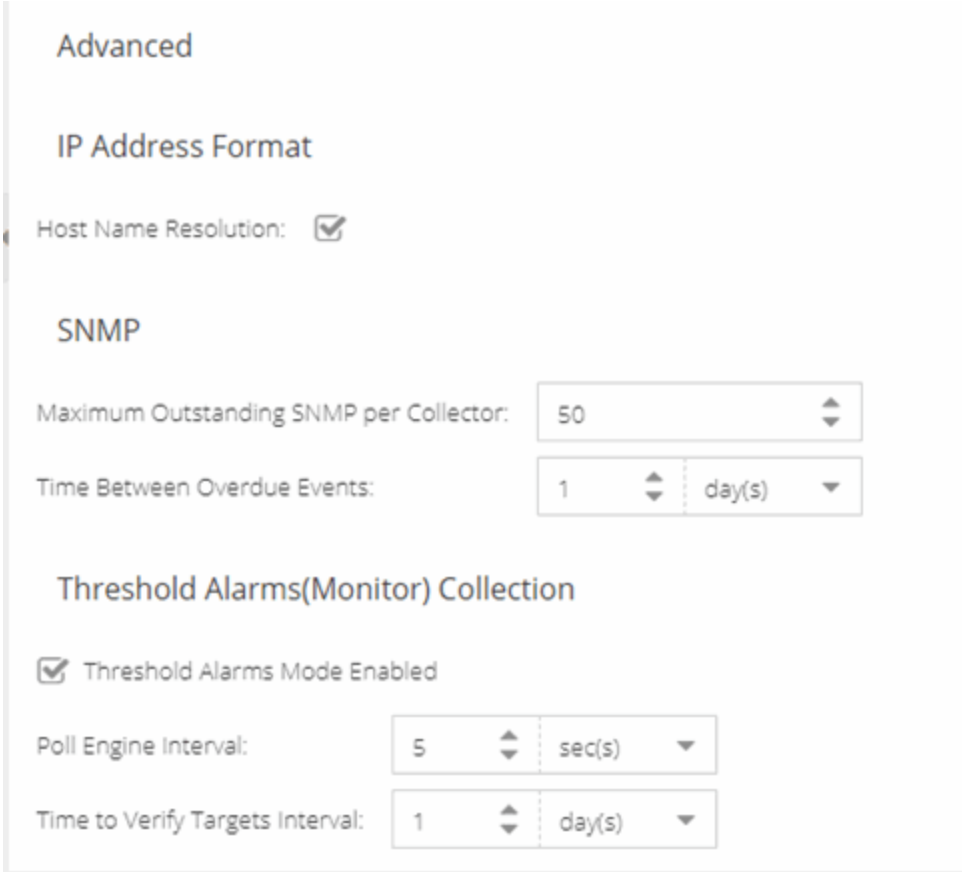
Collection Client Limit

The maximum number of wireless clients for which statistics are stored per collection interval. Valid values are 1 to 30,000.

Time Between Collection Client Limit Events

During a client cleanup, if a client is inactive for the amount of time specified here, then the client is aged out. Historical statistics already persisted are not removed.

Advanced



Host Name Resolution

Select this option to resolve host names to IP addresses and IP addresses to host names, if possible. This option enables you to disable host name resolution for this feature only. (Host name resolution is enabled globally using the **Enable Name Resolution** option.)

Maximum Outstanding SNMP per Collector

The number of simultaneous SNMP requests a collector can make. The data collector works with blocks of SNMP requests, starting a new block each time the outstanding block completes. Valid values are 1-500.

Time Between Overdue Events

During a client cleanup, if a client is inactive for the amount of time specified here, then the client is aged out. Historical statistics already persisted are not removed.

Threshold Alarms (formerly Monitor) Mode Enabled

Use this option to enable or disable threshold alarms mode statistic collection. If threshold alarms mode is disabled, the **Threshold Alarms Mode** option is not available when configuring

device or interface statistics collection. All threshold mode statistic collection is stopped and the cache is cleared. For additional information, seeEnable Report Data Collection.

Poll Engine Interval

This interval specifies the frequency the data collector polls the collection targets. Polling is performed in blocks specified by the **Maximum Outstanding SNMP per Collector** value, with a new block scheduled according to the interval specified here.

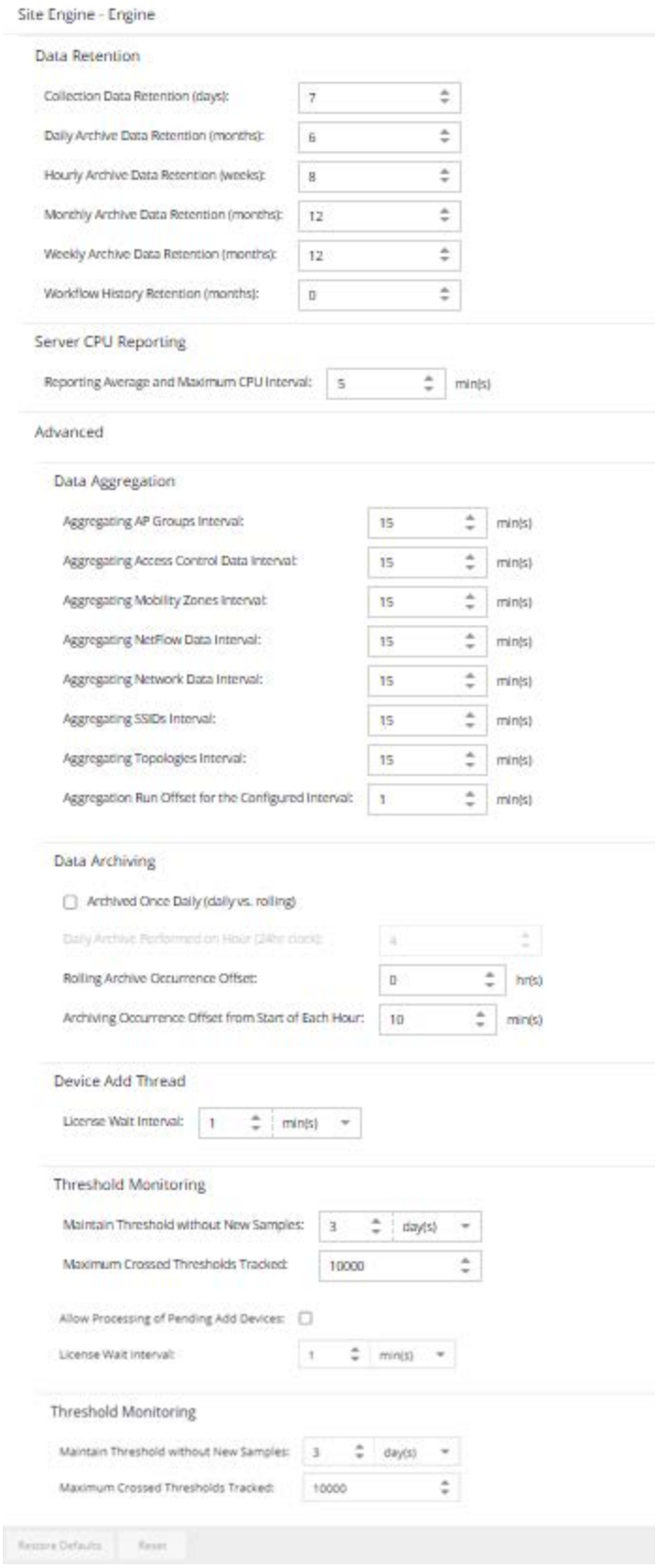
Time to Verify Targets Interval

The interval between a check of all targets (devices and interfaces) set to Threshold Alarms mode statistic collection. The check generates a summary event in the **Alarms and Events** tab event log (one for devices and one for interfaces) that shows the number of targets where corresponding threshold alarms are not configured. Disable Threshold Alarms mode for those targets or configure appropriate threshold alarms in order to reduce unnecessary statistic collection.

Engine Options

Selecting ExtremeCloud IQ Site Engine Engine in the left panel of the **Options** tab provides the following view, where you can specify data aging options and advanced settings for data archiving and aggregation.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.


Site Engine - Engine
Data Retention
Collection Data Retention (days): 7
Daily Archive Data Retention (months): 6
Hourly Archive Data Retention (weeks): 8
Monthly Archive Data Retention (months): 12
Weekly Archive Data Retention (months): 12
Workflow History Retention (months): 0
Server CPU Reporting
Reporting Average and Maximum CPU Interval: 5 min(s)
Advanced
Data Aggregation
Aggregating AP Groups Interval: 15 min(s)
Aggregating Access Control Data Interval: 15 min(s)
Aggregating Mobility Zones Interval: 15 min(s)
Aggregating NetFlow Data Interval: 15 min(s)
Aggregating Network Data Interval: 15 min(s)
Aggregating SSIDs Interval: 15 min(s)
Aggregating Topologies Interval: 15 min(s)
Aggregation Run Offset for the Configured Interval: 1 min(s)
Data Archiving
Archived Once Daily (daily vs. rolling)
Daily Archive Performed on Hour (24hr clock): 4
Rolling Archive Occurrence Offset: 0 hr(s)
Archiving Occurrence Offset from Start of Each Hour: 10 min(s)
Device Add Thread
License Wait Interval: 1 min(s)
Threshold Monitoring
Maintain Threshold without New Samples: 3 day(s)
Maximum Crossed Thresholds Tracked: 10000
Allow Processing of Pending Add Devices:
License Wait Interval: 1 min(s)
Threshold Monitoring
Maintain Threshold without New Samples: 3 day(s)
Maximum Crossed Thresholds Tracked: 10000
Restore Defaults
Reset

Data Retention

Collection Data Retention (days)

This setting specifies how long (in days) to retain the raw data collected by the data collector. Valid values are 1-1000 days.

Daily Archive Data Retention (months)

Every day, the hourly data is condensed into daily average values and archived. This setting specifies how long (in months) to maintain the archived daily data. Valid values are 1-200 months.

Hourly Archive Data Retention (weeks)

Every hour, the raw data is condensed into hourly average values and archived. This setting specifies how long (in weeks) to maintain the archived hourly data. Valid values are 1-800 weeks.

Monthly Archive Data Retention (months)

Every month, the weekly data is condensed into monthly average values and archived. This setting specifies how long (in months) to maintain the archived monthly data. Valid values are 1-200 months.

Weekly Archive Data Retention (months)

Every week, the daily data is condensed into weekly average values and archived. This setting specifies how long (in months) to maintain the archived weekly data. Valid values are 1-200 months.

Workflow History Retention (months)

This setting specifies how long (in months) to retain the workflow history data logged. Valid values are 0-36 months. The default value 0 retains all workflow history indefinitely.

Server CPU Reporting

Reporting Average and Maximum CPU Interval

ExtremeCloud IQ Site Engine collects CPU usage statistics monitoring for the ExtremeCloud IQ Site Engine server. At 5 minute intervals (the default interval) the collected usage data is averaged, and the average and maximum statistics are reported to the ExtremeCloud IQ Site Engine database to provide data for the ExtremeCloud IQ Site Engine Server CPU Utilization report. You can change the default interval setting here, if desired. A shorter interval provides a more granular picture of CPU usage while a longer interval would mean that less data is stored in the database. Valid values are 1-59 minutes.

Advanced

Data Aggregation

Use the data aggregation settings to specify how often collected data is aggregated into one statistic for AP Groups, Mobility Zones, SSIDs, Topologies, Policy Rule Hits, Network, ExtremeControl, and NetFlow. For example, the data collected for all the APs in an AP group are aggregated into one AP Group statistic according to the specified interval. Intervals are based on the 0 minute of the hour, so with an interval of 15 minutes, the aggregation is performed every 15 minutes starting from the top of the hour. The offset allows for the time it takes for data to be collected and reported to the database. If the offset is too short, then the aggregation can be performed before all the data is reported to the database. In the case where there is a long latency in reporting data to the database, increase the offset in order to make sure all the data is included in the aggregation.

Data Archiving

Use the data archiving settings to specify whether collection data should be archived on a daily basis or rolling basis (the default).

- **Daily Archive** — Select this checkbox to archive all the collection data (including the raw data, and the hourly, daily, weekly, and monthly data) one time daily at a certain time. The **Daily Archive Performed on Hour (24)** field displays, where you can specify the hour of day to perform the daily archive. The number entered in this field represents the time, so a value of **0** signifies midnight, while a value of **20** signifies 8:00 PM.
- **Rolling Archive** — If you want the collection data to be archived on a rolling basis (archives are performed on an hourly, daily, weekly, or monthly basis as needed), specify the offset (in hours and minutes) the rolling archive is performed, following the end of the data collection period. The offset allows for the time it takes for data to be collected and reported to the database. If the offset time is too short, then the archive can be performed before all the data is reported to the database. In cases with a long latency in reporting data to the database, you can increase the offset in order to make sure all the data is included in the archive.

Device Add Thread

These settings apply to pending devices:

- **Allow Deleting of Pending Devices:** — Select the check box to allow a device in the process of being added to ExtremeCloud IQ Site Engine can be deleted. This is not recommended unless instructed by GTAC.
- **Allow Processing of Pending Add Devices** — Select the check box to allow any device currently waiting for a license from ExtremeCloud IQ to complete the add process while in the pending state. Add Actions that require a license will be skipped. This setting will revert back to unchecked after processing the pending device queue.
- **License Wait Interval:** Select the poll interval to check for new devices being added to ExtremeCloud IQ Site Engine that are waiting for a license from ExtremeCloud IQ.

Threshold Monitoring

These settings apply to threshold alarms:

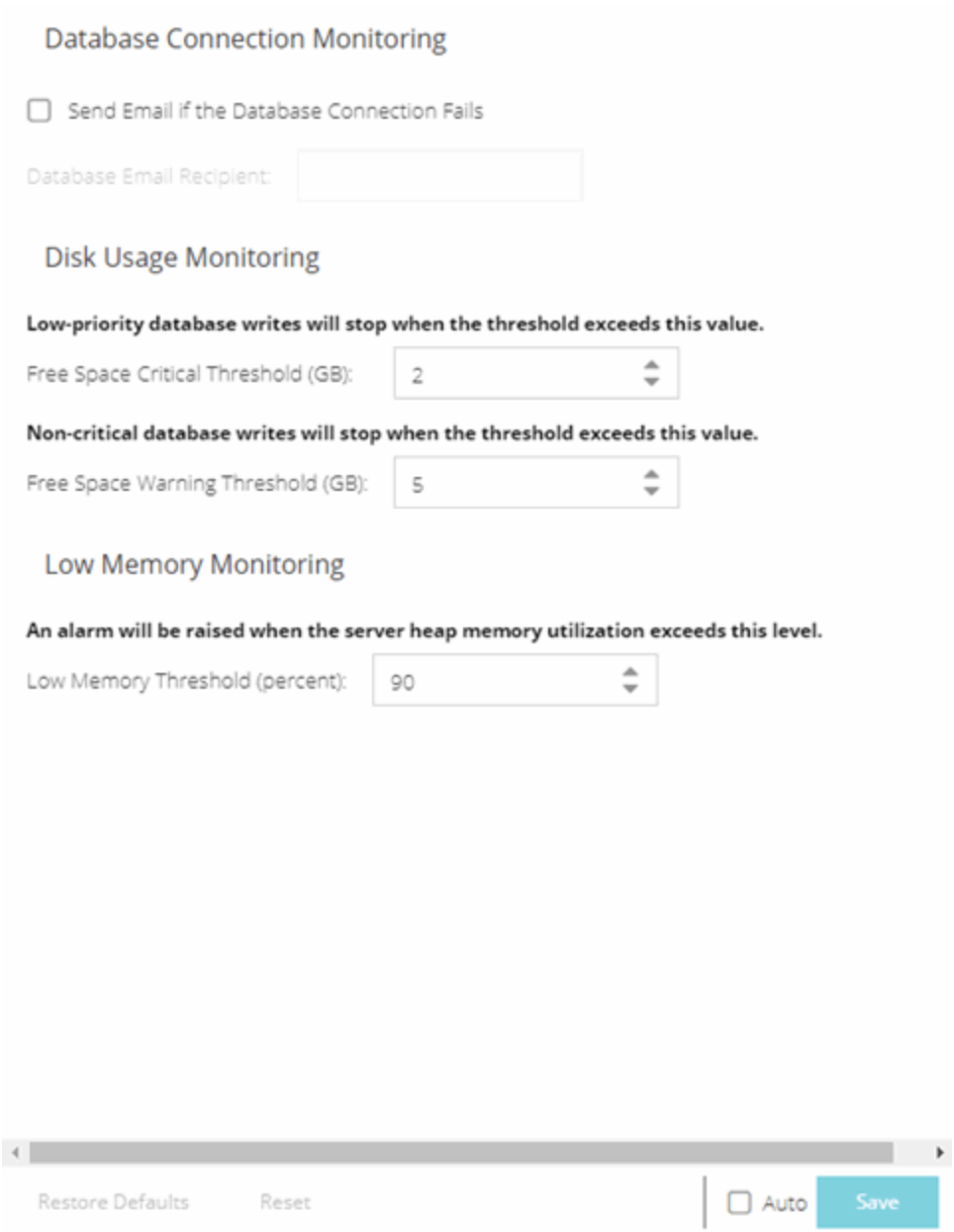
- **Maintain Threshold without New Samples** — Determines when a crossed threshold state expires due to inactivity (no new samples received). The default length of time is 72 hours. If there are no samples received during this time period, the threshold state is deleted and the associated alarm is cleared.
- **Maximum Crossed Thresholds Tracked** — To prevent memory over-utilization, there is a maximum number of crossed threshold states that are maintained. The default maximum number is 10,000. If this number is exceeded, the oldest 10% are deleted and the associated alarm is cleared.

- Administration

Server Health Options

Selecting Site Engine - Server Health in the left panel of the **Options** tab provides the following view, where you can configure warnings to help monitor the ExtremeCloud IQ Site Engine server health.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.



Database Connection Monitoring

Send Email if the Database Connection Fails

Select the checkbox to send an email notification if the ExtremeCloud IQ Site Engine database goes down, and when the database comes back up again.

Database Email Recipient

If **Send Email if the Database Connection Fails** is selected, enter an email address where the email notification is sent in the event the database connection fails.

Disk Usage Monitoring

Free Space Critical Threshold (GB)

Enter the amount of disk space (in GB) below which the ExtremeCloud IQ Site Engine server stops writing low-priority data to the database.

Free Space Warning Threshold (GB)

Enter the amount of disk space (in GB) below which ExtremeCloud IQ Site Engine stops writing non-critical data to the database and sends you a low-disk space warning.

Low Memory Monitoring

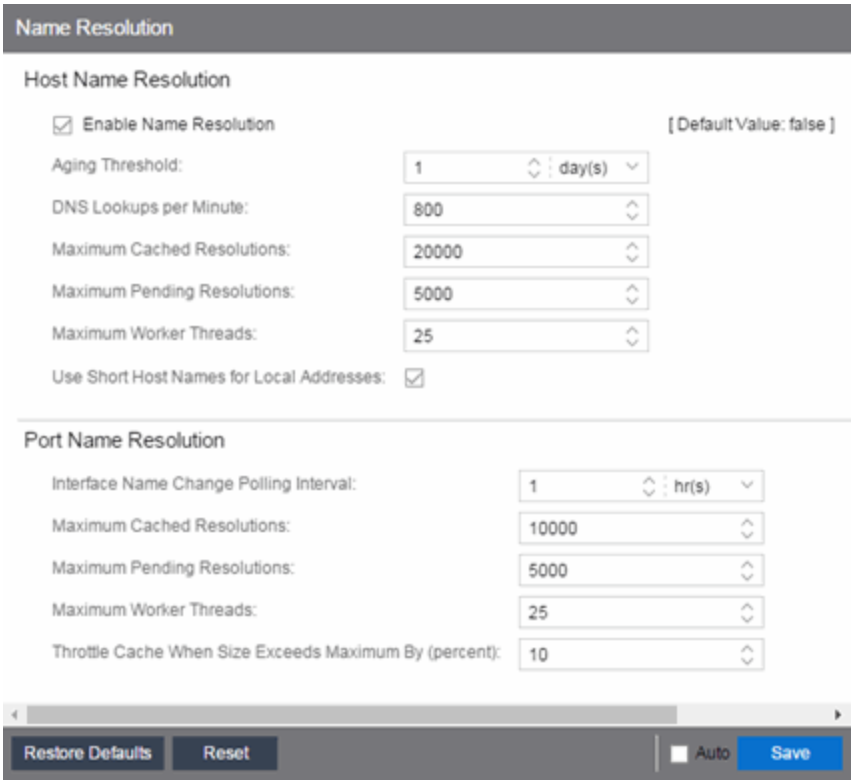
Low Memory Threshold (percent)

Enter a percentage to specify the server heap memory utilization percentage above which an alarm is raised. If the memory utilization falls more than five percent below the threshold percentage, the alarm is automatically cleared.

Name Resolution Options

Selecting Name Resolution in the left panel of the **Options** tab displays the following view, where you can configure options related to host name and port name resolution.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.



Host Name Resolution

Use this section to set options for resolving host names to IP addresses and IP addresses to host names.

Enable Name Resolution

Select this option display host names in place of IP addresses throughout ExtremeCloud IQ Site Engine. This feature is primarily used by NetFlow. With name resolution enabled, flow data shows "Client=rsmith-ws Server=proxy-usa", rather than "client=10.20.0.2 server = 10.20.0.1". The option is off by default because name resolution can add additional load on the network's DNS server.

Aging Threshold

Use this option to determine how long IP/host name pairs are cached in memory. After the aging threshold time has passed, the IP/host name pair is removed from the cache in order to prevent stale IP/host name associations. This option addresses the fact that DHCP assigns a new IP address to users frequently, especially on reboots. Without an aging threshold, host names continue to be associated to the IP they had at the first lookup. The default value is 24 hours; the minimum value is 1 hour.

DNS Lookups per Minute

The maximum number of host name lookups that the DNS server can perform each minute. This prevents host name resolution from using so many resources on a switch, which can affect switching of real traffic.

Maximum Cached Resolutions

The maximum number of IP/host name pairs that can be cached in memory. This number can be adjusted to control the amount of memory used by this service.

Maximum Pending Resolutions

The maximum number of host name resolution requests that can be queued up. This number can be adjusted to control the maximum amount of time spent waiting for a resolution.

Maximum Worker Threads

The maximum number of host name lookups that can be done at the same time. This number can be adjusted to control the amount of system resources used by host name resolution.

Use Short Host Names for Local Addresses

This option is enabled by default when host name resolution is enabled. When enabled, the host name cache removes the fully qualified host name's domain if it matches one of the specified local address domains. For example, "jsmith-ws.mycompany.com" displays as "jsmith-ws" if mycompany.com is listed as a local address domain. Disable this option when troubleshooting problems with host name resolution, or if IP addresses are preferred.

Port Name Resolution

Use this section to set options for resolving device port indices to port names and port aliases, and device port names and port aliases to port indices.

Interface Name Change Polling Interval

This option specifies how often the port name resolution service checks devices to see if port information has changed.

Maximum Cached Resolutions

The maximum amount of port data that can be cached in memory. This number can be adjusted to control the amount of memory used by this service.

Maximum Pending Resolutions

The maximum number of port name resolution requests that can be queued up. This number can be adjusted to control the maximum amount of time spent waiting for a resolution.

Maximum Worker Threads

The maximum number of port name lookups that can be done at the same time. This number can be adjusted to control the amount of system resources used by port name resolution.

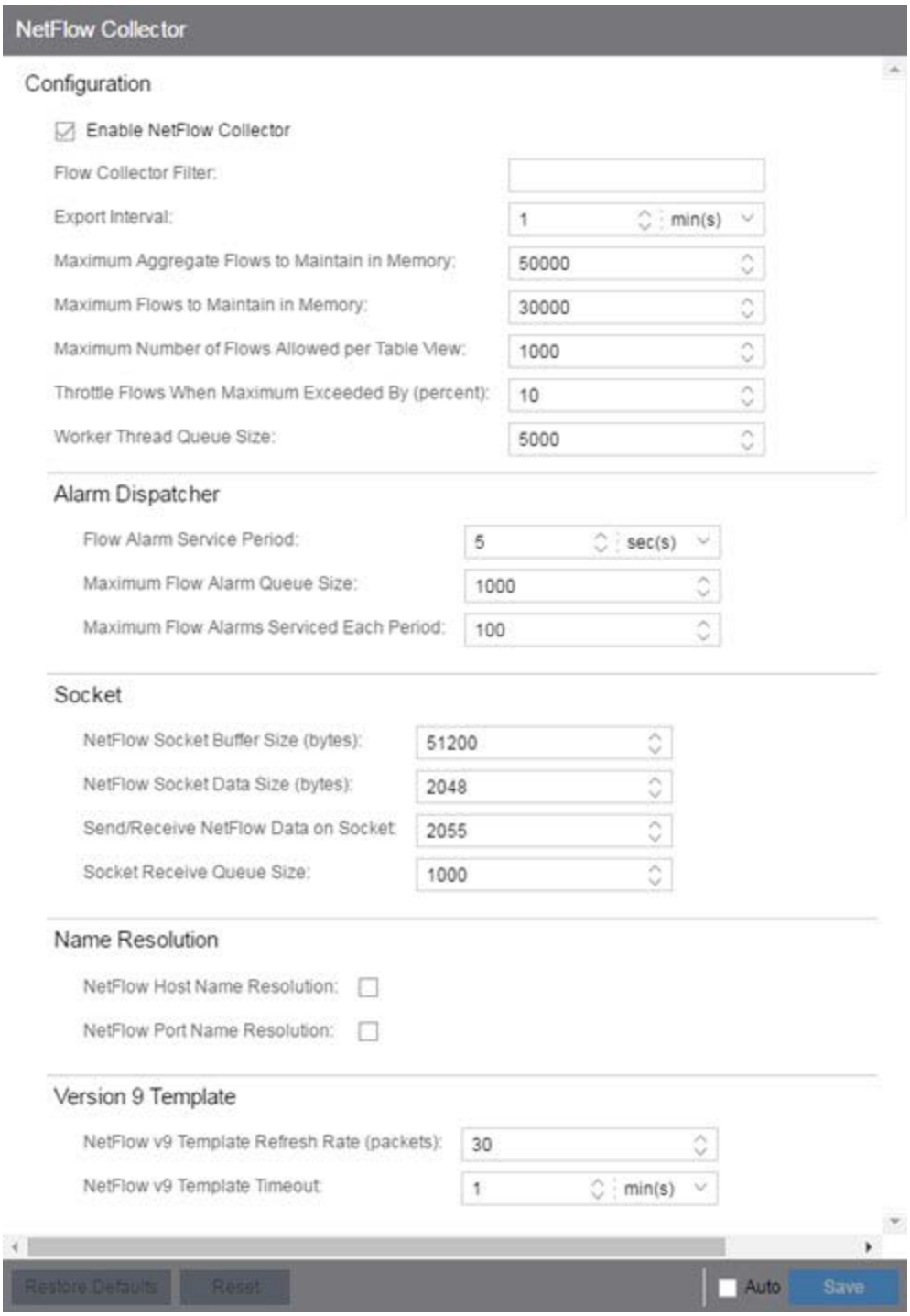
Throttle Cache When Size Exceeds Maximum By (percent)

This option controls how much port data is discarded from the cache when its size is exceeded. Adjust this to control how an overfull cache is reduced.

NetFlow Collector Options

Selecting NetFlow Collector in the left panel of the **Options** tab provides the following view, where you can configure NetFlow Collector settings in ExtremeCloud IQ Site Engine.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.


NetFlow Collector
Configuration
Enable NetFlow Collector
Flow Collector Filter:
Export Interval:
1
min(s)
Maximum Aggregate Flows to Maintain in Memory:
50000
Maximum Flows to Maintain in Memory:
30000
Maximum Number of Flows Allowed per Table View:
1000
Throttle Flows When Maximum Exceeded By (percent):
10
Worker Thread Queue Size:
5000
Alarm Dispatcher
Flow Alarm Service Period:
5
sec(s)
Maximum Flow Alarm Queue Size:
1000
Maximum Flow Alarms Serviced Each Period:
100
Socket
NetFlow Socket Buffer Size (bytes):
51200
NetFlow Socket Data Size (bytes):
2048
Send/Receive NetFlow Data on Socket:
2055
Socket Receive Queue Size:
1000
Name Resolution
NetFlow Host Name Resolution:
NetFlow Port Name Resolution:
Version 9 Template
NetFlow v9 Template Refresh Rate (packets):
30
NetFlow v9 Template Timeout:
1
min(s)
Restore Defaults
Reset
Auto
Save

Configuration

Enable NetFlow Collector

Select this checkbox to enable NetFlow packet processing on the ExtremeCloud IQ Site Engine server. Deselecting this checkbox disables all other fields in this panel and turns off NetFlow for troubleshooting purposes. Whether NetFlow is enabled or disabled, a message is logged to the event log as well as the ExtremeCloud IQ Site Engine server log. When NetFlow is disabled, the Application Flows report on the **Flows** tab is cleared.

Flow Collector Filter

Use this field to filter all incoming flows as they are processed by the flow collector. Flows not matching the filter are discarded and not maintained in memory on the server. If you add a filter here, the current flows stored in the cache are trimmed to only include matching flows.

Use this option if you want to use flow collection to look for specific results, but not process unrelated flows. For example, to only process flows pertaining to a particular subnet.

Export Interval

This is the active timer that determines the maximum amount of time a long-lasting flow remains active before expiring. When a long-lasting active flow expires due to the active timer expiring, another flow is immediately created to continue the ongoing flow. The ExtremeCloud IQ Site Engine flow collector rejoins these multiple flow records to report a single logical flow.

Maximum Aggregate Flows to Maintain in Memory

This indicates the amount of memory used to store aggregated flows.

Maximum Flows to Maintain in Memory

This indicates the amount of memory used to store flows.

Maximum Number of Flows Allowed per Table View

This indicates the maximum number of flows displayed in NetFlow reports.

Throttle Flows When Maximum Exceeded By (percent)

Flow collection is throttled when the **Maximum Flows to Maintain in Memory** is exceeded by the percentage entered here.

Worker Thread Queue Size

Decoded flow records are put into one of several fixed-size queues for processing. If the decoding rate exceeds the processing rate, the queue can overflow. This option allows you to configure the queue size (number of flow records).

Alarm Dispatcher

Flow Alarm Service Period

This controls how often the queue is checked for matched flows to process. The dispatcher

runs one time every service period. So by default, the dispatcher processes matches every 5 seconds.

Maximum Flow Alarm Queue Size
The maximum number of matched flows queued. By default, the dispatcher drops matched flows after 1000 matches are queued.

Maximum Flow Alarms Serviced Each Period
The maximum number of matched flows pulled from the queue for processing during a service period. By default, the dispatcher processes 100 matches every service period.

Socket

NetFlow Socket Buffer Size (bytes)
The buffer size (in bytes) set aside by the ExtremeCloud IQ Site Engine server for buffering incoming flows.

NetFlow Socket Data Size (bytes)
The socket data size in bytes. Do not change this setting unless it is required on your network.

Send/Receive NetFlow Data on Socket
The port on the ExtremeCloud IQ Site Engine server that listens for flow collection data. If you change this port number here, you also need to reconfigure the port number on the switch.

Socket Receive Queue Size
Network packets are retrieved from a datagram socket and put into a fixed-size queue for decoding into flow records. The queue can overflow if the receive rate exceeds the decoding rate. This option allows you to configure the queue size (number of network packets).

Name Resolution

NetFlow Host Name Resolution
Select this option to resolve host names to IP addresses and IP addresses to host names, if possible. This option enables host name resolution for NetFlow only. Host name resolution for ExtremeCloud IQ Site Engine is enabled globally using the ExtremeCloud IQ Site Engine Name Resolution option. The Name Resolution option must also be enabled for this NetFlow option to take effect.

NetFlow Port Name Resolution
Select this option to resolve device port indices to port names and port aliases, and device port names and port aliases to port indices, if possible. This option allows you to disable port name resolution for NetFlow only. (Port name resolution is enabled globally using the Name Resolution option.)

Version 9 Template

NetFlow v9 Template Refresh Rate (packets)

The number of export packets the flow sensor sends before retransmitting a template to the collector when using NetFlow Version 9.

NetFlow v9 Template Timeout

The amount of time the flow sensor waits before retransmitting a template to the collector when using NetFlow Version 9.

Network Monitor Cache Options

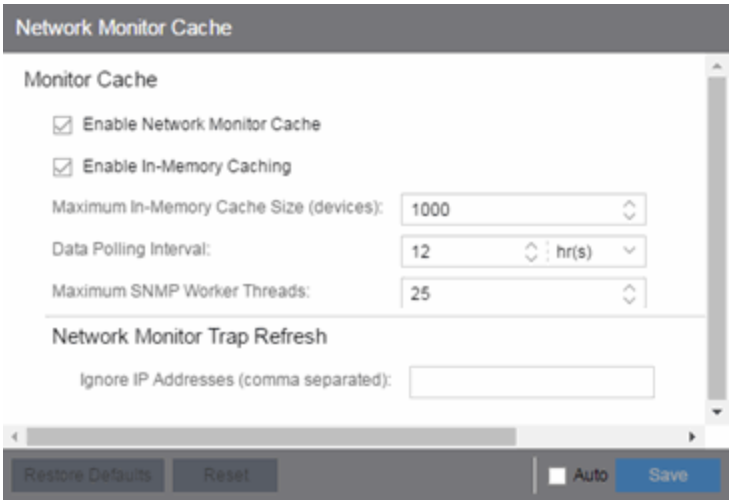
Selecting Network Monitor Cache in the left panel of the **Options** tab provides the following view, where you can edit network monitor cache settings. The network monitor cache stores information about the physical topology of a device, with additional emphasis on port information. Data is pulled from multiple places including slot and port details (Entity, ifTable), default role (Policy), neighbor link details (CDP, EDP, LLDP), Ethernet Automatic Protection Switching (EAPS), and Multi System Link Aggregation (MLAG).

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.

The cache is maintained in a two-tiered structure: device physical data is cached to the database and a fast in-memory cache maintains a subset of this data in memory on the server. The in-memory cache can contain all or a subset of devices stored in the database.

On the specified polling interval, the data is validated and automatically updated as necessary. Decreasing the poll interval increases background SNMP performed by the server.

Storing this information greatly improves performance for views in ExtremeCloud IQ Site Engine that request it. Enable the cache for the best experience.



Monitor Cache

Enable Network Monitor Cache

Select this option to enable the network monitor cache. Enabling the cache improves performance for ExtremeCloud IQ Site Engine views that request this information. Deselecting this option disables all other fields in this panel.

Enable In-Memory Caching

Select this option to enable the in-memory cache. To limit memory usage, disable the in-memory cache and configure the device cache to rely directly on the database.

Maximum In-Memory Cache Size (devices)

If Enable In-Memory Caching is enabled, enter the maximum number of devices whose data is stored in the in-memory cache. This option lets you adjust the amount of memory the cache uses.

Data Polling Interval

Enter the frequency that the device data is checked for changes. If the device data is stale, the data is refreshed in the cache. Reducing the interval increases background SNMP queries performed by the server.

Maximum SNMP Worker Threads

Enter the maximum number of threads that send SNMP queries in parallel if multiple devices are added to the cache at the same time. The cache is populated with results from SNMP queries to devices.

Network Monitor Trap Refresh

Ignore IP Addresses (comma separated)

Enter a comma-separated list of the IP addresses for which you do not want ExtremeCloud IQ Site Engine to be the trap destination.

Policy Options

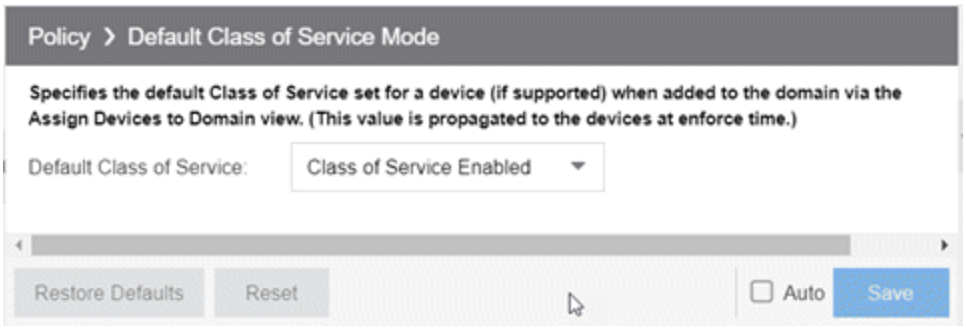
Selecting Policy in the left panel of the **Options** tab provides the following view, where you can edit options that apply to policy functionality found in the **Policy** tab.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.

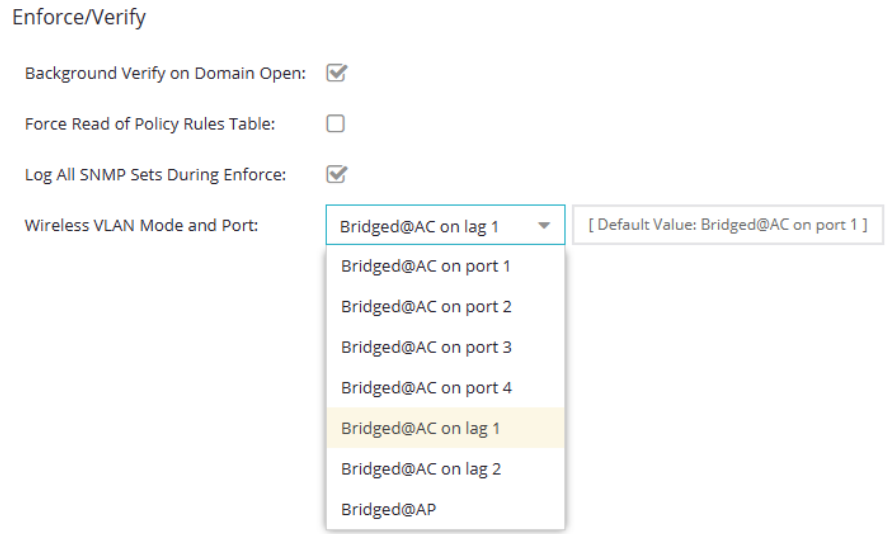
Default Class of Service Mode

Use the **Default Class of Service** option to enable the Class of Service (CoS) mode to set on a device (if supported) when it is created in ExtremeCloud IQ Site Engine or added to the domain via the **Policy** tab. The CoS mode is written to the devices when an Enforce operation is performed. This setting applies to all users. For additional information, see Getting Started with Class of Service.

The **Default Class of Service** option is enabled by default, but you can disable it by selecting **Class of Service Disabled**.



Enforce/Verify



Background Verify on Domain Open

Select the check box to enable a background verify to run when you open a domain. This action sets the “needs enforce” flag proactively without requiring a manual verify and reports the status via an icon on the title bar of the Devices/Port Groups sub-panel.

Force Read of Policy Rules Table

To improve performance during the verify operation, ExtremeCloud IQ Site Engine uses the "Last Changed" attribute on the device to determine if any rules changed. Selecting the **Force Read of Policy Rules Table** option causes ExtremeCloud IQ Site Engine to perform the verify operation using the rules table instead of the attribute. This can cause the verify operation to take longer to perform. Do not select this option unless instructed by Extreme Networks Support.

Log All SNMP Sets During Enforce

Select the check box to enable logging for all SNMP sets during an enforce.

Wireless VLAN Mode and Port

Use the drop down to select a topology bridge option policy deployment for ExtremeCloud IQ Controller. The default is to Enforce Policy over Bridged@AC on port 1.
If the default port 1 is in a read-only mode such as from a LAG configuration, the policy enforcement will fail.
Select a mode with an available port for your ExtremeCloud IQ Site Engine global VLAN configuration:

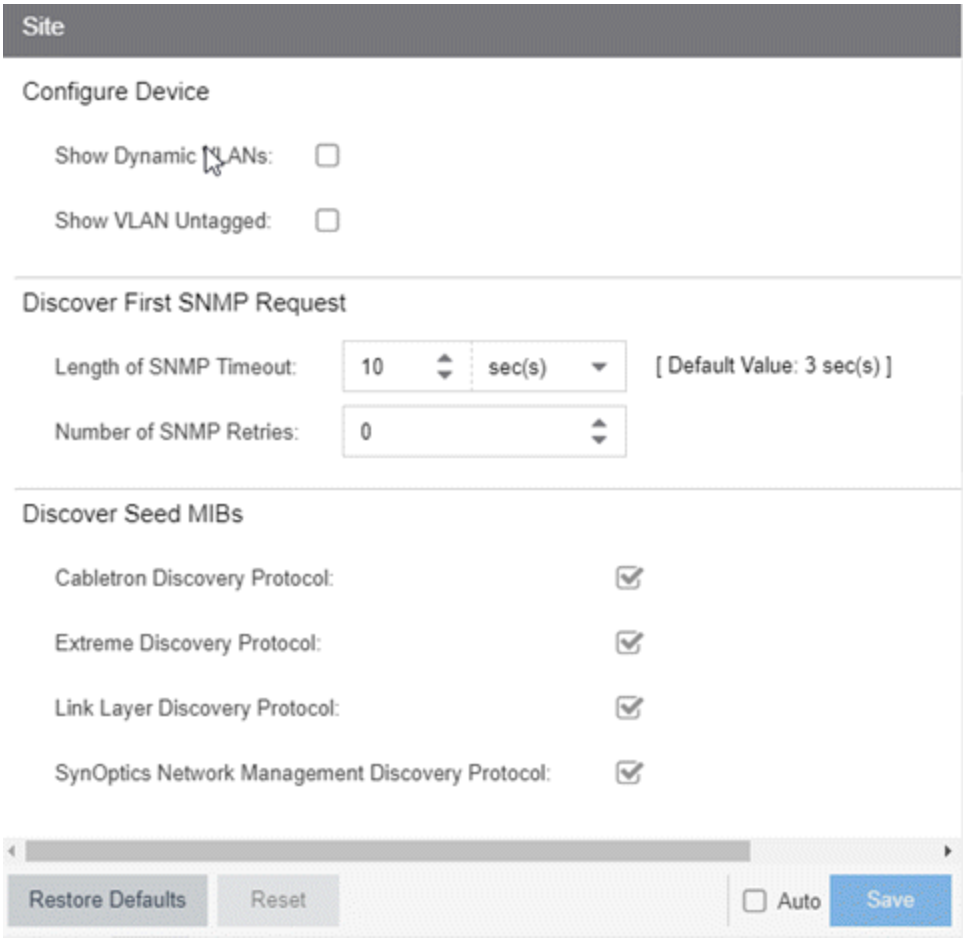
- Bridged@AC on port 1
- Bridged@AC on port 2
- Bridged@AC on port 3

- Bridged@AC on port 4
- Bridged@AC on lag 1
- Bridged@AC on lag2
- Bridged@AP

Site Options

Selecting Site in the left panel of the **Options** tab provides the following view, where you can enable or deny specific protocols when discovering devices for a site.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.



Configure Device

Show Dynamic VLANs

ExtremeCloud IQ Site Engine displays your dynamic VLANs on the **VLAN Definition** tab of the **Configure Device** window for devices included in the site.

Show VLAN Untagged

ExtremeCloud IQ Site Engine displays your untagged VLANs on the **VLAN Definition** tab of the **Configure Device** window for devices included in the site.

Discover First SNMP Request

Length of SNMP Timeout

The amount of time ExtremeCloud IQ Site Engine waits before trying to contact a device again during Discovery. The default value for this setting is 3 seconds. The value for this setting must be between 1 and 60 seconds.

Number of SNMP Retries

The number of attempts made to contact a device after an attempt at contact fails during Discovery. The default setting is 0 retries, which means that ExtremeCloud IQ Site Engine does not retry contacting a device after the initial attempt is made. The value for this setting must be between 0 and 10 retries.

Discover Seed MIBs

Cabletron Discovery Protocol

Select this option to enable each Site Seed IP Address to use the Cabletron Discovery Protocol (ctCDP) to detect devices to add to ExtremeCloud IQ Site Engine.

Extreme Discovery Protocol

Select this option to enable each Site Seed IP Address to use the Extreme Discovery Protocol (EDP) to detect devices to add to ExtremeCloud IQ Site Engine.

Link Layer Discovery Protocol

Select this option to enable each Site Seed IP Address to use the Link Layer Discovery Protocol (LLDP) to detect devices to add to ExtremeCloud IQ Site Engine.

SynOptics Network Management Discovery Protocol

Select this option to enable each Site Seed IP Address to use the SynOptics Network Management Discovery Protocol (SONMP) to detect devices to add to ExtremeCloud IQ Site Engine.

Email Configuration (SMTP/API) Options

Selecting **Email Configuration (SMTP/API)** in the left panel of the **Options** tab provides the view where you can specify the SMTP email server used by ExtremeCloud IQ Site Engine when sending emails to users. You can configure ExtremeCloud IQ Site Engine to send emails to users in a variety of circumstances, including as an alarm action and when sending scheduled network reports. These settings apply to all users. You must be assigned the appropriate user capability to configure these options.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.

Email

Sender's Email Address
The sender's email address used to send outgoing email notification messages. Enter the address in a fully qualified format, such as "sender's name@sender's domain."

Use Microsoft Entra ID for Sending Email
Select the checkbox to enable Entra ID authentication for sending email. If selected, SMTP Email settings are not used.

Outgoing Email (SMTP) Server
The email server used for outgoing messages.

SMTP Password/Access Token
The password for the user account entered in the **Sender's Email Address** field. Select the **Eye** icon to display your password.
When **Use OAUTH Authentication Method** is selected in the SMTP OAUTH Configuration section, this **SMTP Password/Access Token** field must contain the Access Token.

Entra ID Tenant ID
The Tenant ID used for Entra ID authentication. Enter the Tenant ID provided by Microsoft during Entra ID registration.

Entra ID Client ID
The Client ID used for Entra ID authentication. Enter the Client ID provided by Microsoft during Entra ID registration.

Entra ID Client Secret
The Client Secret used for Entra ID authentication. Enter the Client Secret provided by Microsoft during Entra ID registration.

SMTP Email Advanced Configuration

SMTP Server Port

The SMTP port used. The default SMTP Server Port is 25. Enter the port number required for your selected SSL or TLS option. For example, common port numbers are 456 for SSL and 587 for TLS.

Use SSL Communication

Select the checkbox to enable legacy SSL. Do not use SSL when TLS is enabled.

Use TLS Encryption

Select the checkbox to enable TLS. Do not use SSL when TLS is enabled.

SMTP OAUTH Configuration

Use OAUTH SMTP Authentication Method

Select the checkbox to enable OAUTH SMTP authentication. If enabled, the SMTP Password/Access token field is used for the Access Token.

Update Access Token

Select the checkbox to enable automatic updates of the Access Token. Requires a configuration to receive access token updates from your OAUTH provider. You must have a valid access token in the **SMTP Password/Access Token** field during the configuration.

- **Interval** - Enter a time of how often to update the access token
- **Host URL** - Enter the URL of the OAUTH provider.
- **Client ID** - Enter the client ID required to update the access token.
- **Client Secret** - Enter the client secret required to update the access token.
- **Refresh Token** - Enter the refresh token required to update the access token.
- **Parameter 1** - Optional additional parameter that can be used to update the access token.
- **Parameter 2** - Optional additional parameter that can be used to update the access token.
- **Parameter 3** - Optional additional parameter that can be used to update the access token.

Examples and How-tos for using OAUTH with Gmail

For information about how to use OAuth 2.0 from Google, go to https://developers.google.com/identity/protocols/oauth2/ for high-level details, and https://support.google.com/cloud/answer/6158849?hl=en for more detailed steps.

The following explains how you can generate the required information to configure ExtremeCloud IQ Site Engine to use Gmail as an OAUTH provider. For additional information, watch this video - OAUTH with Gmail

- You can create the OAUTH 2.0 Client IDs in the credentials menu and select Desktop app as the application type.
  Then download the JSON file as it contains the **Client ID**, **Client Secret**, and **Host URL** information required to configure the **Update Access Token** option.
- Creating an OAUTH consent application example:
  - Publishing Status - In production
  - User type - External
  - App logo - Empty
  - App domain - Empty
  - Authorized domains - Empty
  - Your non-sensitive scopes - See your primary Google Account email address
  - Your sensitive scopes - Empty
  - Your restricted scopes - Empty
- You can use an oauth2.py script by Google, located in ExtremeCloud IQ Site Engine <install directory>/scripts/ to generate an access token and refresh token:
  - An example script syntax is shown below, you must input your user google email address, client ID, client secret, and an accurate directory path for your installation:

    ```
    python /usr/local/Extreme_Networks/NetSight/scripts/oauth2.py --
    user=<email_address> --client_id=<id> --client_secret=<secret> --
    generate_oauth2_token
    ```

    Running the oauth2.py script generates a URL for authorization and waits for a verification code.

  - Copy the script generated URL into a web browser and authorize the application. The URL redirects to 127.0.0.1 (and a timeout occurs) with a verification code generated in the redirected URL between code= and &scope, for example:

    http://127.0.0.1:81/?code=4/0AWtgzh5sUJhblPSKS4zFGIC-wWOpnPNYBNemiwxNiEn35RhTZNFkJXZP8mBTGJqaGVlcM3w&scope=https://mail.google.com/

- Enter the verification code into the waiting script. The script responds with the **Refresh Token**, **Access Token**, and Expiration time **Interval.**.

  NOTE: When configuring the OAUTH update access token interval field in ExtremeCloud IQ Site Engine, enter an interval value that is less than the expiration time output by the oauth2.py script.

- Use the information you obtained from the JSON file and the oauth2.py script to configure the ExtremeCloud IQ Site Engine SMTP Email OAUTH Configuration with the **Update Access Token** option enabled.
  Here are additional example configuration parameters for using OAUTH with Gmail:
  - Outgoing Email (SMTP) Server: smtp.gmail.com
  - SMTP Server Port: 587
  - Use SSL Communications: No
  - Use TLS Encryption: Yes

How-to Enable SMTP with Microsoft Office 365

NOTE: The following SMTP authentication configuration is being deprecated by Microsoft starting in December 2026. For more information, see https://techcommunity.microsoft.com/blog/exchange/updated-exchange-online-smtp-auth-basic-authentication-deprecation-timeline/4489835.

The deprecated configuration replacement is to select **Use OAUTH Authentication Method** and select **Use Microsoft Entra ID for sending Email** options in **Oneview > Administration > Options > Email Configuration (SMTP/API)** and provide the required Tenant ID, Client ID, and Client Secret from Microsoft Entra ID registration.

1. Open the Microsoft 365 admin center and select **Users > Active users**.
2. Select the user who will send the email, and in the flyout that appears, select **Mail**.
3. In the **Email apps** section, select **Manage email apps**.
4. Verify the **Authenticated SMTP** setting is checked = enabled.
5. Select **Save changes**.

   It may take several minutes for the change to take effect.
6. Open **Oneview > Administration > Options > SMTP Email.**
7. Configure the following fields:

a. Specify the **Outgoing Email (SMTP) Server** as `smtp.office365.com`.

b. Specify the **Sender's Email Address.**

c. Specify the **SMTP Password/Access Token.**

d. Specify the **SMTP Server Port** as `587`.

e. Specify the **Use SSL Communication** as `unchecked`.

f. Specify the **Use TLS Encryption** as `checked`.

g. Specify the **Use OAUTH Authentication Method** as `unchecked`.

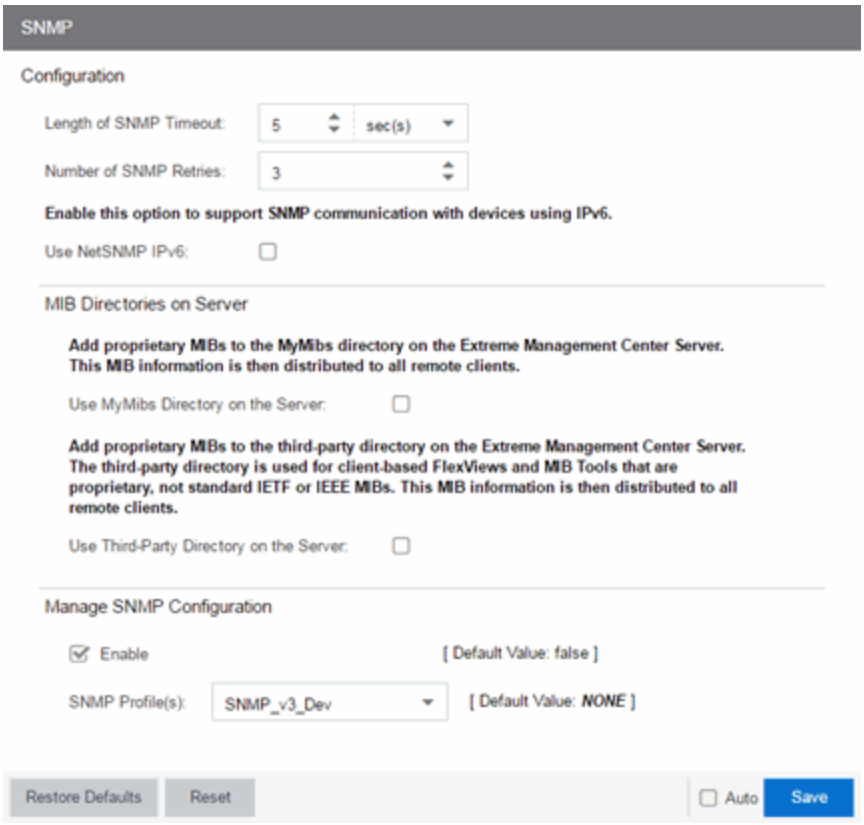
For additional information, see: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission#use-the-microsoft-365-admin-center-to-enable-or-disable-smtp-auth-on-specific-mailboxes.

SNMP Options

Selecting SNMP in the left panel of the **Options** tab provides the following view, which enables you to configure SNMP options.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.

These options apply to all users. For these settings to take effect, the ExtremeCloud IQ Site Engine Server must be restarted.



Configuration

Length of SNMP Timeout

The amount of time ExtremeCloud IQ Site Engine waits before trying to contact a device again. The default value for this setting is 5 seconds. The value for this setting must be between 1 and 60 seconds.

Override this value on a per-device basis in the **SNMP Timeout** field in the Configure Device window.

NOTE: When SNMP requests are redirected through the server, all SNMP timeouts are extended by a factor of four (timeout X 4) to provide time for the delays incurred by redirecting requests through the server.

Number of SNMP Retries

The number of attempts made to contact a device after an attempt at contact fails. The default setting is 0 retries, which means that ExtremeCloud IQ Site Engine does not retry contacting a device after the initial attempt is made. The value for this setting must be between 0 and 10 retries.

Override this value on a per-device basis in the **SNMP Retries** field in the Configure Device window.

Use NetSNMP IPv6

The **Use NetSNMP IPv6** option enables you to use SNMP to manage network devices to which IPv6 addresses are assigned. You must have this option selected in order to be able to add a device with an IPv6 address.

MIB Directories on Server

Use MyMibs Directory on the Server

Select this checkbox to enable the ExtremeCloud IQ Site Engine Server to also use the MyMibs directory (e.g. the MIBs are included in the SNMP server stack). This MIB information is then distributed to the ExtremeCloud IQ Site Engine remote clients.

Use Third-Party Directory on the Server

Select this checkbox to enable the ExtremeCloud IQ Site Engine Server to also use the third-party directory, where proprietary, client-based FlexViews and MIB Tools (Enterprise MIBs owned by other companies) are stored, not standard IETF or IEEE MIBs. This MIB information is then distributed to the ExtremeCloud IQ Site Engine remote clients.

CAUTION: Do **not** use the MyMibs or third-party directories unless it is required on your network, as selecting these options can cause ExtremeCloud IQ Site Engine Server instability and undesirable consequences.

Manage SNMP Configuration

Enable

Select this checkbox to enable SNMP access to the ExtremeCloud IQ Site Engine server for the profiles you select in the **SNMP Profile(s)** drop-down list. Deselecting this checkbox only enables SNMP access to the ExtremeCloud IQ Site Engine server for the credentials you configured when you installed ExtremeCloud IQ Site Engine.

SNMP Profile(s)

Select the profiles with SNMP access to the ExtremeCloud IQ Site Engine server. The type of SNMP access (e.g. read-only or read-write) is configured for the profile by assigning a set of SNMP credentials to the profile on the **Administration** > **Profiles** tab.

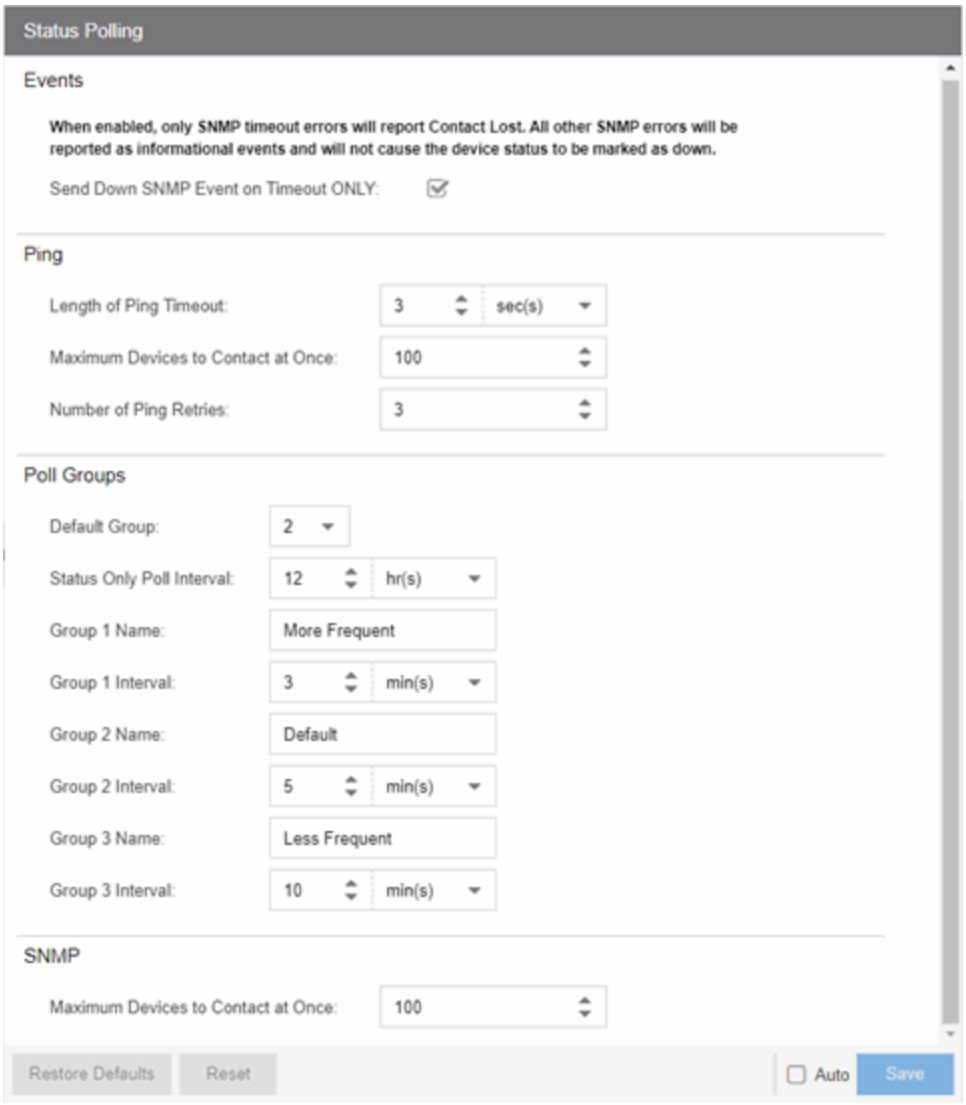
You can also configure these options directly by editing the `/etc/snmp/snmpd.conf` file.

NOTE: There are certain cases when these options are not available. In the event that these options are unable to be edited, configure the options directly via the `snmpd.conf` file.

Status Polling Options

Selecting Status Polling in the left panel of the **Options** tab provides the following view, where you can specify options that determine how ExtremeCloud IQ Site Engine polls devices. ExtremeCloud IQ Site Engine uses the polling options and poll groups defined here to contact the devices and update tree information. When a device is added to the ExtremeCloud IQ Site Engine database using the Add Device menu option or a device discover, it is added to the default poll group selected here. (A device discover lets you assign devices to any of the three poll groups.) Reassign individual devices or device groups to a different poll group using the Configure Device window. These settings apply to all users. You must be assigned the appropriate user capability to configure these options.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.



Events

When the **Send Down SNMP Event on Timeout ONLY** option is selected, only SNMP timeout errors result in a **Contact Lost** device status. All other SNMP errors are reported as informational events in the **Alarms and Events** > **Events** tab and do not cause the device status to be marked as "down" with a red down arrow.

Ping

Use these options to configure status polling settings for devices whose poll type is set to **Ping**.

Length of Ping Timeout
The amount of time ExtremeCloud IQ Site Engine waits before trying to ping a device again. The default setting is 3 seconds. The maximum value for this field is 60 seconds.

Maximum Devices to Contact at Once
The maximum number of IP addresses that ExtremeCloud IQ Site Engine attempts to contact simultaneously. The maximum value for this field is 1,000.

Number of Ping Retries
The number of attempts made to ping a device. The default setting is 3 retries, which means ExtremeCloud IQ Site Engine retries a timed-out request three times, making a total of four attempts to contact a device. The maximum value for this field is 10.

Poll Groups

Status Only Poll Interval
The frequency with which ExtremeCloud IQ Site Engine contacts devices for which you only need to monitor their status. The default polling interval for **Status Only** devices occurs every 12 hours. **Status Only** devices do not support collection of statistics, FlexViews, Network Status Monitor, map links, or enforcement via ExtremeCloud IQ Site Engine. You can add a maximum of 10,000 **Status Only** devices in ExtremeCloud IQ Site Engine, which do not count against your licensed device limit.

There are three distinct poll groups, and each device belongs to one of the three groups. Use these settings to poll critical devices at a more frequent interval, while polling non-essential devices less frequently. The poll frequency for each group specifies the actual length of the poll cycle. Set the interval for poll groups according to your network's needs using the guidelines below.

Select one group as the default poll group in the Default Group drop-down list. When a device is added to the ExtremeCloud IQ Site Engine database using the Add Device menu option or a CDP seed IP discover, it is added to the default poll group selected here. (IP range discover lets you assign devices to any of the three poll groups.) You can also assign individual devices or device groups to a specific poll group using the Configure Device window.

The overall density of polling for devices whose poll type is set to Ping and SNMP is controlled by the Maximum Devices to Contact at Once setting in the Ping and SNMP section, respectively. This determines the maximum number of devices from each group polled at any given time. ExtremeCloud IQ Site Engine always attempts to poll up to the maximum number of devices until all of the devices in the three groups are polled. As responses are received and devices are removed from the poll queue, other devices are added to the queue. After all the devices are polled, ExtremeCloud IQ Site Engine stops polling and batches information to update clients.

If the Maximum Devices to Contact at Once is set too high, such that the poll density is too high, system performance degrades quickly. The optimal poll setting is dependent on many factors including, but not limited to, CPU speed, RAM, and network devices. As the number of devices that you

are polling increases, reduce the poll density (**Maximum Devices to Contact at Once**) to increase performance.

The default **Maximum Devices to Contact at Once** setting and poll group intervals provided as defaults are a good starting point. If necessary, adjust the values to optimize status polling for your network.

SNMP

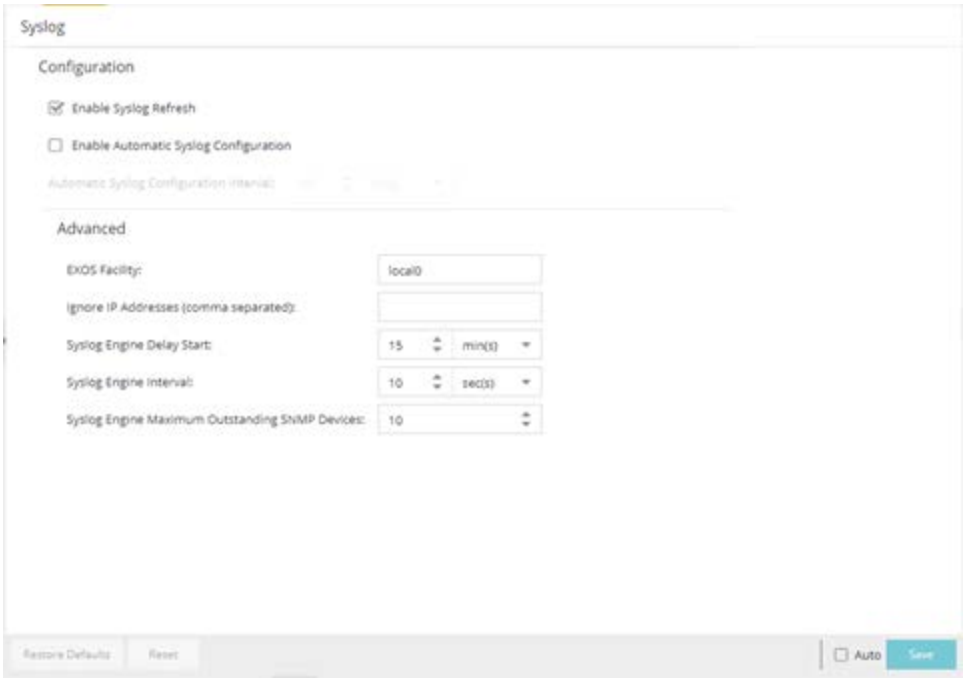
Use this option to configure status polling settings for devices whose poll type is set to **SNMP**.

Maximum Devices to Contact at Once
: The maximum number of IP addresses that ExtremeCloud IQ Site Engine attempts to contact simultaneously. The maximum value for this field is 1,000.

Syslog Options

Selecting Syslog in the left panel of the **Options** tab provides the following view, where you can set ExtremeCloud IQ Site Engine to automatically configure devices to send syslog information.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.



Configuration

Enable Syslog Refresh

Select the checkbox to enable ExtremeCloud IQ Site Engine to verify the current syslog configuration during Discovery, Re-discovery or automatic Network Monitor Cache updates. The result will update the Syslog Status column in Network Devices with the current state.

Enable Automatic Syslog Configuration

Select the checkbox to configure ExtremeCloud IQ Site Engine on supported switch platforms to verify the current syslog configuration on the defined interval, and automatically reconfigure syslog if it is not currently enabled.

Automatic Syslog Configuration Interval

Select the time interval that Automatic Syslog Configuration will occur. The default is 12 hours.

Advanced

ExtremeXOS/Switch Engine Facility

The Syslog facility to be used by the script when registering/unregistering syslog forExtremeXOS/Switch Engine devices.

Ignore IP Addresses (comma separated)

Enter any IP addresses you do not want automatically logged to the syslog.

Syslog Engine Delay Start

The amount of time ExtremeCloud IQ Site Engine waits before information in the syslog is aggregated and archived.

Syslog Engine Interval

The amount of time ExtremeCloud IQ Site Engine waits before checking whether a device is properly configured to send syslog information. If the device is not properly configured and **Enable Automatic Syslog Configuration** is selected, ExtremeCloud IQ Site Engine automatically configures the device.

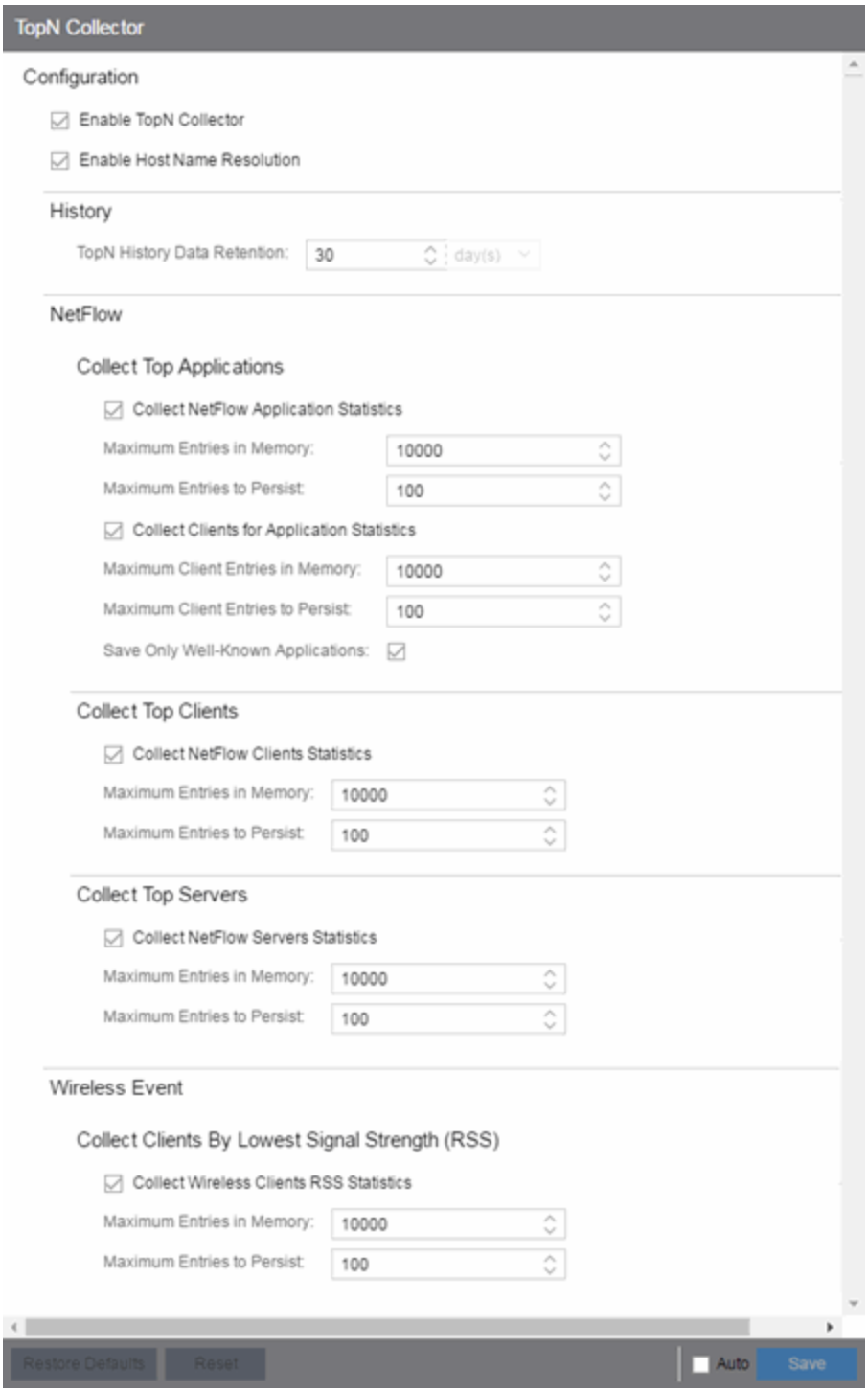
Syslog Engine Maximum Outstanding SNMP Devices

The maximum number of outstanding SNMP devices archived by the syslog.

TopN Collector Options

Selecting TopN Collector in the left panel of the **Options** tab provides the following view, where you can enable the TopN collector and host name resolution, and configure the number of days ExtremeCloud IQ Site Engine maintains the TopN history. The TopN Collector gathers the application, client application, client, and server data used in TopN reports. It also collects the signal strength data reported by Wireless Controllers.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.



Enable TopN Collection

Select this option to enable the TopN Collector. Deselecting this option disables all other fields in the panel. Changes to this option take place immediately.

Enable Host Name Resolution

Select this option to resolve host names to IP addresses and IP addresses to host names, if possible. This option allows you to disable host name resolution for TopN only. (Host name resolution is enabled globally using the Enable Name Resolution option.) Changes to this option take place immediately.

History

TopN History Data Retention

Use this setting to determine the number of days TopN information remains available for viewing in reports. The default number of days is 30, with a minimum value of 1 day and a maximum value of 180 days. Changes to this option take effect with the next nightly TopN history cleanup task performed by the ExtremeCloud IQ Site Engine server.

NetFlow

The TopN Collector collects the data used in TopN reports for applications, client applications, clients, and servers. The collector collects data over a one hour time period. At the end of the hour, the collector evaluates the data and stores only the most significant details collected for that hour. When changing the value for **Maximum Entries in Memory** or **Maximum Entries to Persist**, the new value takes effect during the next hour of data collection. For example, if you change the value at 3:05 or 3:55, the new value takes effect during the hour that starts at 4:00.

If more entries are needed during the hour than the maximum, additional entries are stored on disk, which is slower. This results in a direct trade-off in memory usage versus CPU usage. Increasing these values might use more memory and decreasing these values might use more CPU.

Collect Top Applications

Collect NetFlow Application Statistics

Select this checkbox to enable the collection of application TopN data.

Maximum Entries in Memory

Specify the number of application entries to save during each hourly interval to use in TopN reporting. The default maximum number of entries in memory is 10,000 with a minimum value of 1,000 and a maximum value of 1,000,000.

Maximum Entries to Persist

Specify the number of application entries to save at the end of each hourly interval. The default number of entries to persist is 100, with a minimum value of 5 and a maximum value of 1,000.

Collect Clients for Application Statistics
Select this checkbox to enable the collection of data about the clients using the applications in TopN data.

Maximum Client Entries in Memory
Specify the number of client entries to save during each hourly interval to use in TopN reporting. The default maximum number of entries in memory is 10,000 with a minimum value of 1,000 and a maximum value of 1,000,000.

Maximum Client Entries to Persist
Specify the number of client entries to save at the end of each hourly interval. The default number of entries to persist is 100, with a minimum value of 5 and a maximum value of 1,000.

Save Only Well-Known Applications
Select this checkbox to save only data from well-known applications in the TopN data.

Collect Top Clients

Collect NetFlow Clients Statistics
Select this checkbox to enable the collection of client TopN data.

Maximum Entries in Memory
Specify the number of client entries to save during each hourly interval to use in TopN reporting. The default maximum number of entries in memory is 10,000 with a minimum value of 1,000 and a maximum value of 1,000,000.

Maximum Entries to Persist
Specify the number of client entries to save at the end of each hourly interval. The default number of entries to persist is 100, with a minimum value of 5 and a maximum value of 1,000.

Collect Top Servers

Collect NetFlow Servers Statistics
Select this checkbox to enable the collection of server TopN data.

Maximum Entries in Memory
Specify the number of server entries to save during each hourly interval to use in TopN reporting. The default maximum number of entries in memory is 10,000 with a minimum value of 1,000 and a maximum value of 1,000,000.

Maximum Entries to Persist
Specify the number of server entries to save at the end of each hourly interval. The default number of entries to persist is 100, with a minimum value of 5 and a maximum value of 1,000.

Wireless Event

Collect Wireless Clients RSS Statistics

Select this checkbox to enable Wireless Controllers to collect signal strength data for TopN reporting.

Maximum Entries in Memory

Specify the number of signal strength entries to save during each hourly interval to use in TopN reporting. The default maximum number of entries in memory is 10,000 with a minimum value of 1,000 and a maximum value of 1,000,000.

Maximum Entries to Persist

Specify the number of signal strength entries to save at the end of each hourly interval. The default number of entries to persist is 100, with a minimum value of 5 and a maximum value of 1,000.

Trap Options

Selecting Trap in the left panel of the **Options** tab provides the following view, where you can set trap options for ExtremeCloud IQ Site Engine.

SNMP traps are messages a device sends to ExtremeCloud IQ Site Engine to indicate its status. Using traps, a network manager can monitor a large number of devices simultaneously without needing to poll them individually.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.



Configuration

Use this section to configure traps to be automatic traps or automatic smart traps. Additionally, you can configure the amount of time in hours between automatic trap configurations as well as select credential names.

Enable Automatic Smart Trap Configuration
Select this option to enable your ExtremeXOS/Switch Engine devices to send ExtremeCloud IQ Site Engine a trap when a change occurs on the device.

Enable Trap Refresh
Select this option to enable ExtremeCloud IQ Site Engine to verify the current trap receiver configuration during Discovery, Re-discovery, or automatic Network Monitor cache updates. The result will update the Trap Status column in Network Devices with the current state.

SNMPv1 Credential Name
Select the SNMPv1 credentials on which the server accepts traps. You can modify the credentials found in this list in the SNMP Credentials section on the **Administration** > **Profiles** tab.

SNMPv2 Credential Name
Select the SNMPv2 credentials on which the server accepts traps. You can modify the credentials found in this list in the SNMP Credentials section on the **Administration** > **Profiles** tab.

SNMPv3 Credential Name
Select the SNMPv3 credentials on which the server accepts traps. You can modify the credentials found in this list in the SNMP Credentials section on the **Administration** > **Profiles** tab.

Server Engine ID
Displays the SNMPv3 Engine ID ExtremeCloud IQ Site Engine is using. ExtremeCloud IQ Site Engine also uses this **Server Engine ID** when configuring ERS and Fabric Engine devices for SNMPv3 informs.

Enable Automatic Trap Configuration
Select this option to enable ExtremeCloud IQ Site Engine on supported switch platforms to verify the current trap receiver configuration on the defined interval, and automatically reconfigure the trap receiver using the SNMP Credential Name fields if not currently enabled.

Automatic Trap Configuration Interval
Select the time interval that Automatic Trap Configuration will occur. The default is 12 hours.

Device Topology Change Trap Threshold

Use this section to count the number of topology change traps the device sends within the defined interval. You can use the Device Topology Change Trap Threshold to detect devices sending a high volume of traps. Devices sending high volume of some traps can cause issues such as high CPU usage, or topology maps constantly reloading.

Device Topology Change Trap Threshold Interval
Defines the threshold interval. Supported range is 10 seconds to 1 hour.

Device Topology Change Trap Threshold Level
Defines the volume of traps for each device within the threshold interval. When the level is reached a "Trap Overflow" event is generated with Event Type: Console, Category: Trap.

Trap Engine

Use this section to enter a list of IP addresses that should be ignored by traps and to configure trap engine options.

Ignore IP Addresses (comma separated)
Enter a comma-separated list of IP addresses of the devices from which the trap engine ignores traps.

Trap Engine Delay Start
Select the amount of time after starting the trap engine to delay receiving traps.

Trap Engine Interval
Select the frequency with which the trap engine collects SNMP traps from devices.

Trap Engine Maximum Outstanding SNMP Devices
Select the maximum number of SNMP devices that send traps to the trap engine.

Trap Poller

Use this section to set advanced options for polling traps.

Trap Poller Block Size
Select the number of traps the trap engine maintains at one time.

Trap Poller Delay Start
Select the amount of time after starting the trap engine that devices are polled by ExtremeCloud IQ Site Engine.

Trap Poller Frequency
Select the frequency with which the trap engine polls devices.

Trap Poller Maximum Capacity

Select the maximum number of devices the trap engine polls for traps.

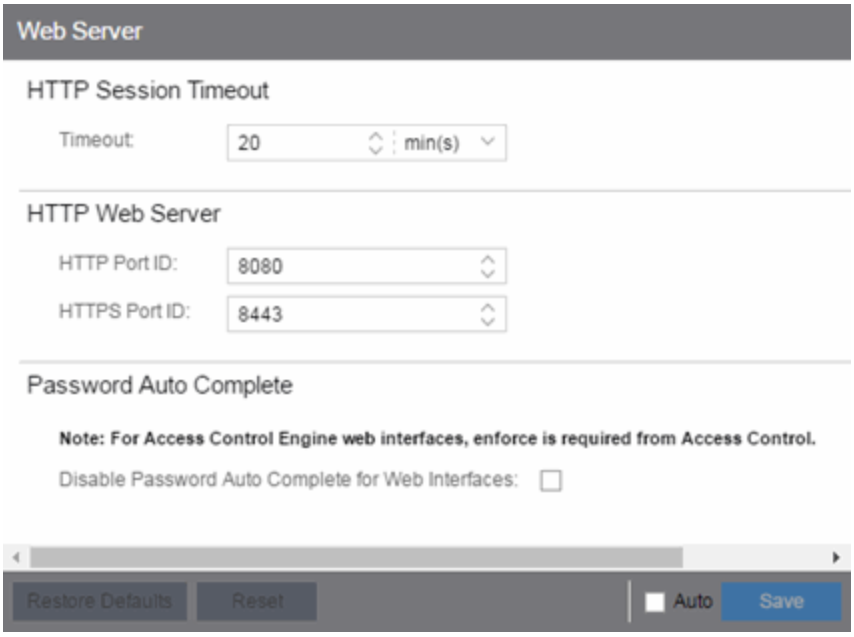
Trap Poller Maximum Rate

Select the maximum number of devices the trap engine polls at one time.

Web Server Options

Selecting Web Server in the left panel of the **Options** tab provides the following view, where you can specify web browser options when using ExtremeCloud IQ Site Engine.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.



HTTP Session Timeout

HTTP Session Timeout

The **Timeout** option lets you specify a session timeout value for all ExtremeCloud IQ Site Engine web-based views.

HTTP Web Server

HTTP Port ID

Use the **HTTP Port ID** field to specify the HTTP port IDs for HTTP web server traffic. This port must be accessible through firewalls for users to install and launch ExtremeCloud IQ Site Engine client applications. By default, ExtremeCloud IQ Site Engine uses port ID 8080. If you change the port ID, you must restart the ExtremeCloud IQ Site Engine Server for the change to take effect.

HTTPS Port ID

Use the **HTTPS Port ID** field to specify the HTTPS port IDs for HTTP web server traffic. This port must be accessible through firewalls for users to install and launch ExtremeCloud IQ Site Engine client applications. By default, ExtremeCloud IQ Site Engine uses port ID 8443. If you change the port ID, you must restart the ExtremeCloud IQ Site Engine Server for the change to take effect.

IMPORTANT: Enforce your Access Controlengines from the **Control** > **Access Control** tab immediately after changing the **HTTPS Port ID**.

When adding a new Access Control engine or using ZTP+, the **HTTPS Port ID** must be **8443**.

Password Auto Complete

Password Auto Complete

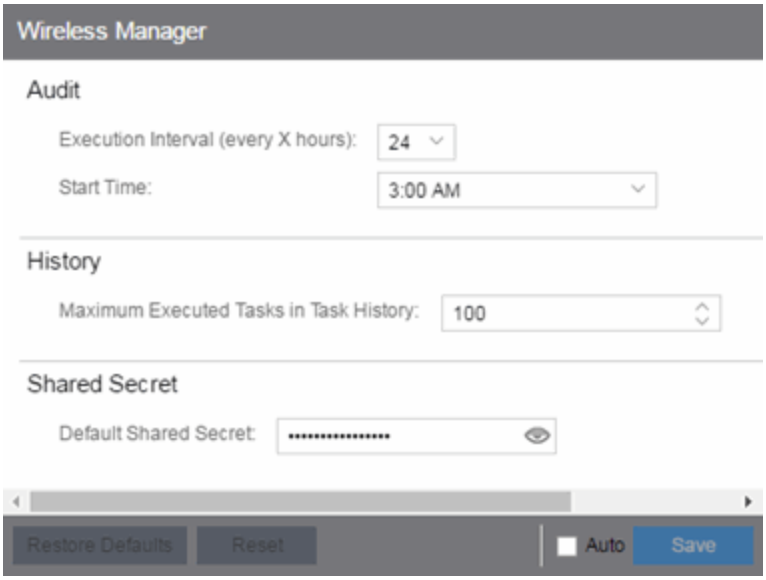
Use the **Disable Password Auto Complete for Web Interfaces** option to disable automatic password completion for users logging into ExtremeCloud IQ Site Engine web interfaces. Note that for Access Control web interfaces, you must enforce from the **Control** > **Access Control** tab for the option to take effect.

These settings apply to all users. You must be assigned the appropriate user capability to change this setting.

Wireless Manager Options

Selecting Wireless Manager in the left panel of the **Options** tab provides the following view, where you can specify options for the Wireless Manager application.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.



Wireless Manager audits controller configurations to ensure that it does not deviate from the deployed templates. When Wireless Manager encounters discrepancies between the template and the actual controller configuration, the audit feature logs an error. You can manually run an audit or you can schedule automatic audits using these Audit options.

Execution Interval (every X hours)
: Use the drop-down list to select the interval in hours between the start of successive audits. Auditing one time every 24 hours is sufficient for most sites, but more frequent auditing can be enabled through this option.

Start Time
: Use the drop-down list to select the time when the audit starts.

Maximum Executed Tasks in Task History
: Enter the number of Wireless Manager tasks you want to save in the Wireless Manager database. Enter **0** if you do not want to execute a Wireless Manager audit.

  After a task has executed, it is retained in the Wireless Manager database to provide a detailed history of task activity. A large amount of information is kept for each executed task, including the complete CLI script executed against each target controller. To maintain the database at a

reasonable size, Wireless Manager keeps only a fixed number of executed tasks in the database. When the task limit is reached or exceeded, Wireless Manager deletes the oldest executed tasks from its database. The History option allows you to control how many task definitions Wireless Manager retains in its database. The default is 100 executed tasks retained, and the maximum is 500 tasks retained.

Default Shared Secret

Enter a **Shared Secret**, which is a password used by ExtremeCloud IQ Site Engine to authenticate with the controller.

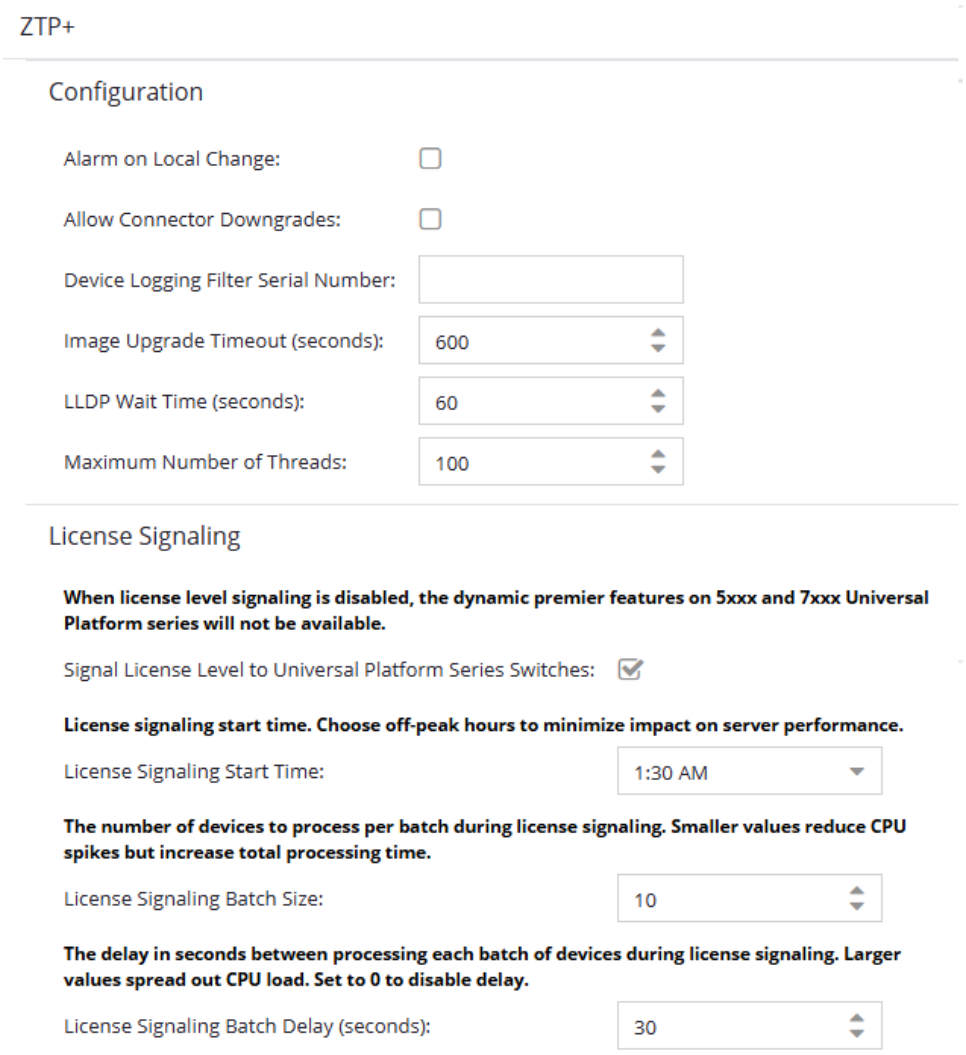
When ExtremeCloud IQ Site Engine discovers a new controller, Wireless Manager attempts to authenticate with the controller using this shared secret. For proper functioning, ExtremeCloud IQ Site Engine and the controller must be configured with the same shared secret. Each controller can be configured with a different **Shared Secret** as long as Wireless Manager knows what it is. You can configure a **Shared Secret** on a per controller basis using Wireless Manager. Select the **Eye** icon to display your password.

ZTP+ Options

Selecting ZTP+ in the left panel of the **Options** tab provides the following view, where you can specify options for zero touch provisioning plus (ZTP+) functionality.

Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.

NOTE: The ZTP+ Poll Type is incompatible with Switch Engine devices running in FIPS mode.



Configuration

Alarm on Local Change

Select the check box to generate an alarm when ExtremeCloud IQ Site Engine detects that the ZTP+ configuration of the device does not agree with the configuration set in ExtremeCloud IQ Site Engine.

When you enable this alarm, ExtremeCloud IQ Site Engine will not write the settings to the device because this would overwrite the changes made locally to the device (typically via the CLI). Instead, an alarm will be generated to alert you that the ExtremeCloud IQ Site Engine settings and the Device settings are different so you can decide on one of the following options:

- Change the values of the settings in ExtremeCloud IQ Site Engine. The settings will then be written to the device at the next ZTP+ poll.
- Use the menu option Overwrite Local Settings to synchronize the device to be the same as ExtremeCloud IQ Site Engine at the next poll.

NOTE: No changes will be written to the device until the alarm is cleared.

Allow Connector Downgrades

Select the check box to allow ExtremeCloud IQ Site Engine to downgrade to a previous version of the cloud connector.

Device Logging Filter Serial Number

Enter the serial number of one of your ZTP+ devices where ExtremeCloud IQ Site Engine records debug information. This allows you to save debug information to only one device, instead of saving identical debug information to all ZTP+ devices in a site.

Image Upgrade Timeout (seconds)

The amount of time (in seconds) ExtremeCloud IQ Site Engine waits for a response before determining the image upgrade is not responding for your ZTP+ devices.

LLDP Wait Time (seconds)

The amount of time (in seconds) ExtremeCloud IQ Site Engine waits for a response when communicating via LLDP.

Maximum Number of Threads

Defines the number of concurrent ZTP+ threads that can be running at any given time. Each thread can serve one ZTP+ device at a time.

License Signaling

Signal License Level to Universal Platform Series Switches

Select the check box to allow ExtremeCloud IQ Site Engine to periodically signal the license level to the Universal Platform series switches 4xxx, 5xxx, and 7xxx. These switches can provide different features based on the license level (unlicensed, licensed with Pilot, licensed with Standard).

Clear the check box to disable. The dynamic premier features on Universal Platform series switches 5xxx and 7xxx are not available, and the full CLI will not unlock dynamically on Universal Platform series switches 4xxx.

License Signaling Start Time

Select the drop down to specify the license signaling start time. Choose an off peak hour to minimize the impact on server performance.

License Signaling Batch Size

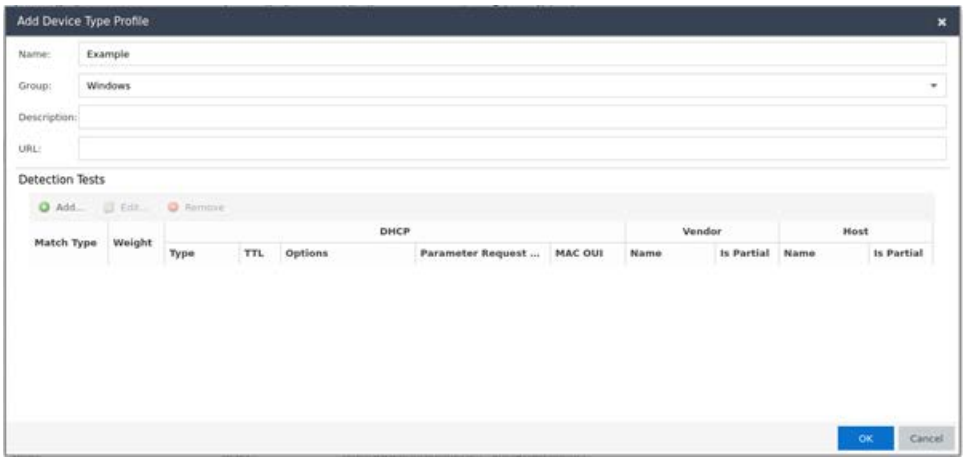
Select the number of devices to process for each batch during license signaling. Choose smaller values to reduce CPU spikes but increase total processing time.

License Signaling Batch Delay (seconds)

Select the delay in seconds between processing each batch of devices during license signaling. Choose larger values to spread out CPU load, choosing 0 disables the delay.

Add Device Type Profile

Use the **Add Device Type Profile** window to add device types for detection and profiling in ExtremeCloud IQ Site Engine. When configured, ExtremeCloud IQ Site Engine uses the information included in the Detection Tests section of the window to identify devices accessing your network.



Name
The name of the Device Type.

Group
The group of devices to which the Device Type belongs. Select from a list of existing Device Type Groups from Control, or edit the field to add it to a new or existing Family.

Description
Information about the device type profile.

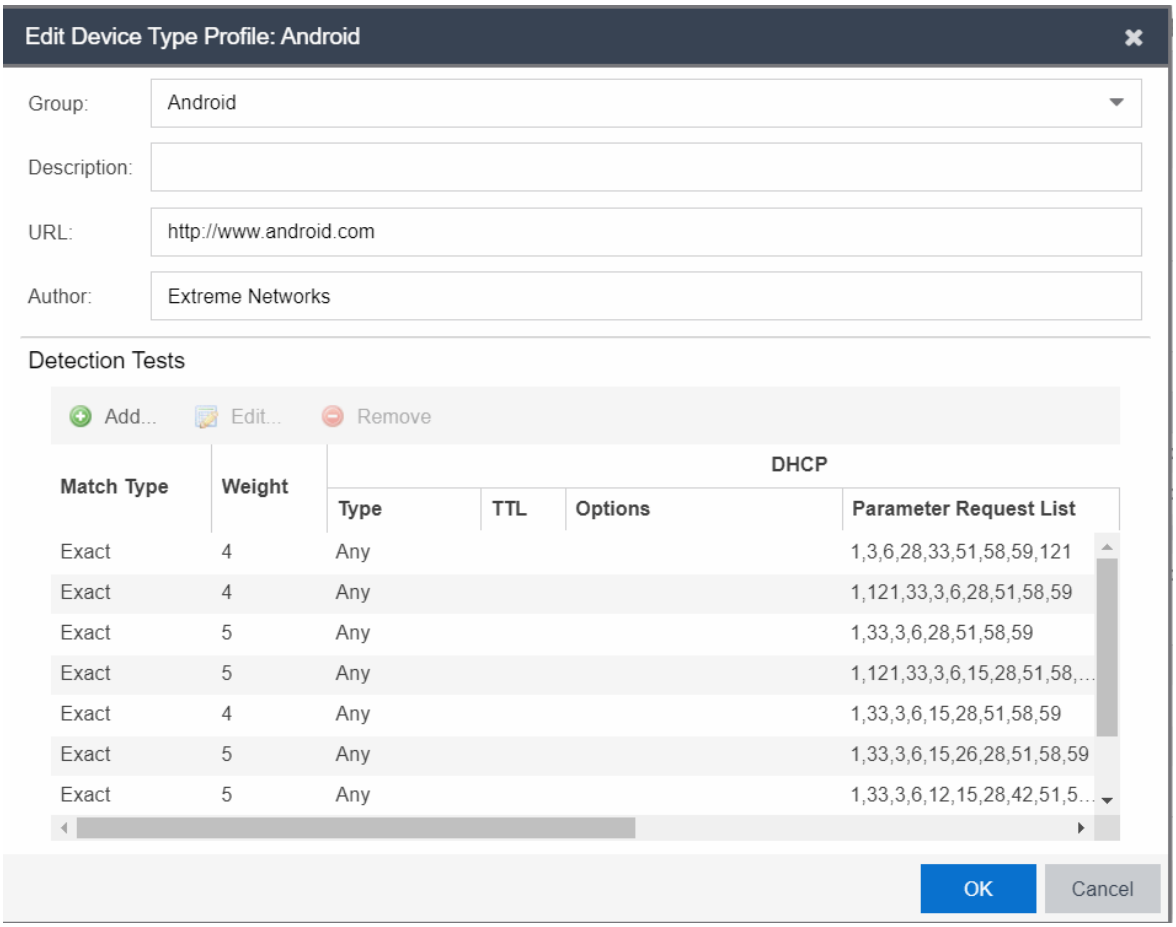
URL
The URL of the vendor of a device type.

Detection Tests
The DHCP fingerprint by which ExtremeCloud IQ Site Engine identifies a device type. Select **Add** or **Edit** to open the **Add/Edit Device Type Detection Test** window, from which you can create or modify the fingerprints ExtremeCloud IQ Site Engine uses to identify a device type. Select **Remove** to delete a fingerprint.

- Device Types
- Add/Edit Device Type Detection Test

Edit Device Type Profile

Use the **Edit Device Type Profile** window to edit device types for detection and profiling in ExtremeCloud IQ Site Engine. When configured, ExtremeCloud IQ Site Engine uses the information included in the Detection Tests section of the window to identify devices accessing your network.



Group
The group of devices to which the Device Type belongs.

Description
Information about the device type profile.

URL
The URL of the vendor of a device type.

Author
The source of the device type profile.

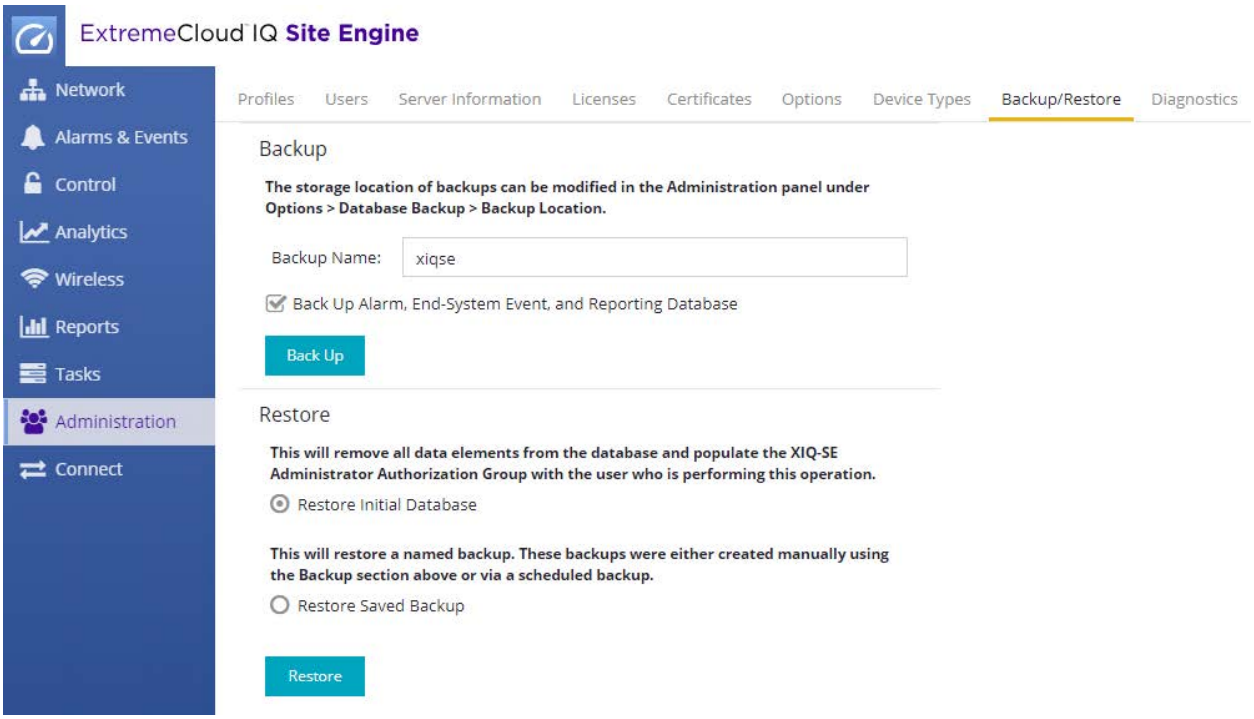
Detection Tests

The DHCP fingerprint by which ExtremeCloud IQ Site Engine identifies a device type. Select **Add** or **Edit** to open the **Add/Edit Device Type Detection Test** window, from which you can create or modify the fingerprints ExtremeCloud IQ Site Engine uses to identify a device type. Select **Remove** to delete a fingerprint.

- Device Types
- Add/Edit Device Type Detection Test

Backup/Restore

Use the **Backup/Restore** tab to save the currently active database as a file, restore the initial database or restore a saved legacy database, and manage the password and connection URL for the database. You must be assigned the appropriate user capabilities to perform these functions.



Backup

Use the Backup section of the tab to save the current database. Specify a directory path in which to save the database backup as a file and name the file.

NOTE: To schedule regular database backups, use the Database Backup option available from **Administration** > **Options** > **Database Backup**.

Backup Name

Enter a name for the database backup file.

Back Up Alarm, End-System Event, and Reporting Database

Select the checkbox to include alarm, end-system event, and reporting information in the backup.

NOTE: Backups created with this checkbox selected can be extremely large.

Back Up
Starts the backup operation.

Restore

Use the Restore section to restore the initial database or restore a saved database. Both functions cause all current client connections and operations in progress to be terminated.

IMPORTANT: After restoring the ExtremeCloud IQ Site Engine server, enforce all Access Control engines.

Restore Initial Database
Select this option to remove all data elements from the database and populate the Netsight Administrator authorization group with the name of the logged-in user.

Restore Saved Backup
Select this option to remove all data elements from the database and then re-populate the database using a saved file created in version 8.0. Use the drop-down list to select the file from which you want to populate the database.

NOTE: If no compatible database backups are present then this option is not displayed.

Devices onboarded to ExtremeCloud IQ after the backup was created become orphaned when the database restore is completed. You might need to manually delete orphaned devices in ExtremeCloud IQ after a backup restoration.

Restore
Starts the restore operation.

Advanced
Displays the Advanced section of the window.

Advanced

Use the Advanced section of the tab to configure the URL and password the ExtremeCloud IQ Site Engine server uses when it connects to the database.

IMPORTANT: When ExtremeCloud IQ Site Engine is installed, it automatically secures the MySQL database server by removing all the root and anonymous users from the MySQL user database. ExtremeCloud IQ Site Engine then adds one generic user name (user = netsight) and password (password = enterasys). Change this password, as all customers who install ExtremeCloud IQ Site Engine know this generic password.

Connection URL

Displays the URL the ExtremeCloud IQ Site Engine server uses when connecting to the database. For troubleshooting purposes, (for example, if you can't connect to the database) you can enter a new connection URL. Enter a new URL in the following format, and select **Apply**:

`jdbc:mysql://[hostname]/<database>` where [*hostname*] is optional.

NOTE: You must restart both the ExtremeCloud IQ Site Engine server and client after you change the **Connection URL**.

Password

Enter the password the ExtremeCloud IQ Site Engine uses when connecting to the database. Select the **Eye** icon to display your password.

NOTE: You must restart both the ExtremeCloud IQ Site Engine server and client after you change the **Connection URL**.

Restore Defaults

Restores the default values for the **Connection URL** and **Password** fields.

Reset

Discards any unsaved changes in the **Connection URL** and **Password** fields.

Save

Saves changes made to the **Connection URL** and **Password** fields.

- Database Backup Options

Client API Access

Use the **Client API Access** tab to display the clients with authentication access to the Event Correlation functionality or the ExtremeCloud IQ Site Engine Northbound Interface API from external applications.

The **Client API Access** tab contains the Registered Clients table, which displays all of the external clients capable of communicating with ExtremeCloud IQ Site Engine.

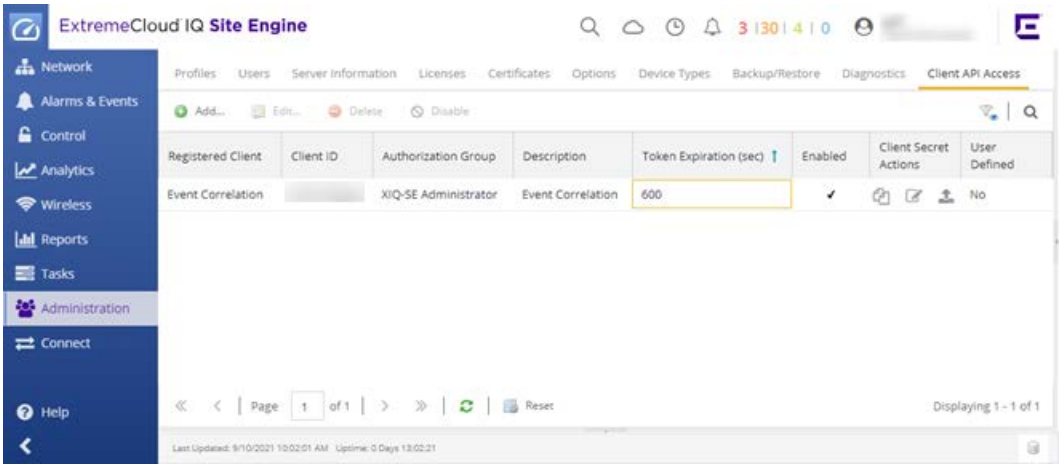
Via this tab, ExtremeCloud IQ Site Engine provides a client ID and secret that can be used by the client to generate a token to use for accessing ExtremeCloud IQ Site Engine. When the external application uses the token to access ExtremeCloud IQ Site Engine, access is granted according the capabilities enabled for the Authorization Group selected.

Select the **Add** or **Edit** buttons to open the **Add/Edit Client** window, from which you can add or edit registered clients. Adding a registered client enables the external application to communicate with ExtremeCloud IQ Site Engine. Additionally, use the **Add/Edit Client** window to display the functional areas of ExtremeCloud IQ Site Engine the external client can access based on the Authorization Group selected at the bottom of the window.

Access to ExtremeCloud IQ Site Engine information from external integrations via an API enables ExtremeCloud IQ Site Engine to correlate similar events and respond to a perceived threat to the network.

NOTES:

- **Event Correlation** is a system-defined client that cannot be deleted.
- For **Event Correlation** and the **Northbound Interface API** to access ExtremeCloud IQ Site Engine information, they must have access privileges (called Capabilities).



Registered Client

The name of the client with access to ExtremeCloud IQ Site Engine. The client name is user-defined and should be one that readily identifies the Client.

Client ID

This column displays a unique, system-defined numeric identifier for the client.

NOTE: To access the following information through NBI using Client API access authentication, the Client ID must be assigned to an Authorization Group with the appropriate NBI capabilities.
If the Client ID is assigned to an Authorization Group other than the XIQ-SE Administrator Authorization Group, only user workflow data is available.

Authorization Group

This column shows the level of access for the user according to the capabilities configured for the Authorization Group.

Description

The description of the client accessing ExtremeCloud IQ Site Engine.

Token Expiration (sec)

The amount of time (in seconds) before the authorization token expires and the client can no longer access ExtremeCloud IQ Site Engine without first generating a new token.

Enabled

Indicates whether or not the client API access connection currently enables access to ExtremeCloud IQ Site Engine.

Client Secret Actions

Select the icons to access the shared secret used to enable the client to communicate with ExtremeCloud IQ Site Engine:

- Copy to clipboard () — Select to copy the shared secret to the clipboard, which you can then paste in the client.
- Generate new () — Select to generate a new shared secret.
- Upload to the client () — Select to upload the shared secret to the external client. This icon is only available for system-defined clients.

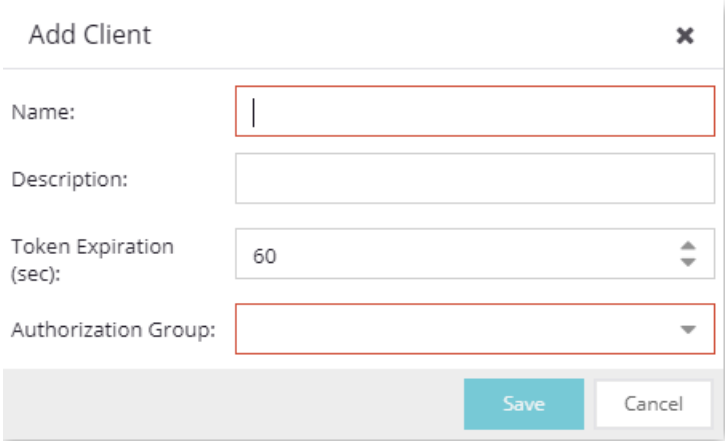
User Defined

Indicates whether the Registered Client was created by an ExtremeCloud IQ Site Engine user or automatically by the system.

Add/Edit Client

Use the **Add/Edit Client** dialog to add or edit authentication access for a client to the ExtremeCloud IQ Site Engine Northbound Interface API from external applications. Adding a registered client via this dialog allows the external application to communicate with ExtremeCloud IQ Site Engine.

Access this dialog by selecting **Add** or **Edit** on the Client API Access tab.



Name
The name of the client for which you are adding access to ExtremeCloud IQ Site Engine.

Description
A description of the client accessing ExtremeCloud IQ Site Engine.

Token Expiration (sec)
The amount of time (in seconds) before the authorization token expires and the client can no longer access ExtremeCloud IQ Site Engine without first generating a new token.

Authorization Group
Select the Authorization Group that includes the capabilities for which the client requires access in ExtremeCloud IQ Site Engine.

Using the Northbound Interface to Integrate with Third-Party Software

Use the instructions in this topic to integrate with third-party software via the Northbound Interface (NBI). ExtremeCloud IQ Site Engine's NBI is an API that allows third-party applications to view and update information in ExtremeCloud IQ Site Engine.

The NBI uses the GraphQL query language to request a JSON object response from ExtremeCloud IQ Site Engine. The JSON response contains the information you are retrieving for your third-party software.

Depending on your credentials, you can use the NBI to read (query) information in ExtremeCloud IQ Site Engine or write to fields in ExtremeCloud IQ Site Engine via mutations.

This topic contains the following sections:

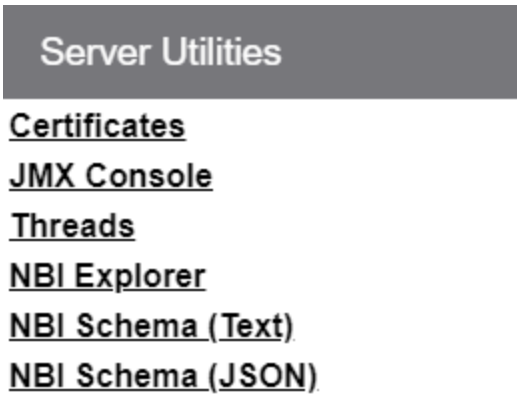
- Accessing NBI Tools in ExtremeCloud IQ Site Engine
- Using the NBI Explorer
- Compound Rules NAC Rule Criteria for NBI

Accessing NBI Tools in ExtremeCloud IQ Site Engine

Using the NBI Tools functionality in ExtremeCloud IQ Site Engine allows you to visually preview the data hierarchy and their types in ExtremeCloud IQ Site Engine.

To access NBI Tools in ExtremeCloud IQ Site Engine:

1. Access the **Diagnostics** tab.
2. Select **Server** in the left-panel menu to expand it and select **Server Utilities**.
   The **Server Utilities** tab opens.



3. Select the **NBI Explorer** to access the NBI Explorer.

NOTE: Select **NBI Schema (Text)** or **NBI Schema (JSON)** to display the format you use when defining your queries and mutations in the NBI in plain text format or in JavaScript Object Notation, respectively.

Using the NBI Explorer

Selecting **NBI Explorer** in the **Server Utilities** tab opens the NBI Explorer in a new tab or window, depending on how your browser is configured.

NOTE: To access the NBI requires access to the **Northbound API** Authorization Group capability.

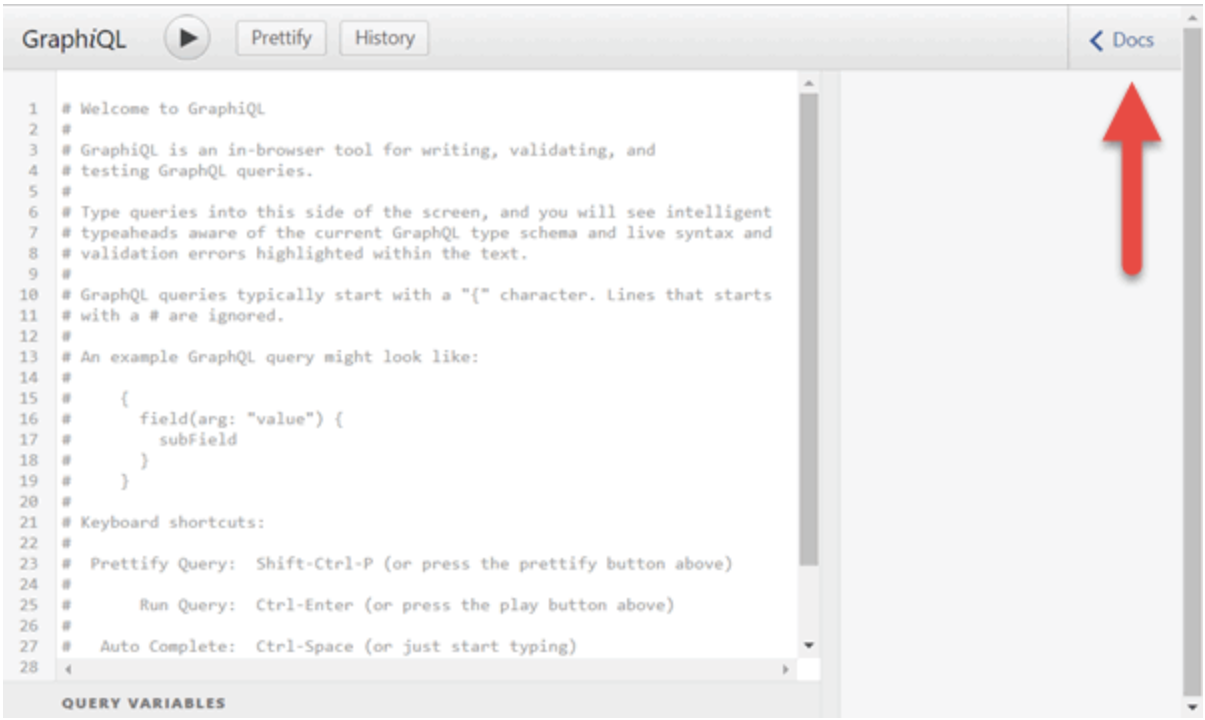
The NBI Explorer provides you with read-only access to queries and write access via mutations, allowing you to preview the data so you know what queries and mutations to use in your third-party applications. You can add NBI queries and mutations via python scripts or use NBI queries and mutations in https via REST calls.

For example, to retrieve the IP address and policy domain for a device, enter:

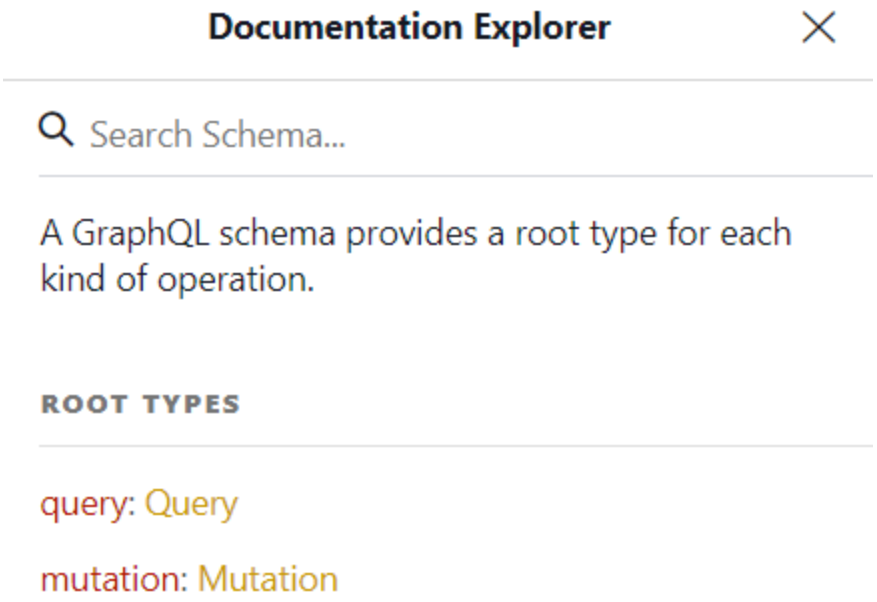
```
#Embedded Python Script

deviceIP = emc_vars['deviceIP']

response = emc_api.query("ExtremeApi { Network { device(ip: deviceIP) { ip
policyDomain}}}");

network = response['network'];

for device in network['devices']:

print " IP: ",device['ip']

print " Policy Domain: ", device['policyDomain']
```

For additional information about the queries and mutations available in the NBI Explorer:

1. Open the NBI Explorer.
2. Select **Docs** at the top-right of the NBI Explorer.

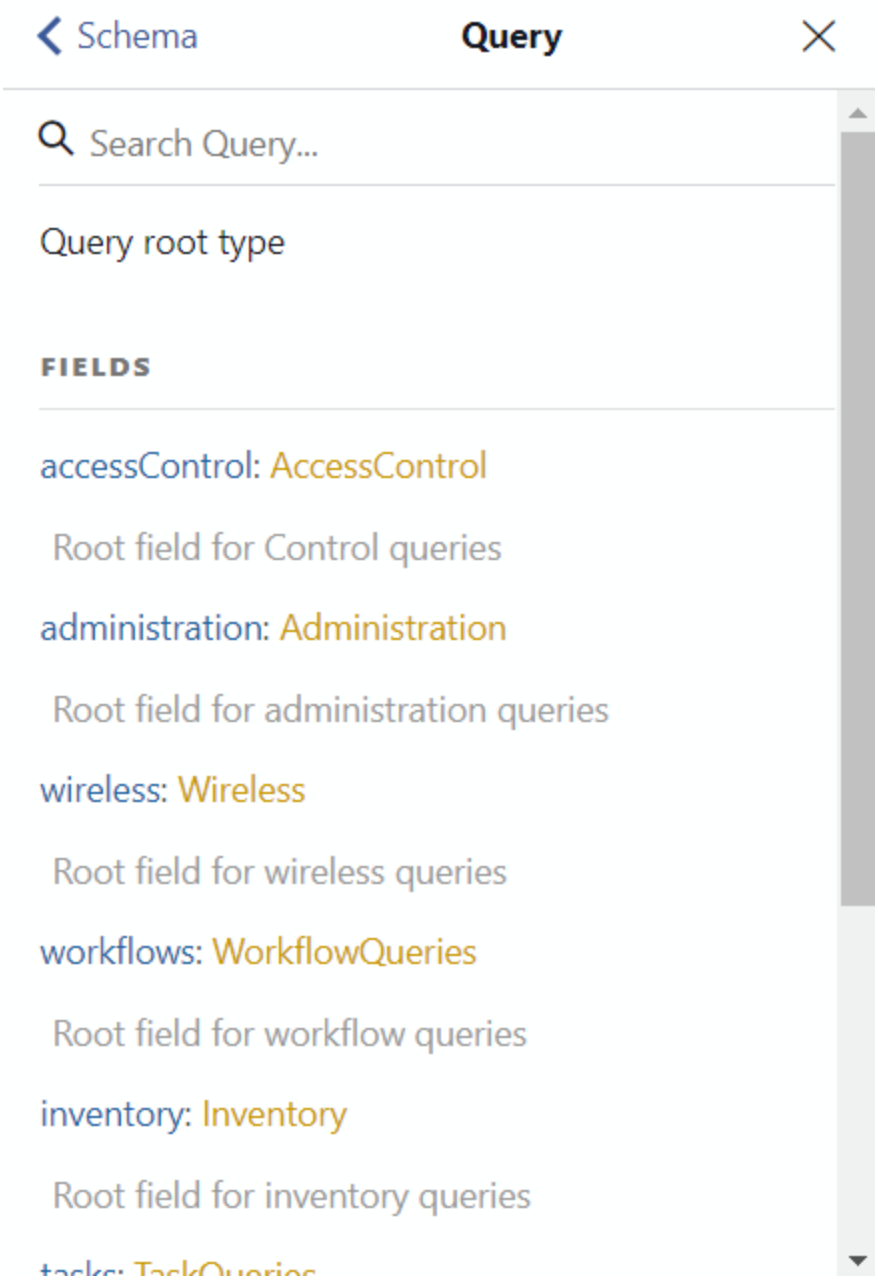


The Documentation Explorer opens.



3. Search for a **Schema** by entering it in the Search Schema field, or select **Query** or **Mutation** to browse for available queries and mutations:
    - If you entered a schema in the **Search Schema** field, the matching fields and schema types display in the Documentation Explorer. Select the query or mutation field you are using in your command in the left side of the NBI.

      If you selected **Query** or **Mutation**, the available query or mutation fields display:



- Select the field that you are using until you find the appropriate query or mutation for your command.

Configure the queries or mutations included in your command in the left side of the window.

When it is complete, select the **Execute Query** button ( ) to run the query or mutation.

For complete schema information, see the NBI API site.

Compound Rules NAC Rule Criteria for NBI

The Northbound Interface (NBI) NAC rule query is updated to support Compound Rules. When you query NAC rules through the NBI, the response returns criteria values using a list-based structure for the User Groups and End-System Groups criteria categories.

Link-Based Response Format

For User Groups and End-System Groups criteria categories, the NBI response includes a list of type and value entries that represent each selected value in the category. Each entry contains the following:

criteriaTypeStr
: The criteria type identifier.

criteriaValue
: The criteria value identifier.

For example, a rule with User Groups specified as "Group A" AND "Group B" returns the following:

```
userGroupCriteria: [
{ criteriaTypeStr: "userGroup", criteriaValue: "Group A" },
{ criteriaTypeStr: "userGroup", criteriaValue: "Group B" }
]
```

Legacy Single-Value Parameters

For backward compatibility, the existing single-value NAC rule parameters are retained. The legacy parameters point to the first value in a multi-value condition. The best practice is to migrate to the list-based parameters to correctly represent and process compound rules.

Important: When a NAC rule contains multiple values in a criteria category, the legacy single-value parameters return only the first value. To retrieve all values in a compound rule, use the list-based parameters. If you integrate with ExtremeControl through the NBI, update your implementations to use the list-based parameters when working with compound rules.

NOTE: For criteria categories that contain only a single value, both the legacy single-value parameters and the list-based parameters return the same result.

- NBI API Site
- Administration
- Client API

Tasks

Tasks allows you to create scripts and workflows and use them to configure tasks. Additionally, you can save a task you run on a device or group of devices, or configure the task to run on a scheduled basis that you define.

The **Tasks** tab contains the following sub-tabs:

- Workflow Dashboard
- Scheduled Tasks
- Saved Tasks
- Scripts
- Workflows

The Menus icon () at the top of the screen provides links to additional information about your version of ExtremeCloud IQ Site Engine.

Workflow Dashboard

Workflow Dashboard allows you to view a list of previously run workflows, information about the status of the elements within the workflow, and information about the devices on which the workflow ran.

The tab also provides a breakdown of the completion status of each of the Activities within the workflow.

Scheduled Tasks

Scheduled Tasks allows you to configure ExtremeCloud IQ Site Engine to automatically generate reports, run a workflow or a script, and discover recently added devices. You can also use it to set SMTP Email Server Options to use when the scheduled task sends an email notification.

Saved Tasks

The Saved Tasks allows you to save a script or workflow as a task after running it on a device or group of devices. This allows you run the task repeatedly on an ad hoc basis.

Scripts

Scripts allows you to view predefined scripts provided by ExtremeCloud IQ Site Engine, and allows to create your own scripts.

ExtremeCloud IQ Site Engine scripts are files containing CLI commands, control structures, and data manipulation functions. Scripts can be executed on one or more devices or ports, simultaneously on multiple devices or ports, or on one device or port at a time.

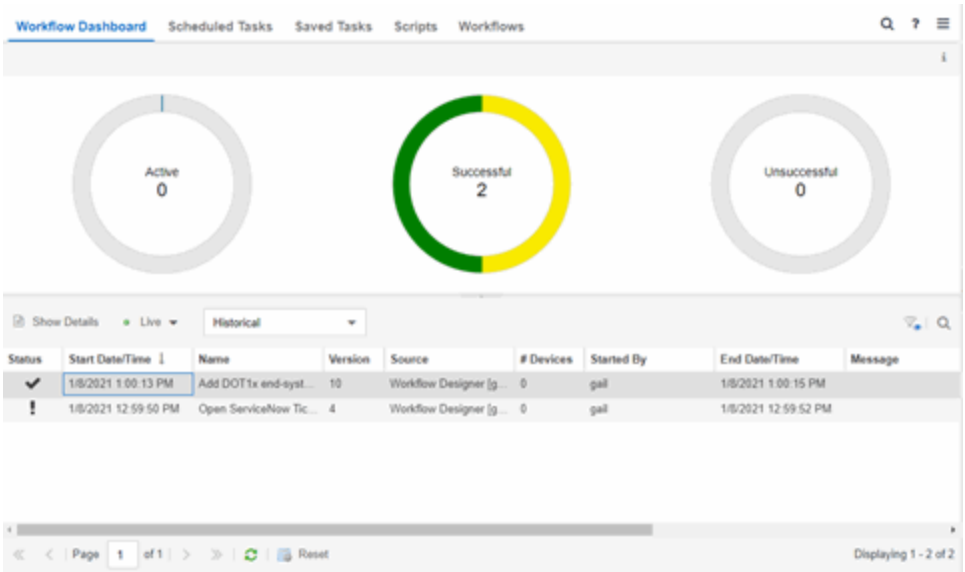
You can create tasks, which run a script on specified devices or ports at specified times, either on a one-time or recurring basis. Tasks execute the script according to a schedule you configure.

Workflows

Workflows allows you to view workflows you create modeled as diagrams, with each action linked in a chain. After you create a workflow, ExtremeCloud IQ Site Engine performs a complex series of steps with a single select. You can also define a set of actions in the event an action occurs successfully and another set of actions in the event an action does not occur successfully. After you create a workflow, you can schedule it to run on a periodic basis in Scheduled Tasks. Other action and task/workflow function sources can also trigger a workflow to run.

Workflow Dashboard

The **Workflow Dashboard** tab allows you to view information about workflows you execute on devices in your network.



The tab contains two sections:

- Workflow Charts
- Workflow Results

Additionally, double-clicking a workflow in the Workflow Results table opens the **Workflow Details** tab.

Workflow Charts

The top of the **Workflow Dashboard** tab displays three charts that provide a summary of Active Workflows, Successful Workflows, and Unsuccessful Workflows. If the Update drop-down list above the Workflow Results table is either **Live** or **Live (Current Page)**, the information in these charts updates automatically as conditions change.



The center of each chart indicates the number of active, completed, and failed workflows. Each chart includes multiple Statuses. Hover over a ring color to display a description of the **Status** for that piece of the chart. Select a section of one of the ring charts to filter the Workflow Results table to display the workflows with a **Status** that matches the color selected.

Active

The center of the Active Workflow ring chart indicates the number of workflows currently running in ExtremeCloud IQ Site Engine.

Successful

The center of the Successful ring chart indicates the number of workflows that completed successfully:

- Yellow — The yellow portion of the ring chart indicates the percentage of completed workflows with a **Status** of **Completed**.
- Green — The green portion of the ring chart indicates the percentage of completed workflows with a **Status** of **Success**.

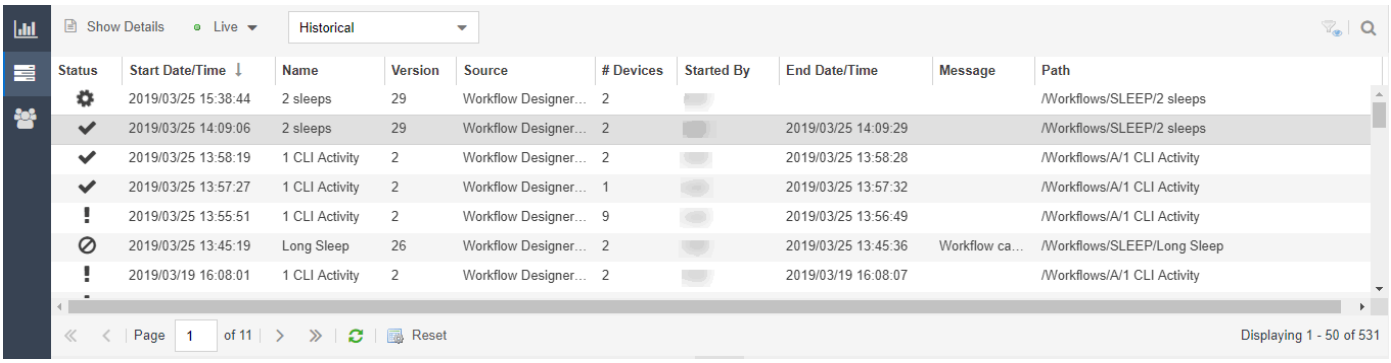
Unsuccessful

The center of the Unsuccessful ring chart indicates the number of workflows that did not complete successfully:

- Orange — The orange portion of the ring chart indicates the percentage of workflows that completed with a **Status** of **Canceled**.
- Red — The red portion of the ring chart indicates the percentage of workflows that completed with a **Status** of **Failed**.
- Dark Red — The dark red portion of the ring chart indicates the percentage of workflows that completed with a **Status** of **Timed-Out**.

Workflow Results

The Workflow Results table displays details about the workflows you run. Select a color in one of the ring charts to filter the table to display the workflows with a **Status** that matches the **Status** selected.



ID

A system-defined ID number for the workflow.

Execution ID

An ID number that refers to the execution of the workflow. This ID number allows you to determine a workflow executed from a location other than the **Workflows** tab (for example, a third-party application via the Northbound Interface).

Show Details

Select a row in the table and select **Show Details** to open the workflow in the **Workflow Details** tab. Double-clicking a workflow also opens it in the **Workflow Details** tab.

Update

Select the **Update** drop-down icon at the top of the table to select whether the workflows in the table update automatically:

- **Live** — ExtremeCloud IQ Site Engine automatically updates the workflows in the table with any changes and new workflows display as they run.
- **Live (Current Page)** — ExtremeCloud IQ Site Engine updates the workflows currently in the table, but does not include new workflows as they run.
- **Paused** — ExtremeCloud IQ Site Engine does not update the workflows in the table.

Type

Select the **Type** drop-down icon at the top of the table to select whether the table displays currently running workflows or completed workflows:

- **Active** — The table displays currently running workflows. Selecting the Active Workflows ring chart automatically changes this drop-down list to **Active**.
- **Historical** — The table displays workflows that are not currently running. This includes workflows that completed successfully, failed, timed out, or are canceled. Selecting the

Completed or Failed Workflows ring charts automatically changes this drop-down list to **Historical**.

Status

Indicates whether the workflow completed successfully, partially completed, timed out, failed, or canceled:

- SUCCESS ( ) — Indicates the workflow completed successfully and all Activities within the workflow succeeded.
- COMPLETED ( ) — Indicates the workflow completed successfully, but not all Activities within the workflow succeeded.
- TIMEDOUT ( ) — Indicates the workflow did not complete in the amount of time configured in the **Timeout** field on the **Inputs** tab for the workflow.
- FAILED ( ) — Indicates the workflow did not complete successfully.
- CANCELED ( ) — Indicates a user canceled the workflow while it was running.

Start Date/Time

Displays the date and time the workflow started.

Name

Displays the name of the workflow.

Version

Displays the version of the workflow run on the devices. Each time you edit the workflow, the **Version** is incremented. This allows you to determine the exact workflow run on a device, even if the workflow is modified. For example, if you configure a workflow as a Scheduled Task (version 1) and then make a modification to the workflow (version 2), the version indicates the iteration of the workflow you are running.

Source

Displays the source from which the workflow ran. Workflow sources can be one of the following:

- Custom Alarm Action
- Notification Action
- Saved Tasks
- Workflow Designer
- Northbound Interface
- Site Discover Action
- Scheduled Tasks
- Device

- Port
- Security

 # Devices
Displays the number of devices on which the workflow is executed.

Description
A description of the workflow. This is defined on the **General** tab in the Details section of the **Workflows** tab.

Started By
Displays the user who initiated the workflow.

End Date/Time
Displays the date and time the workflow ended.

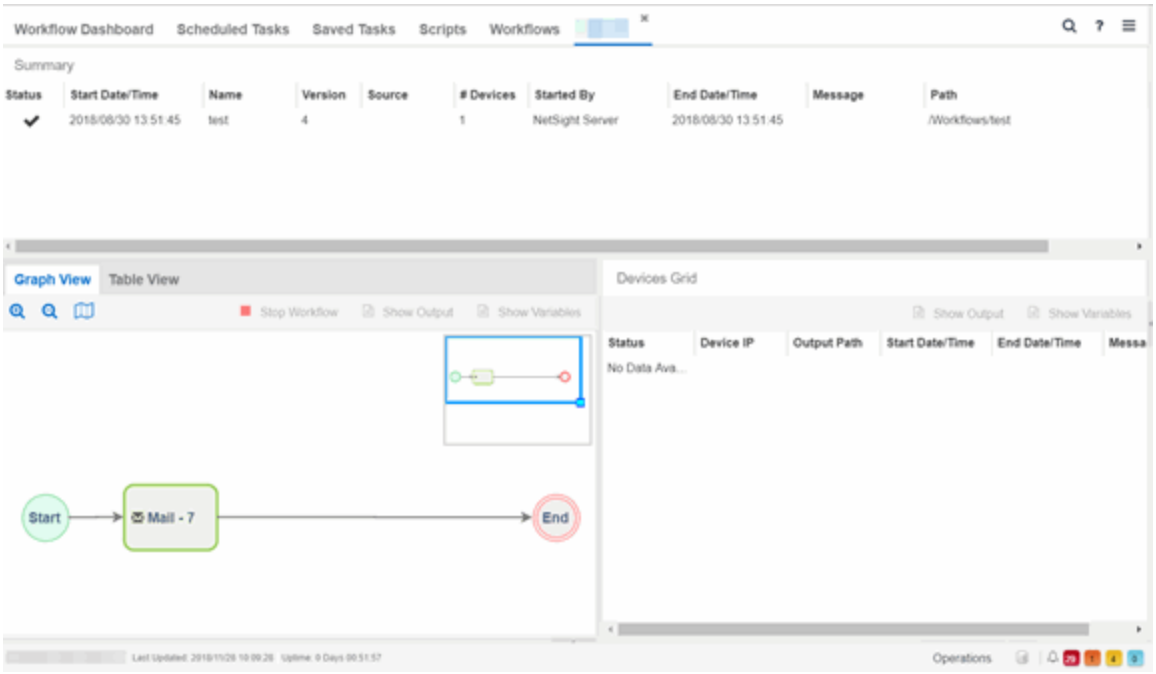
Message
Displays information regarding the reason for the Status (for example, Exceeded default time out).

Path
Displays the path on the **Workflows** tab in which the workflow is saved.

Select the **Refresh** icon to update the Workflow Results table to include any newly executed workflows.

Workflow Details

The **Workflow Details** tab displays when you double-click a workflow in the Workflow Results table of the **Workflow Dashboard** tab.

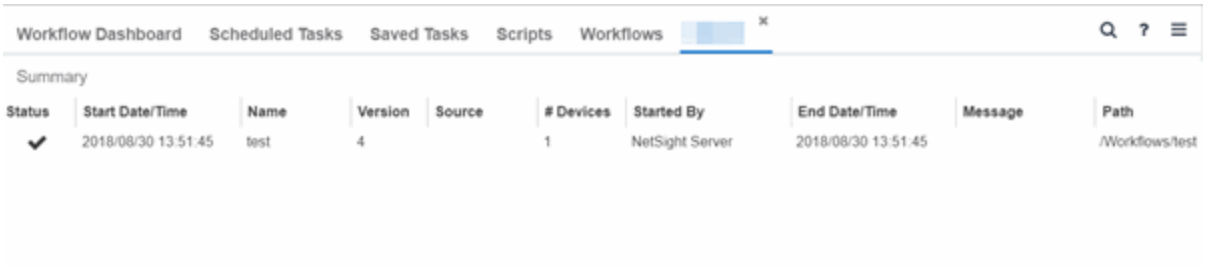


The **Workflow Details** view contains three sections:

- Workflow Summary
- Activities
- Devices Grid

Workflow Summary

The Workflow Summary table provides basic information about the workflow you select in the Workflow Results table.



ID

A system-defined ID number for the workflow.

Status

Indicates whether the workflow completed successfully, partially completed, timed out, or failed:

- SUCCESS (✔) — Indicates the workflow completed successfully and all Activities within the workflow succeeded.
- COMPLETED (❗) — Indicates the workflow completed successfully, but not all Activities within the workflow succeeded.
- TIMEDOUT (❓) — Indicates the workflow did not complete in the amount of time configured in the **Timeout** field on the **Inputs** tab for the workflow.
- FAILED (✖) — Indicates the workflow did not complete successfully.
- CANCELED (⊘) — Indicates a user canceled the workflow while it was running.

Start Date/Time

Displays the date and time the workflow started.

Name

Displays the name of the workflow.

Version

Displays the version of the workflow run on the devices. Each time you edit the workflow, the **Version** is incremented. This allows you to determine the exact workflow run on a device, even

if the workflow is modified. For example, if you configure a workflow as a Scheduled Task (version 1) and then make a modification to the workflow (version 2), the version indicates the iteration of the workflow you are running.

Source
Displays the source from which the workflow ran. Workflows can be initiated from the following features:

- Custom Alarm Action
- Notification Action
- Saved Tasks
- Workflow Designer
- Northbound Interface
- Site Discover Action
- Scheduled Tasks
- Device
- Port
- Security

 # Devices
Displays the number of devices on which the workflow is executed.

Description
A description of the workflow. This is defined on the **General** tab in the Details section of the **Workflows** tab.

Started By
Displays the user who initiated the workflow.

End Date/Time
Displays the date and time the workflow ended.

Message
Displays information regarding the reason for the Status (for example, Exceeded default time out).

Path
Displays the path on the **Workflows** tab in which the workflow is saved.

Activities

The Activities section displays details about each of the activities in the workflow you select in the Workflow Results table. It contains two tabs - graphical and tabular - each providing a different view of the workflow:

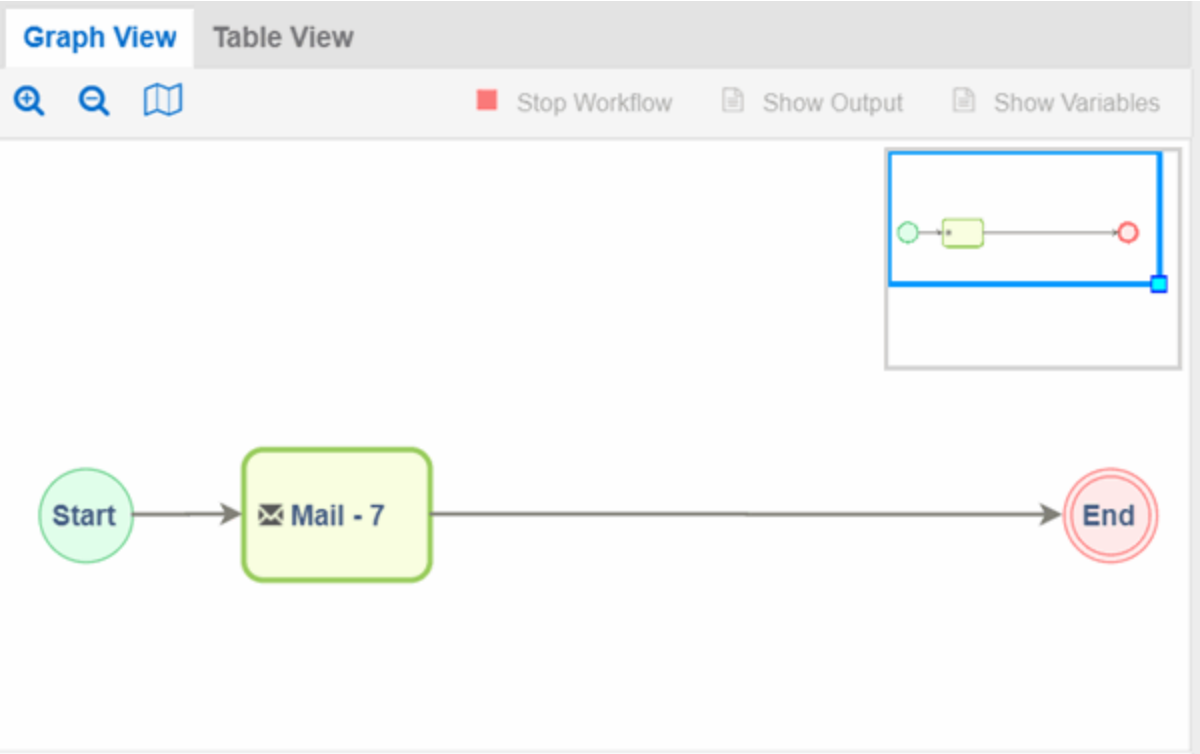
- Graph View
- Table View

Graph View

The **Graph View** tab provides a visual representation of active or historical workflows. This allows you to view the workflow version ExtremeCloud IQ Site Engine is using or did use when executing the workflow, regardless of the difference between the version run and the current version.

The Graph View includes the following features:

- Buttons
- Workflow Mini Map
- Workflow Run



Buttons

Use the buttons at the top of the **Graph View** tab to perform the following functions:

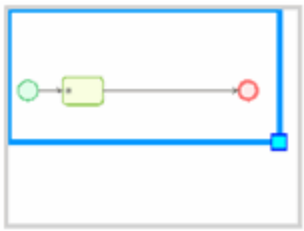
- **Zoom** ( ) - Use to zoom in and out of the graph view.
- **Toggle Mini Map** ( )- Opens a mini map displaying an overview of the entire workflow.
- **Stop Workflow** - Select to stop an active workflow currently running.

- **Show Output** - Select an activity and select to open a new window displaying the output generated by the activity. This information is also contained in the text file found in the **Output Path** on the device.
- **Show Variables** - Select an activity and select to open a new window displaying the variables included in the activity.

NOTE: If a workflow is run against more than one device, select the activity in the Graph or Table View and then select the device in the Devices Grid and use the **Show Output** and **Show Variables** buttons in that area.

Workflow Mini Map

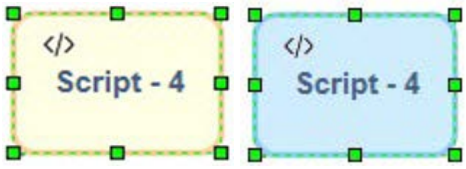
The mini map view displays the workflow run and the surrounding space in the graph view area.



To move the area of focus in the graph view, move the cursor over the blue focus box in the mini map until the cursor changes to a **Move** icon ( ). Select the blue focus box and move it in the mini map to the area on which you want to focus the Designer. Additionally, you can shrink or expand the blue focus box to automatically zoom in or out of the workflow, respectively. Select the light-blue box in the bottom-right corner of the blue focus box and resize the blue focus box as needed.

Workflow Run

The **Graph View** tab displays active and historical workflows as workflow runs. Select each element in the workflow run to display details about that element in the Devices Grid. When you select an activity in the workflow run, it is selected in the Table View as well. Selected items display with a green broken line border:



Activities that are active and currently being executed display in the workflow run in blue and are flashing. When the workflow finishes executing, the activity output and execution path taken is displayed in the workflow run.

The color of the activity represents its status in the workflow run:

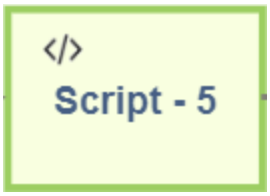
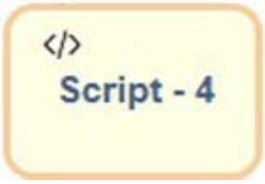
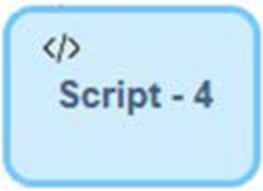
	Green	The activity completed successfully.
	Orange	A user canceled the activity.
	Blue	The activity is active.
	Red	The activity failed to complete.
	Grey	The workflow skipped the activity.

Table View

The **Table View** tab provides the results of each activity in the workflow selected in the Workflow Results section as a table.



Status

Indicates the result of the activity (for example, SUCCESS, FAILED, TIMEDOUT, CANCELED).

Name

Displays the name of the activity.

Custom ID
A user-defined ID number for the selected activity.

History ID
A system-defined ID number for the selected activity.

Activity Type
The type of activity (e.g. script) run as part of the workflow.

Description
A description of the activity. This is defined on the **General** tab in the Details section of the **Workflows** tab.

Message
Displays information regarding the reason for the **Status** (for example, Exceeded default time out).

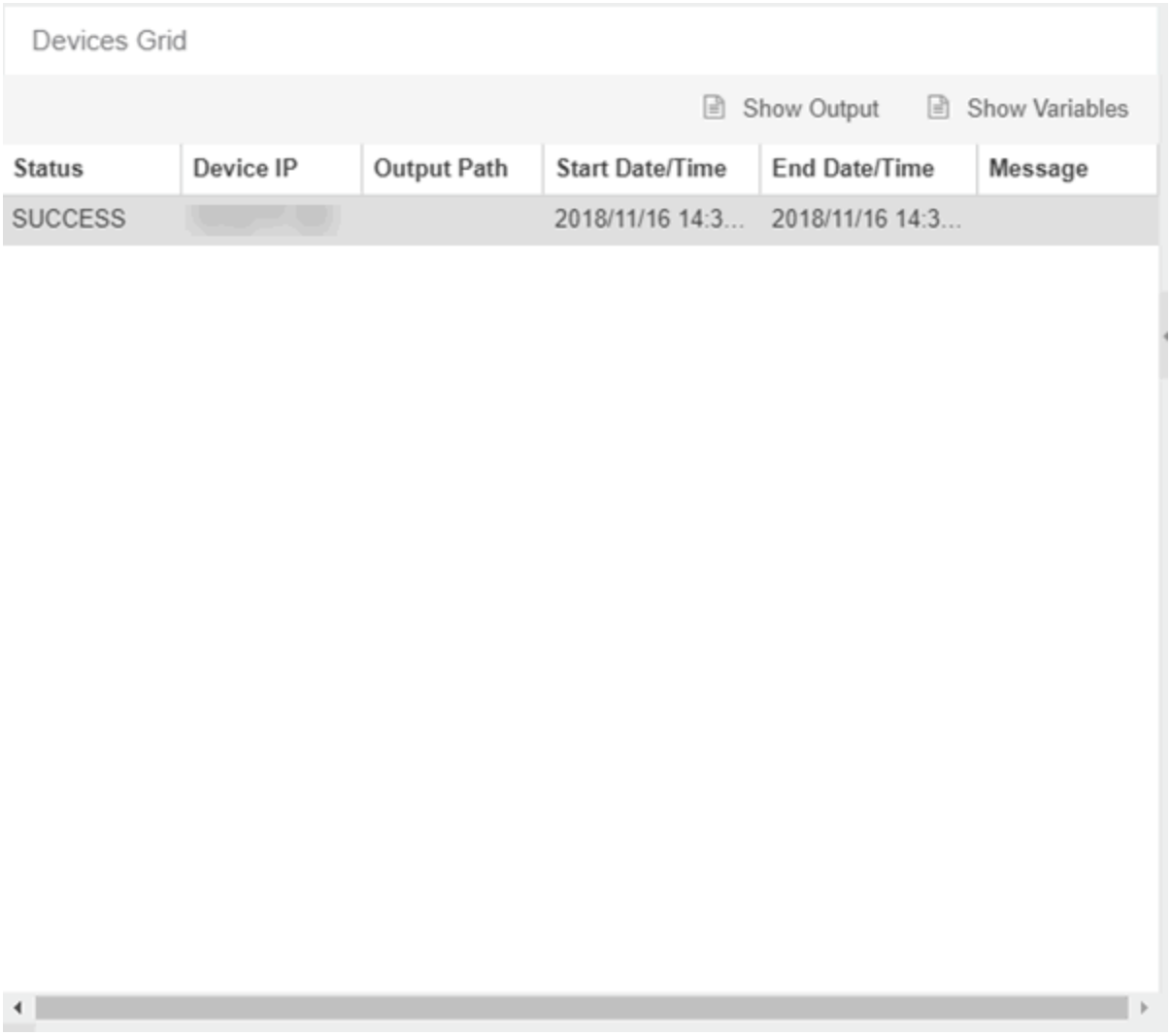
Start Date/Time
Displays the date and time the activity started.

End Date/Time
Displays the date and time the activity ended.

Select an activity and select the Show Output icon to open a new window displaying the output generated by the activity. This information is also contained in the text file found in the Output Path on the device. Select an activity and select the Show Variables icon to open a new window displaying the variables included in the activity. When you select an activity in the table, it is also selected in the workflow run in the Graph View tab and displays with a green broken line border.

Devices Grid

The Activity Device Results section of the window provides information about the devices on which the workflow ran.



Status

Indicates result of the workflow (for example, **SUCCESS**, **FAILED**, **TIMEDOUT**, **CANCELED**) for the device. **SKIPPED** indicates the workflow ran on a device on which the operating system defined in the **Network OS** tab is not installed.

Device IP

The IP address of the device on which the workflow ran.

Output Path

The path on the device where a text file is created that displays the output generated on the device by the workflow.

Start Date/Time

Displays the date and time the workflow started running on the device.

End Date/Time

Displays the date and time the workflow finished running on the device.

Buttons

Use the buttons at the top of the **Table View** tab to perform the following functions:

- **Show Output** - Select an activity and select to open a new window displaying the output generated by the activity. This information is also contained in the text file found in the **Output Path** on the device.
- **Show Variables** - Select an activity and select to open the **Variables** window, which displays the variables included in the activity. Double-click a variable in the window to open the **Variable Details** window, which displays the **Name** and **Value** of the variable and allows you to copy and paste the information.

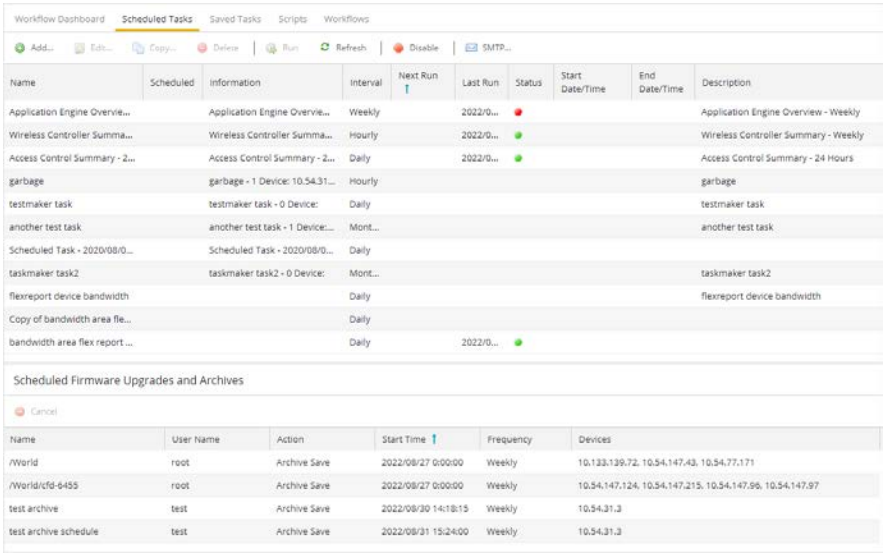
NOTE: If a workflow is run against more than one device, select the activity in the Graph or Table View and then select the device in the Devices Grid and use the **Show Output** and **Show Variables** buttons in that area.

Scheduled Tasks Overview

The **Scheduled Tasks** tab allows you to configure ExtremeCloud IQ Site Engine to automatically perform the following tasks:

- Generate a subset of available reports in PDF format
- Run a workflow
- Run a script
- Set SMTP Email Server Options to use when the scheduled task sends an email notification.

  NOTE: For the email notification to work, configure your SMTP Email Server options. Select the **SMTP** button to open SMTP Email Server , where you can specify the SMTP email server used by ExtremeCloud IQ Site Engine when sending emails to users.
- Discover newly added devices
- Cancel scheduled inventory tasks (firmware upgrades and archive saves)



Scheduled Tasks table lets you view currently scheduled tasks and use toolbar buttons to add, edit, copy, and delete a scheduled task. Select the **Disable** button to disable all active scheduled tasks. Scheduled Tasks referencing invalid workflows cannot be executed, cannot be copied, can be edited but not saved, and can be deleted. The user can investigate the values that were entered for the scheduler.

In the table, a green icon (🟢) in the **Status** column indicates the task ran successfully and a red icon (🔴) indicates an error occurred the last time the task ran. Select the red icon for error details.

Select the **Run** button to run a scheduled task immediately without having to change the scheduled run times. This facilitates the testing of scheduled tasks.

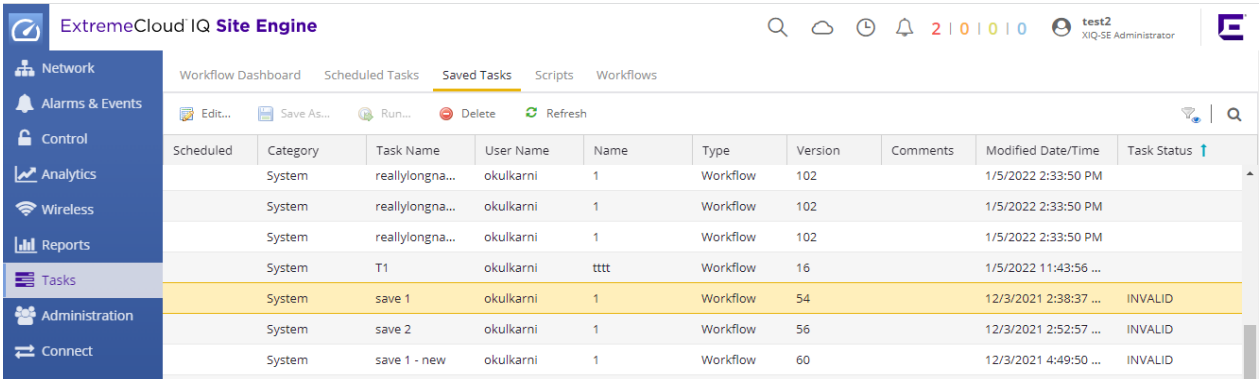
Access the event log from the Alarms and Events > **Events** tab, which allows you to display the status of events in ExtremeCloud IQ Site Engine. Select **Scheduled Task** from the drop-down list at the top of the table to view task execution events and errors.

The Scheduled Firmware Upgrades and Archives table lets you view and manage scheduled inventory tasks. To cancel a scheduled inventory task, select a row and then select **Cancel**.

Note: If you set the frequency for an archive task to On Startup, Now, or Never, the action is not considered scheduled, so the archive cannot be canceled from the **Scheduled Tasks** tab. It can only be set to Never in the **Archives** tab.

Saved Tasks

The **Saved Tasks** tab allows you to view tasks (scripts and workflows) you save after running them on a device or group of devices. After a task is saved, you can quickly run it again later.



Edit
: Select **Edit** to open the **Edit Saved Task** window, where you can edit the task configuration, the devices on which the task is run, and whether the task is automatically run on a scheduled basis.

Save As
: Select **Save As** to save the task with a new **Name**, which you can then edit.

Run
: Select **Run** to run the task as configured.

Delete
: Select **Delete** to remove the task from the **Saved Tasks** tab.

Refresh
: Select **Refresh** to update the list of saved tasks.

Scheduled
: A check mark in this column indicates the task is performed on a scheduled basis.

Category
: The task category, if configured. **Category** indicates the purpose of the task.

Name
: The name of the script or workflow running as a result of executing the task. The **Name** is defined when creating the script or workflow and can not be edited.

User Name
: The name of the user who saved the task.

Name
: The name assigned to the saved task. The **Name** is defined when saving the script or workflow as a saved task and can not be edited.

Type
: The type of task, either **Script** or **Workflow**.

Version
: When the saved task is a workflow, this indicates the version of the workflow run on the devices. Each time you edit the workflow, the **Version** is incremented. This allows you to determine the exact workflow run on a device, even if the workflow is modified. For example, if you configure a workflow as a Saved Task (version 1) and then make a modification to the workflow (version 2), the version indicates the iteration of the workflow you are running.

  When the saved task is a script, **Version** is **0** as ExtremeCloud IQ Site Engine always uses the most recently saved version of a script initiated from the **Saved Tasks** tab.

Script/Workflow ID
: Displays the system-defined ID for the script or workflow. This number is determined when the script or workflow is created.

Comments
: Comments or a description of the task.

Modified Date/Time
: The date the task was last modified.

Task Status
: **Task Status** is either valid (column is blank) or invalid (column contains **Invalid**). If the workflow is changed, some changes to the workflow can cause the task to become invalid. Examples of changes that can change the status to invalid are:

  - Adding an activity to the workflow.
  - Removing an activity from the workflow.
  - Adding information to the workflow.
  - Removing information from the workflow.

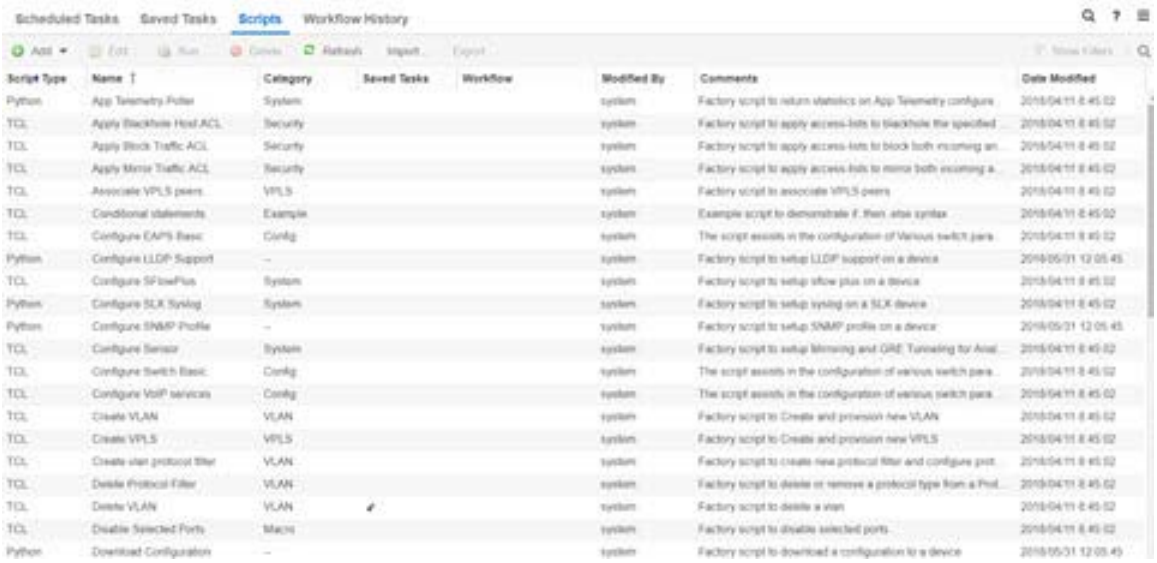
Scripts Overview

The Scripts tab allows you to view pre-defined scripts provided by ExtremeCloud IQ Site Engine, and allows you to create your own scripts.

ExtremeCloud IQ Site Engine scripts are files containing python scripts, CLI commands, control structures, and data manipulation functions. Scripts can be executed on one or more devices or ports: simultaneously on multiple devices or ports, or on one device or port at a time.

You can create tasks, which run a script on specified devices or ports at specified times, either on a one-time or recurring basis. Tasks execute the script according to a schedule you configure.

To display the scripts configured in ExtremeCloud IQ Site Engine, open Tasks > Scripts.



Script Type
: The language in which the script is written.

Name
: The name of the script. The script **Name** is defined when adding the script and can not be edited.

Category
: The script category, if configured. The **Category** indicates the purpose of the script.

Saved Tasks
: A check mark in this column indicates the script is configured as a saved task and is available on the **Saved Tasks** tab.

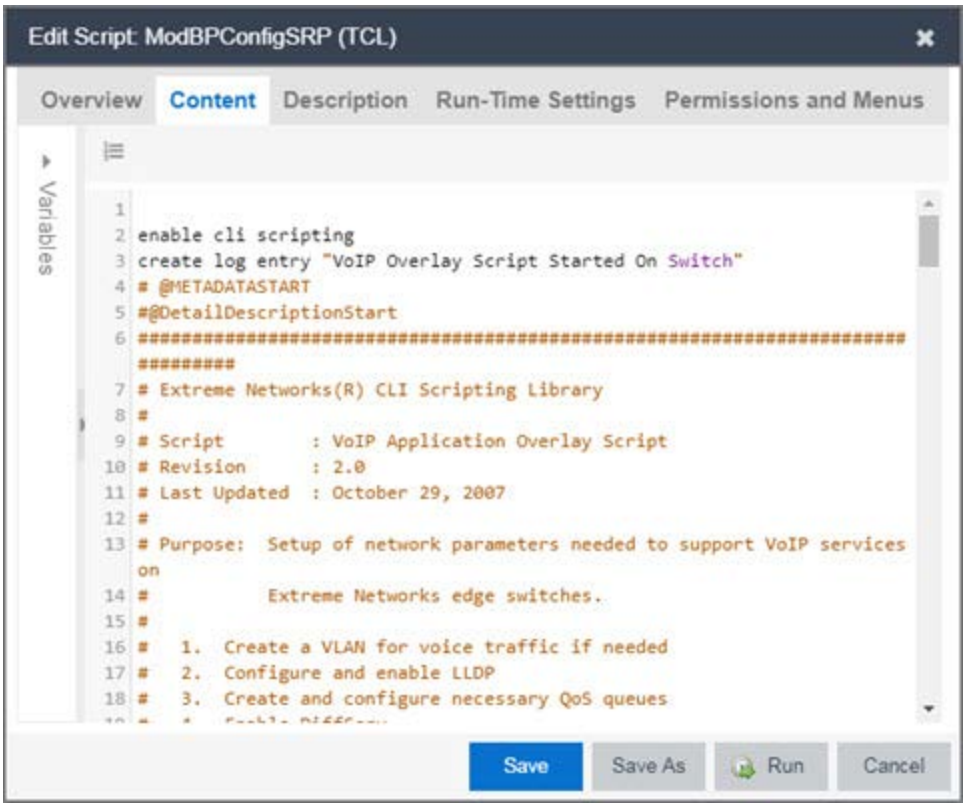
Workflow
: A check mark in this column indicates the task is included in a workflow.

Modified By
: The name of the last user to modify the script.

Comments
: Comments or a description of the script.

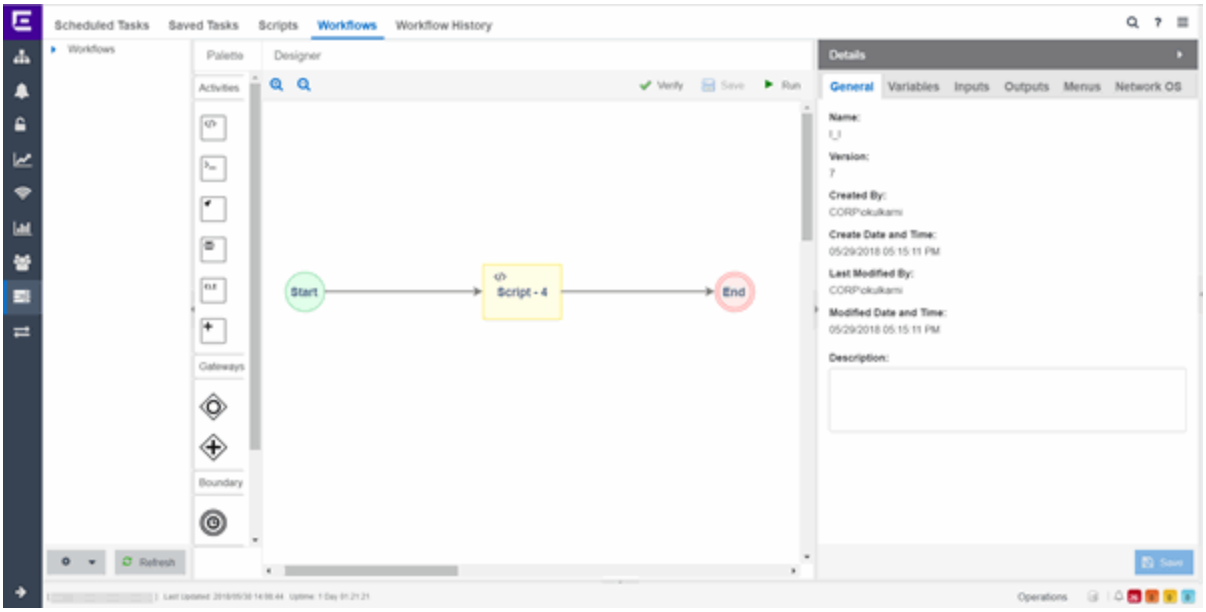
Date Modified
: The date the script was last modified.

Double-click a script to open the **Edit Script** window.



Workflows

The **Workflows** tab allows you to view workflows you create modeled as diagrams, with each action linked in a chain. After you create a workflow, ExtremeCloud IQ Site Engine performs a single action or a complex series of steps with a single select. You can also define a set of actions in the event an action occurs successfully and another set of actions in the event an action does not occur successfully.



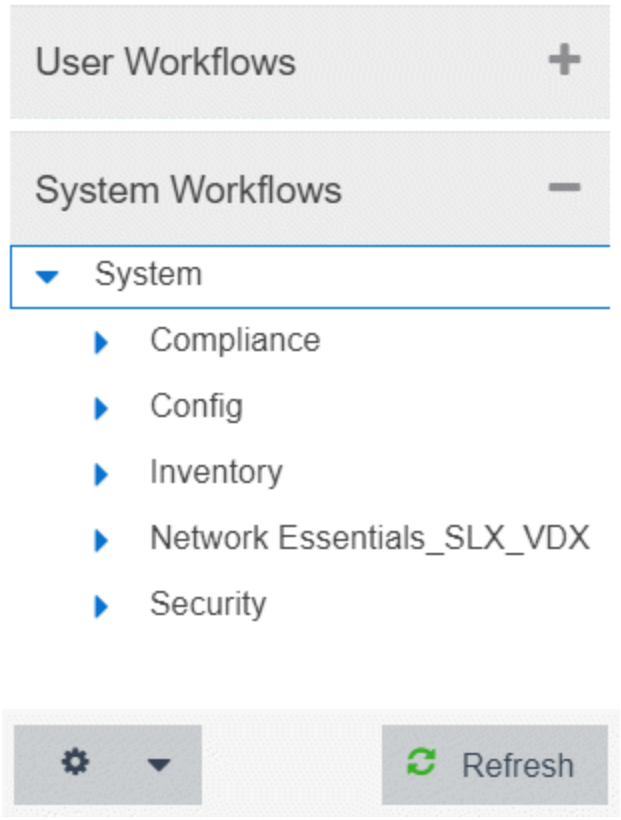
After you create a workflow, you can configure it as a task. You can then run the workflow task on specified devices or ports, either on a one-time or recurring basis via the **Saved Tasks** or **Scheduled Tasks tab**, respectively. Additionally, you can configure a workflow to automatically begin when an alarm occurs in ExtremeCloud IQ Site Engine on the **Alarm & Events** tab.

The **Workflows** tab contains four sections:

- Workflows List
- Palette
- Designer
- Details

Workflows List

The Workflows list displays user- and system-defined workflows in the User Workflows panel and System Workflows panel, respectively.



User Workflows

The user-defined workflows, contained in the User Workflows panel, are workflows you create manually. You can also select a system-defined workflow, right-click and select Save As, then enter a new name for a workflow to use a system-defined workflow as a template when creating a new workflow. Additionally, you can import a saved workflow into ExtremeCloud IQ Site Engine by right-clicking Workflows or a Workflow Group in the User Workflows left-panel and selecting **Import**.

NOTE: Not all configuration information is imported when importing a workflow.

System Workflows

The system-defined workflows, contained in the System Workflows panel, provide you with sample workflows designed to perform tasks in ExtremeCloud IQ Site Engine. These workflows and workflow groups cannot be deleted or modified, but can be copied by right-clicking the workflow in the Workflows list and selecting **Save As**. Use the copies you create as templates to create additional workflows.

Gear

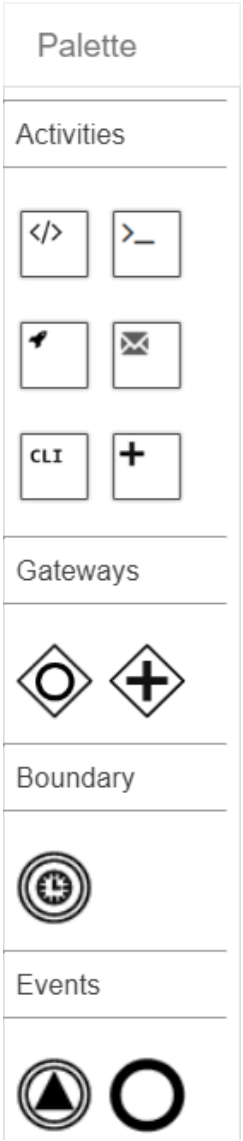
Select the **Gear** icon ( ) to open a menu from which you can create a new workflow or workflow group, rename or delete the selected workflow or workflow group, or import or export a workflow as an encrypted file.

Refresh

Select the **Refresh** icon to update the Workflows list to display any recent changes.

Palette

The Palette section contains the components available to create your workflow.



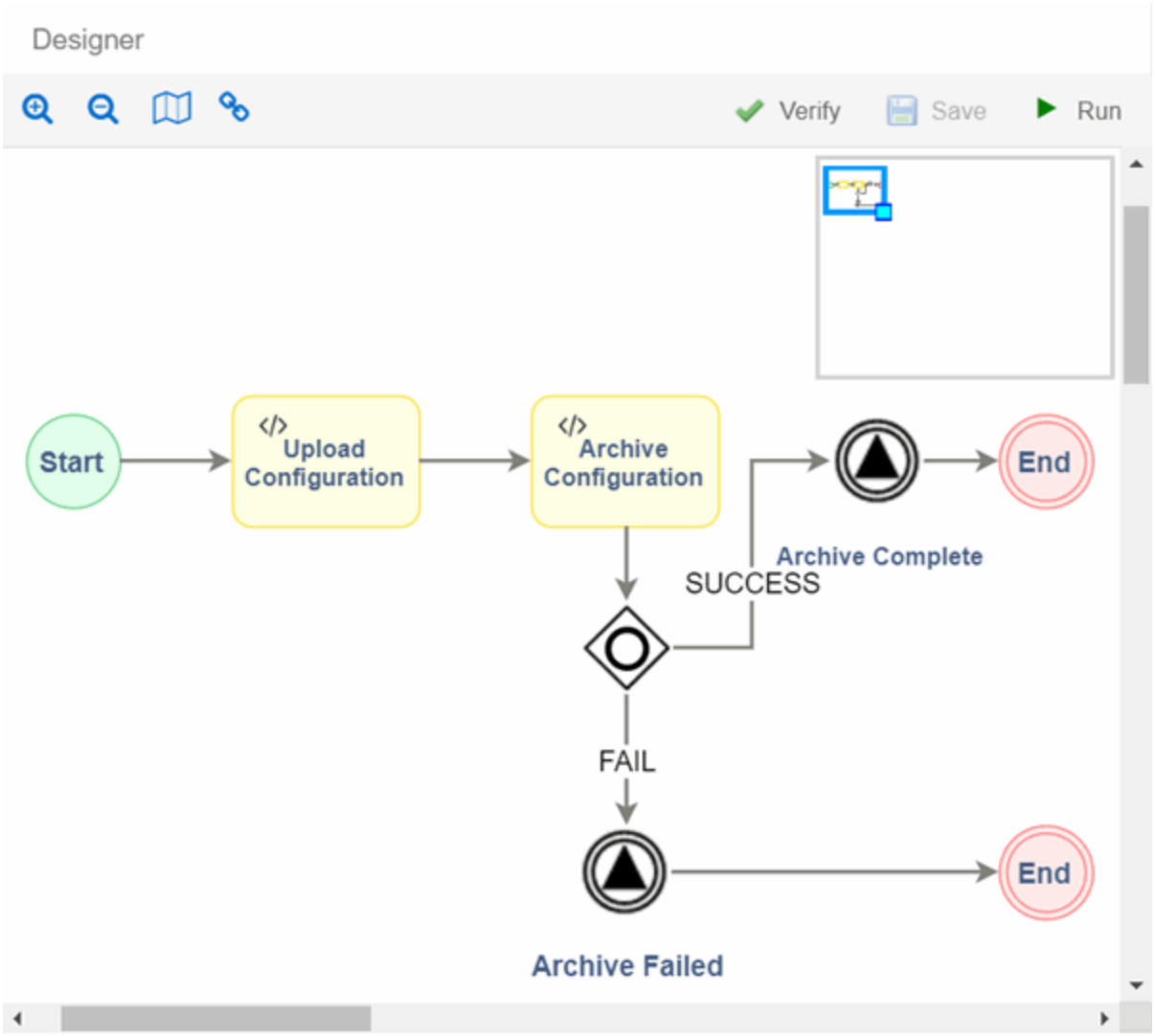
Drag and drop the icon from the Palette section into the Designer to add it to your workflow. Each icon represents a component you can use to create your workflow. Components are organized into subsections depending on their purpose.

Type	Icon	Description
Activities	 Script Activity	Use the **Script Activity** icon to add a script to your workflow. Drag the **Script Activity** icon into the Designer at the location in the workflow where you want the script to execute. Select the script and use the **Details** section to configure the script for the workflow.
	 Shell Activity	Use the **Shell Activity** icon to configure a shell command that is run locally on the server as part of your workflow. Drag the **Shell Activity** icon into the Designer at the location in the workflow where you want the shell command to execute. Select the shell command and use the **Details** section to configure the command for the workflow.
	 HTTP Activity	Use the **HTTP Activity** icon to receive or distribute data. Drag the **HTTP Activity** icon into the Designer at the location in the workflow where you want the HTTP activity to occur. Select the **HTTP Activity** and use the **Details** section to configure the call for the workflow.
	 Mail Activity	Use the **Mail Activity** icon to send an email if SMTP email options are configured. Drag the **Mail Activity** icon into the Designer at the location in the workflow where you want the email to occur. Select the **Mail Activity** and use the **Details** section to configure the email for that step of the workflow.
	 CLI Activity	Use the **CLI Activity** icon to run a CLI command remotely on a device as part of your workflow. ExtremeCloud IQ Site Engine uses the CLI credentials specified in the profile of each device to run the CLI activity. Drag the **CLI Activity** icon into the Designer at the location in the workflow where you want the command to occur. Select the **CLI Activity** and use the **Details** section to configure the command for the workflow.
	 Activity Group	Use the **Activity Group** icon to group multiple activities together, which allows you to use a common set of variables and receive a single output from the activities in the group. Drag the **Activity Group** icon into the Designer at the location in the workflow where you want to include the group. Drag the appropriate activities into the Designer and then drag them into the **Activity Group** box to add them to the group. The **Activity Group** box displays a dark blue border when activities are successfully added to the group.

Type	Icon	Description
Gateways	 Inclusive Parallel	Use the **Inclusive Parallel** gateway to create multiple paths for the workflow. The **Inclusive Parallel** gateway executes each path based on the output from the previous activity or activity group and then uses the conditions defined for each link. Using the **Inclusive Parallel** gateway, you can configure one path to execute if the previous activity completed successfully and another path to execute if the previous activity failed. You can also define conditions on each path, such that only the conditions that are **TRUE** are executed. For example, you can configure the gateway to execute a path based on the output of the previous activity (e.g. Firmware is less than version 10). Gateways execute all paths before moving on to the next activities.
	 Parallel	Use the **Parallel** gateway to create multiple paths that execute simultaneously. This gateway executes all paths, regardless of the output of the previous activity. Unlike paths following an **Inclusive Parallel** gateway, paths following a **Parallel** gateway do not contain conditions. Gateways execute all paths before moving on to the next activities.
Boundary	 Boundary Timer	If an activity does not complete in the time specified in the **Boundary Timer**, the path of the timer is executed. For example, if the timer is set to 20 seconds (and the workflow engine performs a check every 10 seconds), then the boundary timer path may be executed between 20-30 seconds after the activity start time. Add the **Boundary Timer** by dragging and dropping the icon from the Palette section to the Designer section onto an activity or by right-clicking an activity and selecting **Attach Boundary Timer**.
Events	 Signal	Add a **Signal** event to the workflow to generate an event when the workflow executes the path within the workflow. Use the **Signal Type** drop-down list on the **Inputs** tab to configure whether the event displays on the **Events** tab or if the event is sent as a **Syslog** message to the server you specify on the **Inputs** tab in the Details section.
	 End	Add an **End** event to indicate the completion of a path in the workflow.

Designer

The Designer section of the tab allows you to organize the Activities, Gateways, Boundaries, and Events you select for your workflows. Drag the icons to reorder your workflow paths.



Double-click the center of an Activity, link, or Event in the Designer and a cursor appears allowing you to change its **Name**.

After organizing your workflow elements in the appropriate order, hover over each Activity and Gateway to link or delete each using the appropriate icon.



Link — Select and drag the **Arrow** icon to link the item to the next item in the workflow. If the element's border around the next item is green, the link is valid. If the element's border is red, the

link is not valid and the link is not created. A pop-up window appears describing the reason the link is not valid.



Delete — Select the **Delete** icon to remove the item, along with the links to and from it, from the workflow.

The top of the section contains icons that allow you to manipulate and execute the workflow:

- **Zoom** — Zooms in and out of the workflow in the Designer.
- **Toggle Mini Map** ( ) — Opens a small map displaying an overview of the entire workflow.

  To move the area of focus for the Designer, move the cursor over the blue focus box in the mini map until the cursor changes to a **Move** icon ( ). Select the blue focus box and move it in the mini map to the area on which you want to focus the Designer.
  Additionally, you can shrink or expand the blue focus box to automatically zoom in or out of the workflow, respectively. Select the light-blue box in the bottom-right corner of the blue focus box and resize the blue focus box as needed.
- **Link Edit Mode** ( ) — Select the **Link Edit Mode** icon to add a new activity, gateway, or event on a link. To add a new activity, gateway, or event in Link Edit Mode, drag and drop it into the Designer, then drag it to the link on which you are adding it.
- **Verify** — Validates the workflow. Does not validate data in the **Inputs** tabs of the Activities included in your workflow.
- **Save** — Saves your changes to the selected workflow. If the workflow you are editing already has an assigned task, the new changes will be accepted and the related task is either updated (**Task Status** column remains blank) or the task will be marked as invalid (**Task Status** column contains **Invalid**).

  Examples of changes that can change the status to invalid are:

  - Adding an activity to the workflow.
  - Removing an activity from the workflow.
  - Adding new workflow input to the workflow.
  - Removing existing input from the workflow.
- **Run** — Opens the **Run Workflow** window, from which you can configure the workflow you are executing. This window allows you to configure Activity Inputs included in the workflow that are undefined or require a prompt to run. Select the **Previous** and **Next** buttons to navigate through the items you need to configure. Select the **Save Task** button to open a menu from which you can save the workflow as a task in the **Saved Tasks** tab. Select the **Run** button to execute the workflow:

- If your workflow includes the **devices** variable, you are prompted to select the devices on which the workflow is run. You have the option of saving the devices if you save the workflow as a task.
- If your workflow includes the **ports** variable, you are prompted to select the ports on which the workflow is run. You have the option of saving the ports if you save the workflow as a task.
- If your workflow includes an Activity for which the **Prompt User** checkbox is selected on the **Inputs** tab, you are prompted to specify variable values prior to running the workflow. The Activity is included as part of the workflow.
- You are prompted to indicate whether the workflow is run on a scheduled basis in the **Schedule Task** window. To configure the workflow to run automatically on a scheduled basis, select the **Enabled** checkbox and select when the workflow runs. Selecting **Enabled** displays additional fields where you define the frequency ExtremeCloud IQ Site Engine runs the workflow, and the date and time range between which ExtremeCloud IQ Site Engine runs the workflow. Use the Email section to configure ExtremeCloud IQ Site Engine to send an email when the workflow is run, if desired.

Details

Use the Details section to configure the behavior of each item in the workflow, or the workflow itself. Select an Activity, Link, Gateway, Boundary, or Event in the Designer section to display the details for that item in the Details section. Use the Details section to configure the behavior of each item in the workflow.

The Details section contains tabs that vary depending on what you select in the Designer section of the tab:

- General (Workflow)
- General (Element)
- Condition
- Variables
- Inputs
- Outputs
- Menus
- Network OS

General (Workflow)

The Workflow Details section includes a **General** tab that displays basic information about the workflow.

Name
The name of the workflow.

Version
: The version number of the workflow.

Created By
: The name of the admin who created the workflow.

Create Date and Time
: The date and time the workflow was created.

Last Modified By
: The name of the admin who last modified the workflow.

Modified Date and Time
: The date and time the workflow was last modified.

Description
: Allows you to enter a description of the workflow.

General (Element)

The **General** tab displays the basic information about the element you select in the Designer section of the tab.

Name
: Name of the selected item. Double-click the center of an Activity, link, or Event in the Designer and a cursor appears allowing you to change its **Name**.

ID
: A system-assigned ID number for the selected item. This can not be edited.

Custom ID
: A user-defined alphanumeric ID for the selected item.

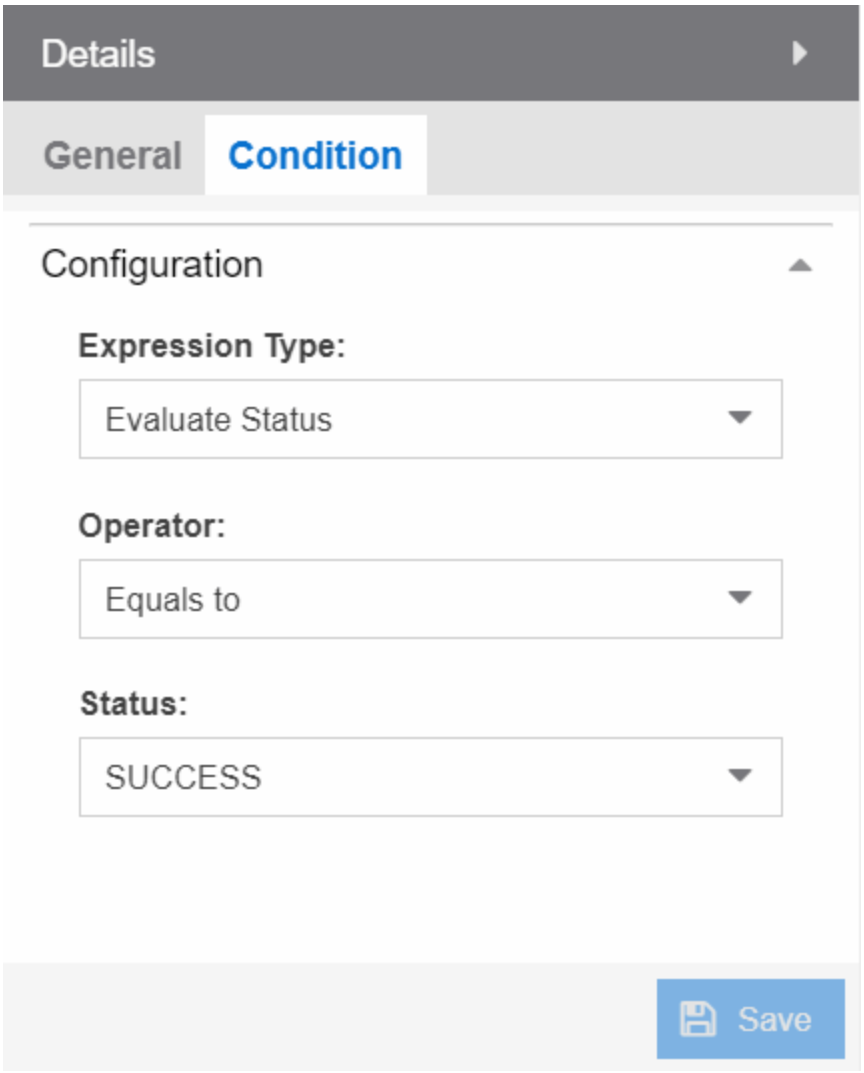
> **NOTE:** The '**-**' and '**_**' characters are also valid.

Description
: A description of the selected item.

Save
: Select **Save** to save your changes to the workflow.

Condition

The **Condition** tab displays when selecting a link following an Inclusive Parallel gateway.



This tab allows you to select the conditions under which the workflow executes the path following the link. The link uses the output from the previous activity to determine whether the workflow continues executing the path.

Save
: Select **Save** to save your changes to the workflow.

Expression Type
: The type of output used to determine the condition under which the workflow continues along the following path.
Valid options are:

- **Always True** — The workflow continues down the path following the link, regardless of the output of the previous activity.
- **Evaluate Status** — The workflow continues down the path following the link based on the **Status** of the previous activity's output (e.g. **SUCCESS**, **FAILED**, and **TIMEDOUT**).

- **Evaluate Variables** — The workflow continues down the path of the link based on a comparative value of the variable's output (e.g. Firmware version is less than 8.2).
- **Custom** — The workflow continues down the path if the output matches the value in the **Expression** field.

Evaluate Status

Operator
: **Operator** indicates the comparison between the output status of the previous activity and the **Status** you select (for example, **Equals to**).

Status
: **Status** indicates the previous activity's output. ExtremeCloud IQ Site Engine compares this value using the relationship defined as the **Operator** against the output status of the previous activity to determine if the workflow continues the path of the link.

Evaluate Variables

Variable
: **Variable** indicates the output variable ExtremeCloud IQ Site Engine uses to compare against the **Value** using the relationship defined as the **Operator** to determine if the workflow continues after the link.

Operator
: **Operator** indicates the comparison between the **Variable** and the **Value** you enter (for example, **Equals to** or **Not Equals to**).

NOTE: When **Operator** is **In**, ExtremeCloud IQ Site Engine compares a variable against the values in a comma-separated list. If the variable contains a comma, the comparison fails. For example, if the variable is "abc,123" and the value is "abc,123", ExtremeCloud IQ Site Engine observes the variable as "abc,123" (one string), while ExtremeCloud IQ Site Engine observes the value as "abc" and "123" (two strings). The comparison fails because the string "abc,123" is not contained in either the "abc" or the "123" string.

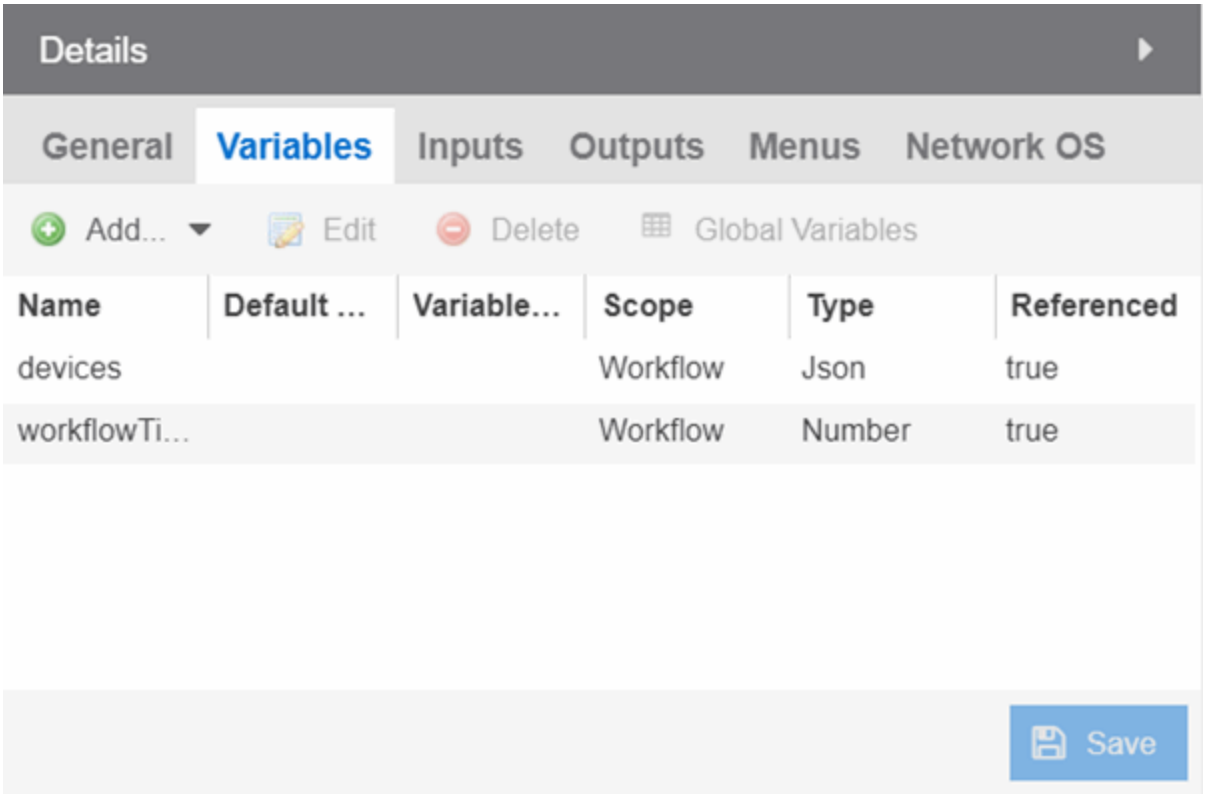
Value
: **Value** indicates the value against which ExtremeCloud IQ Site Engine compares the **Variable** using the relationship defined as the **Operator** to determine if the workflow continues after the link.

Expression

Expression
: **Expression** indicates a custom expression ExtremeCloud IQ Site Engine uses to determine if the workflow continues after the link.

Variables

The **Variables** tab displays when selecting an activity or when nothing is selected for the entire workflow.



This tab allows you to add, edit, or delete variables used in your workflow. Variables you create serve as a placeholder for a specific value. After you create a variable, ExtremeCloud IQ Site Engine automatically substitutes the **Value** you define in the workflow or activity when the variable is selected. You can also configure the workflow to prompt you for a **Value** when the workflow is running.

ExtremeCloud IQ Site Engine comes with two system-defined variables, devices and ports.

The devices variable substitutes the device name in place of the variable, while the ports variable substitutes the port number in place of the variable. Devices and ports ExtremeCloud IQ Site Engine substitutes are specified when you run the workflow.

NOTE: If you delete the devices or ports variables, you need to add them back to the workflow. Use the **Add** > **Pre-defined** drop-down list in the Workflow Variables tab to add devices or ports variables back to a workflow.

Name

Displays the name of the variable.

Default Value
: Displays the value ExtremeCloud IQ Site Engine uses, if no other value has been specified, when substituting the variable. Enter a value associated with the variable type you define. This column is optional.

Variable Reference
: Displays the variable on which the variable you are creating is dependent. For example, if you are creating a variable named **Variable B**, which uses the value of **Variable A** as its input, **Variable A** displays in this field. This field is only available when **Scope** is **Activity**.

Scope
: Displays the extent to which the variable is used. Valid options are **Workflow** or **Activity**, depending on whether the variable is used throughout the entire workflow, or only for the currently selected activity, respectively.

Type
: Defines the type of information the variable is substituting. Valid options are:

  - **String** — Select to substitute a string. Additionally, select a **Type** of **String** when substituting a custom variable created on the **Custom Variables** tab with a **Type** of **IP**, **MAC Address**, **Subnet**.
  - **Boolean** — Select to substitute the variable with a boolean operator.
  - **Number** — Select to substitute the variable with a number.
  - **JSON** — Select to substitute the variable with a JSON file.

Referenced
: A value of **True** in this field indicates that the variable is used as the **Variable Reference** of another variable, or if the variable is used as the Input for an activity.

Add
: Select the **Add** icon to add a new line to the table from which you can create a new variable.

Edit
: Select the **Edit** icon to edit an existing variable.

Delete
: Select the **Delete** icon to remove a variable from the list.

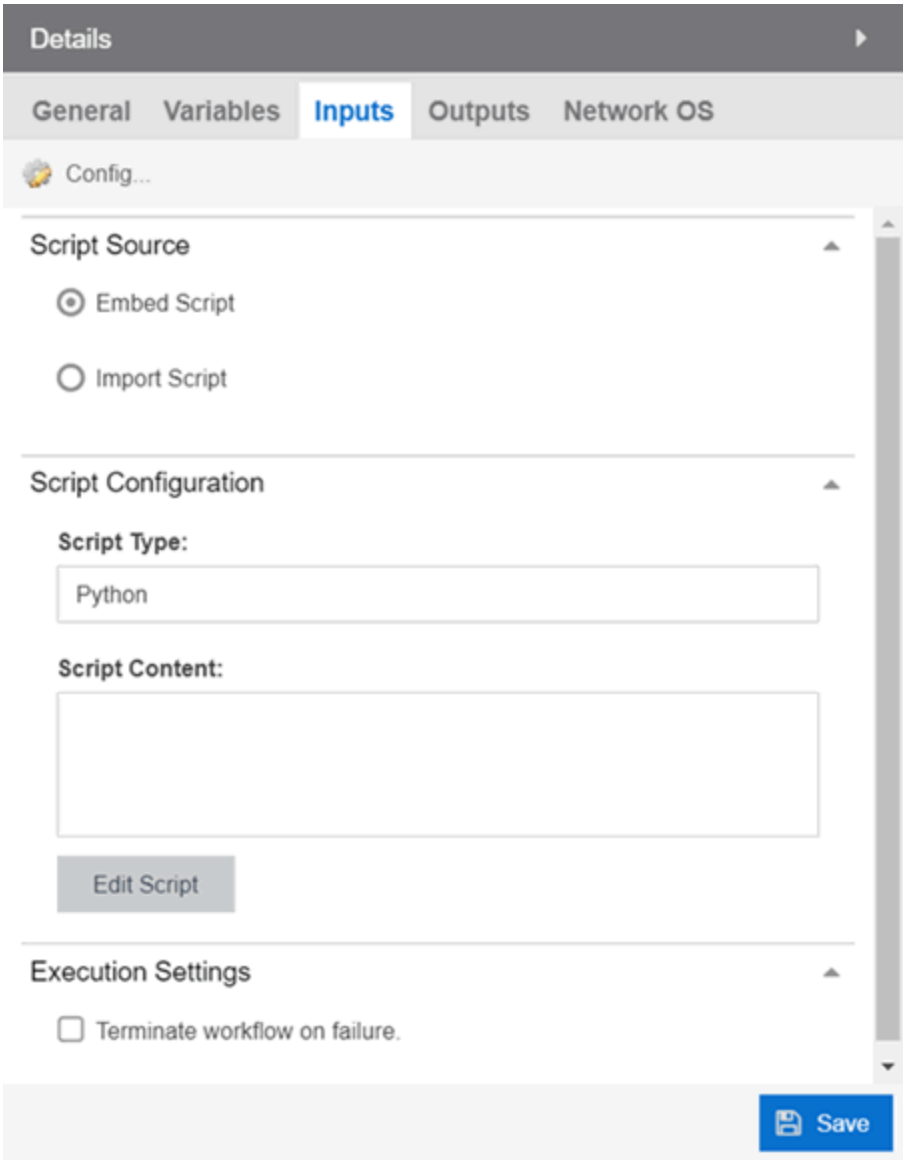
NOTE: Variables for which **Referenced** is **True** cannot be deleted.

Custom Variables
: Select the button to open a new window, where you can select custom variables to include in your activity. Custom variables include system-defined variables and those user-defined variables you create on the Site > **Custom Variables** tab.

Save
: Select **Save** to save your changes to the workflow.

Inputs

The **Inputs** tab displays inputs for the selected activity or inputs for the workflow when you select an activity or when nothing is selected for the entire workflow, respectively.



The fields on this tab change depending on the type of activity you select:

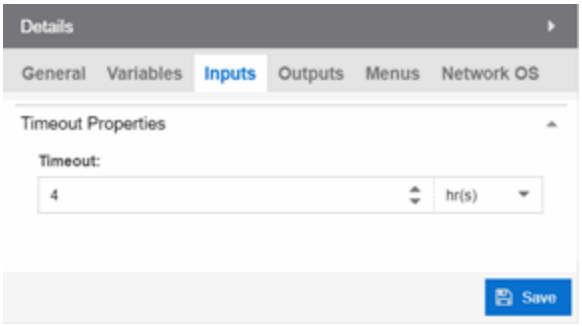
- Workflow
- Script
- Shell
- HTTP

- Mail
- CLI

Enter the appropriate input configuration for your workflow.

Workflow

Selecting the **Inputs** tab when nothing is selected in the Designer section allows you to configure inputs for the entire workflow.



Timeout

Enter the amount of time the workflow will run before it times out. Because ExtremeCloud IQ Site Engine performs a check every 10 seconds to ensure all workflows are running within the specified duration, workflows may actually run up to 10 seconds longer than the timeout time you enter. For example, if you enter a timeout of 5 minutes for a workflow to execute, the workflow will cease execution within 10 seconds of the five-minute timeout designation.

Script

Selecting the **Inputs** tab when a script is selected in the Designer section allows you to configure inputs specific to that script.



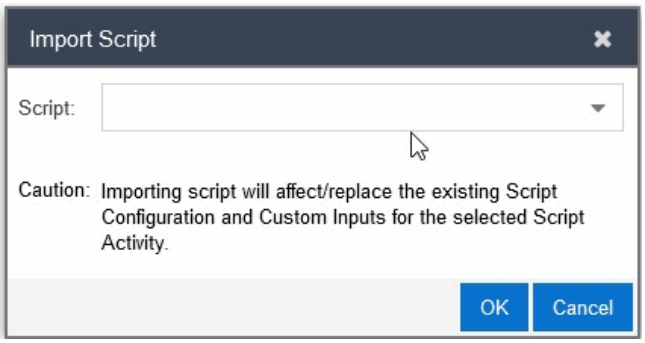
Manage Inputs

Select to open the **Manage Inputs** window to display a list of the variables the activity uses.

Script Configuration

Select a button to indicate the source of the script:

- **Import Script** — Select this option to import a script saved on the **Scripts** tab.



NOTE: If you make changes to the script content in the activity, the changes are not saved to the script on the **Scripts** tab. If you make changes to the script on the Scripts tab, use the Import button to use the updated script in the Script Activity.

- **Clear Script** — Select this option to clear the contents of the script in the **Script Content** field.

Script Origin
: The name of the script most recently imported (for reference).

Script Type
: The language in which the script is written.

Script Content
: The python scripts, CLI commands, control structures, and data manipulation being executed.

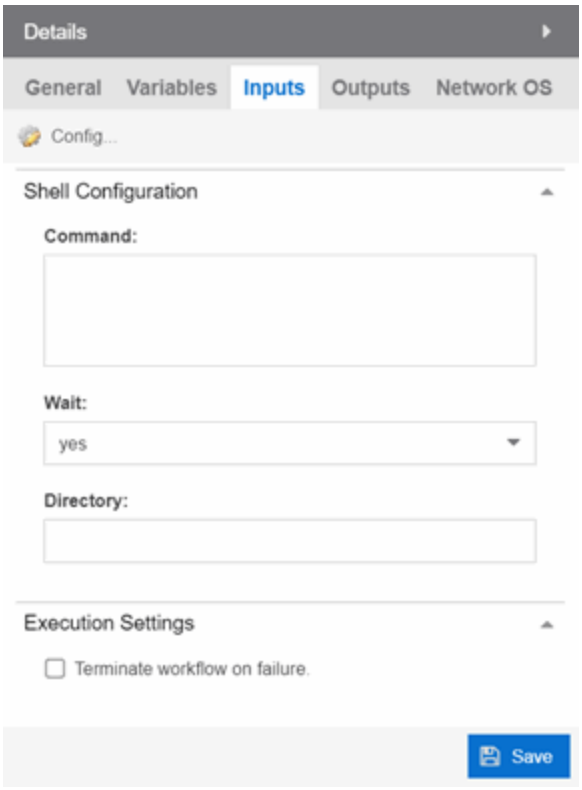
Edit Script
: Select the **Edit Button** to change the **Script Content**.

Execution Settings
: Select the **Terminate workflow on failure** check box to stop the workflow if the workflow does not complete the activity successfully.

Save
: Select **Save** to save your changes to the workflow.

Shell

Selecting the Inputs tab when a shell activity is selected in the Designer section allows you to configure inputs specific to that shell activity.



Manage Inputs

Select to open the **Manage Inputs** window to display a list of the variables the activity uses.

Command

Shell activity scripts must include a command, followed by one or more options or variables. Shell commands may also include subcommands, which would follow the options or variables in the script construction.

The Command field requires the absolute path to the script of the shell activity. Enter the shell commands to run this activity locally on the server as part of your workflow.

Following are examples of shell commands with options/variables and subcommands:

Example 1: cat command using absolute path:

```
/bin/sh -c "sudo /bin/cat /var/log/syslog | egrep -e "CLILOG|CLIAUDIT" |
sed 's/</\n/g'"
```

Example 2: cat command from the system PATH for the user running ExtremeCloud IQ Site Engine (for example, `root`):

```
/bin/sh -c "export PATH; sudo cat /var/log/syslog | egrep -e
"CLILOG|CLIAUDIT" | sed 's/</\n/g'"
```

Example 3: cat command that uses workflow variable called `CAT_GREP_VAR`:

```
/bin/sh -c "export PATH; sudo cat /var/log/syslog | egrep -e "${CAT_GREP_
```

```
VAR}" | sed 's/</\n/g'"
```

Example 4: Execute a custom command called 'foo' stored in an ExtremeCloud IQ Site Engine directory. /home/foo, which includes a single option stored in a variable. Set the "Working Directory" to `/home/foo`, so the variable starts in the correct directory to find foo: `/bin/sh -c "export PATH; ./foo ${CUSTOM_VAR}"`

NOTE: If a command includes subcommands, spaces, or uses quotes or special OS characters (for example, |), use quotes around the options/variables and subcommands. If the command uses spaces, use quotes around the entire command construction.

The `timeout` and `outputMaxSize` variables limit the processing time and output used for the shell activity.

The `timeout` variable is the maximum time (displayed in seconds) that the shell activity will wait for the command to complete execution. The default timeout is 180.

The `outputMaxSize` variable is the maximum number of bytes allowed for the output produced by the shell activity command. The default is 1MB.

NOTE: If a shell activity script does not include the `timeout` or `outputMaxSize` variables, the following default values will be used:
`timeout`: 180
`outputMaxSize`: 1000000

Wait
: Select **yes** or **no** from the drop-down list to indicate whether or not the workflow waits for the shell command to complete before continuing.

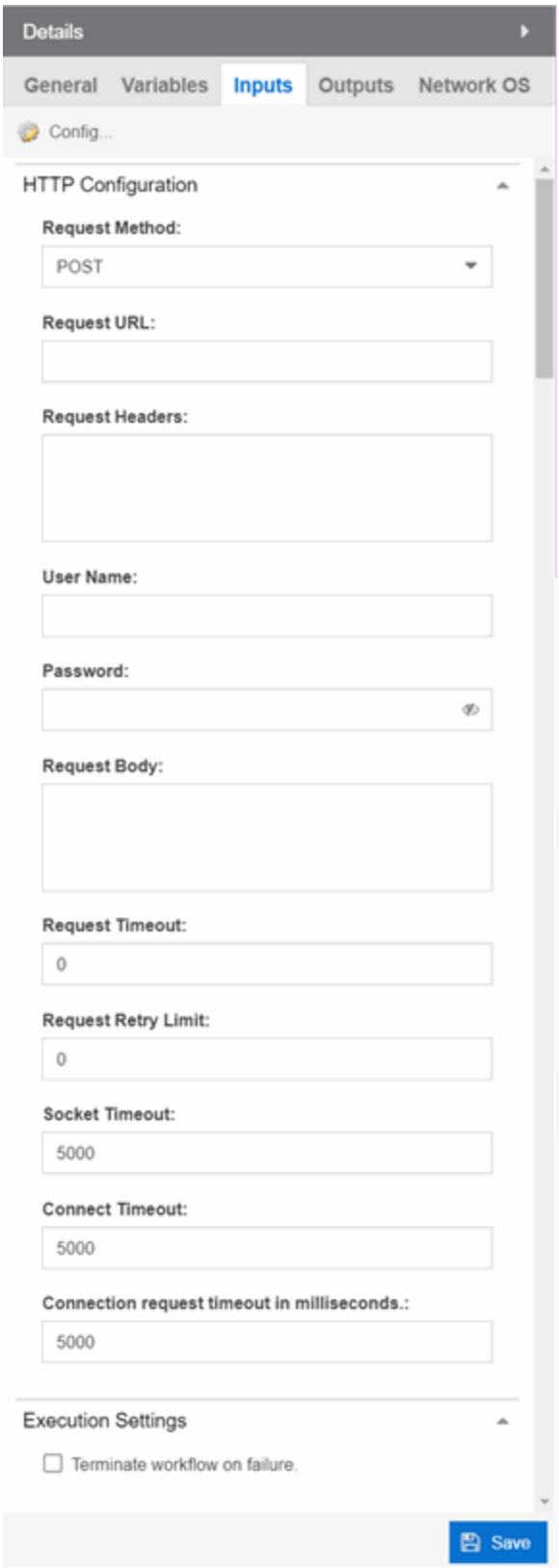
Directory
: The location of the shell script on the server.

Terminate workflow on failure
: Select the checkbox to stop the workflow if the workflow does not complete the activity successfully.

Save
: Select **Save** to save your changes to the workflow.

HTTP

Selecting the **Inputs** tab when an HTTP activity is selected in the Designer section allows you to configure the inputs specific to that HTTP activity.


Details
General
Variables
Inputs
Outputs
Network OS
Config...
HTTP Configuration
Request Method:
POST
Request URL:
Request Headers:
User Name:
Password:
Request Body:
Request Timeout:
0
Request Retry Limit:
0
Socket Timeout:
5000
Connect Timeout:
5000
Connection request timeout in milliseconds.:
5000
Execution Settings
Terminate workflow on failure.
Save

Manage Inputs
: Select to open the **Manage Inputs** window to display a list of the variables the activity uses.

Request Method
: The action the HTTP activity is performing:

- **GET** — Requests resource information from a specified URI.
- **POST** — Submits resource information to a specified URI.
- **PUT** — Overwrites resource information at the specified URI with the information contained in **Request Body**.
- **DELETE** — Deletes the resource at the specified URI.

Request URL
: The URL at which the resource is located.

Request Header
: The HTTP header included with the request.

NOTE: Use the **User Name** and **Password** fields to include credential information without exposing it in the header.

User Name
: Your user name to access the resource at the **Request URL**.

Password
: The password required to access the resource at the **Request URL**.

Request Body
: The HTTP message body data included with the request.

Request Timeout
: The amount of time (in milliseconds) before the HTTP request times out.

Request Retry Limit
: The number of times ExtremeCloud IQ Site Engine attempts the HTTP request before the request is canceled.

Socket Timeout
: The amount of time (in milliseconds) ExtremeCloud IQ Site Engine waits for a packet before the HTTP request times out. ExtremeCloud IQ Site Engine performs a check every 10 seconds, so if the timeout is set to 10 seconds for an activity, then the boundary timer path may be executed between 10-20 seconds after the activity start time.

Connect Timeout
: The amount of time (in milliseconds) ExtremeCloud IQ Site Engine waits until a connection is established. ExtremeCloud IQ Site Engine performs a check every 10 seconds, so if the timeout is set to 10 seconds for an activity, then the boundary timer path may be executed between 10-20 seconds after the activity start time.

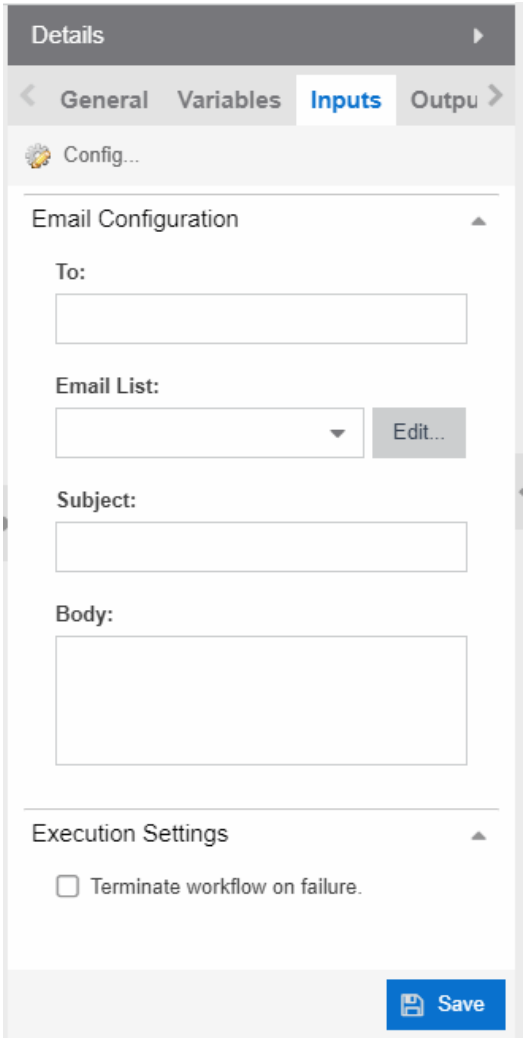
Connection request timeout in milliseconds
: The amount of time (in milliseconds) ExtremeCloud IQ Site Engine waits when requesting a connection from the connection manager. ExtremeCloud IQ Site Engine performs a check every 10 seconds, so if the timeout is set to 10 seconds for an activity, then the boundary timer path may be executed between 10-20 seconds after the activity start time.

Terminate workflow on failure
: Select the checkbox to stop the workflow if the workflow does not complete the activity successfully.

Save
: Select **Save** to save your changes to the workflow.

Mail

Selecting the **Inputs** tab when a Mail activity is selected in the Designer section allows you to configure the inputs specific to that Mail activity.



Manage Inputs
: Select to open the **Manage Inputs** window to display a list of the variables the activity uses.

To:
: Enter the email address or addresses to which ExtremeCloud IQ Site Engine sends an email when running the workflow. This field also supports the use of a variable in place of an email address. ExtremeCloud IQ Site Engine automatically sends the email when the progress of the workflow reaches the activity.

  Use a semicolon to separate multiple email addresses. If you enter an email address in the To field and also select an email list from the Email List drop-down list, the email is sent to both the address and the address list. If you do not enter an email address in the To field or select an email address list from the Email List field, no emails are sent.

Email List:
: Select the email address list from the drop-down list that includes the address or addresses to which ExtremeCloud IQ Site Engine sends an email when running the workflow. ExtremeCloud IQ Site Engine automatically sends the email when the progress of the workflow reaches the activity.

  If you enter an email address in the To field and also select an email list from the Email List drop-down list, the email is sent to both the address and the address list. If you do not enter an email address in the To field or select an email address list from the Email List field, no emails are sent. Select the **Edit** button to open the **Edit Email Lists** window, from which you can configure your available email lists.

Subject:
: The subject line of the email ExtremeCloud IQ Site Engine sends for the activity when running the workflow.

Body:
: The body of the email ExtremeCloud IQ Site Engine sends for the activity when running the workflow.

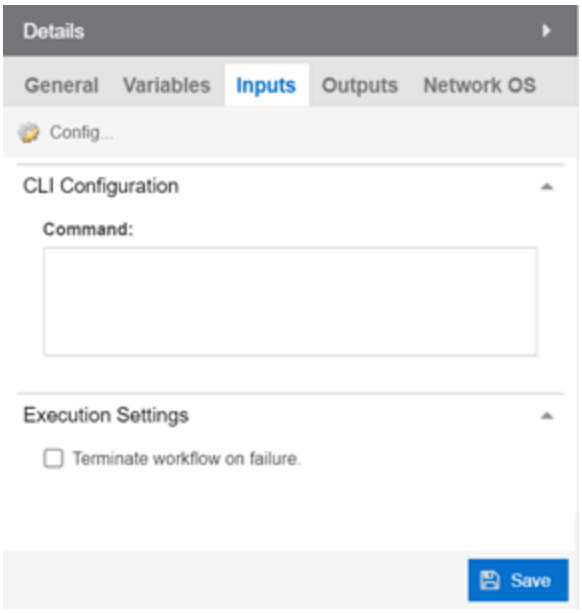
Terminate workflow on failure
: Select the checkbox to stop the workflow if the workflow does not complete the activity successfully.

Save
: Select **Save** to save your changes to the workflow.

CLI

Selecting the **Inputs** tab when a CLI activity is selected in the Designer section allows you to configure the inputs specific to that CLI activity. These

NOTE: Workflow CLI activities are run on devices using the specified in the ExtremeCloud IQ Site Engine Administration Profile.



Manage Inputs
: Select to open the **Manage Inputs** window to display and edit a list of the variables the activity uses.

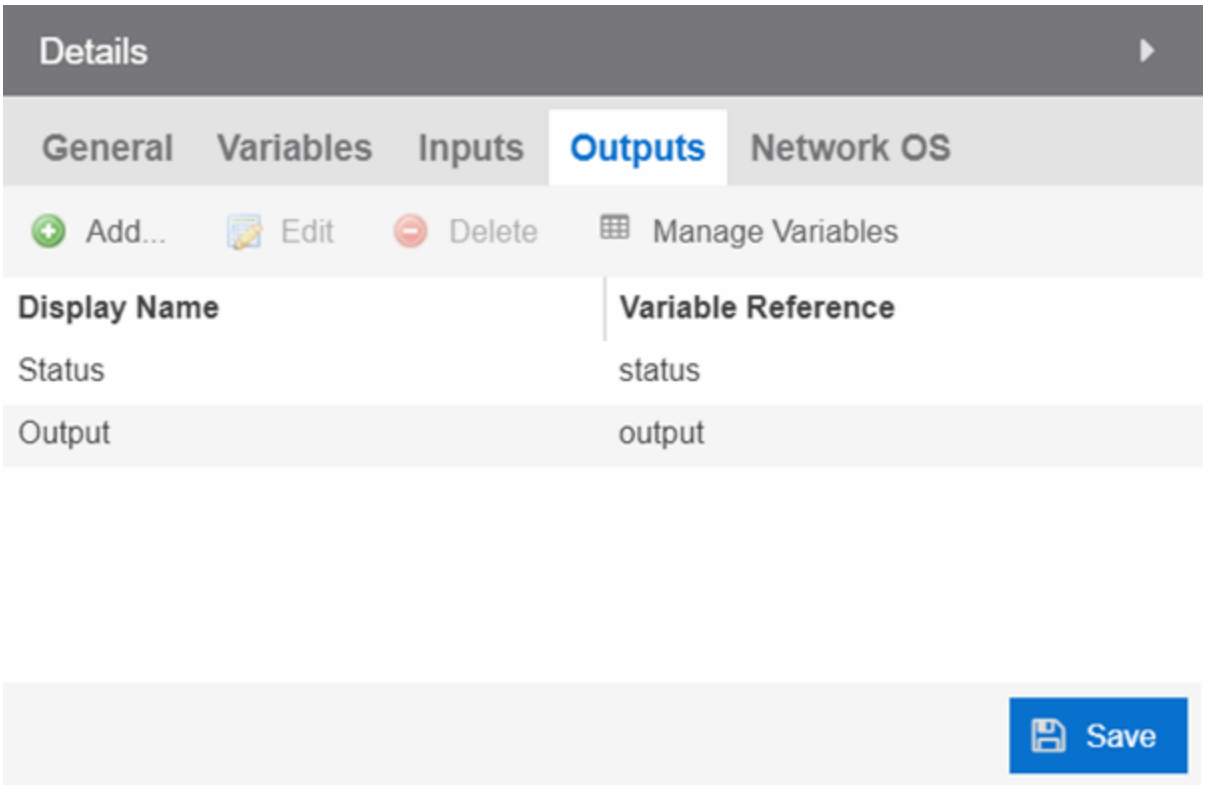
Command
: The CLI command or commands run as part of your workflow.

Terminate workflow on failure
: Select the checkbox to stop the workflow if the workflow does not complete the activity successfully.

Save
: Select **Save** to save your changes to the workflow.

Outputs

The **Outputs** tab displays when you select an activity or when nothing is selected for the entire workflow.



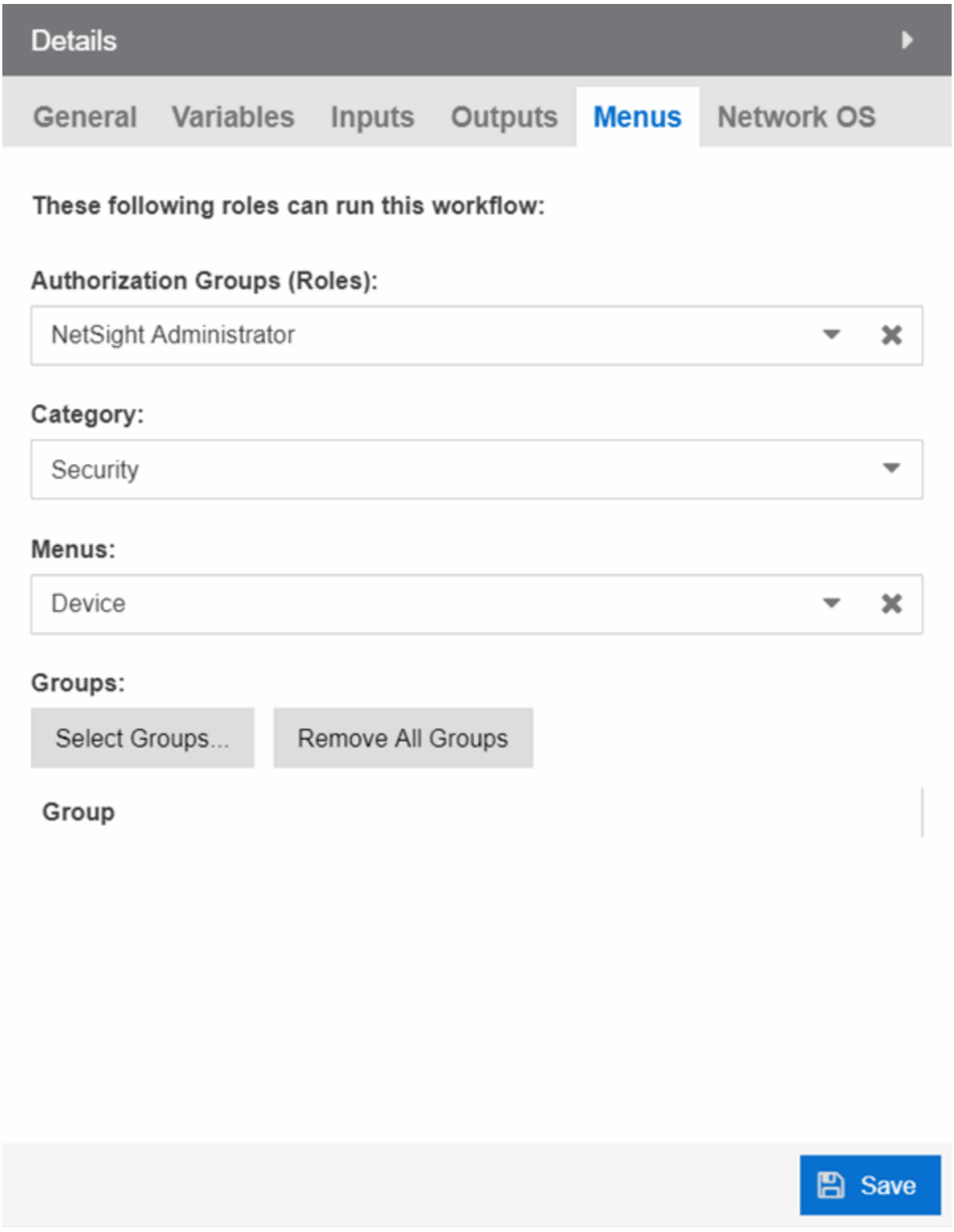
The **Outputs** tab allows you to specify the output variable you use to determine the result of the activity. You can then use this variable as the input variable for the next activity in the workflow, or as the final output in the workflow.

NOTE: Output variables configured via **Output** tab are only applicable to the Shell and HTTP activities.

Select **Save** to save your changes to the workflow.

Menus

The **Menus** tab displays for the workflow level (for example, when nothing is selected in the Designer section). This tab allows you to select the users who can run the workflow by specifying the Authorization Group, the workflow's category, the menus in which you can access the workflow, and the device groups to which the workflow applies.


Details
General
Variables
Inputs
Outputs
Menus
Network OS
These following roles can run this workflow:
Authorization Groups (Roles):
NetSight Administrator
Category:
Security
Menus:
Device
Groups:
Select Groups...
Remove All Groups
Group
Save

Authorization Group (Roles)
: Select the Authorization Groups with the ability to execute the workflow from the drop-down list.

Category
: Select the **Category** group from the drop-down list, which defines the Tasks submenu in which the workflow is grouped throughout ExtremeCloud IQ Site Engine. The locations in ExtremeCloud IQ Site Engine in which the workflow is available is determined based on what you select in the **Menus** drop-down list.

Menus
: Select the locations in ExtremeCloud IQ Site Engine in which you want the workflow to display, depending on its purpose.

  The following are the locations in ExtremeCloud IQ Site Engine where workflows are available:

  - **Access Control Events** — Includes the workflow in the list of **Actions** drop-down list available on the **Access Control** > **Configuration** > **Notifications** tab.
  - **Alarm** — Includes the workflow in the list of task actions for custom criteria alarms. Selecting this location in the **Menus** drop-down list makes it available for a workflow to run from it, and it displays in the **Source** column on the **Workflow Results** table on the **Workflow Dashboard**.
  - **Device** — Includes the workflow in the list of tasks available on the **Network** > **Devices** tab. Selecting this location in the **Menus** drop-down list makes it available for a workflow to run from it, and it displays in the **Source** column on the **Workflow Results** table on the **Workflow Dashboard**.
  - **Multi-Device** — Includes the workflow in the list of tasks available when right-clicking a User Device Group on the **Network** > **Devices** tab.
  - **None** — The workflow is only available via the **Workflows** tab.
  - **Port** — Includes the workflow in the list of tasks on the **Port Tree** tab. Selecting this location in the **Menus** drop-down list makes it available for a workflow to run from it, and it displays in the **Source** column on the **Workflow Results** table on the **Workflow Dashboard**.
  - **Security** — Includes the workflow in the list of tasks available on the **Security** tab. Selecting this location in the **Menus** drop-down list makes it available for a workflow to run from it, and it displays in the **Source** column on the **Workflow Results** table on the **Workflow Dashboard**.

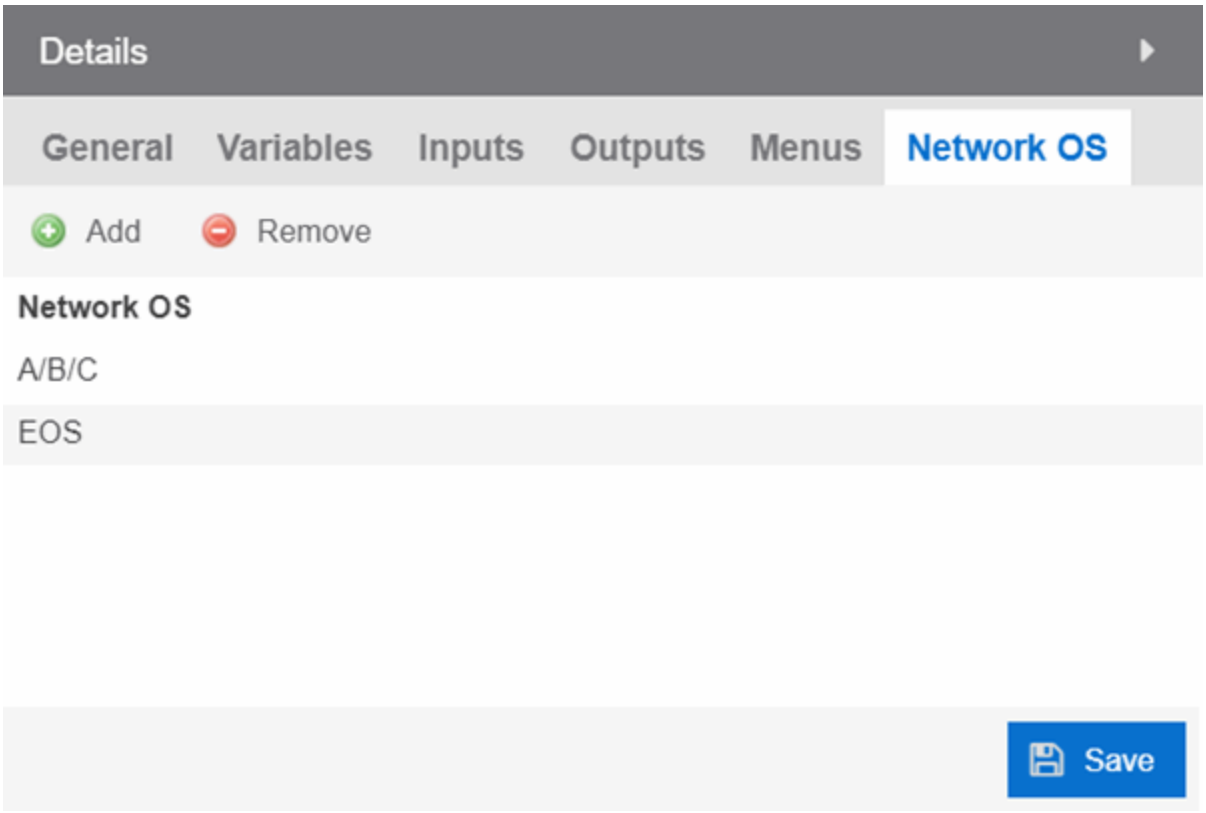
Groups
: Select the button to open the **Select Device Groups** window, from which you can select the device groups for which the workflow displays in the Tasks submenu.

Select Save to save your changes to the workflow.

Network OS

The **Network OS** tab displays when you select an activity or when nothing is selected for the entire workflow. This tab allows you to limit the workflow to run only on those devices with an operating system to which the workflow applies. The Network OS assigned to a device is included on the **Vendor Profile** tab.

NOTE: Select **Unknown** when creating scripts or workflows that include devices before their Network OS has been determined (for example, onboarding new devices).



Running a workflow with no Network OS listed on the **Network OS** tab, the workflow runs on all selected devices, regardless of the **Network OS** configured for the device.

Running a workflow on a device whose Network OS is not listed on the **Network OS** tab for the workflow or activity, the Operations panel displays the message "No compatible devices found".

Select **Save** to save your changes to the workflow.

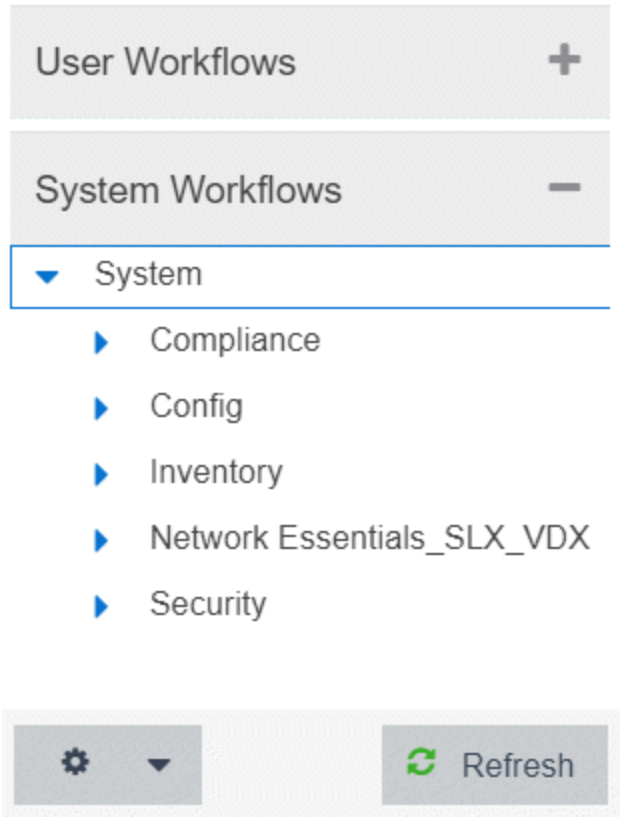
System Workflows

The **Workflows** tab contains system-defined workflows as well as workflows you create. The System Workflows are not executable and must be copied before use. To copy the workflow:

1. Select the workflow and right-click
2. Select **Save As**
3. Give the workflow a name
4. Select the **User Workflows** group from **Group**
5. Select **OK**

System-defined workflows are saved in the System Workflows left-panel.

NOTE: The version number of each workflow is indicated on the **General (Workflow)** tab in the Details section of the window. A change to this number indicates workflows are updated from the previous release.



Workflows are available in the following functional areas:

- Compliance
- Config
- Inventory
    - Backup
    - Restart
    - Restore
    - Upgrade
- Network Essentials SLX VDX
    - ACL Management
    - Edge Ports Configuration
    - Utility Actions
    - Validation and Troubleshooting
- Security

Compliance

Workflows in the Compliance folder configure devices to perform tasks related to ExtremeCompliance functionality.

Add Login Banner

Adds a login message banner on a device. This is an example workflow you can configure to run if an Alarm occurs after an ExtremeCompliance audit runs. The workflow relies on the message sent by the alarm to display. This workflow supports Fabric Engine, ERS, WiNG, MLX, ICX, SLX and VDX devices. After the workflow completes, it sends an email to a user you select.

Enable HTTPS

Enables an HTTPS connection to access the web view of a device. This is an example workflow you can configure to run if an Alarms occurs after an ExtremeCompliance audit runs. The workflow relies on the message sent by the alarm to access the web view of the device. The workflow supports Fabric Engine, ERS, MLX, and ICX devices. After the workflow completes, it sends an email to the user you select.

Enable SSH

Enables an SSH login for a device. This is an example workflow you can configure to run if an Alarms occurs after an ExtremeCompliance audit runs. The workflow relies on the message sent by the alarm to log into the device. The workflow supports Fabric Engine, Summit, and 200 Series devices. After the workflow completes, ExtremeCloud IQ Site Engine triggers an event.

Config

Workflows in the **Config** folder configure your devices so they are compatible with specific functionality in ExtremeCloud IQ Site Engine.

Basic Support

The workflows contained in the Basic Support folder allow you to use basic ExtremeCloud IQ Site Engine functionality with certain device types.

Disable DvR Leaf boot config mode

Disables the DvR (Direct Virtual Routing) leaf boot config flag for Fabric Engine devices.

NOTE: This forces the device to reset.

Enable DvR Leaf boot config mode

Enables the DvR (Distributed Virtual Routing) leaf boot config flag for Fabric Engine devices.

NOTE: This forces the device to reset.

Enable SPBM boot config mode

Enables the SPBM boot config flag for Fabric Engine devices.

NOTE: This forces the device to reset.

ICX-SLX Config Basic Support

Configures basic monitoring and topology support for ICX and SLX devices. Use this workflow to configure an SNMP profile for an ICX or SLX device with no default credentials. In addition, it configures LLDP required to resolve links in topology maps. After the workflow completes, ExtremeCloud IQ Site Engine triggers an event.

MLX Config Basic Support

Configures basic monitoring and topology support for MLX devices. Use this workflow to configure an SNMP profile for an MLX device with no default credentials. In addition, it configures LLDP required to resolve links in topology maps. It also generates the client SSH keys on MLX devices, so the devices can use SCP to communicate with the server to upload a configuration file. After the workflow completes, ExtremeCloud IQ Site Engine triggers an event.

VDX Config Basic Support

Configures basic monitoring and topology support for VDX devices. Use this workflow to configure an SNMP profile for a VDX device with no default credentials. In addition, it configures LLDP required to resolve links in topology maps. It also configures the 3-tuple ifName needed for MIB data. After the workflow completes, ExtremeCloud IQ Site Engine triggers an event.

EXOS-VPEX

The workflows in EXOS-VPEX folder configure devices so you can onboard or remove VPEX Bridge Port Extenders on Switch Engine devices.

Onboard VPEX Bridge Port Extender on EXOS
Configures VPEX Bridge Port Extenders to a single CB or dual CBs.

Remove VPEX Bridge Port Extender fromEXOS
Removes slot assignments from VPEX Bridge Port Extenders on single CB and dual CB topologies.

LAG-MLAG

The workflows in the LAG-MLAG folder configure devices so you can configure LAGs and MLAGs on the devices.

Configure ISC and MLAG Peers on EXOS
Configures MLAG between Fabric Engine vIST cluster devices and ExtremeXOS/Switch Engine devices.

MLAG port on CBs and LAG on remoteEXOS
Configures MLAG between Fabric Engine vIST cluster devices and ExtremeXOS/Switch Engine devices.

MLAG with VOSS Cluster
Configures MLAG between Fabric Engine vIST cluster devices and ExtremeXOS/Switch Engine devices.

VOSS Fabric NNI LAG
Configures devices to support creation and deletion of LAG and enabling Network to Network Interfaces (NNI) in an SPB network.

VOSS Virtual IST
Configures devices to support creation and deletion of Virtual IST in an SPB network.

Inventory

Workflows in the Inventory folder perform inventory-related functions on supported devices, including creating a backup of the device configuration, restarting the device, restoring a saved device configuration backup, and upgrading the firmware on a device.

Backup

Workflows in the Backup folder initiate a backup of a device's configuration.

ICX-MLX Backup Configuration
Creates a backup of the configuration for ICX and MLX devices.

VDX Backup Configuration
Creates a backup of the configuration for VDX devices and VCS fabrics.

Restart

Workflows in the Restart folder restart devices of a specific device type.

ICX-SLX-MLX Restart Device
Restarts ICX, SLX, and MLX devices. When the device is restarted, ExtremeCloud IQ Site Engine generates a **Device Restart** event.

VDX Restart Device
Restarts VDX devices. When the device is restarted, ExtremeCloud IQ Site Engine generates a **Device Restart** event.

Restore

Workflows in the Restore folder restore a saved configuration to a device.

ICX-MLX Backup Configuration
Restores a saved configuration on ICX and MLX devices.

VDX Backup Configuration
Restores a saved configuration on VDX devices and VCS fabrics.

Upgrade

Workflows in the Upgrade folder upgrade the firmware on a device.

ICX Upgrade Firmware
Upgrades the firmware on ICX devices.

MLX Upgrade Firmware
Upgrades the firmware on MLX devices.

VDX Upgrade Firmware
Upgrades the firmware on VDX devices.

Network Essentials SLX VDX

Workflows in the Network Essentials SLX VDX folder perform functions that allow ExtremeCloud IQ Site Engine to configure SLX and VDX devices.

ACL Management

Add IPv4 ACL Rule
Adds a Layer 3 IPv4 ACL rule to an already existing ACL.

Add IPv6 ACL Rule
Adds a Layer 3 IPv6 ACL rule to an already existing ACL.

Add Or Remove L2 ACL Rule
Adds or removes an ACL rule to or from a Layer 2 ACL.

Apply ACL
Applies an ACL to a physical port, port channel, VE or management interface.

Create ACL
Creates an Access Control List.

Delete ACL
Deletes an existing Access Control List.

Delete IPv4 ACL Rule
Deletes the IPv4 ACL rule from an existing IPv4 ACL.

Remove ACL
Removes an ACL from physical port, port channel, VE or mgmt interface.

Edge Ports Configuration

Create L2 Port Channel
Creates a Layer 2 port channel (LAG or vLAG) in Static or LACP mode.

Create Switch Port Access
Configures a port channel or a physical interface as an access interface, or adds a untagged port to a VLAN for NI.

Create Switch Port Trunk
Configures the port channel or a physical interface as a Trunk or Trunk-no-default-native or add a tagged port to a VLAN or list of VLANs interface.

Create VE
Creates a VE and assigns IP addresses, VRF on one or more switches.

Create VLAN
Creates a single or range of VLANs on a switch.

Create VRF
Creates a Virtual Routing and Forwarding (VRF) instance on a switch for Layer 3 tenants.

Create VRRPe
Creates a VRRPe session on multiple switches by creating VRRPe group and assigning virtual IP.

Delete L2 Port Channel
Deletes the port channel interface and deletes the port channel configuration from all the member ports.

Delete Switch Port
Deletes the Switch port on an interface.

Delete VE
Deletes a VE along with router interface mappings under a VLAN.

Delete VLAN
Deletes one or more VLANs on a device.

Delete VRF
Deletes a VRF.

Delete VRRPe
Deletes a VRRPe group.

Set Interface Admin State
Enables or disables a physical port, port-channel, loopback or VE interface on a device. Optionally, sets the interface description. For MLX, port-channel admin state changes means it changes member port's admin state.

Set L2 MTU
Sets the Layer 2 MTU size on physical or port channel interfaces.

Set L3 MTU
Sets the Layer 3 MTU size on physical or VE interface.

Utility Actions

Execute CLI
Executes CLI commands and returns the result. The device type should be appropriate to get reliable output.

Validation and Troubleshooting

Ping VRF Targets
The PING target IPs from the switch using the specified VRF, uses the default VRF if VRF is not provided.

Security

Workflows in the Security folder perform a variety of network security-related functions.

Collect Traffic Forensics
Creates a package capture (PCAP) file for an IP address ExtremeAnalytics believes may be a threat to the network using the ExtremeAnalytics engine.

Create Trouble Ticket
Creates a trouble ticket based on the Malicious IP, URL, DNS, and behavior anomaly.

Quarantine End System
Quarantines an end-system ExtremeControl believes may be a threat to the network.

Quarantine PCAP Flow
Quarantines an end-system ExtremeControl believes may be a threat to the network, adds a policy to block the end-system, and creates a PCAP file for the end-system.

Revert Quarantine End System
Removes an end-system from quarantine.

Importing Workflows

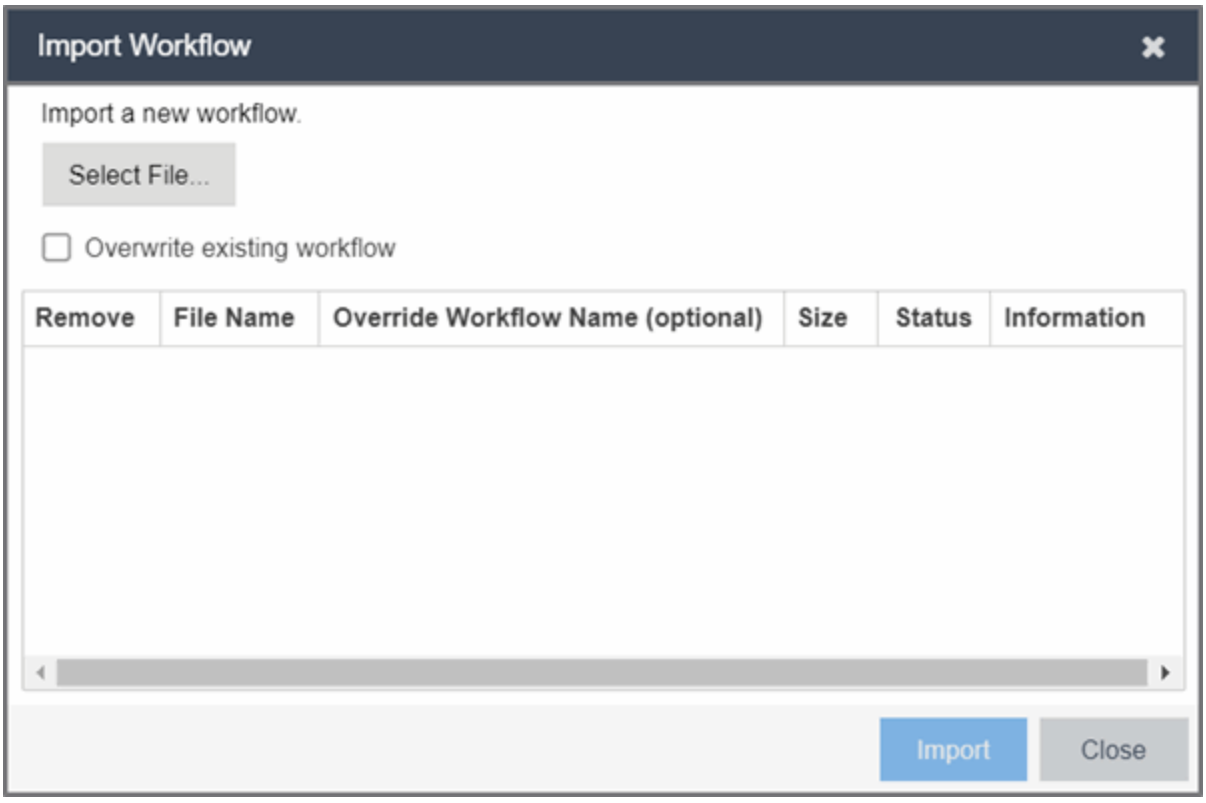
The **Workflows** tab allows you to define a complex series of activities that run in the order in which you configure them.

You can import saved User Workflows[1] to ExtremeCloud IQ Site Engine using the following steps:

1. Access the **Tasks** > **Workflows** tab.
2. Select the **Gear** icon () at the bottom of the left-panel or expand the User Workflows folder and right-click Workflows or a Workflow Group.
3. Select **Import**.

   The **Import Workflow** window displays.

[1]Only User Workflows can be imported or exported. System Workflows cannot be imported or exported.



4. Select **Select File** to open a window from which you can browse your local drive or a mapped server.
5. Select the saved workflow file you are importing and select **Open**.
6. Select the **Overwrite existing workflow** checkbox to overwrite a workflow currently saved in ExtremeCloud IQ Site Engine with the same name.
7. Select Import.

ExtremeCloud IQ Site Engine imports the workflow.

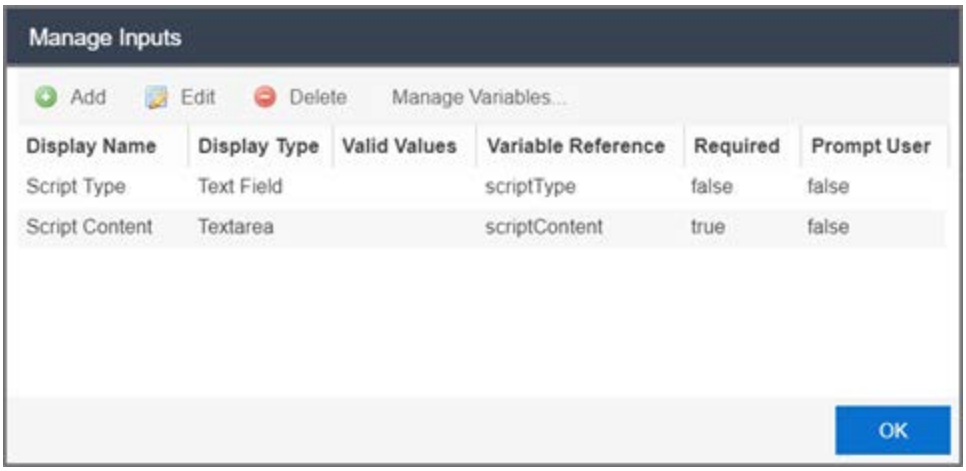
NOTE: The following information that may be configured as part of your workflow is not imported or exported when importing or exporting a workflow via the **Gear** icon:

- Custom variables
- Authorization Groups (Roles)
- Menus
- Device Groups
- Email lists
- Syslog server –The syslog server is an Events Activities setting that is not preserved during import.
- Network OS configurations that are customized on the original server and are not available on the destination server

Manage Inputs

Use the **Manage Inputs** window to configure the variables available on the Inputs tab of an activity included in a workflow on the Tasks > **Workflows** tab.

Access this window by selecting an activity in a workflow on the Tasks > **Workflows** tab, selecting the **Inputs** tab in the right panel and selecting **Manage Inputs**.



Display Name

The name of the field on the **Input** tab.

Display Type

The type of field you are adding, which determines the way in which values are selected or entered.

Valid options include:

- Text Field — Provides an open field into which text is entered.
- Display Field — Provides a text field.
- Email — Provides a field into which an email address is entered.
- Password — Provides an open field into which users enter a password. The password field contains an **Eye** icon that exposes or hides the password when selected.
- Textarea — Provides a open field into which users can enter a large amount of text.
- Timer — Provides a box into which users select an amount of time.
- ComboBox — Provides a drop-down list from which users select values. Configure the available values in the drop-down list using the Valid Values field.

Valid Values

If the **Display Type** is **ComboBox**, enter the values you are able to select from the drop-down list in a comma-separated list.

NOTE: Valid Values can contain alphanumeric characters as well as special characters (for example, a period (.), but can not contain a comma (,) as it is reserved for separating values. The list of values configured in the **Valid Values** field allows up to 1024 characters.

Variable Reference

Select the variable on which the variable you are creating is dependent via the drop-down list.

Required

Indicates whether the field is required for the activity.

Prompt User

Indicates whether the field prompts users for a value when the workflow runs.

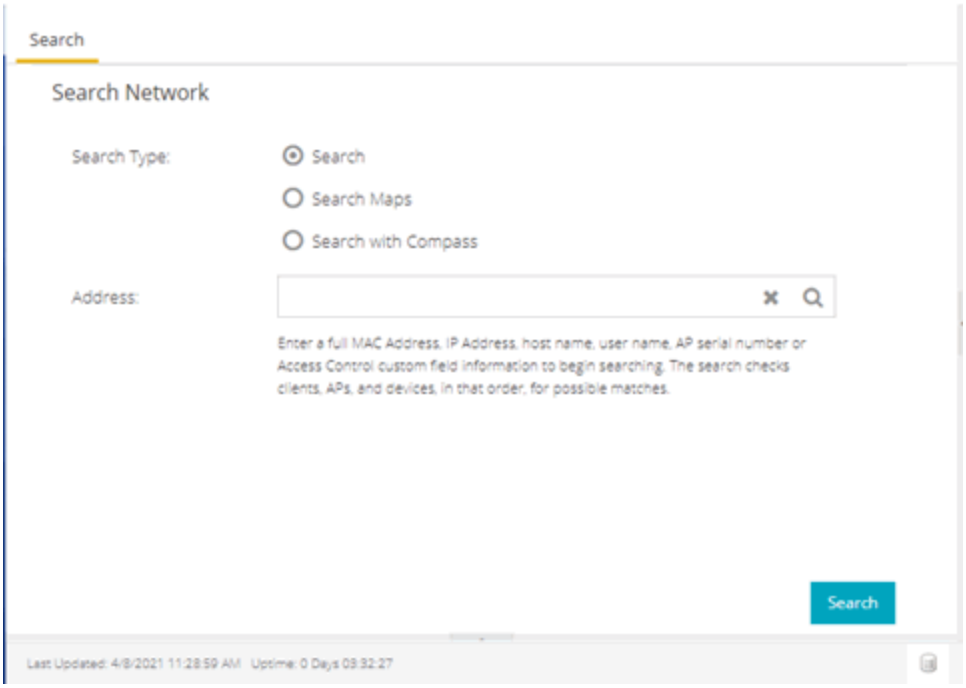
NOTE: Select an activity and enter a value in the **Custom Inputs** field on the **Inputs** tab to populate a default value you can override when running an activity with the **Prompt User** checkbox selected.

Search Network

ExtremeCloud IQ Site Engine's Search is a powerful diagnostic tool for locating a network device or end-system you wish to troubleshoot by allowing you to display it in PortView. You can search by MAC address, IP address, or AP serial number, as well as ExtremeControl end-system name, username, and registration custom field attributes. Additionally, you can search for a device in a map, or perform a Compass search. A device must be in the ExtremeCloud IQ Site Engine database, or it must be a client of a device in the database, for the search to function. For a client device, either statistics collection must be enabled for the device, or the client must be an Access Control authenticated client.

To view ExtremeCloud IQ Site Engine Search Network, you must be a member of an authorization group assigned the XIQ-SE OneView > Access OneView Search capability. To perform a Search with Compass, you must also have the ExtremeCloud IQ Site Engine Console > Launch a ExtremeCloud IQ Site Engine Console Client capability.

To access the **Search** tab, select the magnifying glass icon at the top of the ExtremeCloud IQ Site Engine window in the menu.



This Help topic provides information on the following topics:

- Using ExtremeCloud IQ Site Engine Search Network
  - Search
  - Search Maps

- Search with Compass
  - Compass Search Types
- Search Examples
  - Search your Network for an End-System MAC Address
  - Search your Network for an ExtremeControl Authenticated Client IP Address
  - Search your Network for a Device IP Address
- Search Options/Limitations

Using ExtremeCloud IQ Site Engine Search

In the **Address** field, enter a MAC address or IP address. You can copy the IP or MAC address from another source and enter it into the **Address** field. You can also search on AP serial numbers, and by Access Control end-system hostname, user name, and registration custom field attributes.

Search

Depending on the type of item for which you are searching, the secondary navigation bar displays one or more **PortView** tabs, with information pertaining to your search item.

The **Overview** tab always displays, which provides a topological display of device relationships. You can right-click on the devices in the topology to launch additional reports for the device. For more information see the PortView Help topic.

Search Maps

Allows you to search your existing maps to find a wired or wireless client or device. If the client or device you searched is included in only one map, it opens. The Search Result field displays multiple map paths if the client or device you searched is included in more than one map. Select any map path to display the map. For more information on maps, see Maps Overview.

Search with Compass

The Search with Compass option provides a variety of search filters, allowing you to narrow your search parameters. Compass is a powerful search tool that provides information about the status, configuration, and activities at the ingress points of your network. It provides an easy way to search for end stations, or users on end stations.

To perform a search, specify the following information:

- Device Group (Search Scope) — Use the drop-down list to limit your search to a specific device group.

- Compass Search Type — There are multiple search types available from the drop-down list. See the following section for a description of each type.
- Address (Search Parameters) — If you provide specific search parameters (such as an IP address or MAC address), Compass returns information on those parameters if it finds them within the selected device group. If you do not provide specific search parameters, Compass returns information on everything within the device group.

When the search is complete, the results display in table form. You can manipulate table data in several ways to customize the view for your own needs:

- Select the column headings to perform an ascending or descending sort on the column data.
- Use the column heading drop-down arrow to select the Columns option and hide or display different columns in the table.
- Use the column heading drop-down arrow to filter, sort, and search the data in each column in the table.

You can define the search options the Compass Search uses on the **Administration** > **Options** tab (Administration > Options > Compass). These options determine the data sources used with Compass searches. In addition to search options, you can also configure search limit settings, which help limit the ExtremeCloud IQ Site Engine server resources used for the searches.

Compass Search Types

The following Compass Search types are available.

- Auto — The Auto search auto-detects the address format you enter in the **Address** field, and performs the appropriate search. Enter the full IP, MAC, or username in the **Address** field and select a device group as a search scope.
- All — The All search finds any network element aware of the devices within the selected scope, and lists the addresses with which they are associated. Data is collected from all the MIBs that Compass implemented. The All search ignores any search parameters entered in the **Address** field.
- MAC Address — The MAC Address search finds any device aware of the specified MAC address within the selected scope and lists the addresses associated with it.
- IP Address — The IP Address search finds any device aware of the specified IP address/hostname within the selected scope and lists the addresses with which it is associated.
- IP Subnet — The IP Subnet search finds any device aware of the specified IP subnet within the selected scope and lists the end stations in the IP subnet. The address must contain both an address and mask separated by "/".
- User Name — The User Name search finds any device aware of the specified user name within the selected scope and lists the addresses with which it is associated.

- Multicast Address — The Multicast Address search finds any device aware of the specified multicast address within the selected scope and lists the addresses with which it is associated.

Search Examples

Following are some examples of different kinds of searches you can perform using the ExtremeCloud IQ Site Engine Search Network.

Search your Network for an End-System MAC Address

You can search on an end-system's MAC address. For example, you can copy an end-system's MAC address listed in the **Control** tab's End-System view and paste the MAC address into the **Search Network** field.

Search your Network for an ExtremeControl Authenticated Client IP Address

You can also search on an Access Control authenticated end-system's IP address. For example, you can copy an end-system's IP address from the **Control** tab's End-Systems view and paste it into the **Search Network** field.

Search your Network for a Device IP Address

To perform a search on a device, you can copy a device IP address from the **Network** tab. The search results show only the single device. Right-click on the device to open additional reports.

Search Options/Limitations

The maximum number of PortView Search results displayed at one time is configured in the Site Engine - Options (Administration > Options > Site Engine - General > Session Limits). The default maximum number is five. When the limit is reached, a dialog displays, indicating the limit is reached and the existing view must be closed.

In the **Overview** (search results) tab, the device topology is displayed showing the relationships between a specific set of devices: Wireless Controller, Identity and Access Gateway, AP, switch, and client. The greatest number of devices displayed is five devices for a wireless client in an Access Control authenticated environment (six devices may be returned if the client is also connected via wire). The number of devices returned becomes smaller as you search for one of the five devices. For example, if you search for an AP instead of a client, four devices are returned. If you search for a Wireless Controller, Access Control Engine, or switch, one device is returned.

Compass SNMP MIBs Descriptions

This topic provides a brief description of the MIBs and Tables that can be chosen as Compass Search Options when setting Compass options.

ipNetToMedia

IP Address Translation table used for mapping from IP addresses to physical addresses. This table is read whenever an entry is found by **IP Route** or **IP CIDR Route** searches, regardless whether the **IPNetToMedia** is checked. Checking the IPNetToMedia checkbox only affects whether or not the entire IPNetToMedia table is read.
Check this MIB when your network includes devices that do not support Node/Alias (ctAlias MIB). You should include your routers in your search scope when this MIB is checked. This selection can be un-checked when your network is comprised only of devices that support Node/Alias, thus improving search performance.

802.1x Authentication (PAE)

Port Access Entity module for managing IEEE 802.1X.

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

MAC Locking

Provides configuration and status objects pertaining to per port MAC Locking.

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

Enterasys IGMP

Extends the Standard IGMP MIB for configuration of IGMP on Enterasys devices.

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

Dot1dTpFdb

This table contains information about unicast entries for which the bridge has forwarding and/or filtering information. This information is used by the transparent bridging function in determining how to propagate a received frame.

Check this MIB to resolve MAC addresses to a port.

Enterasys 802.1x Ext.

Supplements/used in connection with the standard IEEE 802.1x MIB. It provides a convenient way to retrieve authentication status for Supplicants living on shared-media ports that use station-based access control. (Here, a MAC address is a much more natural table index than a port or interface number.)

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

Node/Alias (ctAlias)

This MIB defines objects that can be used to discover end systems per port, and to map end system addresses to the layer 2 address of the port.

Check this MIB to resolve IP addresses to MAC addresses when the devices in your network support the Node/Alias (ctAlias) MIB.

IGMP Standard

MIB module for IGMP Management, it contains an IGMP Interface Table, having one row for each interface on which IGMP is enabled, and an IGMP Cache Table with one row for each IP multicast group for which there are members on a particular interface.

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

IP Route

An entity's IP Routing table. This selection provides the ability to resolve IP addresses to MAC addresses.

Check this MIB when your network includes devices that do not support Node/Alias (ctAlias MIB). You should include your routers in your search scope when this MIB is checked. This selection can be un-checked when your network is comprised only of devices that support Node/Alias, thus improving search performance.

Dot1qTpFdb

A table that contains information about unicast entries for which the device has forwarding and/or filtering information. This information is used by the transparent bridging function in determining how to propagate a received frame.

PWA (Enterasys Port Web Authentication)

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

MAC Authentication

Used for authentication using source MAC addresses received in traffic on ports under control of MAC-authentication.

Check this MIB to find other occurrences of an IP address or MAC address within your search scope. The values returned by searching this MIB are often duplicates of the values returned from other MIBs, so checking this MIB is usually not necessary.

IP CIDR Route

The IP CIDR Route Table obsoletes and replaces the ipRoute Table current in MIB-I and MIB-II and the IP Forwarding Table. It adds knowledge of the autonomous system of the next hop, multiple next hops, and policy routing, and Classless Inter-Domain Routing.

Check this MIB when your network includes devices that do not support Node/Alias (ctAlias MIB). You should include your routers in your search scope when this MIB is checked. This selection can be un-checked when your network is comprised only of devices that support Node/Alias, thus improving search performance.

Dot1q VLAN Static

A table containing static configuration information for each VLAN configured into the device by (local or network) management. All entries are permanent and are restored after restarting the device.

Dot1q VLAN Current

A table containing current configuration information for each VLAN currently configured into the device by (local or network) management, or dynamically created as a result of GVRP requests received.

Enterasys Multiple Authentication

This MIB is used for authentication using source MAC addresses received in traffic on ports under control of MAC-authentication. Check this MIB to find ports that allow authentication of multiple users on a port.

Enterasys Convergence End Point

This MIB contains information about devices that support End Point Convergence. Check this MIB to find IP addresses running applications (e.g. Voice over IP) using Endpoint Convergence.

Site Engine How-tos

Discover Devices

ExtremeCloud IQ Site Engine allows you to discover the devices of your network and add them to the ExtremeCloud IQ Site Engine database.

NOTE:

Before discovering devices, create the maps to which they belong. For additional information on creating maps, see How to Create and Edit Maps.

For a list of instructions outlining the initial setup of your network in ExtremeCloud IQ Site Engine, see ExtremeCloud IQ Site Engine Initial Configuration Checklist.

You can discover new devices based on the following criteria:

- Seed addresses for CDP, LLDP, EDP, or SONMP-compliant devices
- IP/Subnet masks
- IP Address Range

Discover automatically explores the defined network segment and creates a list of discovered devices. You can then save the discovered devices to the ExtremeCloud IQ Site Engine database, where they are displayed in the left-panel tree on the **Network** > Devices tab.

NOTE: When adding an ExtremeXOS/Switch Engine device in ExtremeCloud IQ Site Engine, enter the following commands in the device CLI:

```
configure snmpv3 add community "private" name "private" user "v1v2c_rw"
configure snmpv3 add community "public" name "public" user "v1v2c_rw"
enable snmp access
enable snmp access snmp-v1v2c
disable snmp access snmpv3
```

To discover devices, begin by using the **Site** tab to configure the default settings that apply to devices you add to ExtremeCloud IQ Site Engine and then configure individual devices and add them to the ExtremeCloud IQ Site Engine database via the **Discovered** tab.

NOTE: ZTP+ enabled devices use a different device discovery process. For additional information on discovering devices using ZTP+, see ZTP+ Device Configuration in ExtremeCloud IQ Site Engine.

Discovering Devices

1. Open the **Network** > **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Select the site from the left panel to which you are adding the devices.
4. Select the **Site** tab in the right-panel.
5. Select the **Discover** tab.
6. Select the **Add** button in the Addresses list to open the Add Address window.
7. Select **Subnet**, **Seed Address**, or **Address Range** in the **Discover Type** drop-down list.
8. Enter the **Subnet**, **Seed Address**, or **Start Address** and **End Address**, depending on the **Discover Type** you select.
   - **Subnet** — Enter the IP address and subnet in the following format: *IP Address*/*Subnet Mask*
     - The *IP Address* must be one of the hosts in the subnet.
     - A **/** is required between the IP Address and Subnet Mask.
     - The *Subnet Mask* must use CIDR or dotted decimal notation.

       NOTE: When using dotted decimal notation, the network bits must be contiguous ones and the host bits must be contiguous zeros.
   - **Seed Address** — Enter the seed address for CDP, LLDP, EDP, SONMP-compliant devices.
   - **Address Range** — Enter the **Start Address** and **End Address** for the IP addresses in the same address range.

   NOTE: ExtremeCloud IQ Site Engine only allows a subnet search of a 16-bit mask or higher when discovering devices.
9. Select the **Add** button in the Profiles section of the window to open the Add Profile window. Select **New** in the drop-down list to create SNMP and CLI credentials for the profile and select the **Save** button.

   Profiles allow you to configure different sets of SNMP and CLI credentials for read access, write access, and maximum access. After you create profiles, assign them to devices to allow users appropriate access based on the credentials they use for a device.
10. Select the profiles you want the devices on your network to **Accept** or **Reject** using the **Profiles** list.
    For additional information about profiles, see **Profiles** tab.

11. Select the **Automatically Add Devices** checkbox to automatically add the devices to ExtremeCloud IQ Site Engine and configure any other appropriate actions for your devices in the Device Actions section of the window.

    NOTE: When **Automatically Add Devices** is selected, devices are automatically added to ExtremeCloud IQ Site Engine and display in the Devices list on the Network > **Devices** tab. When **Automatically Add Devices** is not selected, devices are displayed on the Network > **Discovered** tab and require you to manually add them.

12. Repeat the process for all devices added to this site.
    For additional information about sites, see **Site** tab.
13. Select **Save**.
14. Select **Discover**.
15. Select the **Clock** icon in the Top menu to open the Operations table at the bottom of the ExtremeCloud IQ Site Engine window to monitor the progress of the device discovery.
16. Access the Network > **Discovered** tab.

    NOTE: The devices displayed on this tab vary depending on whether you selected **Automatically Add Devices** in Step 11.

17. Configure and add any devices displayed to ExtremeCloud IQ Site Engine:
    - If you selected **Automatically Add Devices**, devices display on the **Discovered** tab only if they require additional attention (for example, devices are potential duplicates of another device). Configure the devices appropriately and add them to ExtremeCloud IQ Site Engine.
    - If you did not select Automatically Add Devices, all devices are staged on the Discovered tab before being added to ExtremeCloud IQ Site Engine. Follow the steps in the Adding Devices section to complete the process of adding your devices to ExtremeCloud IQ Site Engine.

Adding Devices

If you did not select **Automatically Add Devices** in Step 11, use the **Discovered** tab to manually add the discovered devices to ExtremeCloud IQ Site Engine.

1. Open the **Network** > **Discovered** tab in ExtremeCloud IQ Site Engine.
2. Select the devices you want to add to the ExtremeCloud IQ Site Engine database and select the **Add Devices** button. The Add Devices window opens.
   The window is populated with the information you entered on the **Site** tab.

3. Enter any device-specific information, or change information that does not match the device defaults set on the **Site** tab.
4. Select the **Add** button.
   The devices are added to the ExtremeCloud IQ Site Engine database and move from the **Network** > **Discovered** tab to the **Network** > **Devices** tab.

Add Users

Users are given access to parts of ExtremeCloud IQ Site Engine based on the authorization group to which they are assigned. Assign a set of capabilities for each authorization group and then add users to each authorization group depending on the capabilities they require.

NOTE:

This topic assumes devices are already added to the ExtremeCloud IQ Site Engine database. For additional information on discovering and adding devices, see How to Discover Devices in ExtremeCloud IQ Site Engine.

For a list of instructions outlining the initial setup of your network in ExtremeCloud IQ Site Engine, see ExtremeCloud IQ Site Engine Initial Configuration ChecklistExtremeCloud IQ Site Engine Initial Configuration Checklist.

When you first log into ExtremeCloud IQ Site Engine the Administrator access through which you are currently logged in is the only set of user credentials.

This topic describes the process for adding users to ExtremeCloud IQ Site Engine, which is accomplished by performing the following steps:

1. Create Authorization Groups
2. Add Users to Authorization Groups
3. Select the Authentication Method

IMPORTANT: ExtremeCloud IQ Site Engine does not save passwords. Users you create are authenticated against the Operating System, the RADIUS server, or the LDAP server, depending on the authentication method you select.

Create Authorization Groups

First, create authorization groups for each group of ExtremeCloud IQ Site Engine users.

1. Access the **Administration** > **Users** tab.
2. Select the **Acquire Lock** button in the Users/Groups Access section at the top of the tab. This button locks access to the tab for all other users and enables you to make changes to the authorization groups and authorized users.
3. Select the **Add** button in the Authorization Groups section at the bottom of the tab.
4. Enter the appropriate information for each authorization group using ExtremeCloud IQ Site Engine.
   The Capability section of the window enables you to expand each capability tree by selecting the arrow to the left of the checkbox to display more specific tasks. Select only those that apply to each user group. Additionally, you can search for a specific capability in the **Search** field above the tree.
5. Select the **Save** button to create the authorization group.
6. Repeat the process to create the necessary authorization groups.

Add Users to Authorization Groups

Next, use of the Administration > Users tab to create the users who require access to ExtremeCloud IQ Site Engine and add them to an authorization group depending on the level of access they require.

1. Select the **Add** button in the Authorized Users section.
2. Enter a User Name, a Domain/Host Name (if necessary), and select the Authorization Group with the appropriate level of access for the user.
3. Select the **Save** button to save the new user.
4. Repeat the process to add all ExtremeCloud IQ Site Engine users for each authorization group.

Select the Authentication Method

Finally, use Administration > Users tab to select the method by which users authenticate when accessing ExtremeCloud IQ Site Engine.

ExtremeCloud IQ Site Engine supports three authentication methods to authenticate users: using the underlying host operating system, using a specified LDAP configuration, or using specified RADIUS servers.

1. Select the **Authentication Type** using the drop-down list in the Authentication Method section.
   The options change based on the **Authentication Type** selected.
2. Select the supplemental information based on the type selected.
3. Select the **Release Lock** button to enable other users to make changes.

The users you added now have access to the functionality you configured for their respective authorization group.

How to Configure 2FA

1. Ensure SMTP is configured and working, see Email Configuration (SMTP/API) Options.
2. Ensure NTP is configured and working.
3. Create or modify the Authorization group (**Administration** > **User** > **Authorization Groups** > select your group > **Edit** > **Enable 2FA**), see Authorization Group Capabilities
4. Add users to the Authorization Group (manually or through Automatic Membership Criteria).

NOTE:

SMTP is required if the user does not have the ability to scan a QR code in the authenticator application.

The correct time is required, use a time synchronization protocol.

The tested authenticator applications are Microsoft Authenticator and Google Authenticator.

You cannot perform a Reset 2FA action on your own account.

How to Pair a 2FA Authenticator App with your Account

1. Login to ExtremeCloud IQ Site Engine OneView with your user credentials.
2. The first time login provides you with a QR code you can use to pair your account with an Authenticator App. If you do not have a QR code scanner, you can enter your email address and use the 2FA recovery token in your Authenticator App.
    - Microsoft Authenticator with QR code:
        1. Open **Microsoft Authenticator**.
        2. Select the **QR code icon**.
        3. Scan the QR code provided from your first log in to ExtremeCloud IQ Site Engine.
    - Microsoft Authenticator with 2FA recovery token:
        1. Open **Microsoft Authenticator**.
        2. Select the **QR code icon**.
        3. Select **Enter code manually**.

4. Select **Other (Google, Facebook, etc.)**
5. Enter an account name in the **Account name** field. For example, "Site Engine - Production".
6. Enter the 2FA recovery token in the **Secret key** field.
7. Select **Finish**.

- Google Authenticator with QR code:
  1. Open **Google Authenticator**.
  2. Select **Add a code**.
  3. Select **Scan a QR code**.
  4. Scan the QR code provided from your first log in to ExtremeCloud IQ Site Engine.
- Google Authenticator with 2FA recovery token:
  1. Open **Google Authenticator**.
  2. Select **Add a code**.
  3. Select **Enter a setup key**.
  4. Enter an account name in the **Account name** field. For example "Site Engine - Production".
  5. Enter the 2FA recovery token in the **Your key** field.
  6. Keep Key type as **Time based**.
  7. Select **Add**.

3. After the Authenticator App is configured, select **Next** in the ExtremeCloud IQ Site Engine OneView.
4. In OneView, Enter the code provided by your paired Authenticator App.

How to Reset 2FA

Perform the following procedure to reset 2FA for a user (Authenticator App was uninstalled)

1. Login to ExtremeCloud IQ Site Engine OneView with administrator credentials.
2. Select **Administration** > **User** > **Authorized Users** > select the user > **Reset 2FA**.
3. Instruct the user to login and pair a 2FA Authenticator App with their account.

Compare Device Configurations

You can compare archived device configurations in ExtremeCloud IQ Site Engine by using either the **Network** > **Devices** tab or the Archive Details Report available in the **Network** > **Reports** tab.

In order to perform the compare configuration operation, you must be a member of an authorization group with the Inventory Manager > Configuration Archive Management > View/Compare Configurations capability.

This Help topic provides the following information:

- Selecting the Files to Compare
- Comparing the Files

Selecting the Files to Compare

Select the files to compare using either the **Network** tab or the **Reports** tab.

From the Network tab:

Use the **Network** tab to compare the last two archived configuration files for a device.

Select a device in the table and use either the **Menu** icon (☰) or the right-click menu off the device to select **More Actions** > **Compare Last Configurations**.

From the Reports tab:

Use the **Reports** tab to compare two configuration files selected from all archived files for the device.

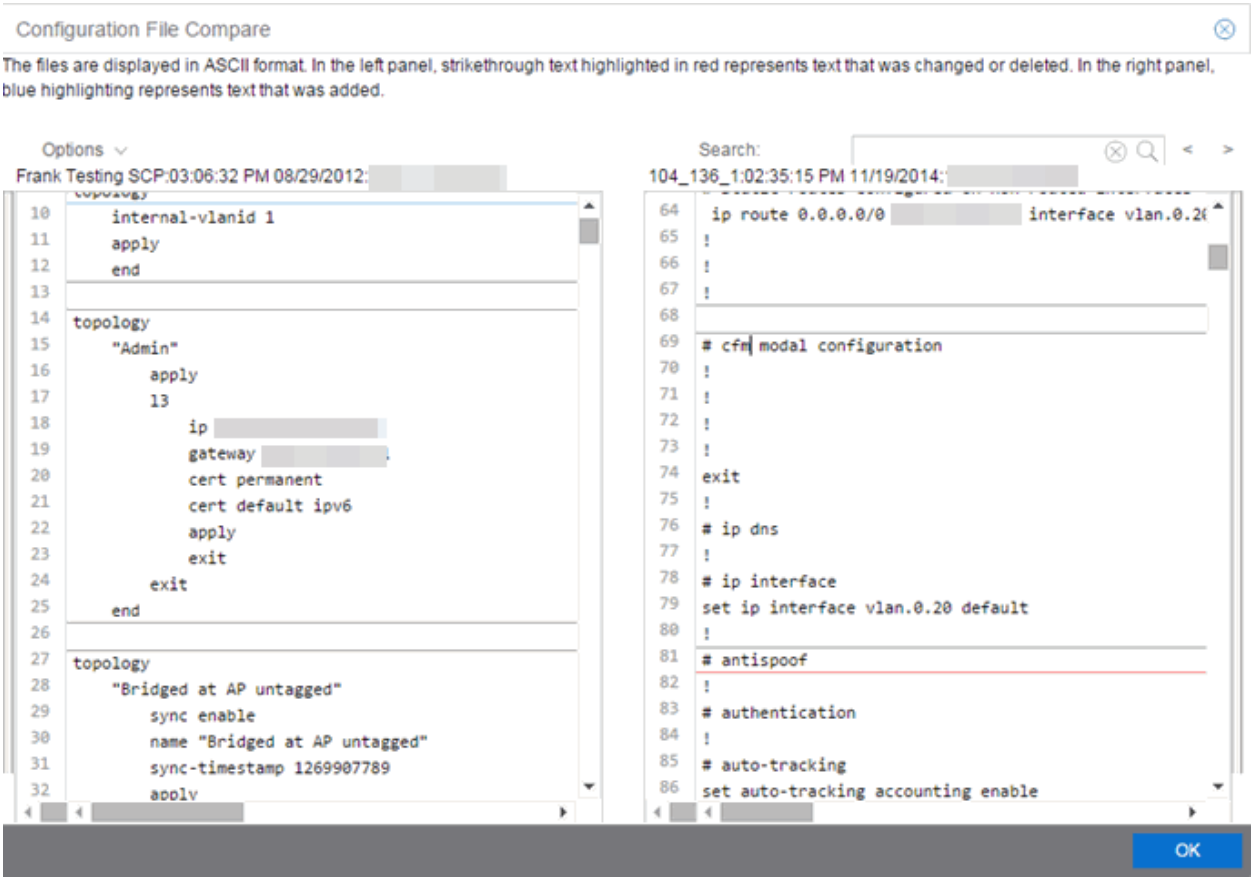
Select the Device > Device Archives report. Select the **Archive Details** tab in the right panel and then select the **Archives by Device** sub-tab.

The tab displays all the ExtremeCloud IQ Site Engine archives by device IP address. Select two files to compare and select **Compare Configuration**.

Comparing the Files

The Configuration File Compare window displays the files in two panels. Titles over each file show the archive name that contains the configuration file, the date, and the IP address of the device from which you create the configuration file.

Scroll through the two files to view file differences. Typically, the newer file displays in the right panel. You can use the "Swap sides" option to swap the files. In the left panel, strikethrough text highlighted in red represents text that is changed or deleted. In the right panel, blue highlighting represents text that is added.



Use the toolbar Options menu to control the look of the display window:

- Enable line numbers displays line numbers alongside the text.
- Wrap lines shows all the text in the column and removes the horizontal scroll bars.
- Enable side bars shows where the text differences are in the whole file.
- Swap sides swaps the files contained in the left and right panels.

TIP: Removing line numbers and side bars may speed up the display of larger files.

Use the **Search** field in the toolbar to perform a search in the panel side that is selected by the cursor. Use the forward and back arrows to search for the next or previous instance of the search term.

Device View

Device View is an ExtremeCloud IQ Site Engine component that provides a wide range of analysis and troubleshooting information for your network wired and wireless devices, including a device summary, FlexViews, and ExtremeCloud IQ Site Engine reports.

The primary launch point for Device View is from the **Network** tab. Device View can also be launched from other locations in ExtremeCloud IQ Site Engine.

This Help topic provides the following Device View information:

- Requirements
  - Access Requirements
  - Data Collection Requirements
- Device View Reports
  - Left-Panel Device Summary
- Launching Device View

Requirements

Access Requirements

Access to Device View reports is determined by the user's membership in an ExtremeCloud IQ Site Engine authorization group and the group's assigned capabilities. The following list shows the capabilities required for full access to all the Device View reports.

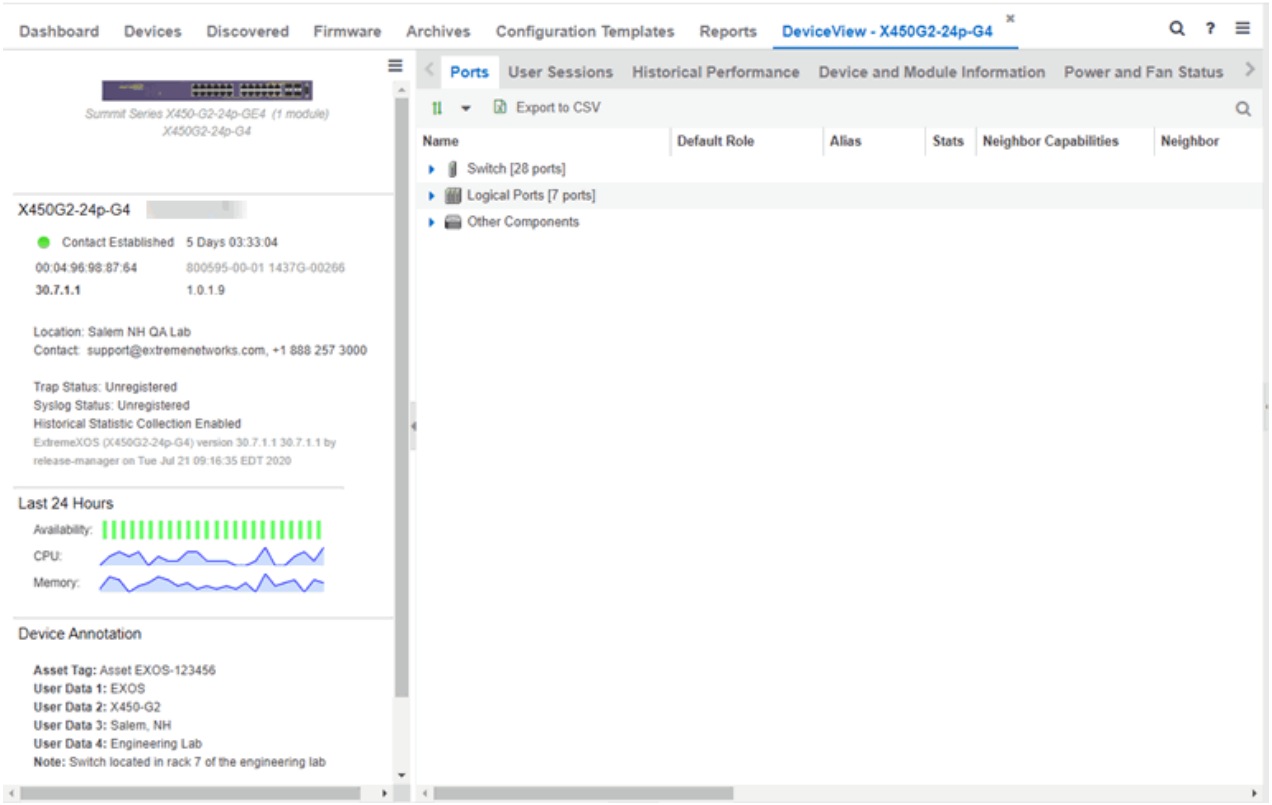
- XIQ-SE OneView > Access OneView
- XIQ-SE OneView > Access OneView Reports
- XIQ-SE OneView > Events and Alarms > OneView Event Log Access
- XIQ-SE OneView > FlexView > OneView FlexView Read Access

Data Collection Requirements

Device View reports require that historical data collection is enabled for the device. For information on configuring data collection, see Collect Device Statistics in the Devices section of the ExtremeCloud IQ Site Engine User Guide.

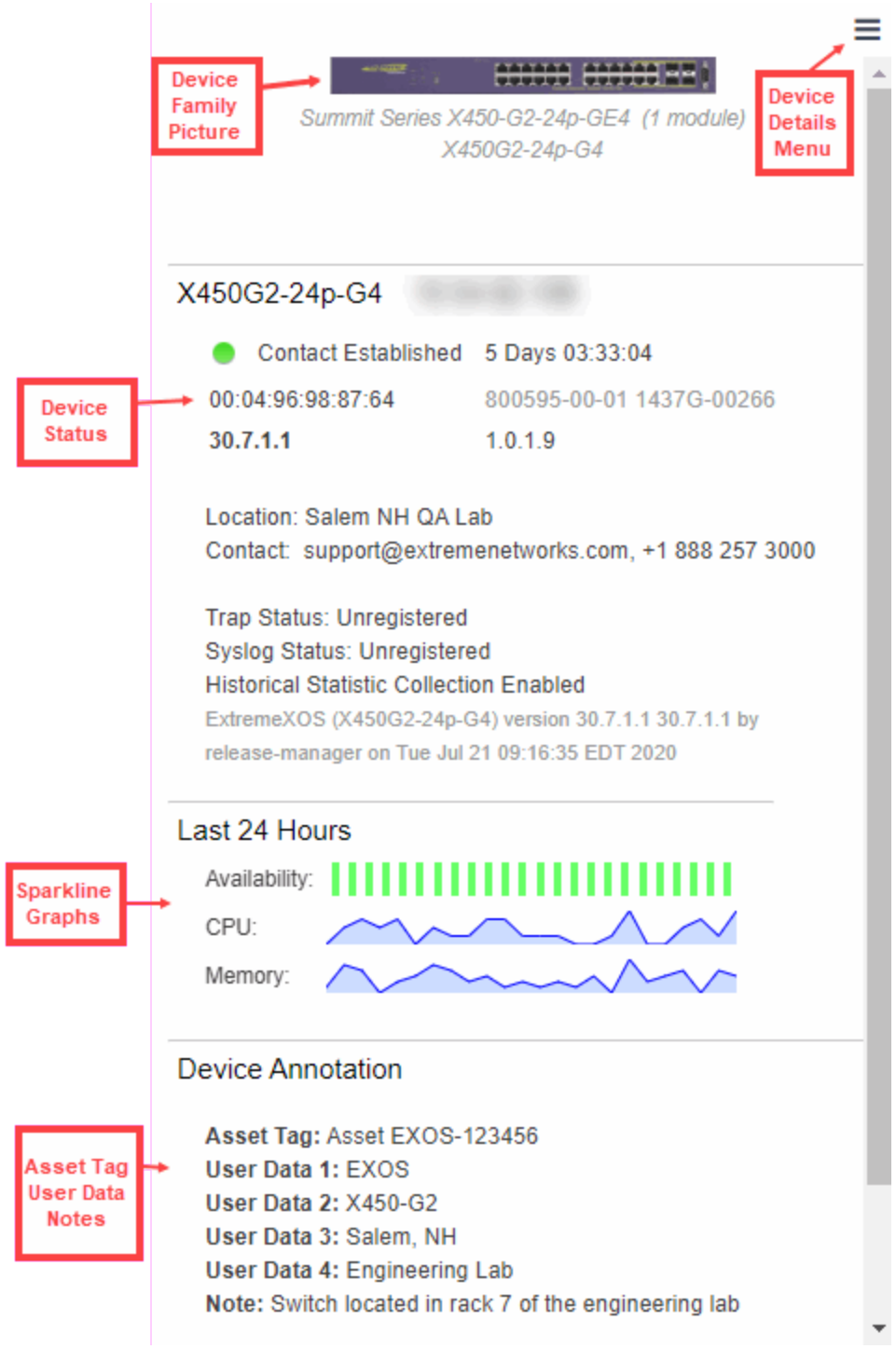
Device View Panels

The Device View is comprised of a left-panel device summary, and a selection of tabbed panels that display FlexViews and reports based on the device family.



Left-Panel Device Summary

The left-panel device summary view (shown below) is displayed in each Device View report.



Each device summary view includes:

- **Device Family Picture** — A generic device family picture for the device.

- **Device Status** — Indicates the alarm/device status for the device. The icon color indicates the severity of the most severe alarm on the device. A red icon indicates a critical alarm or the device is down. A green icon indicates that there are no alarms and the device is up.
- **Sparkline Graphs** — Provides network trends in dense, succinct charts that present report data in an easy to read, condensed format. You must have Historical Statistic Collection enabled in order to see the Sparkline graphs and other report data. If Historical Statistic Collection is not enabled, you will see a line that says, "Historical Statistic Collection Disabled." For information on configuring data collection, see Collect Device Statistics in the Devices section of the ExtremeCloud IQ Site Engine User Guide.
- **Asset Tag, User Data, Notes** - Displays the Asset Tag, User Data and notes about the device. This data is only displayed if you have configured these values in ExtremeCloud IQ Site Engine.
- **Device Details Menu** — Select the **Menu** icon (☰) in the upper right corner to access additional device reports.

Right-Panel Device Summary

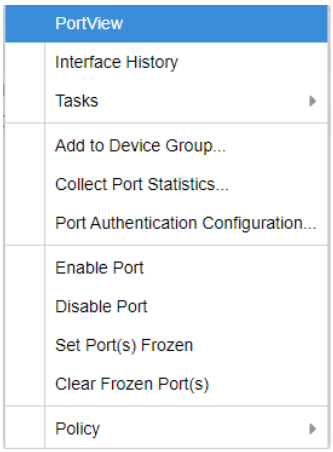
The following tabs and reports are available in the Device View. The reports displayed in a Device View vary according to the selected device. For most reports, right-click a device in the table to export the table details or details about the selected device to a .csv report.

Ports

Use the Ports report to view details about the ports and other components associated with the Device Family. The following columns are included in the Ports report:

- Name - The name assigned to the port
- Default Role - The policy role assigned to the selected port.
- Alias - An alternate name for the port.
- Stats - Displays whether statistics collection is enabled or disabled on the port. A black check indicates that historical collection is enabled, and a blue check indicates that threshold alarms collection (formerly monitor collection) is enabled.
- Neighbor Capabilities - Displays capabilities for neighbor ports.
- Neighbor - Displays neighbor details from CDP/EDP/LLDP. Place your mouse over the column to see the protocol type.
- Port Speed - Displays the speed of the port
- PVID - The port's VLAN ID.
- VLANs - Displays the name of the VLAN.
- Description - A description of the port.
- Port Type Details - Displays the port type and other information about the port type.
- Serial Number - Displays the port's serial number.

Select an entry in the table, expand to display a port, and right-click to open the following drop-down list:



- PortView - Access PortView for that port.
- Interface History - view interface history including interface utilization, availability, and bandwidth/packets/flows statistics (Flows stats display only for S/K series and PF-FC-180 devices).
- Add to Device Group - Use to select a Device Group to which you will add the port.

  NOTES:

  Right-clicking ports and selecting Add to Device Group opens the Add to Device Group window, which allows you to select a device group to which to add the selected ports.

  Right-click a port and select the **Application Telemetry** menu to view the Interface Top Applications Treemap or Top Clients by Interface report for the port. If Application Telemetry is not enabled on the device, the Application Telemetry menu does not display.

  Only VLANs to which ports are assigned are displayed in this report. Additionally, VLAN reports for ExtremeXOS/Switch Engine devices may display duplicate VLANs as VLANs are assigned by slot.

- Collect Port Statistics - Opens a window from which you can select your statistics collection mode (Historical, Threshold Alarms), or disable statistics collection.
  - In **Historical mode**, port statistics are saved to the database and aggregated over time, for use in reports. The statistics are also used for threshold alarms configured in the Console Alarms Manager. In the Active Threshold Alarm Summary box, you can see all active threshold alarms configured in the Console

Alarms Manager that use these statistics.

NOTE: Enabling Historical Statistics Collection may use substantial disk space.

- In **Threshold Alarms (formerly Monitor) mode**, port statistics are saved for one hour and then dropped. You can use these statistics for threshold alarms, but not for ExtremeCloud IQ Site Engine reporting. In the Active Threshold Alarm Summary box, you can see all active threshold alarms configured in the **Alarms and Events** tab that use these statistics. (Note that you do not see the Threshold Alarms mode option if you have disabled threshold alarms collection in the OneView Collector Advanced Settings in **Administration** > **Options**.)
- **Disable** — Select this check box to disable statistic collection mode.

- Port Authentication Configuration - Access the Authentication Configuration for the port.
- Enable Port - Enables the port for the device.
- Disable Port - Disables the port for the device.
- Set Port(s) Frozen - Select to freeze the selected port.
- Clear Frozen Port(s) - Select to clear the selected frozen port.
- Policy - Use to create policy profiles, called roles, that are assigned to the ports in your network.

- MAC Addresses
- Device Logs
- Alarms
- Events
- Archives
- User Sessions
- Historical Performance
- Switch Resources
- Device and Module Information
- Controller History
- Power and Fan Status
- Active Access Points
- Storage Utilization
- Process Utilization
- WLAN Services

- CPU and Process Utilization
- VLAN
- Active Clients
- IP Traffic Summary
- MLAG
- Alarms and Events
- VPLS

Launching Device View

Device View can be launched from a variety of locations in ExtremeCloud IQ Site Engine.

Network Tab

The primary launch point for Device View is from the **Network** tab.

1. Open the **Network** > **Devices** tab.
2. Place your mouse over the first column and select the Device View icon .
3. The Device View opens as a separate tab.

Control Tab

Use the following steps to launch Device View from the **Control** tab.

1. Open the **Control** > **Dashboard** tab.
2. Select the **System** view.
3. In the Engine Information report, select an engine IP address to open a Device View for the engine.

ExtremeCloud IQ Site Engine Maps

Use the following steps to launch Device View from a map.

1. Open ExtremeCloud IQ Site Engine Maps and select a map.
2. In the map, right-click on a device icon and select Device View.

Search

Use the following steps to launch Device View from the **Search** tab.

1. Open **Search** and search for a device.
2. In the Overview, right-click on the device icon and select Device View.

Upgrade Firmware

Use ExtremeCloud IQ Site Engine to upgrade device firmware for your Extreme Networks devices.

NOTE: Prior to upgrading firmware, you must access the Extreme Networks website to obtain information about the latest Extreme Networks firmware releases available for download.

You can upgrade firmware in one of three ways:

- For a particular device on your network
- For all devices of a device type
- For a Fabric Manager

You must be a member of an authorization group that includes Inventory Manager > Firmware/Boot PROM Management > Firmware/Boot PROM Upgrade Wizard capability to see this menu option.

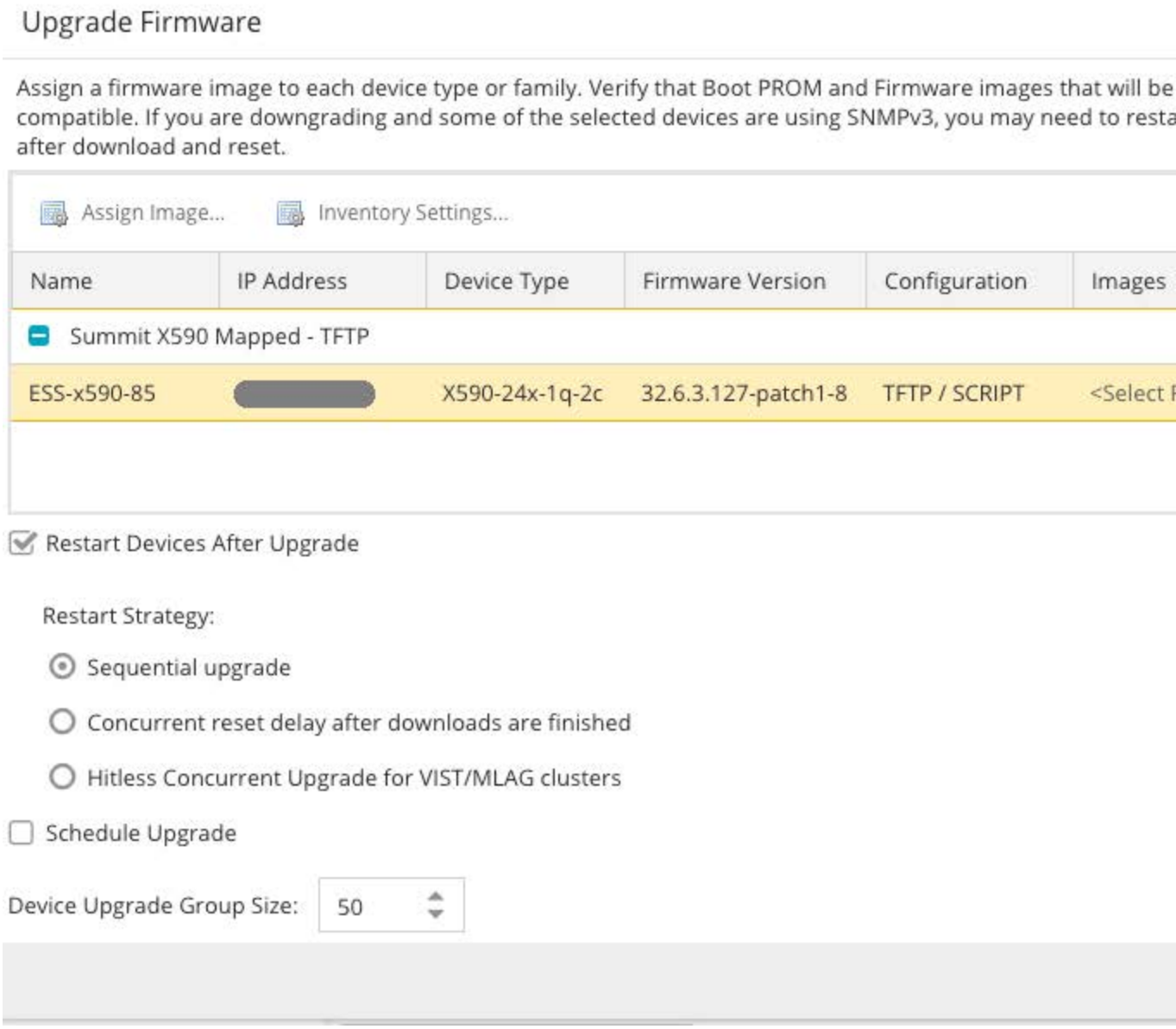
Upgrading for a Device

To upgrade firmware for a particular device:

1. Open the **Network** tab.
2. Select the **Devices** tab.
3. Select **All Devices** from the left-panel drop-down list, or select a **Map** or **Site**, depending on the location of the device you are upgrading.
4. Select the **Devices** tab in the right-panel.
5. Select the devices for which you are upgrading firmware in the Devices table in the right-hand panel.
6. Select the **Menu** icon (☰) or right-click in the Devices list.
7. Select **Upgrade Firmware**.

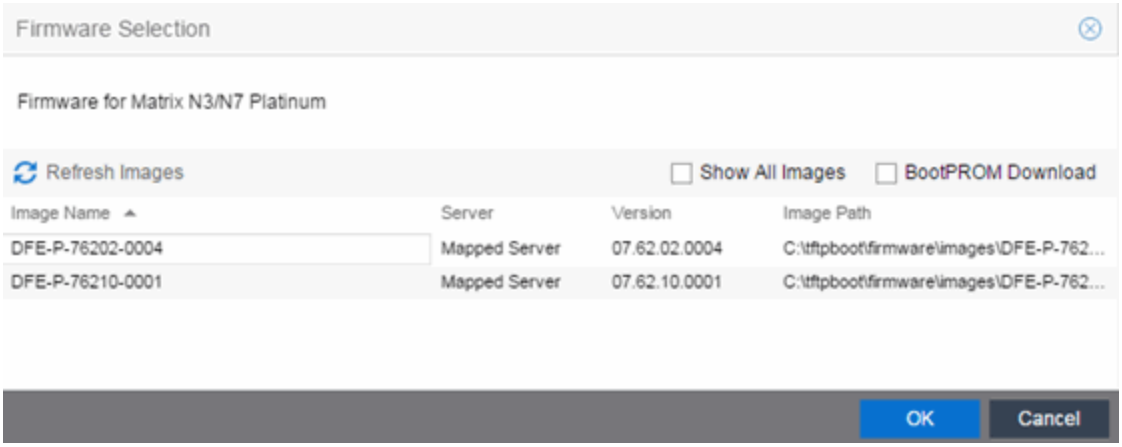
   NOTE: You can also right-click a single device in the left-panel and select **Upgrade Firmware**.

   The Upgrade Firmware window opens, displaying the devices you selected grouped by device family.



8. Select one or more devices and select **Assign Image**.

   The Firmware Selection window opens, displaying the firmware versions compatible with the device type.



9. Select the **Show All Images** checkbox to show all available firmware images.
10. Select the firmware image to download to the device.
11. After the upgrade operation completes, verify the boot PROM and firmware images on the device are compatible. Refer to the boot PROM and firmware release notes for more information. To upgrade the boot PROM, select the **BootPROM Download** checkbox in the Firmware Selection window. This clears any images already assigned and only displays boot PROM images for selection.
12. Select **OK**.
13. Repeat the process for all of the devices in the Upgrade Firmware window.

NOTE: Right-click the device in the **Upgrade Firmware** window to configure how the firmware is downloaded and installed on the device (e.g. to change the server from which the firmware image is downloaded, the file transfer method, or the MIB or script used to download the firmware image).

14. Select the **Restart Devices After Upgrade** checkbox to automatically restart devices that support restarting immediately after upgrading the firmware image.

NOTES:

Selecting the **Restart Devices After Upgrade** checkbox displays the Supports Restart column in the **Upgrade Firmware** window. A check mark indicates devices that support this functionality.

You can also restart a device manually in the **Restart Devices** window, accessible from the **Network** tab in ExtremeCloud IQ Site Engine by right-clicking the device and selecting **More Actions** > **Restart Device** option.

15. Select the **Schedule Upgrade** checkbox to run the firmware image upgrade at a future date. Selecting this checkbox displays additional fields where you can configure the scheduled upgrade.

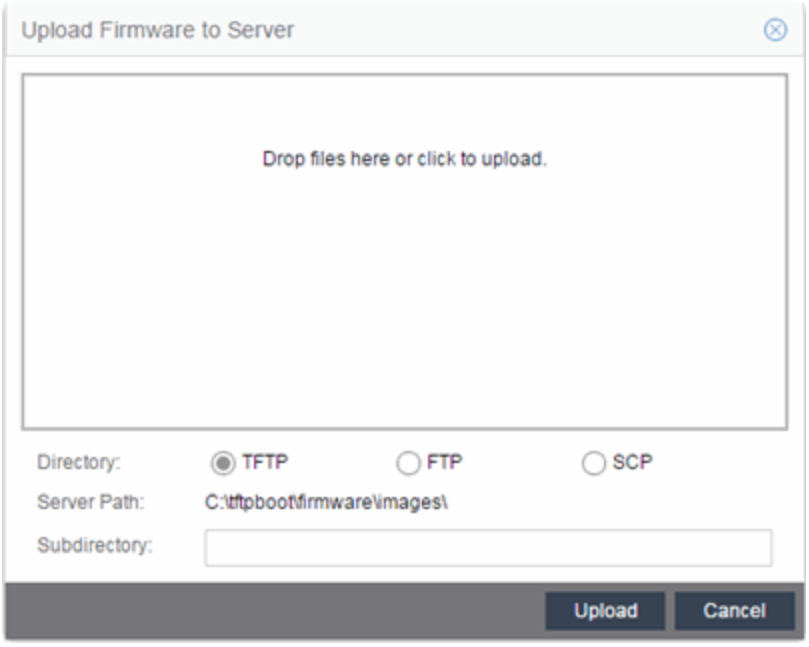
- **Name** — The name for the scheduled upgrade. The default name automatically populates with the creation date and time of the firmware upgrade.
- **Select Date** — The date and time the upgrade automatically runs. Enter a date in the mm-dd-yyyy format or select the **Calendar** icon to open a monthly calendar from which you can select the date of the upgrade. Enter the time for the scheduled upgrade or select the drop-down arrow to select the time from a drop-down list.
- **Abort on Failure** — Selecting this checkbox causes the upgrade to terminate in the event it is not successful.

16. Enter the number of downloads upgraded simultaneously in the **Device Upgrade Group Size** field. Enter a value of **1** to have the downloads performed serially (one device at a time).
17. Select **Start** if you are upgrading the firmware immediately or **Schedule** if the upgrade is scheduled for a future date.
    Note: To view or cancel a scheduled firmware upgrade, select **Tasks > Scheduled Tasks**.
18. If upgrading the firmware image immediately, a progress column appears on the **Upgrade Firmware** window. When the upgrade is complete, a Status section appears, displaying whether the upgrade occurred successfully.
19. Select **Close**.

Upgrading for a Device Type

To upgrade the firmware for all devices of a particular device type:

1. Open the **Network** tab.
2. Select the **Firmware** tab.
3. Select the device type from the Firmware tree in the left panel.
4. Upload the firmware or boot PROM image, if necessary.
    a. Select the **Upload** button to open the Upload Firmware to Server window from which you can save image files to the ExtremeCloud IQ Site Engine server.



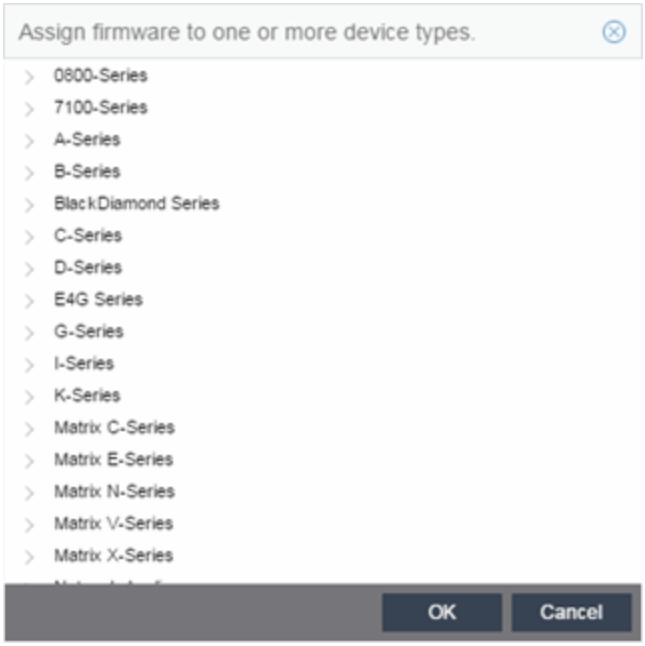
b. Drag the file or files into the box in the main part of the window or select the box to open a window from which you can navigate to the appropriate directory.

c. Select **TFTP**, **FTP**, or **SCP** to indicate whether you are upgrading the firmware or boot PROM image using a TFTP, FTP, or SCP server, respectively.

d. Type the Subdirectory within the Server Path where the firmware or boot PROM images are uploaded.

e. Select the **Upload** button.
A status bar displays over the file icon and a check mark indicates when the upload is complete. Anyone with access to ExtremeCloud IQ Site Engine is now able to download the image file to a device.

5. Right-click the firmware or boot PROM image from the Device Type Images section of the window and select **Assign Firmware** from the menu.
The Assign Firmware to One or More Device Types window appears.



6. Select the device type on which you are assigning the firmware or boot PROM image.
7. Select **OK**.

If you did not select **Restart Devices After Upgrade**, restart your devices.

Upgrading for Fabric Manager

To upgrade the firmware image for Fabric Manager, follow the instructions in Upgrading Fabric Manager.

Restart a Device

Use the **Devices** tab to restart a single device or multiple devices. The tab lets you restart devices that support Timed Restart as well as those devices that do not. Timed Restart lets you configure your restart operation with a time delay, so that the actual device restarts take place at a later time.

To restart a device:

1. Access the **Network** > **Devices** tab.
2. Use the left-panel drop-down list to select **All Devices**, **Maps**, or **Sites**, depending on the devices you are restarting. You can also use the drop-down list to select how the devices are organized (e.g. by IP address, by Device Type).
3. Select the **Devices** tab in the right-panel.
4. Select the device or devices you want to restart (using the **Ctrl** or **Shift** keys).
5. Select the **Menu** icon (☰) or right-click in the Devices list.

6. Select **More Actions** > **Restart Device**.

   NOTE: You can also right-click a single device in the left-panel and select **More Actions** > **Restart Device**.

   The **Restart Devices** window displays.

7. Select the devices you want to restart by selecting the checkbox in the **Selected** column.

   NOTE: The **Restart Devices** window contains additional fields for devices that support timed restart.

8. Select the date and time you want to restart the device for devices that support timed restart using the **Restart Time** fields. This field defaults to the current date and time, so to restart the devices now, do not change this field.
9. Select **Start** to initiate the device restarts or to schedule a future device restart. **Elapsed Time** displays the elapsed time since beginning the restart process.
10. Select **Finish** to close the window

Add a New Regime (Legacy)

The Compliance tab provides you with regimes that include predefined audit tests. You can also create your own regimes, composed of audit tests you can copy from existing regimes, or configure yourself.

To create a new regime:

1. Open the **Compliance** > **Audit Tests** tab.
2. Select the **Menu** icon (☰) and select **Add** > **Regime**.

   The Create Regime window displays.

3. Enter a **Regime Name**, describing the overarching standard or regulation against which you are testing compliance.
4. Enter a **Description** for the regime, if necessary.
5. Select **Test Wireless Events** to include wireless events in the ExtremeCompliance audit.

   NOTE: Because of the number of wireless events potentially stored by ExtremeCloud IQ Site Engine, wireless events are not included in an ExtremeCompliance audit the first time it is run. When the audit is run the first time, older wireless events are moved, so older events are not included in the results.

6. Select **Save**.

7. Copy existing audit tests to the new regime, if necessary.
    a. Right-click the audit test in left-panel and selecting **Copy Audit Test**.

       The **Copy Audit Test** window displays.
    b. Enter a new name for the audit test, if necessary.
    c. Select the new regime in the **Regime** drop-down list.
    d. Select the device type to which the audit test applies in the **Device Type** drop-down list.
    e. Select **Copy**.
8. Create your own audit tests.
    a. Select the **Menu** icon (☰) and select **Add** > **Audit Test**.
    b. Complete the fields in the **Audit Test Editor** tab to test for a device configuration.
    c. Complete the fields in the **Dependent Tests** tab, if necessary.
    d. Select **Save**.

Your custom regime is now available on the Compliance tab.

ZTP+ Device Configuration

Using Extreme Networks' ZTP+ (Zero Touch Provisioning Plus) functionality, you can quickly add new ZTP+-enabled devices to your network and configure them in ExtremeCloud IQ Site Engine.

Typically, when adding a new device to the network, a network administrator connects a console cable to the device to access the local console and manually configure the device.

IMPORTANT: Stacked ExtremeXOS/Switch Engine systems must be running ExtremeXOS/Switch Engine version 30.3 or later to support ZTP+ configuration.

In ExtremeCloud IQ Site Engine, new devices are automatically discovered on the network the moment they are connected. ZTP+-enabled devices send information to ExtremeCloud IQ Site Engine automatically, including the serial number, the number and speed of the ports, and the firmware version. When a ZTP+-enabled device is connected, you can add it to ExtremeCloud IQ Site Engine with minimal server configuration. In addition, the latest updates are automatically downloaded to the new device. This process minimizes the amount of time needed to configure a new device and deploy it on the network.

Prerequisites

Before connecting your devices, configure the following:

- Select the Reference Firmware Image Location
- Default Device Configuration in ExtremeCloud IQ Site Engine
- Download XMODs (ExtremeXOS/Switch Engine devices only)
- General Network Configuration
- NOS Persona Change from Switch Engine to Fabric Engine

Select the Reference Firmware Image Location

You can configure ExtremeCloud IQ Site Engine to automatically update your device's firmware and application versions. When upgrading the firmware image on your device, access the appropriate firmware image for your version from ExtremeNetworks.com and save it on your server to a directory you configure in ExtremeCloud IQ Site Engine. After the firmware image is saved on the ExtremeCloud IQ Site Engine server, it is available in ExtremeCloud IQ Site Engine and can be downloaded to the device.

For the device to recognize a new version is available, the firmware image must be downloaded from ExtremeNetworks.com to your server and saved in a directory you configure in ExtremeCloud IQ Site Engine.

To configure the file transfer directory:

1. Access the **Options** tab.
2. Select **Inventory Manager** in the left panel.
3. Enter the **Firmware Directory Path** in either the FTP Server Properties, SCP Server Properties, or TFTP Properties section of the right panel, depending on the file transfer settings used.
4. Download the latest firmware image for your device from ExtremeNetworks.com and save it in the specified directory.

When you download the firmware image from ExtremeNetworks.com and save it on the ExtremeCloud IQ Site Engine server, use the **Firmware** tab in ExtremeCloud IQ Site Engine to download the image from the ExtremeCloud IQ Site Engine server to the device.

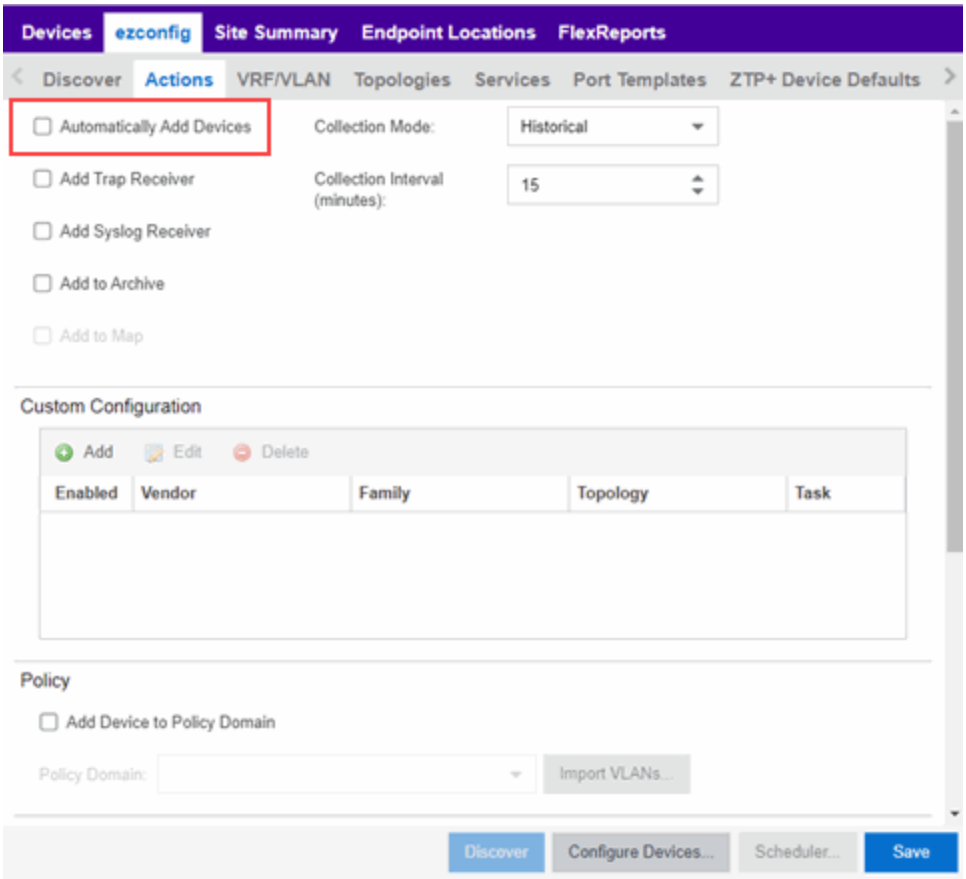
1. Access the **Network** > **Firmware** tab.
2. Expand the **Device Type** navigation tree in the left-panel for the device family you are configuring and select the folder for the type of device.
3. Right-click the firmware file you downloaded (specified in the section above) and select **Set as Reference Image**.

   Your device automatically updates with this firmware image when it restarts and is logged in the Event log with a **Category** of **Inventory**.

Default Device Configuration in ExtremeCloud IQ Site Engine

Before connecting your devices, you can configure the default settings that ExtremeCloud IQ Site Engine applies to all devices you add to the network. This is accomplished using the **Site** tab.

1. Access the **Devices** tab in ExtremeCloud IQ Site Engine.
2. Expand the World Site navigation tree and select the map in the left panel into which you are adding the devices.
3. Select the **Site** tab in the right panel.
4. Select the **Automatically Add Devices** checkbox in the Discovered Device Actions section and any other actions you want to occur on your devices discovered in ExtremeCloud IQ Site Engine.



5. Use the Custom Configuration section to automatically run a script on devices being added to the site, if necessary.

CAUTION:	If the script or workflow task selected for the Custom Configuration restarts the device, other actions selected to execute during discovery might not execute (for example, Add Trap Receiver).

6. Select **Add Device to Policy Domain** or **Add Device toAccess ControlEngine Group** to automatically add devices being added to the site to a Policy Domain or Access Controlengine group.
7. Add the VLANs that are used on your devices on the **VLAN Definition** tab by selecting the **Add** button and entering the **Name** and **VID**.
8. Use the **Port Templates** tab to create a port configuration, if necessary.
9. Enter the **Gateway Address**, **Domain Name**, and **DNS Server** address on the **ZTP+ Device Defaults** tab. Additionally, you can configure the NTP Server address and select the protocols to enable on your devices, if necessary.
10. Select **Save**.

    The default configuration for this site is complete and any devices you discover with this site selected use this criteria.

Download XMODs (ExtremeXOS/Switch Engine devices only)

XMODs are files that work in conjunction with firmware image upgrades to enhance ZTP+ functionality on ExtremeXOS/Switch Engine devices as well as provide bug fixes for existing features. Like firmware image upgrades, they are posted by Extreme Networks on github and ExtremeNetworks.com. Save XMODs in the directory you specify in the **Firmware Directory Path** field. Do not set an XMOD as the reference image.

IMPORTANT:	ExtremeXOS devices running version 21.1.1.4 require an update to the CloudConnector XMOD for ZTP+ to function properly. Save the most recent XMOD in the **Firmware Directory Path** specified above to update the device, allowing ZTP+ to function as intended. Recent ExtremeXOS/Switch Engine firmware images already include the CloudConnector XMOD, and no updates are required for ZTP+ functionality If multiple CloudConnector XMOD files exist in the same directory on the ExtremeCloud IQ Site Engine server as the reference image, ExtremeCloud IQ Site Engine downloads the XMOD file with the higher version number on the device.

General Network Configuration

In order for the switch to communicate to the ExtremeCloud IQ Site Engine server:

- The DHCP Server needs to return a DNS Server and Domain Name to the ZTP+ device.
- The DNS Server needs to map the name **extremecontrol.<*domain-name*>** to the IP address of the ExtremeCloud IQ Site Engine server.

NOS Persona Change from Switch Engine to Fabric Engine

You can configure the ExtremeCloud IQ Site Engine to change the persona of a switch from Switch Engine to Fabric Engine during the ZTP+ process. For a persona change to occur, you must:

- Upload the Fabric Engine firmware to both the TFTP and SFTP directories (Network > Firmware > Upload...)
- Configure the Fabric Engine firmware in the SFTP directory as a reference image
- Configure the NOS Persona Change field as **To Fabric Engine** for a specific site, or manually during the ZTP+ process

Adding the Device to the ExtremeCloud IQ Site Engine Database

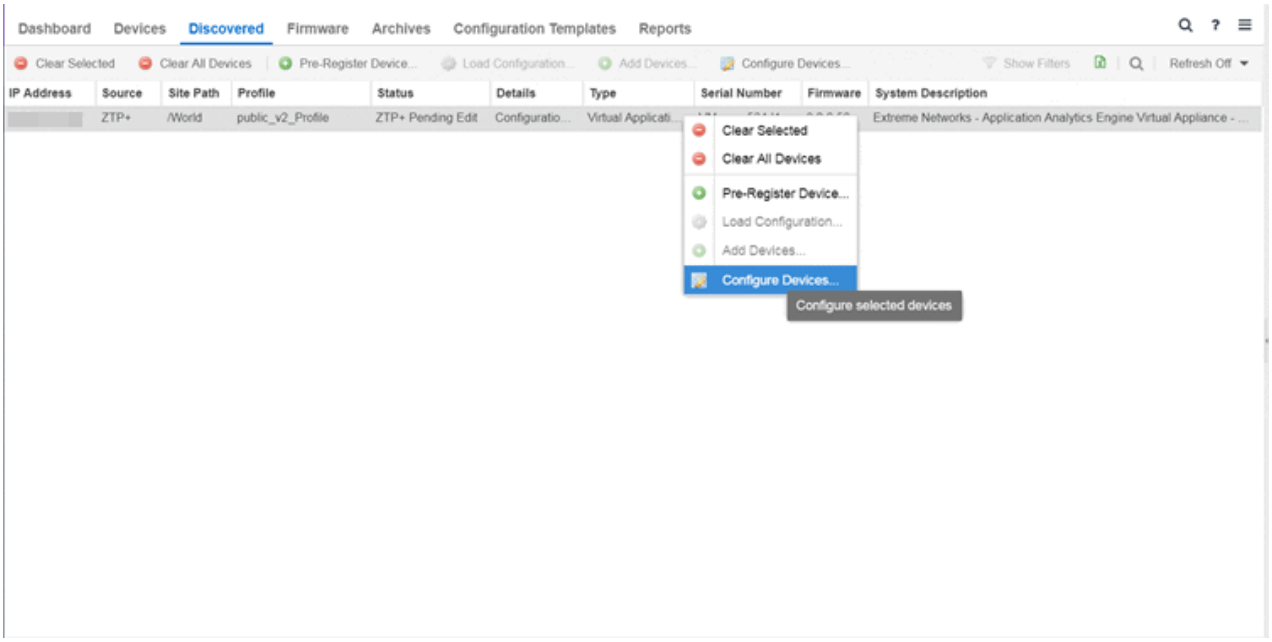
Now that the default criteria is configured for devices added to the World Site and you set up the DHCP and DNS servers allowing the device to communicate with the ExtremeCloud IQ Site Engine database, connect the device and add it to ExtremeCloud IQ Site Engine.

1. Connect the device to your network.

   ZTP+ enabled devices communicate with ExtremeCloud IQ Site Engine securely via an HTTPS connection and transmit information to ExtremeCloud IQ Site Engine, including the serial number, firmware version, MAC address, operating system, and port information. ExtremeCloud IQ Site Engine determines the status of devices and if new updates are available in the **Firmware** tab and set as Reference images, they are automatically installed.

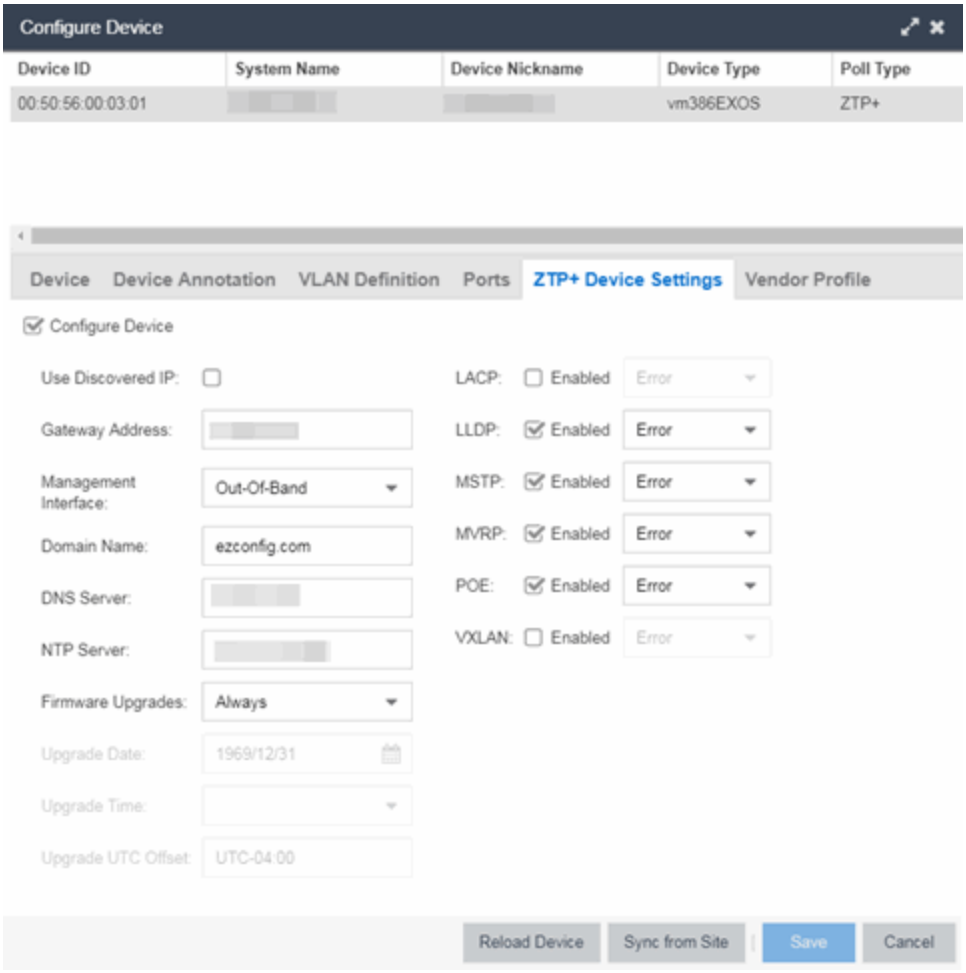
2. Open the **Discovered** tab in ExtremeCloud IQ Site Engine.

   The device is listed with a **Status** of **ZTP+ Pending Edit**, indicating the device configuration needs to be edited before adding it to the ExtremeCloud IQ Site Engine server.



3. Select the device and select the **Configure Devices** button.

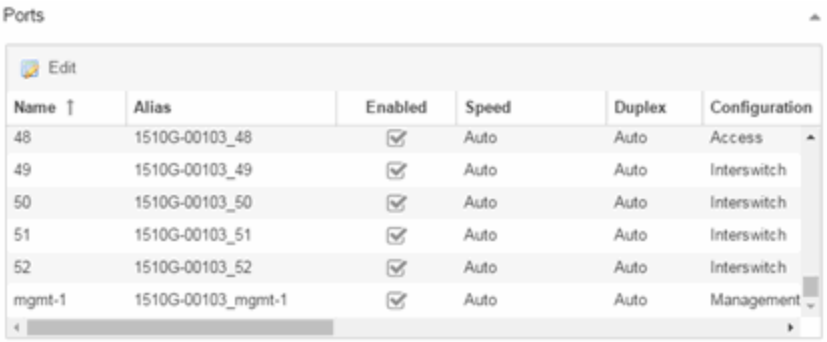
   The **Configure Device** window opens.



4. Select the **Default Site** for the device.
5. Select the **Poll Group** for the device, which indicates the frequency with which ExtremeCloud IQ Site Engine checks for new configurations or updates.
6. Select the appropriate **Poll Type**, which determines how devices are managed on your network:
   - **ZTP Plus** — Devices are polled using ZTP+ functionality.
   - **SNMP** — After devices are added to ExtremeCloud IQ Site Engine via ZTP+, devices are polled using SNMP and are managed manually.
7. Open the **ZTP+ Device Settings** tab.
8. Configure the fields on the **ZTP+ Device Settings** tab to determine how the device is managed by ExtremeCloud IQ Site Engine using ZTP+ functionality.
9. Open the Ports section of the window by selecting the section heading.

   The Ports section opens, displaying the ports transmitted by the device to ExtremeCloud IQ

Site Engine when connected to the network.



10. Select a port in the list to configure the port Name, Alias, Configuration, or port VLAN ID.

    You can also add and delete ports by selecting the **Add** and **Delete** buttons, respectively:

    a. Enter the port **Alias**.

    b. Select the port **Configuration**, which is its role or purpose for the device.

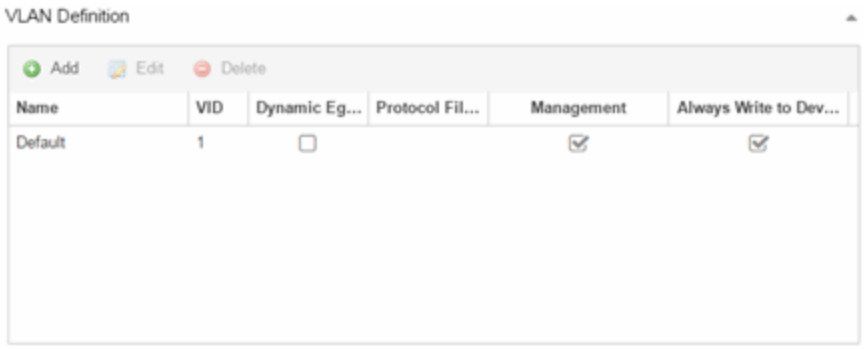
    - **Access** — The port provides access to end-systems.
    - **Interswitch** — The port connects the switch to another switch.
    - **Management** — The port is used to manage the network via ExtremeCloud IQ Site Engine.

    c. Enter a VLAN ID for the port in the **PVID** field.

    d. Configure the port **Speed** and **Duplex**.

11. Open the ZTP+ VLAN Definition section of the window by selecting the section heading.

    The ZTP+ VLAN definition section opens, containing any VLANs you configured on the **Site** tab.



12. Add any device-specific VLANs to those already included in the list by selecting the **Add** button.

13. Change any incorrect fields in the Device, Device Annotation, or Discovered Device Actions sections.
14. Select **Save** at the bottom of the window.

    The device is added to the ExtremeCloud IQ Site Engine database and moves from the **Discovered** tab to the **Devices** tab.

NOTES:

If you did not select **Automatically Add Devices** on the **Site** tab, the device remains on the **Discovered** tab with a **Status** of **ZTP+ Complete**. Select the device, select the **Add Devices** button (the **Add Device** window appears), and select the **Add** button to add the device to the ExtremeCloud IQ Site Engine database.

In the event a configuration is not correctly transmitted to the switch or if connectivity is lost during any part of this process, the device resets and allows the process to restart.

The device **Status** (displayed on the Discovered tab) is now **ZTP+ Staged**, indicating ExtremeCloud IQ Site Engine will push the configuration to the device the next time the device contacts ExtremeCloud IQ Site Engine.

When ExtremeCloud IQ Site Engine pushes the configuration to the device, the device **Status** is **ZTP+ Complete**.

ExtremeCloud IQ Site Engine generates an event indicating it is upgrading a device image, when the device image is upgraded to the latest version, and when a configuration is sent to a device.

ExtremeAnalyticsEngine ZTP+ Configuration

Using Extreme Networks' ZTP+ (Zero Touch Provisioning Plus) functionality, you can quickly add new ExtremeAnalyticsengines to your network and configure them in ExtremeCloud IQ Site Engine.

IMPORTANT: Logging in to the engine and running the initial engine configuration script will result in the ZTP+ configuration process being shutdown.

Once ZTP+ enabled devices are configured and connected in ExtremeCloud IQ Site Engine, you can view important data and flow collector information on the **ExtremeAnalytics** tab.

General Network Configuration

In order for the engine to communicate with the ExtremeCloud IQ Site Engine server:

- The DHCP Server needs to return a DNS Server and Domain Name to the ZTP+ device.
- The DNS Server needs to map the name **extremecontrol.<*domain-name*>** to the IP address of the ExtremeCloud IQ Site Engine server.

Once ExtremeCloud IQ Site Engine and the ZTP+ device are pre-configured, you can add the site definition to the ExtremeCloud IQ Site Engine database.

Adding the Device to the ExtremeCloud IQ Site Engine Database

When the default criteria is configured for devices added to the World Site and you set up the DHCP and DNS servers allowing the device to communicate with the ExtremeCloud IQ Site Engine database, connect the device and add it to the Discovered tab.

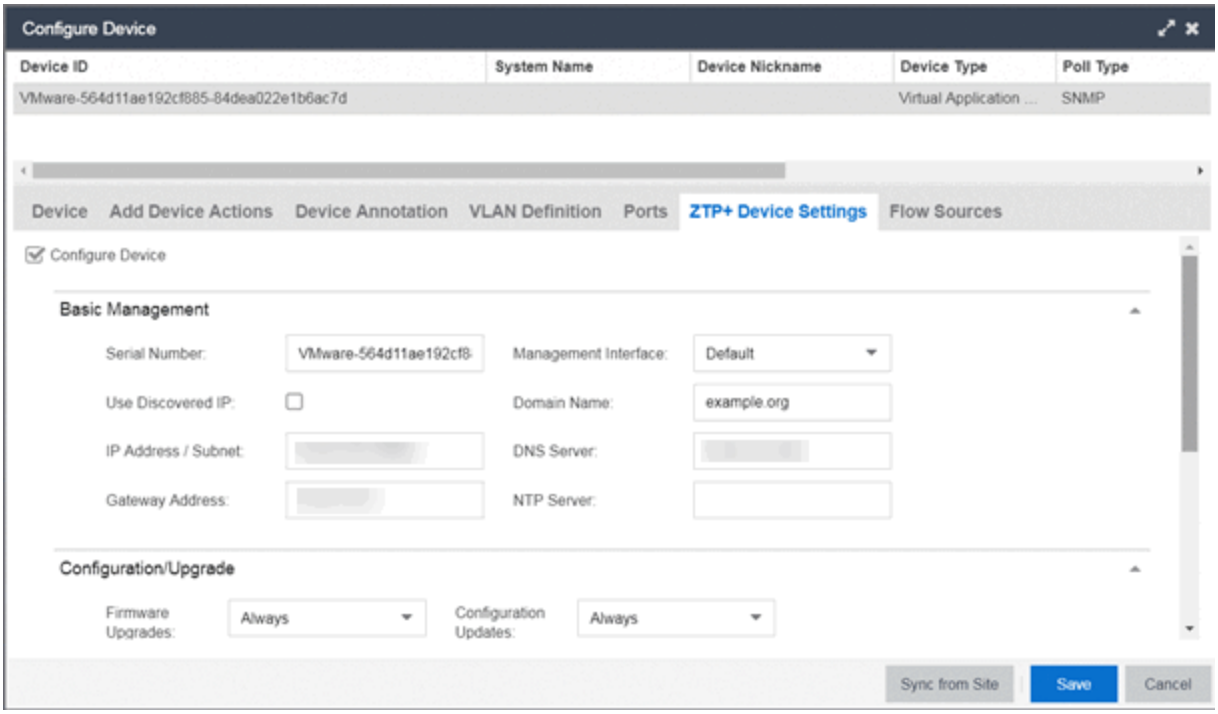
1. Open the **Discovered** tab in ExtremeCloud IQ Site Engine.

   The device is listed with a **Status** of **ZTP+ Pending Edit**, indicating the device configuration needs to be edited before adding it to the ExtremeCloud IQ Site Engine server. Add the ZTP device settings and the flow source information.

2. Right-click the device and select **Configure Devices** tab from the drop-down list.

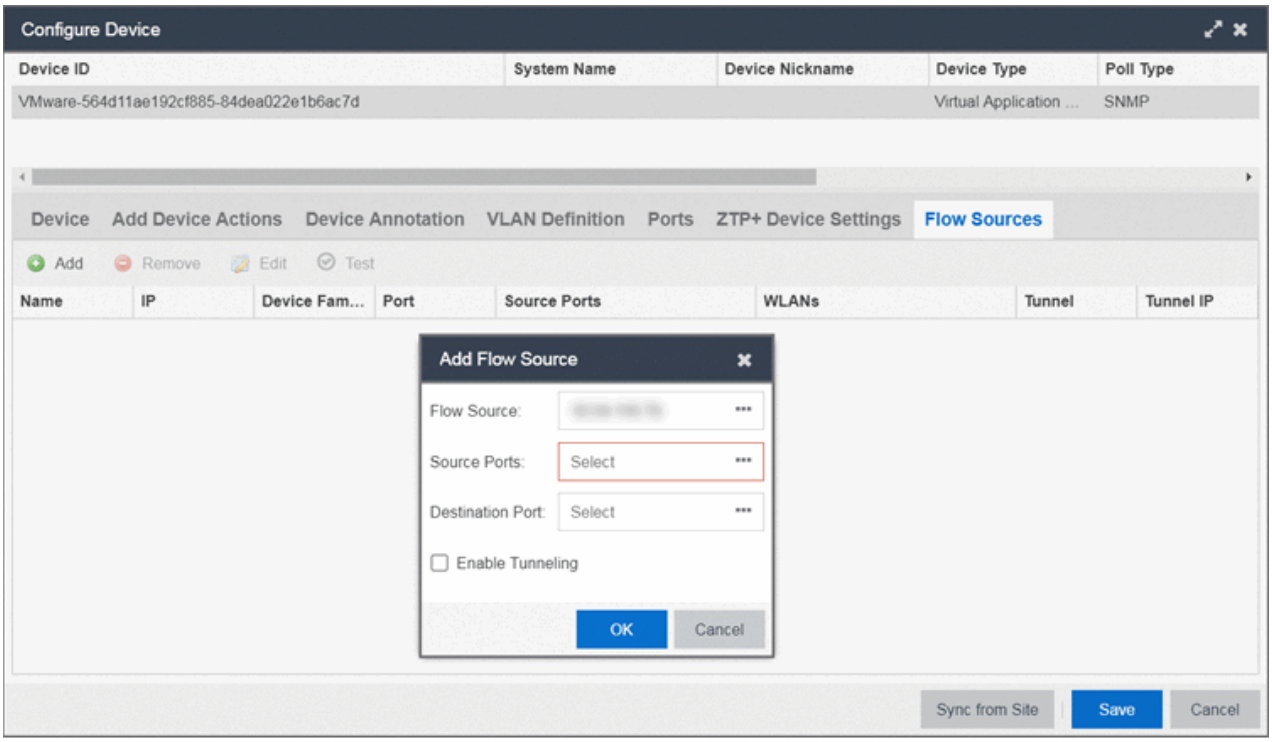
   The **Configure Device** window opens.

3. Select the **ZTP+ Device Settings** tab.



4. Configure the fields on the **ZTP+ Device Settings** tab to determine how the ExtremeAnalyticsengine is managed by ExtremeCloud IQ Site Engine using ZTP+ functionality.

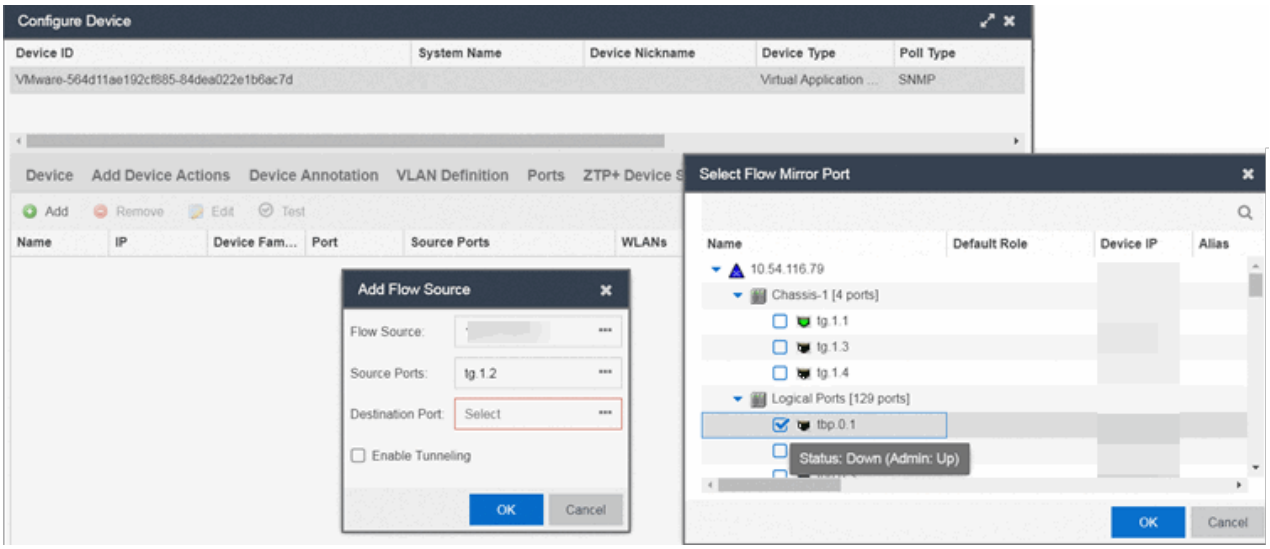
5. Select the **Flow Sources** tab in the **Configure Device** window.



6. Select the ExtremeAnalyticsengine flow information.
    1. Select the **Add** ( ) button.

       The **Add Flow Source** window displays.
    2. Select **FC-180** from the **Flow Source** drop-down list.
    3. Select the **Source Ports** from the drop-down list.

4. Select the **Destination Port** from the drop-down list.



5. Select the **Enable Tunneling** checkbox.
6. Select the **Tunnel IP** address from the drop-down list.
7. Select **OK** to complete the Flow Source configuration.

NOTES:

If you did not select **Automatically Add Devices** on the **Site** tab, the ExtremeAnalyticsengine remains on the **Discovered** tab with a **Status** of **ZTP+ Complete**. Select the engine, select the **Add Devices** button (the **Add Device** window appears), and select the **Add** button to add the engine to the ExtremeCloud IQ Site Engine database.

In the event a configuration is not correctly transmitted to the switch or if connectivity is lost during any part of this process, the engine resets and allows the process to restart.

Completing Configuration and Enforcing the Engine in ExtremeAnalytics

The engine**Status** (displayed on the Discovered tab) is now **ZTP+ Staged**, indicating ExtremeCloud IQ Site Engine will push the configuration to the device the next time the device contacts ExtremeCloud IQ Site Engine.

Open the **Configuration** tabConfiguration tab. The engine is configured with the ZTP+ enabled device and is displayed in the **Overview** window. Enforce the engineEnforce the engine to complete the process.

PortView

PortView is an ExtremeCloud IQ Site Engine component that provides port analysis and troubleshooting information including NetFlow data and ExtremeControl end-system details, for your network wired and wireless devices.

The primary launch point for PortView is from the ExtremeCloud IQ Site Engine Search. Depending on the type of item you are searching for, one or more PortView tabs display with information pertaining to your search item. You can also launch PortView from other locations in ExtremeCloud IQ Site Engine.

PortView lets you:

- View a topological display of device relationships.
- Analyze flow details, applications, senders, and receivers.
- Analyze real-time status, utilization, errors, and packets for a port.
- View the map of devices to which the end-system is connected.
- Analyze historical utilization and availability for a port.
- View all end-systems attached to a port and critical end-system information.

This Help topic provides the following PortView information:

- Requirements
  - License and Data Collection Requirements
  - Access Requirements
- Launching PortView
  - Launching from ExtremeCloud IQ Site Engine
  - Launching from Console
  - Launching from NAC Manager

Requirements

License and Data Collection Requirements

The information provided in each report depends on the selected switch and the report data collections you configure. For information on configuring data collection, see Enable Report Data Collection.

The following chart describes the complete set of PortView reports and provides the data collection requirements for each report (if applicable). Some of these reports are available as PortView tabs, others are launched from the right-click menu in the graphical Overview report.

PortView Report	Description	Requirements
Overview	Topological display of device relationships.	
Application Summary	View reports that present a summary of application information.	
Details	The tabs within the report contain the following information: Access Profile — Displays an interactive fingerprint containing information about the end-system. Select an icon to open additional details. End-System — View information about the end-system. End-System Events — View the Access Control Dashboard end-system events table filtered to display all events for the end-system based on the MAC address. Health Results — Displays risk information for the selected end-system.	Switch must have Access Control authentication enabled.
Map	Displays the map containing the device to which the end-system is connected.	
Sessions	The tabs within the report contain the following information: Interface History — Historical interface utilization and availability. Client History — Historical statistics for wired or wireless clients. End-System Events — View the Access Control Dashboard end-system events table filtered to display all events for the end-system based on the MAC address. NetFlow — NetFlow data for the selected port.	Requires active interface statistics collection. Client statistics collection must be enabled. Switch must have Access Control authentication enabled. The switch must support NetFlow and flow collection must be enabled on the port.
Network Information	The tabs within the report contain the following information: Wireless Details — Presents controller, AP, or client information, depending on your search. Interface Details — Real-time interface status, utilization, and errors. AP History — Contains historical data for your APs. Switch Resources — Switch CPU and memory utilization statistics. Device Resources — Device CPU and memory utilization statistics.	Requires active device statistics collection. Requires active device statistics collection.

Access Requirements

Access to PortView reports is determined by the user's membership in an ExtremeCloud IQ Site Engine authorization group and the group's assigned capabilities. The following table lists the capabilities required for access to the different PortView reports.

PortView Report	Required Capability
Network Information Interface History Client History Client Event History Switch History Controller History	XIQ-SE OneView > Access OneView or XIQ-SE OneView > Access OneView and Access OneView Administration
Sessions > NetFlow	XIQ-SE OneView > NetFlow Read Access
Modify Flow Collection	XIQ-SE OneView > NetFlow Read/Write Access
Map	XIQ-SE OneView > Maps > Maps Read Access or Maps Read/Write Access
Details Sessions > End-System Events	XIQ-SE OneView > Access Control > OneView End-Systems Read Access or XIQ-SE OneView > Access Control > OneView End-Systems Read/Write Access

Launching PortView

You can launch PortView from a variety of locations in ExtremeCloud IQ Site Engine. By default, you can have five active PortView searches displayed in ExtremeCloud IQ Site Engine at one time. You can change this display limit in the **Maximum PortViews Displayable** field in Site Engine - General (Administration > Options > Site Engine - General > Session Limits).

NOTE: A single PortView search returns a maximum of five matching results. If the number of matching results exceeds five, an error message appears asking you to refine the search term and try again.

Launching from ExtremeCloud IQ Site Engine

ExtremeCloud IQ Site Engine Search Tab

The primary launch point for PortView is from ExtremeCloud IQ Site Engine Search. The Search page provides a search field where you can enter a MAC address, IP address, host name, AP serial number, or Access Control custom field information to begin searching. Depending on the type of item for which you are searching, the search results return one or more PortView tabs, with information pertaining to your search item. You can right-click on the different devices in the topology results to launch additional reports.

1. Open the **Search** tab.
2. Enter a MAC address, IP address, host name, AP serial number, or Identity and Access custom field information, and press **Enter** to begin the search. You can copy the IP or MAC address from another source and enter it into the **Search** field. For example, you can copy an end-system MAC address from the **Control** tab End-Systems view, and then paste the MAC address into the search field and press **Enter**.

3. Depending on the type of item for which you are searching, the secondary navigation bar displays one or more PortView tabs, with information pertaining to your search item, similar to the search results shown below.

ExtremeCloud IQ Site Engine Interface Summary FlexView

Use the following steps to launch PortView from an ExtremeCloud IQ Site Engine Interface Summary FlexView.

1. On the **Network** tab, select on the device Name link to open the Interface Summary FlexView.
2. In the Interface Summary, select the interface Name or Alias link to open PortView.

Launching from Console

You can launch PortView from Console using any of the following methods:

- In the **Port Properties** tab, right-click on one or more ports and select **Port Tools** > **PortView**.
- In the Compass Results table, right-click on up to four entries and select **Port Tools** > **PortView**.
- In the Interface Summary FlexView, right-click on one or more ports and select **Port Tools** > **PortView**.

Launching from NAC Manager

You can launch the PortView Access Control reports from NAC Manager using either of the following two methods:

- In the **End-Systems** tab, right-click on an end-system in the table and select **PortView** from the menu.
- On the **Control** tab's End-Systems view, right-click the entry with the desired switch port and select **PortView** from the menu.

AP Wireless Real Capture

Real Capture allows real-time collection of Access Point (AP) wireless traffic for troubleshooting and problem resolution. Real Capture collects traces on the AP wireless interface and transmits them to Wireshark running on a local Windows client. It allows Wireshark to capture RF/wireless traffic as if it were running directly on the AP, providing visibility into network connectivity and performance issues. All Wireshark features are supported, including filters and I/O graphs.

NOTE: APs must be running firmware version 8.x or later. The AP2600 series of Access Points does not support the Real Capture feature.

Real Capture can be enabled for each AP individually from PortView in the ExtremeCloud IQ Site Engine. When it is enabled, Real Capture runs a daemon on the AP that allows it to interface with Wireshark using port 2002 or 2003. The AP then captures all the wireless traffic (except for management traffic) originating from the AP and sends it to Wireshark for analysis.

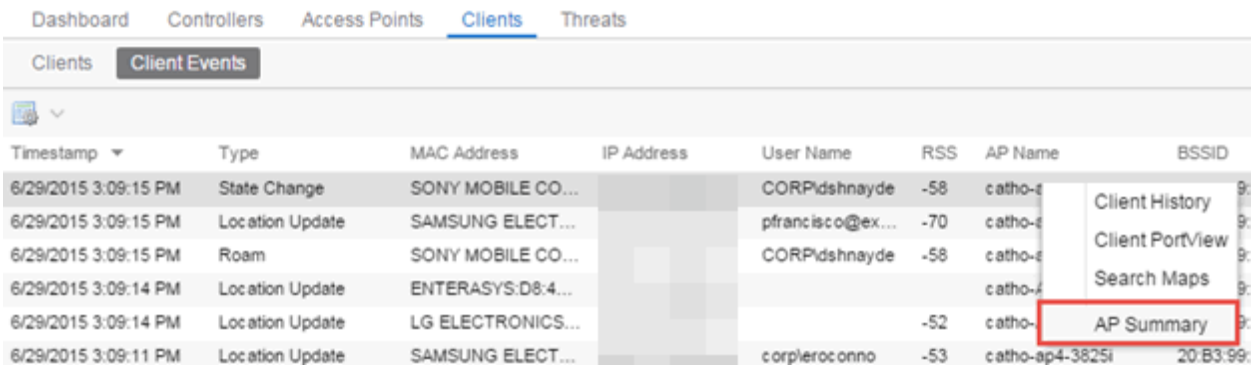
In addition to capturing network traffic for analysis in Wireshark, the AP also collects RF information. The RADIOTAP header format delivers RF information. You must use Wireshark 1.6 or later to read the full RADIOTAP header information. For troubleshooting features like TxBF/STBC, you can enable capturing the 802.11n preamble header using the AP CLI commands.

NOTE: When capturing client traffic on the AP, if the topology is bridged at AP, client traffic is captured and can be analyzed in the resultant trace. However, if the topology is bridged at controller, only WASSP traffic is captured as the AP tunnels this communication back to the controller. This traffic must be sent to the Extreme Networks Support for analysis because it needs to be decoded. In this scenario, it may be better to mirror the switch port where the controller connects to the LAN.

Configure and Use Real Capture

Use the following steps to configure and use the Real Capture feature.

1. Launch ExtremeCloud IQ Site Engine.
2. Launch PortView for the AP from the Wireless Client Event History report.
    a. Select the **Wireless** tab and then select the **Clients** tab and the **Client Events** sub-tab. Right-click on the AP Name and select **AP Summary** from the menu.

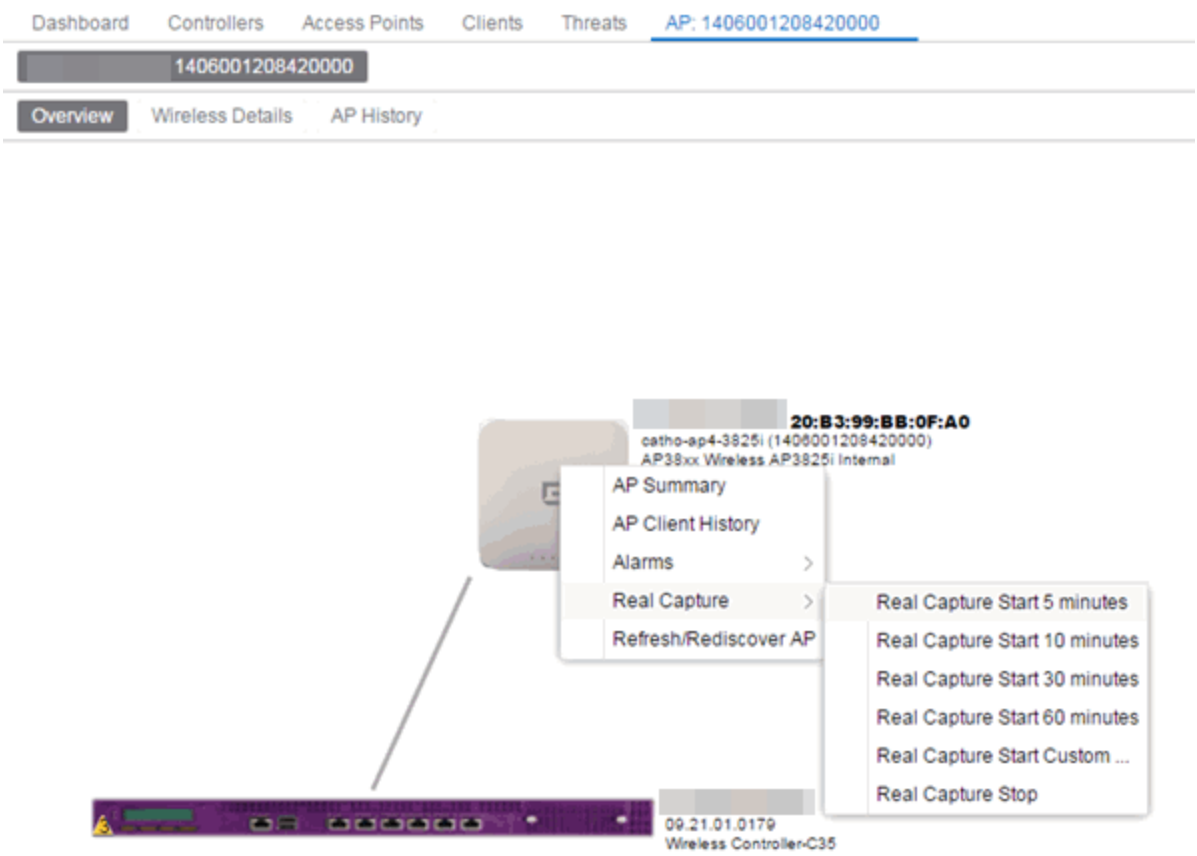


b. The AP PortView opens.

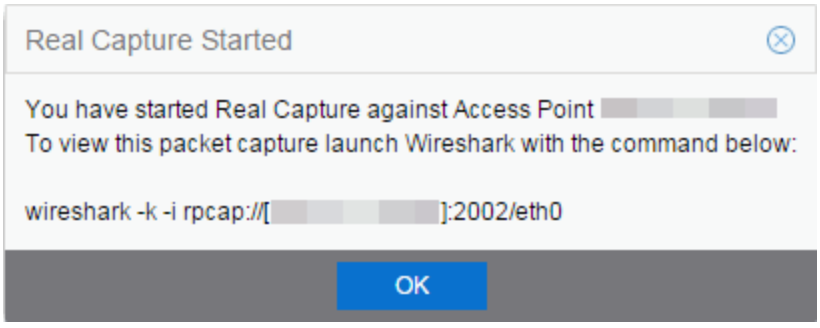


NOTE: You can also launch PortView for the AP using the **Search** tab. Open the **Search** tab, enter the search criteria (MAC, IP, hostname, or AP serial number) and press **Enter** to display the AP PortView.

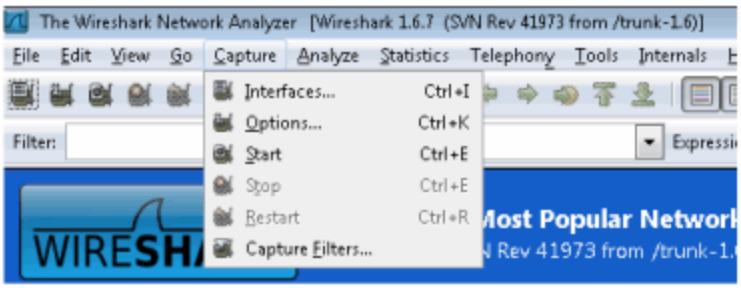
3. Right-click on the AP in the PortView topology display and select **Real Capture** > **Real Capture Start xx minutes**. Select the desired amount of time to run the capture or create a custom capture duration value. If you need to, you can stop the Real Capture by selecting **Real Capture Stop**.



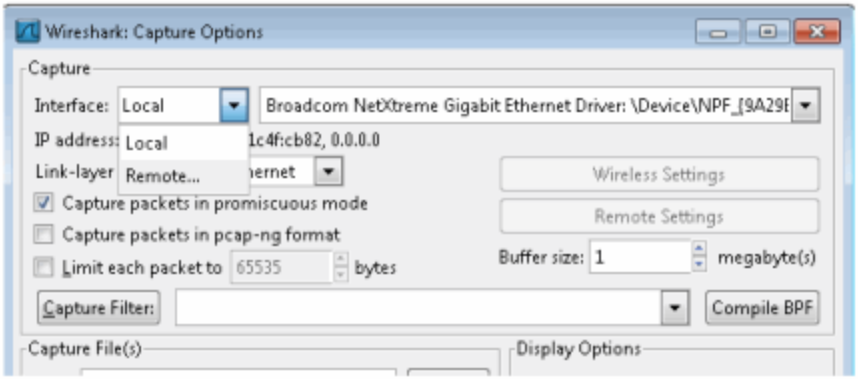
4. A message appears to inform you Real Capture has started, and provides a CLI command you can use on a client on which Wireshark is installed, to launch Wireshark against the AP and view the captured traffic.



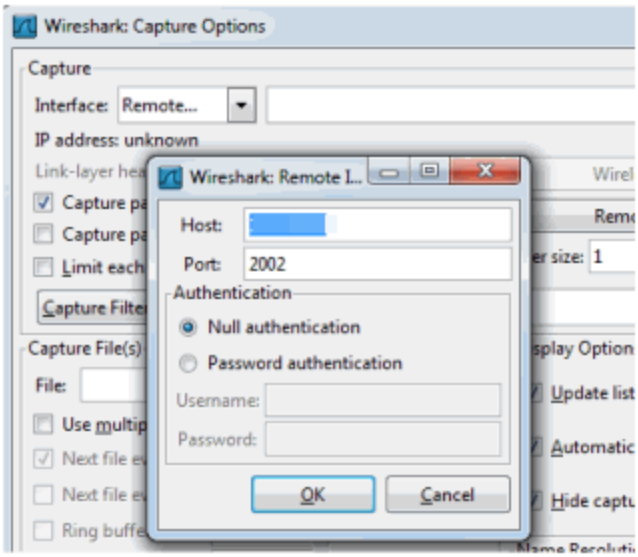
5. You can also access the captured traffic in Wireshark using the following steps:
   a. In Wireshark, select **Capture** > **Options** from the menu bar.



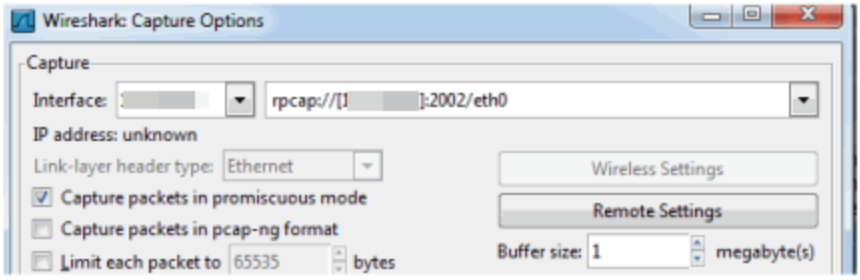
   b. In the Capture Options window, set the **Interface** value to **Remote**.



   c. The Remote Interface window appears. Enter the AP's IP address in the **Host** field, and the port number (2002 or 2003) in the **Port** field (you can see this information in the CLI command message described in step 4). In the Authentication section, select **Null authentication**. Select **OK**.



d. Wireshark adds the command information to the Capture options.

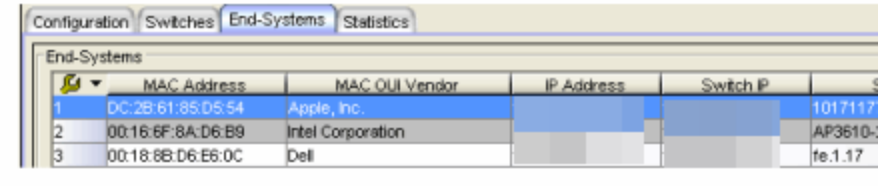


e. Select **OK** in the Capture Options window to begin viewing the captured traffic in Wireshark. When you have the data you need, you can stop the capture and save it to a file for further diagnosis and troubleshooting.

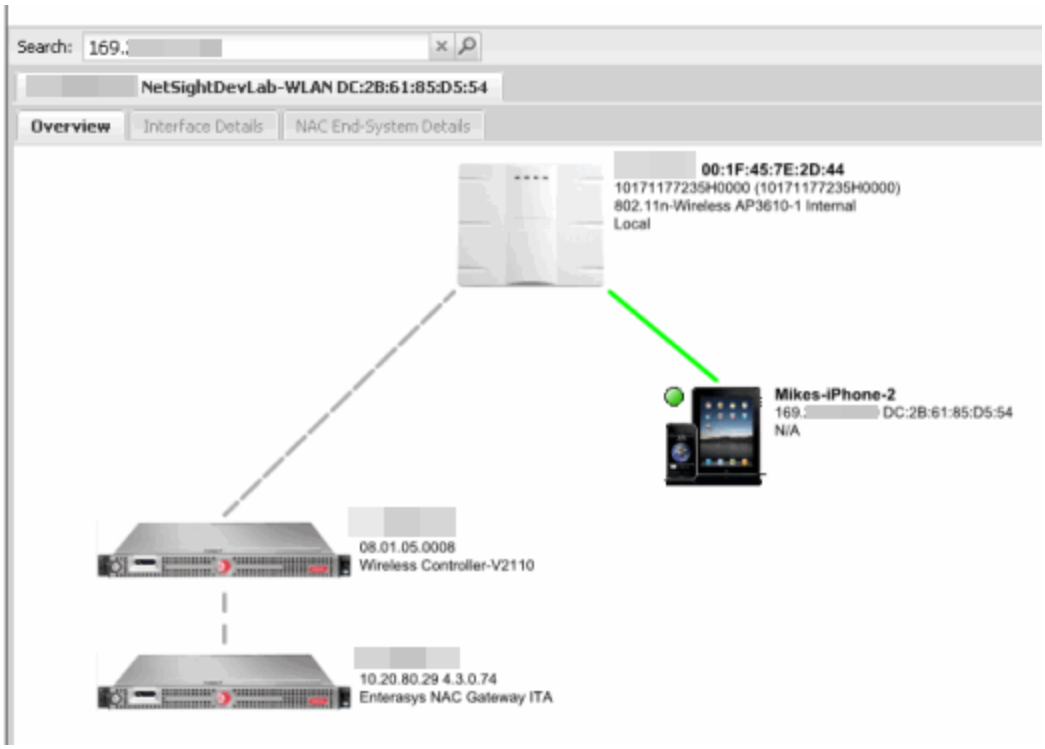
Real Capture Example

The following example shows how to use Real Capture to diagnose an end-system connection problem in NAC Manager.

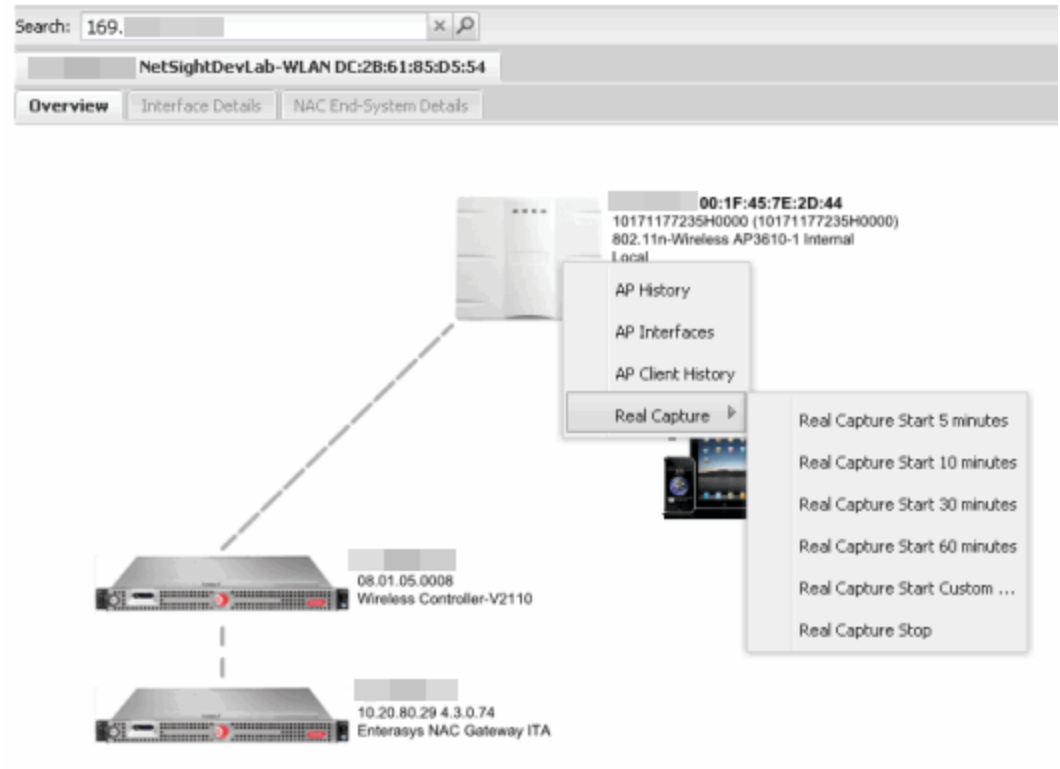
The problem starts when an end-system in NAC Manager is not able to obtain an IP address.



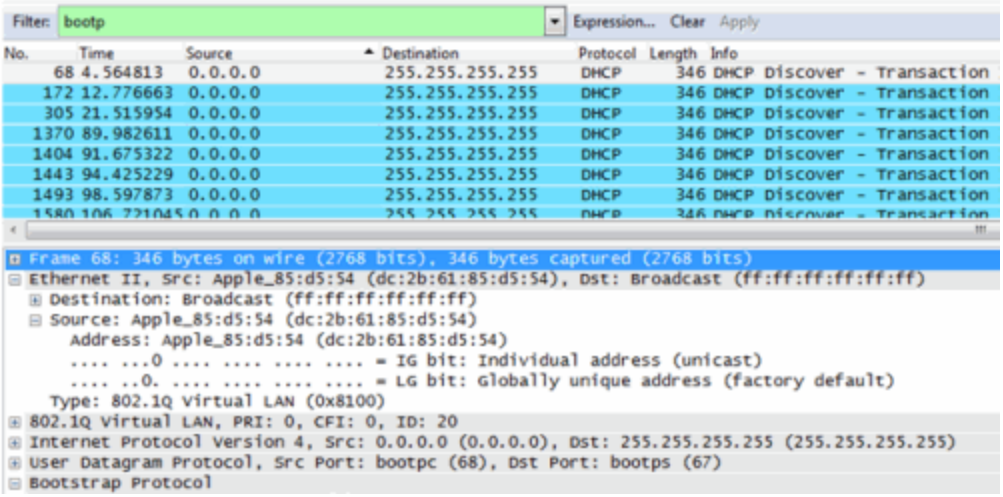
A search is performed on the 169.x.x.x IP address.



The traffic capture is started on the AP to which the end-system is connected.



The resulting trace in Wireshark shows the end-system sending out DHCP Discover packets with no response, perhaps indicating a VLAN or network-related issue.



Restoring the Database Using the CLI

Use the instructions in this topic to restore an ExtremeCloud IQ Site Engine database backup using the CLI (command line). Restoring a database using the CLI may be necessary after making significant unwanted configuration changes.

NOTE:

For ExtremeCloud IQ Site Engine 24.2 and earlier, a database backup created by the Backup/Restore procedure, with **Back Up Alarm**, **End-System Event**, and **Reporting Database** enabled, is required prior to running the following database restore procedure. This procedure does not work if **Back Up Alarm**, **End-System Event**, and **Reporting Database** are disabled.

In release 24.2 and earlier, the backup script is `mysqlbackup_restore.sh`

The restore runs using the `backup_restore` script in the *<install directory>*`/scripts` directory.

To restore the backup from another instance of ExtremeCloud IQ Site Engine, the backup needs to be transferred first. The content of `<install directory>/backup>` including subdirectories should be transferred to the new instance. To restore the ExtremeCloud IQ Site Engine database backup:

1. Ensure you are running the **same version** of ExtremeCloud IQ Site Engine used when creating the database backup on the ExtremeCloud IQ Site Engine server.
2. Log into the system shell (via the local console or SSH) on the ExtremeCloud IQ Site Engine server as root.

3. Navigate to the scripts directory:
   - Enter `cd <install directory>/scripts`.
4. Run the backup_restore script:
   - Enter `./backup_restore.sh <full backup directory structure configured on tab, including path>`

     (for example, `./backup_restore.sh /usr/local/Extreme_Networks/NetSight/backup/xiqse_03302021/`).

NOTE: If you restore a backup for troubleshooting purposes, disable the connection to ExtremeCloud IQ to prevent influencing the production statistics. The restoration script will offer you the option to disable the connection to ExtremeCloud IQ.

For air gap deployment mode, the option to disable the ExtremeCloud IQ connection is not relevant.

The database backup is restored. Devices onboarded to ExtremeCloud IQ after the backup was created become orphaned when the database restore is finished. Manual deletion of orphaned devices in ExtremeCloud IQ might be needed.

IMPORTANT: The deployment mode (connected or air gap) is part of the database backup. Restoring from the backup will not change the deployment mode. The serial number is part of the database backup. Restoring the backup also restores the serial number. The air gap license file is bound to the serial number. Neither license keys nor license files are part of the database backup.

In Connected deployment mode, the following sequence is recommended:

1. Delete ExtremeCloud IQ Site Engine from ExtremeCloud IQ
2. Wait for all devices managed byExtremeCloud IQ Site Engine to disappear from ExtremeCloud IQ
3. Restore the backup of ExtremeCloud IQ Site Engine
4. Onboard ExtremeCloud IQ Site Engine to ExtremeCloud IQ

If you are restoring the backup to a clean installation, license files and license keys should be inserted into ExtremeCloud IQ Site Engine after the restore.

Restore Device Configuration

On the **Network** tab, you can easily restore a device configuration to an active network device using a "cloned" configuration from an existing network device or a configuration template created on the

Network > **Devices** tab. In addition, you also have the ability to download the latest firmware on the active device.

This Help topic provides the following information:

- Preliminary Steps
  - Required Capabilities
  - Device Firmware
- Restoring a Configuration
  - Using a Configuration Template
  - Cloning a Device Configuration

Preliminary Steps

Required Capabilities

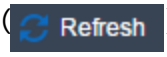
In order to perform the restore configuration operation, you must be a member of an authorization group with the following capabilities.

Required Capability
Inventory Manager > Firmware/Boot PROM Management > Firmware/Boot PROM Upgrade Wizard
Inventory Manager > Configuration Archive Management > Archive Restore Wizard
Inventory Manager > Configuration Templates Management > Configuration Templates Download Wizard
XIQ-SE Suite > Devices > Add, Discover, and Import

Device Firmware

If you are updating the device's firmware, you must first add the new firmware version to the left-panel Firmware folder on the **Network** > **Firmware** tab. It is then available when configuring the device.

For information on obtaining firmware, contact your Extreme Networks representative, or access the firmware download library at: https://extremeportal.force.com/.

1. Place your new firmware in your firmware directory. ExtremeCloud IQ Site Engine uses the default tftpboot\firmware\images directory for storing your firmware.
2. In the left-panel Firmware folder, select the **Refresh** icon (

). ExtremeCloud IQ Site Engine automatically adds your new firmware to the appropriate firmware groups in the left-panel Firmware folder.

The new firmware version is available when configuring the device in ExtremeCloud IQ Site Engine.

Restoring a Configuration

When restoring a configuration to an active device, there are two options for selecting a configuration to use. One option is to "clone" an existing device on the network for a configuration. Another option is to use a Configuration Template you create.

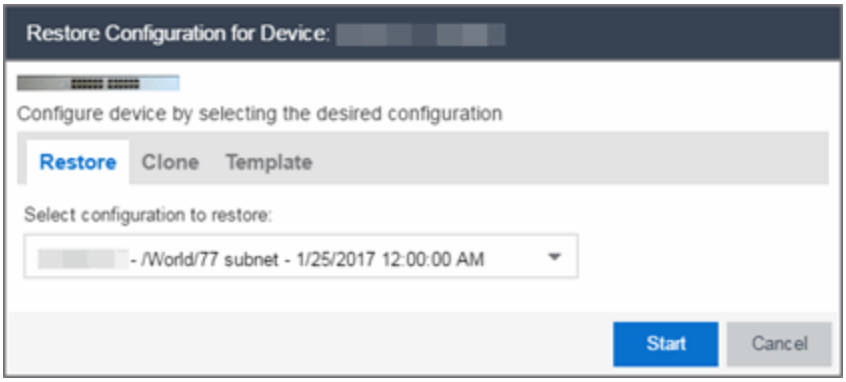
Cloning a device configuration is useful when you want to use the exact same configuration on another device. If you are cloning a device configuration, you must have an existing configuration for that device archived.

Using a configuration template allows you to restore a complete or partial configuration to the device with variables you can define specifically for that device. If you are going to use a configuration template for your device, you must create the Configuration Template to use as the source configuration for a device.

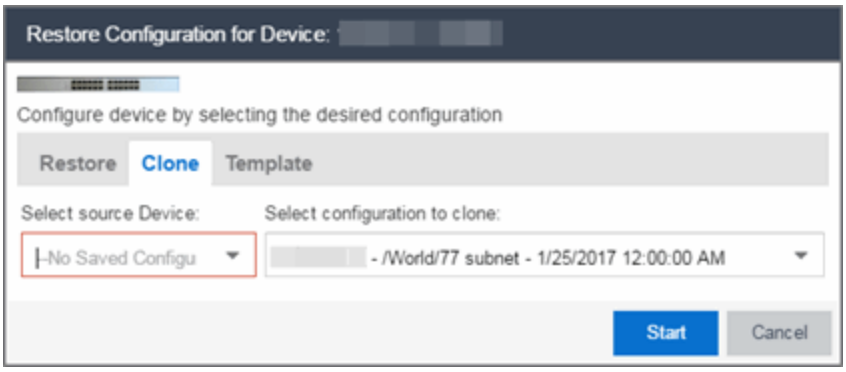
Cloning a Device Configuration

When cloning a device configuration, use an existing configuration of a network device archived in ExtremeCloud IQ Site Engine. The cloned device (the archived device you are using) must **not** be active on the network to prevent two devices from having the same IP address on the network.

1. Launch ExtremeCloud IQ Site Engine. On the **Network** > **Devices** tab, right-click on the active device and select **More Actions > Restore Configuration**. The Restore Configuration window opens.



2. Select the **Clone** tab.

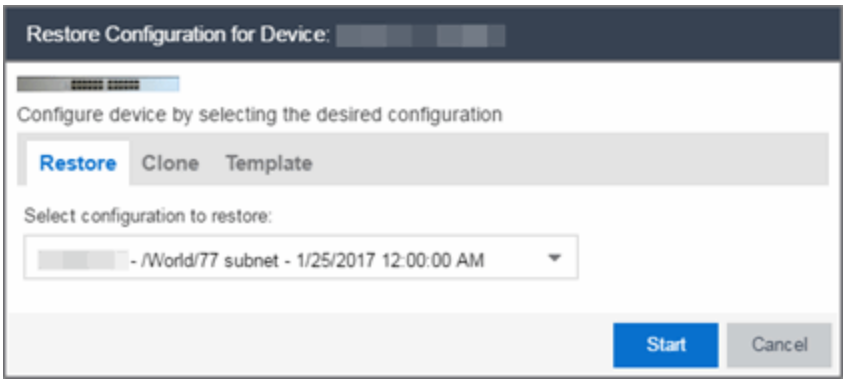


3. If desired, select a new version of firmware to download to the device. (You must add the new firmware version to ExtremeCloud IQ Site Engine. For more information; see "Device Firmware".)
4. Select the Device option as the Configuration Source.
5. Select the source device for the configuration. The selected device must be Inactive on the network or you cannot perform the restore operation. This prevents two devices from having the same IP address on the network.
6. Select the archived device configuration to clone.
7. Select **Start**. First, the firmware is updated (if that option is selected) and then the configuration is loaded and the device is restarted.

Using a Configuration Template

The following steps describe how to use a configuration template as the source configuration for a device.

1. Launch ExtremeCloud IQ Site Engine. On the **Network** > **Devices** tab, right-click on the active device and select **More Actions > Restore Configuration**. The Restore Configuration window opens.



2. Select the Template option as the Configuration Source.

3. Select the appropriate template from the **Template** drop-down list and enter the required variables.
4. Select the **Profile** for the new device from the drop-down list.
5. Select **Start**. The configuration is loaded and the device is restarted.

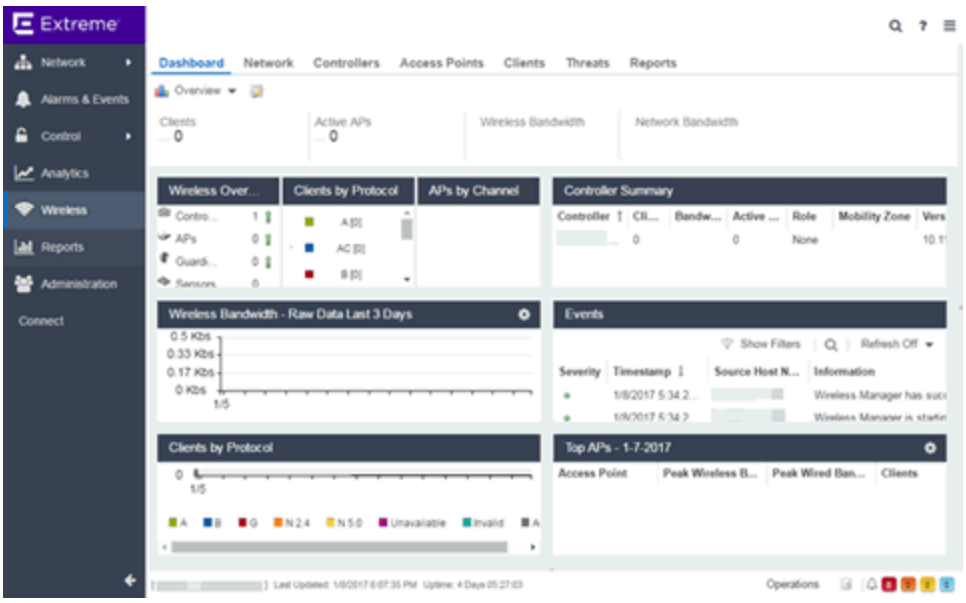
Configuring Enhanced Netflow for Extreme Analytics and Extreme Wireless Controller Version 10.21 in ExtremeCloud IQ Site Engine

When adding a Wireless Controller as a flow source in ExtremeCloud IQ Site Engine, a mirror port is automatically created. Wireless Controllers on which a firmware version of 10.21 or higher is installed use IPFIX, so the mirror port is unnecessary.

NOTE: Wireless Controllers on which a firmware version lower than 10.21 is installed still require the mirror port be configured.

To remove a mirror port on a Wireless Controller running version 10.21:

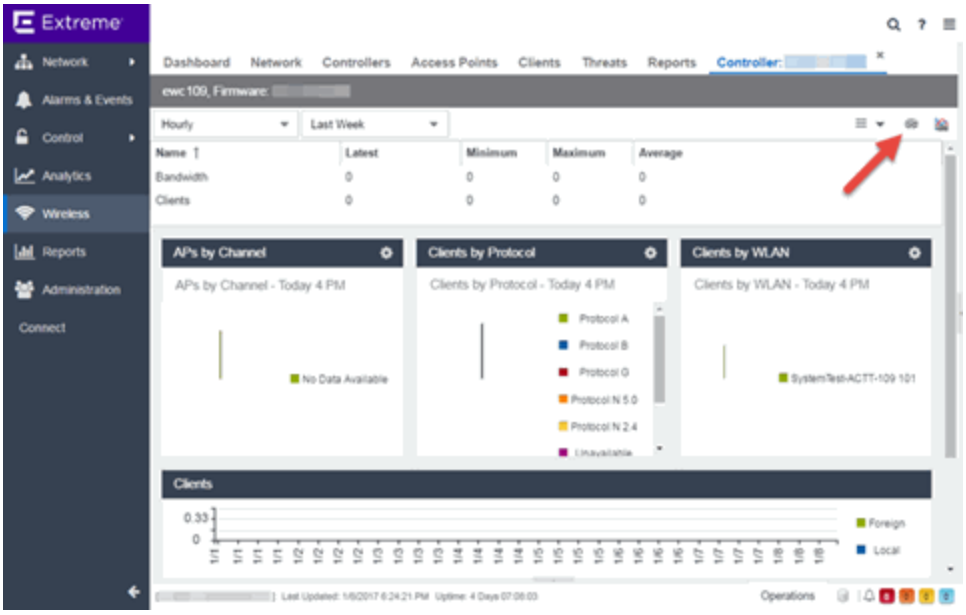
1. Access the **Wireless** tab in ExtremeCloud IQ Site Engine.
   The **Wireless** tab opens.



2. Select the **Controllers** tab.
   The **Controllers** tab opens.

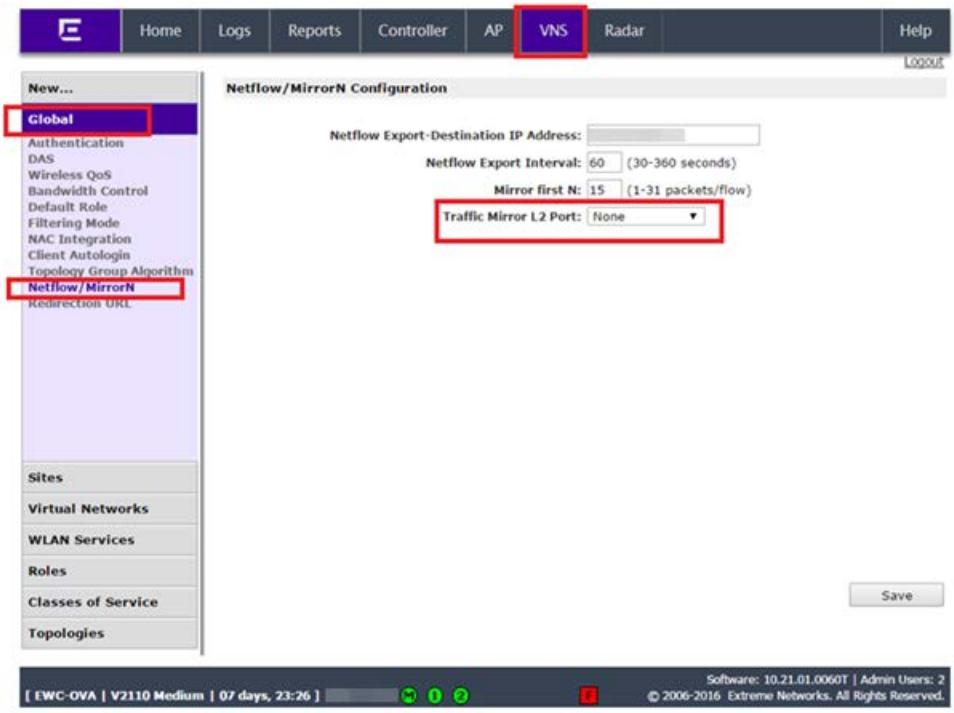


3. Select the **IP address** for the controller, located in the **Controller** column.
   The Wireless Controller Summary page opens.



4. Select the **WebView** icon ( ) at the top right of the Wireless Controller Summary page.
   The WebView opens for the controller.

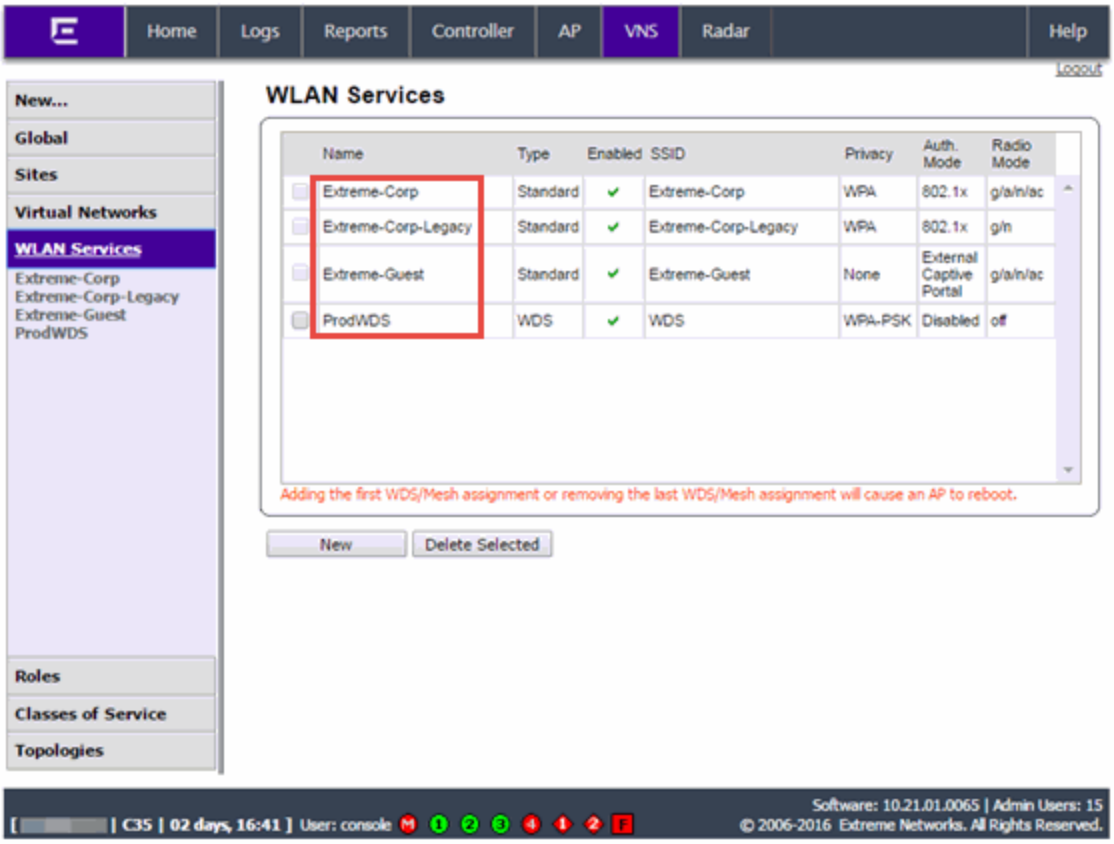
5. Select the **VNS** tab.
   The **VNS** tab opens.



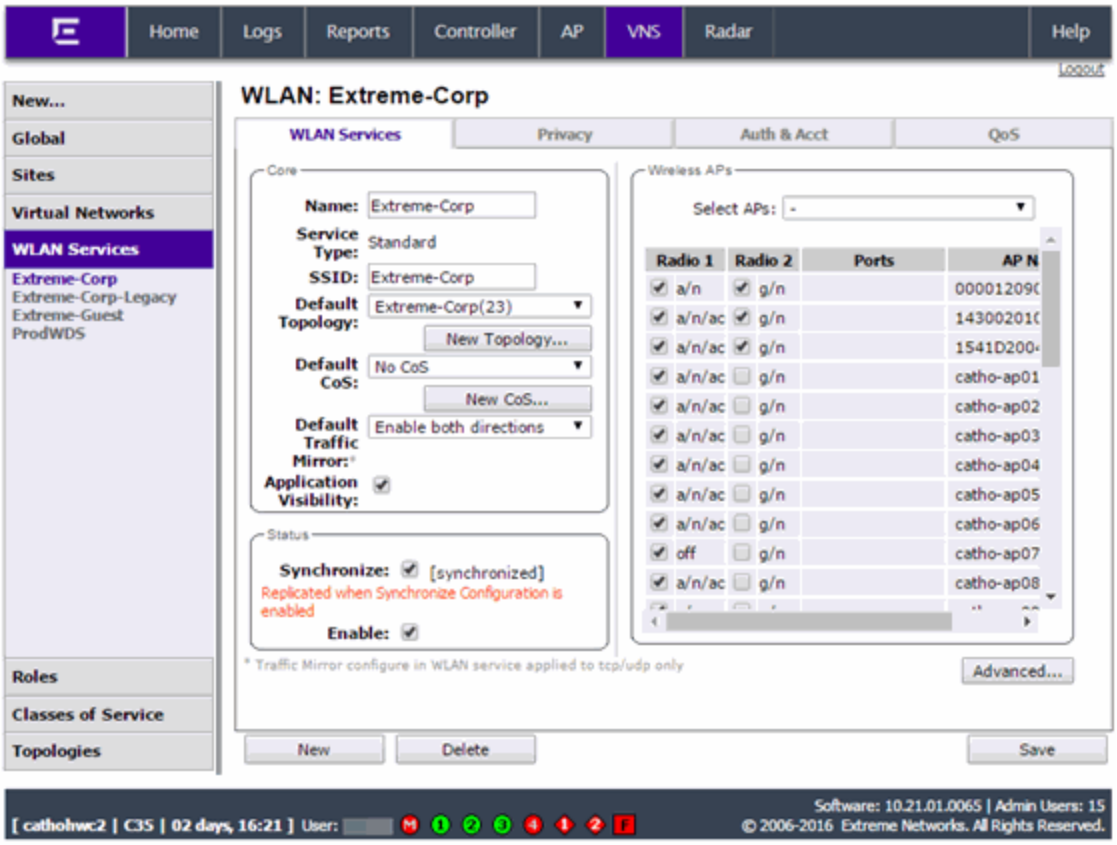
6. Select **Netflow/MirrorN** from the left-panel.
   The Netflow/MirrorN Configuration page opens.
7. Select **None** from the **Traffic Mirror L2 Port** drop-down list.
8. Select the **Save** button.

NOTE: The Mirror Port in the Wireless Control Flow Sources section of the **Analytics** > **Configuration** > Configuration tab is not available when the **Traffic Mirror L2 Port** is disabled.

9. Select **WLAN Services** from the left-panel.
   The WLAN Services page opens.

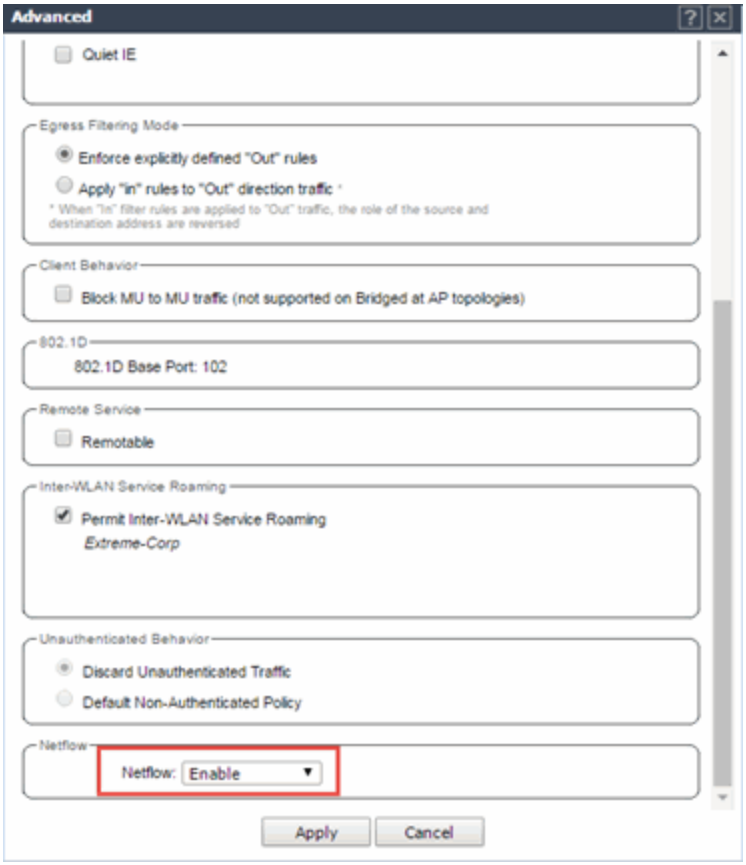

Home
Logs
Reports
Controller
AP
VNS
Radar
Help
Logout
New...
Global
Sites
Virtual Networks
WLAN Services
Extreme-Corp
Extreme-Corp-Legacy
Extreme-Guest
ProdWDS
Roles
Classes of Service
Topologies
WLAN Services
Name
Type
Enabled
SSID
Privacy
Auth. Mode
Radio Mode
Extreme-Corp
Standard
Extreme-Corp
WPA
802.1x
g/a/n/ac
Extreme-Corp-Legacy
Standard
Extreme-Corp-Legacy
WPA
802.1x
g/n
Extreme-Guest
Standard
Extreme-Guest
None
External Captive Portal
g/a/n/ac
ProdWDS
WDS
WDS
WPA-PSK
Disabled
off
Adding the first WDS/Mesh assignment or removing the last WDS/Mesh assignment will cause an AP to reboot.
New
Delete Selected
C35 | 02 days, 16:41] User: console
Software: 10.21.01.0065 | Admin Users: 15
© 2006-2016 Extreme Networks. All Rights Reserved.

10. Select a wireless LAN in the table.
    The WLAN page opens for the selected wireless LAN.



11. Select the **Advanced** button.
    The **Advanced** window opens.

12. Scroll to the bottom of the window and ensure the **Netflow** drop-down list is set to **Enable**.



13. Select the **Apply** button.

The wireless controller is now configured.

NOTE: **Rx Packets** and **Rx Bytes** can incorrectly be **0** when flow data is gathered via a wireless controller running version 10.21 or higher. Additionally, application response times and some meta data can be blank. This is a known issue and will be addressed in a future release.

Configure ExtremeXOS/Switch Engine Identity Manager to Send Events to ExtremeCloud IQ Site Engine

This chapter describes how to use the Identity Management — Configuration script on a Summit series or Black Diamond series switch to send events to ExtremeCloud IQ Site Engine.

In order to run the Identity Management — Configuration script on a device, you must be a member of an authorization group assigned the ExtremeCloud IQ Site Engine Suite > Common Web Services > Web Services APIs Read/Write Access capability.

To run the Identity Management — Configuration script on a device:

1. Open the **Network** > **Devices** tab in ExtremeCloud IQ Site Engine.
2. Right-click a Summit series or Black Diamond series switch in the Devices table or in the Device Groups left-hand panel.
3. Select the Identity Management — Configuration script in the Scripts > Access Control menu. The Run Script window opens.
4. On the **Device Selection** tab, the selected device is automatically included. Use the arrows to add additional devices or remove devices and to control the order of the selected devices.
5. Select **Next**.
6. On the **Overview** tab of the **Device Settings** tab, set the configuration properties for the script. If desired, select the **Description** tab to view the description defined for the script.
    - Stop on error? — Indicates whether the script stops if an error occurs.
    - Target Server IP Address — The IP address to which notifications are sent.
        - Entering a value of $serverIP automatically enters the IP address of the ExtremeCloud IQ Site Engine server IP.
        - Enter the IP address of the Access Controlengine if using the Extreme NetworksExtremeControl solution.
    - Target Server Type — Selecting ExtremeCloud IQ Site Engine monitors the IP, username, and port of the user accessing the device. Users with the Extreme Networks ExtremeControl solution can select nac, which provides you with the ability to run Kerberos authentication (if enabled) on the device.

      NOTE: In order to give elevated access to users when using the Kerberos authentication type on the device, the Target Server Type must be **nac** to allow the Access Controlengine to learn the Kerberos traffic.

    - Target Server Username — The username of the user to which the web service request is made.
    - Target Server Password — The password of the user to which the web service request is made.
    - Target Server HTTPs Port — The port that the ExtremeCloud IQ Site Engine server or Access Controlengine uses for HTTPS communication. The default port is 8443, but if the port was changed when configuring the ExtremeCloud IQ Site Engine server or Access Controlengine, enter the custom port used.
    - XML Target Name — The name of the targets on the switch to which IDM events are sent. Using the default predefined XML Target Name creates a unique name for each server.
    - Choose Action — The action that occurs on the device when the script is run.
        - Enable ID Monitoring — This option sets up the XML notification, configures ports for Identity Management (if specified), and enables or disables ports for devices

you can use with Identity Management.

- Manage Ports — This option only configures ports for Identity Management (if specified).

7. On the Run-Time Settings tab, set the run-time settings for the script (for more information about defining run-time variables when creating a script, see Specifying Run-Time Settings for a Script).
    - Save configuration in the background after running script successfully — Device configuration is saved after the script is run.
    - Timeout if script is not completed on each device (in seconds) — The amount of time in seconds before a timeout occurs if a device does not respond.
    - Run now, don't save as a task — Select to run the script now and do not save the script as a task.
    - Save as a task and run now — Select to run the script now and save it as a task. Type a name for the task in the Task Name box below. The task appears on the Script Tasks tab (see "Save Script as a Task").
    - Save as task. I'll run later — Select to save running the script as a task. The script does not run at this time. Type a name for the task in the Task Name box below. The task appears on the Script Tasks tab (see "Save Script as a Task").
8. Select **Next**. On the Verify Run Script tab, verify your script selections, and then select **Next**.
9. Select **Next**.
10. On the Results tab, you see the results of the script including any errors.
11. Select **Close**.

Schedule Tasks

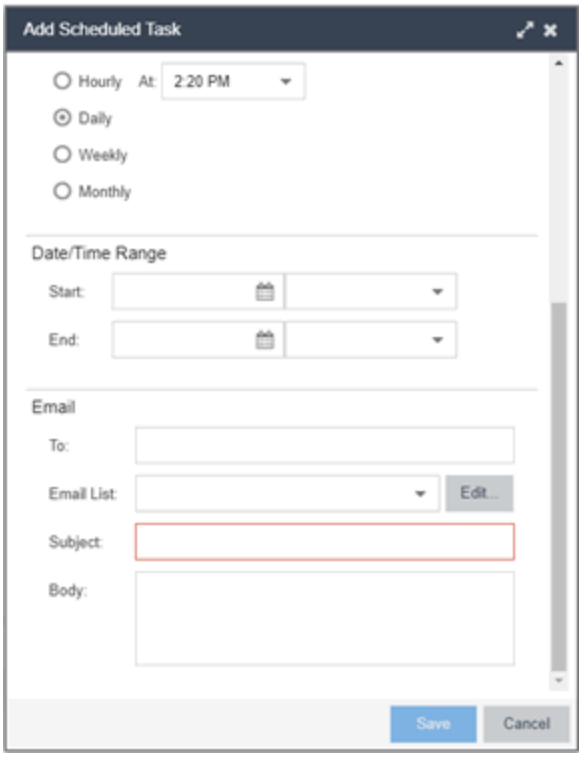
The **Scheduled Task** tab allows you to configure ExtremeCloud IQ Site Engine to automatically perform the following tasks:

- Generate a subset of available reports in PDF format
- Run a script or workflow
- Set SMTP Email Server Options to use when the scheduled task sends an email notification.
- Discover newly added devices

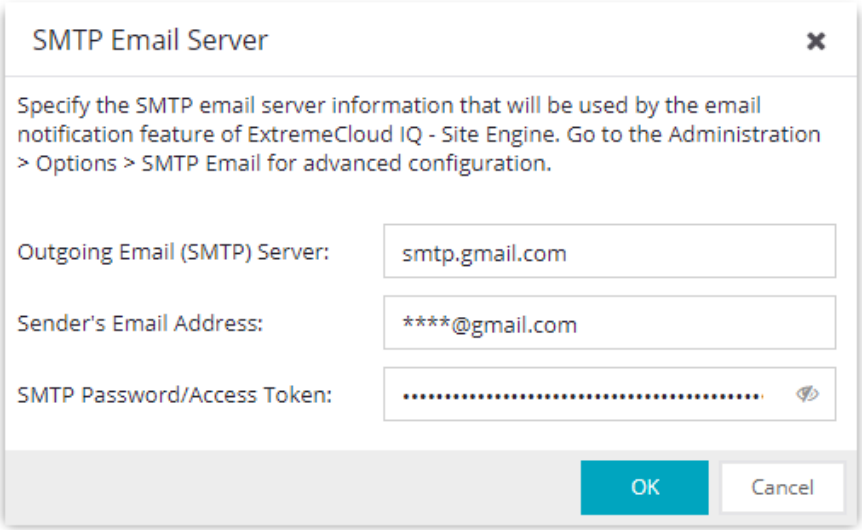
Create a New Scheduled Task

1. Launch ExtremeCloud IQ Site Engine.
2. Select the **Tasks** tab and select the **Scheduled Tasks** tab.

3. Select the **Add** button. The Add Scheduled Task window opens.



If no SMTP email settings are configured, the SMTP Email Server window also opens, where you can define the SMTP email settings. You can also configure the SMTP email settings in the **SMTP Email Options** tab.



4. Enter the outgoing SMTP email settings, if necessary, and select **OK**.

5. Select the type of task from the **Type** drop-down list in the Add Scheduled Task window:
    - **Device Export** — Exports the list of devices on your network from the **Network** > **Devices** tab.
    - **Disable Alarms** — Disables enabled alarms for the amount of time you define on a scheduled basis. Use this task to avoid alarms during times you reserve for network maintenance activity. You can manually ignore enabled alarms on the **Alarm Configuration** tab.
    - **FlexReports** — Creates a FlexReport for the devices you select on a scheduled basis.
    - **FlexViews** — Creates a FlexView for the devices you select on a scheduled basis.
    - **Compliance** — Emails the most recently run ExtremeCompliance report on a scheduled basis in PDF format.
    - **Port Usage** — Creates a Port Usage report for the devices you select on a scheduled basis.
    - **Port Usage Details** — Creates a Port Usage Details report for the devices you select on a scheduled basis.
    - **Reporting** — Emails a report you select (created on the **Report Designer** tab) on a scheduled basis.
    - **Scripting Task** — Runs a script saved on the **Saved Tasks** tab on a scheduled basis.
    - **Support** — Emails debugging data on a scheduled basis that provides information to Extreme Networks Support in the event of an issue with your network. ***Only select this option if instructed to do so byExtreme NetworksSupport.***
    - **Site** — Runs a device discover for a site (created on the **Site** tab) on a scheduled basis.
    - **Workflow Task** — Runs a workflow saved on the **Saved Tasks** tab on a scheduled basis.
6. Select the report, saved task, support task, or site you want to schedule in the **Report Name**, **Saved Task Name**, **Support Task Name**, or **Site to Discover** drop-down list, respectively. Depending on what you select, you may need to make other selections such as specifying the source engine or controller.
7. Edit the task name and description, if desired.
8. Select or deselect the **Enabled** checkbox to enable or disable the task, respectively. A disabled task is not performed.
9. Select whether you want the task to occur on an hourly, daily, weekly, or monthly basis.
    - **Hourly** — specify the minute each hour you want the task performed.
    - **Daily** — specify the time each day you want the task performed.
    - **Weekly** — specify the day or days of the week and the time you want the task performed.
    - **Monthly** — specify the day of the month and the time you want the task performed.

10. Specify a start and end date and time for the task, if desired.
11. Enter an email address or list of email addresses (separated by semicolons) to which generated PDF reports are sent in the **To** field, if desired.
12. Select a list of email addresses to which PDF reports are sent in the **Email List** field, if desired.

    Select the **Edit** button to create a new email list or edit an existing email list.
13. Enter the subject line and body text for the email, if desired.
14. Select **Save**.

    The task appears in the Scheduled Tasks table.

    Additionally, use the toolbar buttons to edit, copy, or delete the task. The **Refresh** button updates the Scheduled Tasks table to display any recent changes. Selecting the **Disable** button causes a task not to run without deleting it from the Scheduled Tasks table.

    Select the **Run** button to run the scheduled task immediately, if desired.

    Select the **SMTP** button to open the SMTP Email Server window to edit your outgoing email options.

For more information about SMTP and an example for how to configure GMAIL OAUTH, see Examples and How-tos for using OAUTH with Gmail.

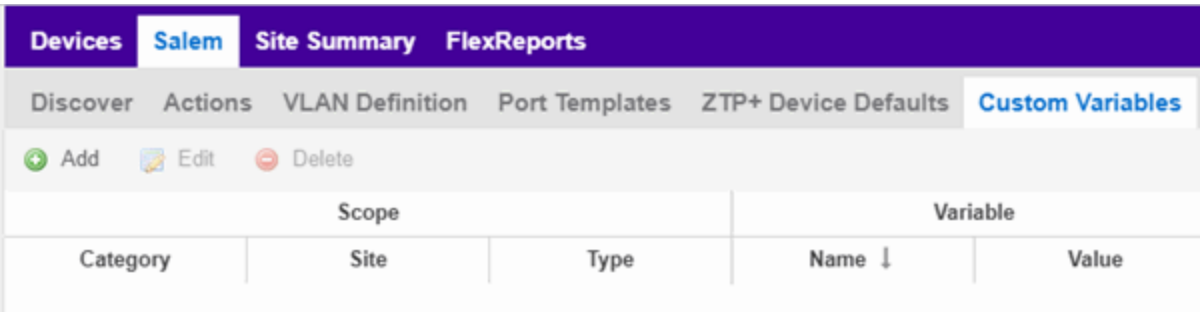
For more information about SMTP and a procedure for how to configure Office 365, see How-to Enable SMTP with Microsoft Office 365.

Create a Variable

Use the **Custom Variables** tab on the**Sites** tab to configure variables. Variables you create serve as a placeholder for a specific value. Use variables you create in a configuration template, script or workflow, in a CLI command, or in a third-party application via the Northbound Interface.

To create a variable:

1. Access the **Network** > **Devices** tab.
2. Use the left-panel drop-down list and select **Sites**.
3. Select the site in which you are adding the variable.
4. Select the tab displaying the site name in the right-panel.
5. Select the **Custom Variables** tab.



6. Select **Add** to add a new row to the table.
7. Select a **Category**, **Site**, and **Type** in the Scope section of the table.
8. Enter a **Name**, select a **Type**, and enter a **Value** in the Variable section of the table.
9. Select **Update** to save the new variable to the table.
10. Select **Save** to save the new variable to the site.

Creating Scripts

This chapter describes the scripting functionality built into ExtremeCloud IQ Site Engine and describes how to use ExtremeCloud IQ Site Engine to create scripts.

ExtremeCloud IQ Site Engine Scripts Overview

ExtremeCloud IQ Site Engine scripts are files containing CLI commands, control structures, and data manipulation functions. ExtremeCloud IQ Site Engine scripts can be executed on one or more devices or ports: simultaneously on multiple devices or ports, or on one device or port at a time.

ExtremeCloud IQ Site Engine allows you to create ExtremeCloud IQ Site Engine tasks, which run a script on specified devices or ports at specified times, either on a one-time or recurring basis. Tasks execute the script according to a schedule you configure.

In general, ExtremeCloud IQ Site Engine scripts support syntax and constructs from the following sources:

- **Python scripting language** — Create scripts using the Python syntax. The script can access ExtremeCloud IQ Site Engine data through API and NBI calls, and can use variables from the **Custom Variables** tab. Python scripts can be saved as tasks, and then run from the **Tasks** menu or run as scheduled tasks.

  To execute a Python script on a device using an ExtremeXOS/Switch Engine operating system, use `Type= JSON-RPC-Python`. For other device operating systems, use `Type=Python`.

- **TCL scripting language version 8.1** — Create scripts using TCL syntax. The script can send CLI commands to devices in ExtremeCloud IQ Site Engine and the resulting responses can be use by the script in ExtremeCloud IQ Site Engine. TCL scripts can be saved as tasks, and then run from the **Tasks** menu or run as scheduled tasks.

  To execute TCL scripts on a device using an ExtremeXOS/Switch Engine operating system, abbreviated commands (such as `sh vlan` instead of `show vlan`) can be used in the script if the commands use the prefix `CLI`.

  Example: `CLI sh vlan`

  To copy the whole script to an ExtremeXOS/Switch Engine device, use `Type=JSON-RPC-CLI`, the script will be executed in the `enable cli scripting` session. For other device operating systems, use `Type=TCL`.

  For general information about the TCL scripting language, see www.tcl.tk. For more information about using CLI scripting, see the *ExtremeXOS/Switch Engine User Guide*.

- **ExtremeXOS/Switch Engine CLI commands** — ExtremeXOS/Switch Engine CLI commands can be combined into a script to execute in sequence using `Type=CLI`. The CLI script is saved and executed in the **Scripts** tab. However, if the sequence of command needs to be accessed or scheduled as a task, then `Type=TCL` should be used as the script type instead. An ExtremeCloud IQ Site Engine script is sent to the device or port and the response can be used by the script.

  CLI commands can also be executed for selected devices using the CLI Commands feature on the **Tasks** menu for devices. The commands are executed sequentially and can be saved to a script but not saved to a task.

  Abbreviated ExtremeXOS/Switch Engine commands do not work unless you prefix the shortened command with CLI. For example, to abbreviate `show vlan`, type `CLI sh vlan`.

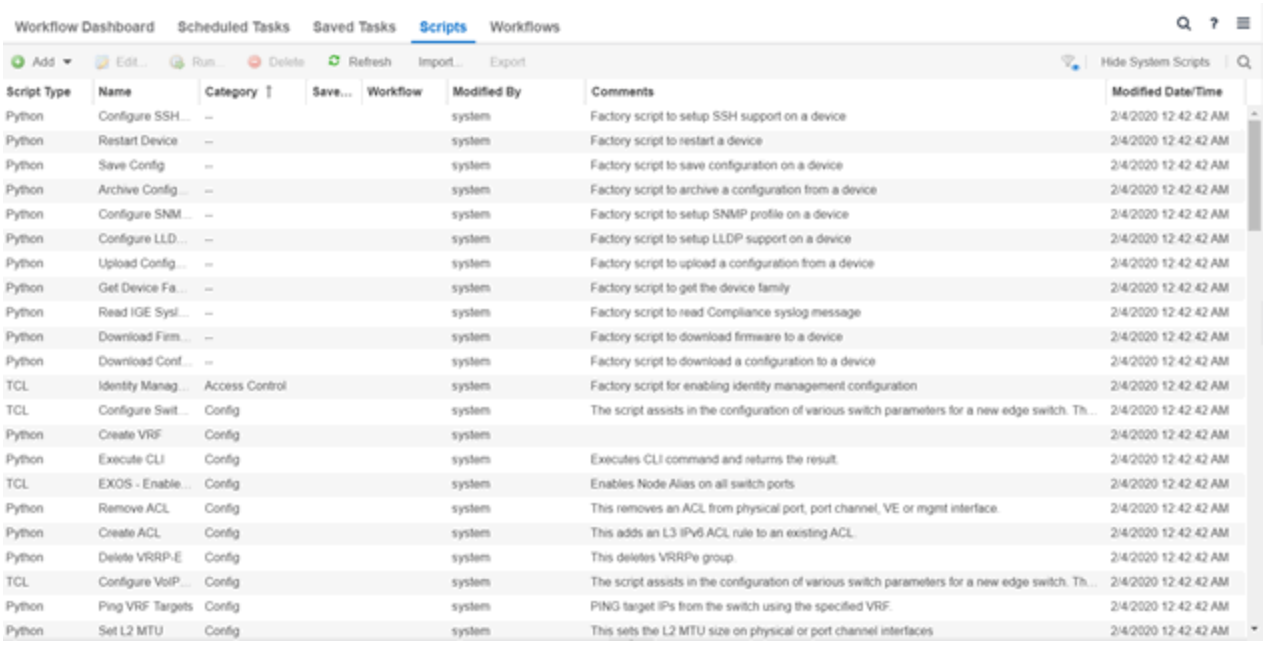
Bundled ExtremeCloud IQ Site Engine Scripts

ExtremeCloud IQ Site Engine includes a number of sample scripts you can use as templates for your own ExtremeCloud IQ Site Engine scripts. These scripts perform such tasks as enable/disable ports, apply ACLs, restart engines, and configure VLANs.

The sample scripts included with ExtremeCloud IQ Site Engine are available to users with an Administrator role. The XML source files for the scripts are located at `<install directory>\appdata\scripting\bundled_scripts`.

The ExtremeCloud IQ Site Engine Script Interface

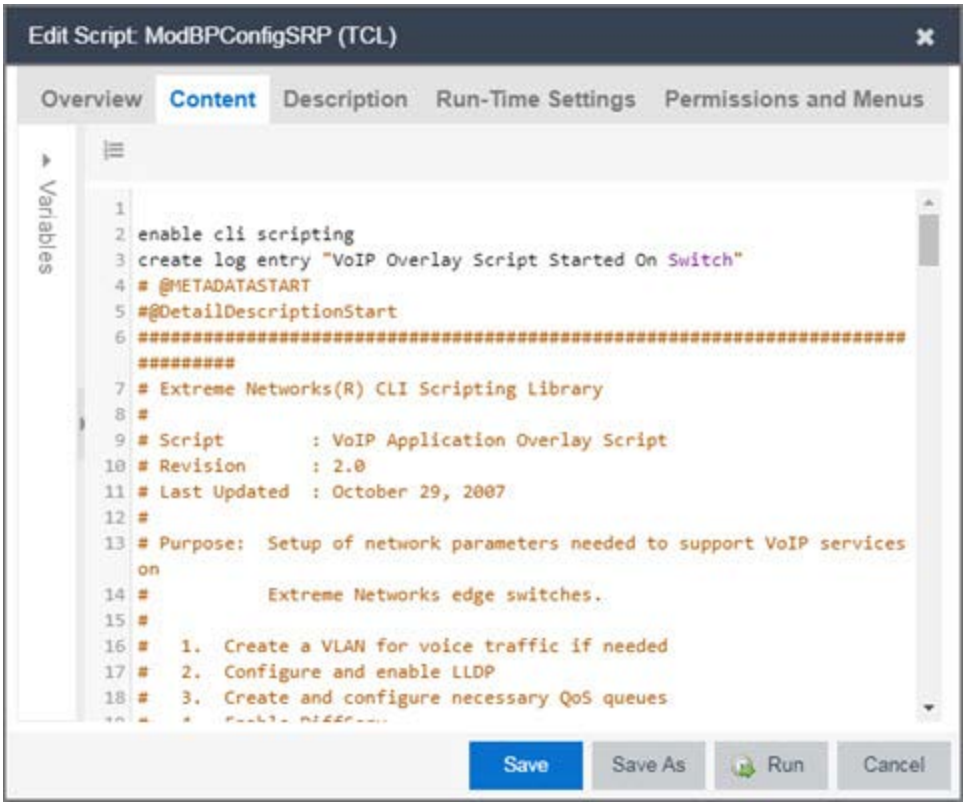
To display the scripts configured in ExtremeCloud IQ Site Engine, select the **Tasks** tab, then select the **Scripts** tab.



The Scripts tab contains the following information:

- **Script Type** — The language in which the script is written.
- **Name** — The name of the script. The script **Name** is defined when adding the script and can not be edited.
- **Category** — The script category, if configured.
- **Saved Tasks** — Indicates whether the script is configured as a saved task and is available on the **Saved Tasks** tab.
- **Workflow** — Indicates if the script is included in a workflow.
- **Modified By** — The name of the last user to modify the script. System scripts that are packaged with ExtremeCloud IQ Site Engine are indicated as **system**.
- **Comments** — Comments or a description of the script.
- **Modified Date/Time** — The date and time the script was last modified.

To view a script, double-click it. **Note:** Systems scripts cannot be edited. However, system scripts can be duplicated (using **Save As**) and the duplicated script can be edited. The duplicated script shows the last user to edit the script in the **Modified By** field.



The ExtremeCloud IQ Site Engine**Edit Script** window allows you to add content to a script, set values for parameters, specify run time settings, and specify the ExtremeCloud IQ Site Engine users with permission to run the script.

Depending on the type of script you are editing, the following tabs may appear in the ExtremeCloud IQ Site Engine**Script Editor** window:

- **Overview** — Displays fields to enter script parameters. The contents of this tab are derived from the metadata specified in the script.
- **Content** — Displays the script in a text editor window, where you can modify it directly.
- **Description** — Contains descriptive information about the script. The script description is specified in the metadata section of the script.
- **Runtime Settings** — Specifies script settings applied when the script is run.
- **Permissions and Menus** — Specifies ExtremeCloud IQ Site Engine user roles with the ability to run the script, and whether or not, and where, the option to run the script appears in the ExtremeCloud IQ Site Engine interface, such as on a menu or in a shortcut menu.
- **Network OS** — Allows you to select the Network Operating Systems that support the script. The script is available on a device's Tasks submenu when the device's Network OS matches one of the Network Operating Systems defined for the script.

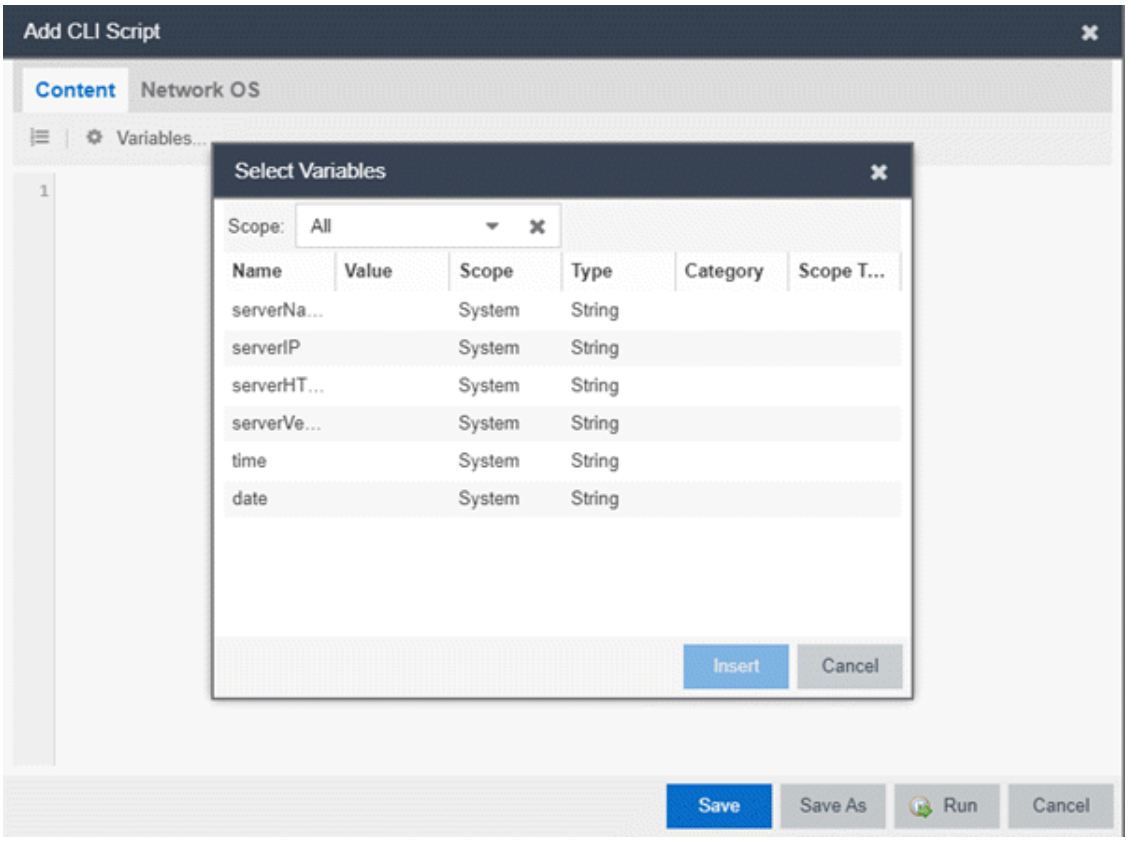
Managing ExtremeCloud IQ Site Engine Scripts

With scripting, you can:

- Create an ExtremeCloud IQ Site Engine Script
- Specify Runtime Settings for a Script
- Specify Permissions and Run Locations for Scripts
- Run a Script
- View Script Results
- Edit a Script
- Delete a Script
- Import Scripts into ExtremeCloud IQ Site Engine
- Export a Script
- Save Script as a Task

Create an ExtremeCloud IQ Site Engine Script

1. Select **Scripts** on the **Tasks** tab.
2. Select the **Add** button.
3. Select the type of script you are creating:
    - **TCL** — A Tool Command Language script. Use TCL instead of CLI if you need to use the script in a task. Proceed to step 5.
    - **Python** — A Python script. Proceed to step 5.
    - **JSON-RPC-Python** — Machine to Machine Interface (used to send a Python script to an ExtremeXOS/Switch Engine device). Proceed to step 5.
    - **JSON-RPC-CLI** — Machine to Machine Interface (used to send CLI commands to an ExtremeXOS/Switch Engine device). Proceed to step 5.
    - **CLI** — A CLI command script. Use CLI instead of TCL if you do not need to use the script in a task. Proceed to step 4.
4. When selecting **CLI** from the **Add** drop-down list, the **Add Script** window opens, where you can enter the CLI commands for the script. Select **Variables** to open the **Select Variables** window, from which you can select variables you define on the **Custom Variables** tab.



Use the **Scope** drop-down list to select either **All**, **Custom**, or **System** from the drop-down list, depending on how you configured the variable you are inserting. Select **Insert** to add the variable to your script.

Select **Save** to save the CLI script on the **Scripts** tab or select **Save As** to save the script to the ExtremeCloud IQ Site Engine server.

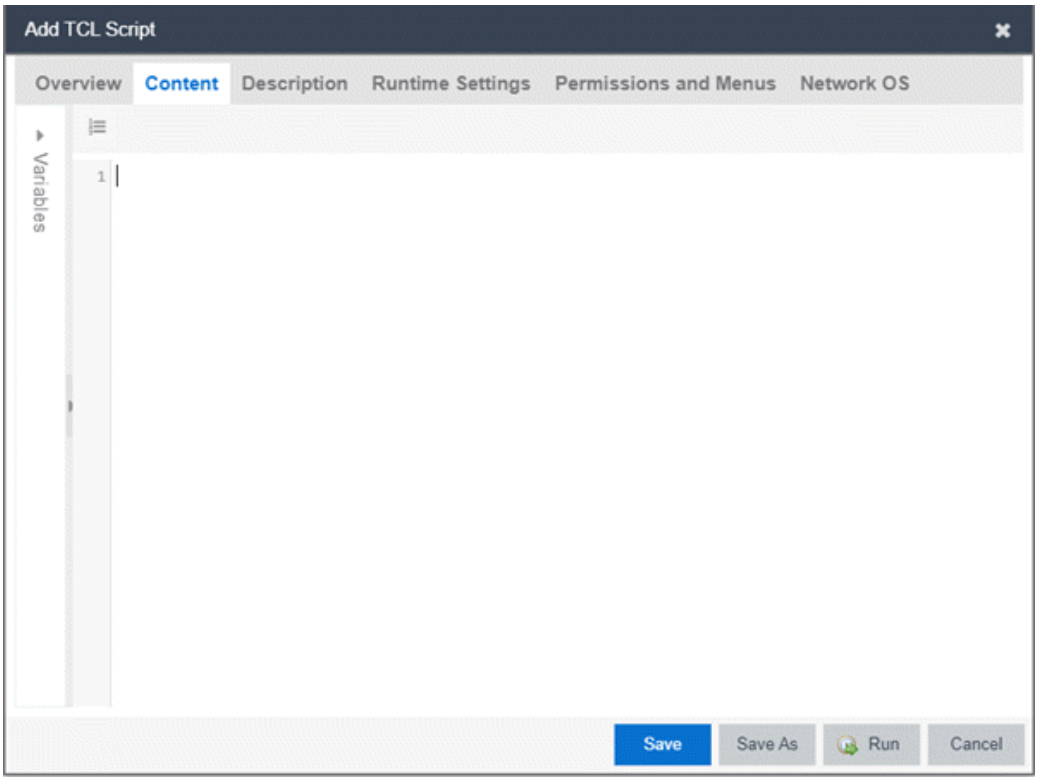
Select **Run** to run the CLI script immediately.

5. When selecting the **TCL**, **Python**, J**SON-RPC-Python**, and **JSON-RPC-CLI**script types, the **Add Script** window also opens, but contains the following tabs:
    - **Overview** — Use to enter script parameters. The contents of this tab are derived from the metadata specified in the script.
    - **Content** — Use to modify the script directly in a text editor window.
    - **Description** — Add descriptive information about the script. The script description is specified in the metadata section of the script.
    - **Runtime Settings** — Specify script settings applied when the script is run.
    - **Permissions and Menus** — Specify ExtremeCloud IQ Site Engine user roles with the ability to run the script, and whether or not, and where, the option to run the script

appears in the ExtremeCloud IQ Site Engine interface, such as on a menu or in a shortcut menu.

- Select the **Network OS** tab to select the select the Network Operating Systems that support the script.

NOTE: Select **Unknown** when creating scripts or workflows that include devices before their Network OS has been determined (e.g. onboarding new devices).



6. Type the metadata tags `#@DetailDescriptionStart` and `#@DetailDescriptionEnd` between the tags `#@MetaDataStart` and `#@MetaDataEnd`, and then type a detailed description between these detailed description tags. This description appears on the **Description** tab.
7. Place variable definition statements in the metadata section (between `#@MetaDataStart` and `#@MetaDataEnd` tags).

   Select a variable by expanding the Variables menu on the left of the **Content** tab. A list of system variables appears under Variables. To add a variable to the script, double-click the variable.
8. Enter script commands after the metadata section of the script.

   The following are examples of types of script commands supported in ExtremeCloud IQ Site

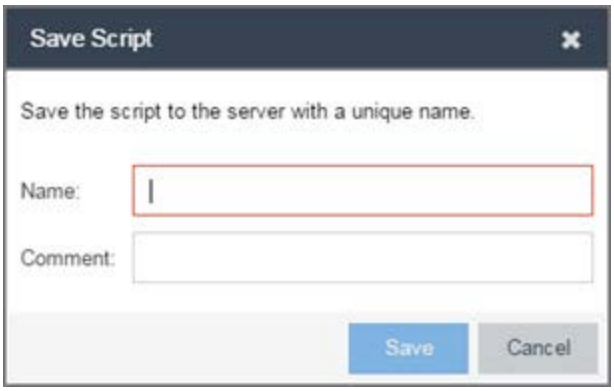
Engine:

- ExtremeXOS/Switch Engine 12.1 and later CLI scripting commands
- TCL commands
- Constructs

9. Select the **Runtime Settings** tab to specify runtime settings.
10. Select the **Permissions And Menus** tab to specify which ExtremeCloud IQ Site Engine user roles have permission to run the script, and whether or not, and where, the script appears in the menu or in a shortcut menu.
11. Select the **Network OS** tab to select the select the Network Operating Systems that support the script.

NOTE: Select **Unknown** when creating scripts or workflows that include devices before their Network OS has been determined (e.g. onboarding new devices).

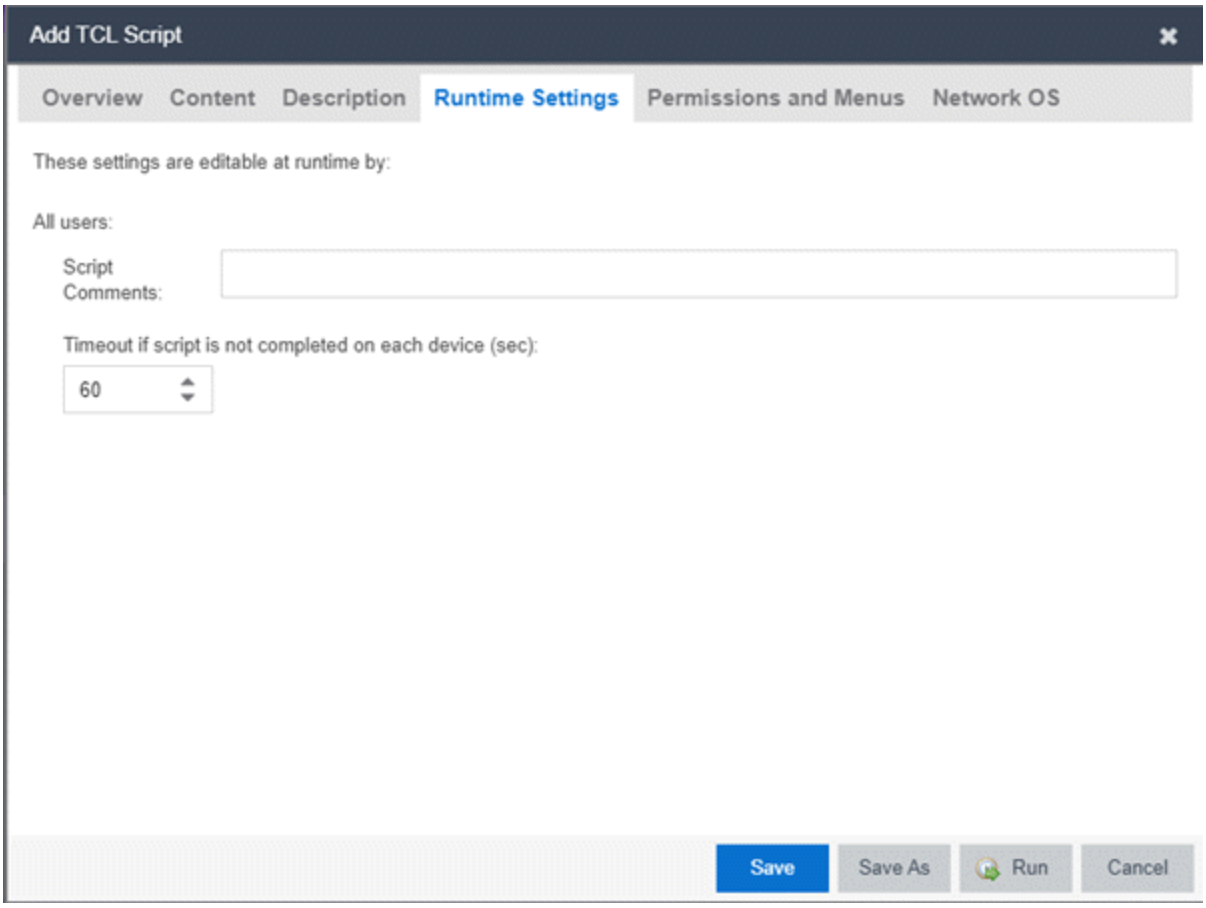
12. Select **Save**. The **Save Script** window appears.



13. Type a name for the script file in the **Name** field and a comment about the script in the **Comment** field, if necessary.
14. Select **Save**.
15. Select **Run** to run the script now or **Cancel** to run the script at a later time.

Specify Runtime Settings for a Script

To specify the runtime settings for a script, select the **Runtime Settings** tab.



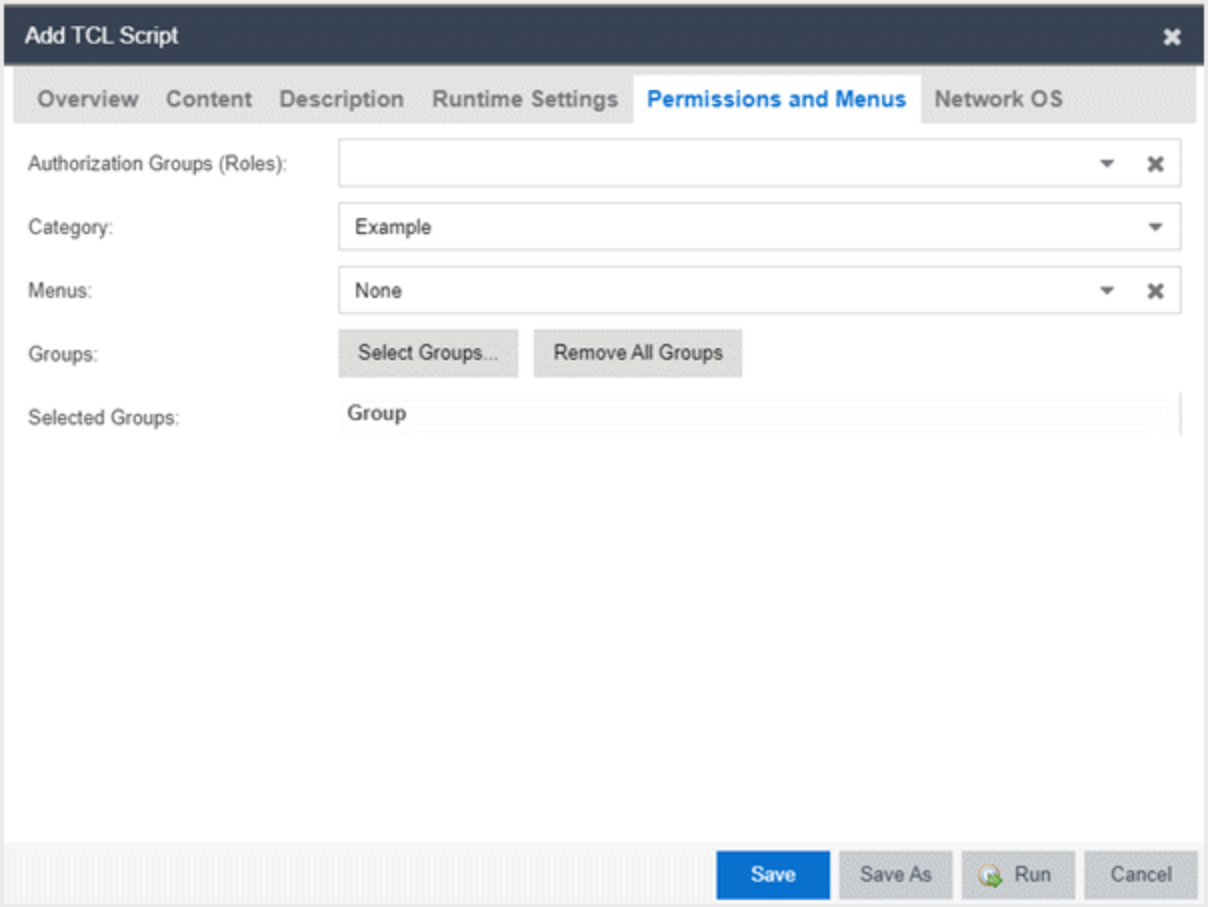
Use this tab to specify the following settings:

- **Script Comments** — Use this field to enter comments or a description of the script.
- **Timeout if script is not completed on each device (in seconds)** — Select the maximum length of time the script runs on each device or port (in seconds) before the process ends. This timeout value applies to each device or port independently.

Specify Permissions and Run Locations for Scripts

Specify which ExtremeCloud IQ Site Engine user roles have permission to run the script, and whether or not, and where, the script appears in the menu or in a shortcut menu.

Select the **Permissions and Menus** tab to set permissions and menu locations for the script.



Authorization Group (Roles)
: Select the Authorization Group credentials required to execute the script from the drop-down list.

Category
: Select the **Category** group from the drop-down list, which defines the Tasks submenu in which the script is grouped throughout ExtremeCloud IQ Site Engine. The default category is Example.

Menus
: Select the Tasks submenus in ExtremeCloud IQ Site Engine in which you want the script to display from the drop-down list. Select **Multi-Device** for User Device Group scripts.

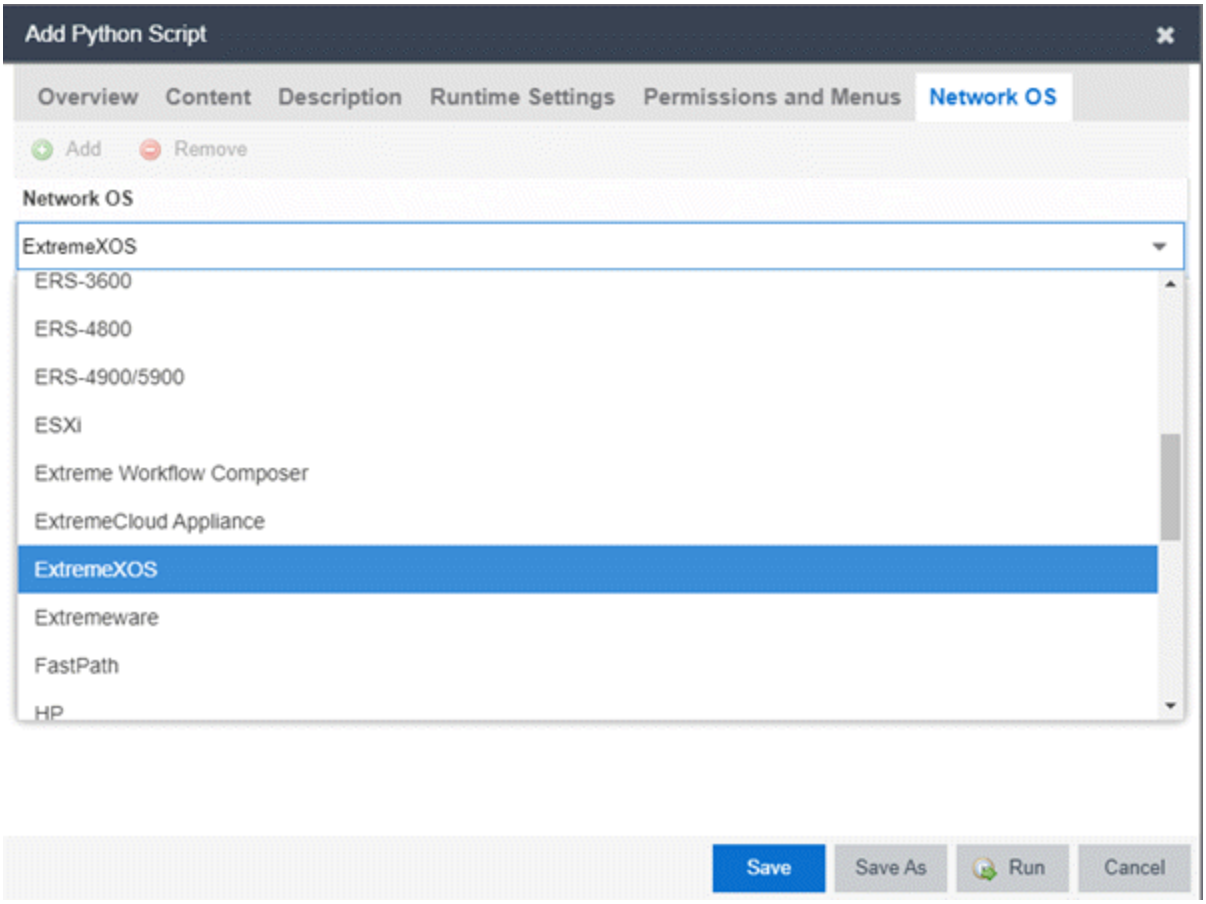
Groups
: Select the **Select Groups** to select the device groups on which the script displays.

Selected Groups
: Displays the Groups in which the script is included.

Specify Network Operating System

Select the **Network OS** tab to select the Network Operating Systems that support the script.

NOTE: Select **Unknown** when creating scripts or workflows that include devices before their Network OS has been determined (e.g. onboarding new devices).



Run a Script

From the **Network** tab

NOTE: The **Runtime Settings** tab is unavailable for scripts run via the **Network** tab. To save a script as a saved task or configure a timeout when running the script, run the script via the **Tasks** tab.

1. Right-click the device in the Devices table or in the Device Groups left-hand panel on the **Devices** tab.
2. Select a script in the Tasks menu. The Run Script window opens.
3. On the **Device Selection** tab, select the device or devices against which you want to run the script. Use the arrows to add/remove devices and to control the order of the selected devices.
4. Select **Next**.

5. On the **Overview** tab of the **Device Settings** tab, set the configuration properties for the script. The options available on this tab vary depending on the script selected. If desired, select the **Description** tab to view the description defined for the script.
6. Select **Next**.

   The **Verify Run Script** tab opens.
7. Verify your script selections, and then select **Run**.
8. On the **Results** tab, you see the results of the script including any errors.
9. Select **Close**.

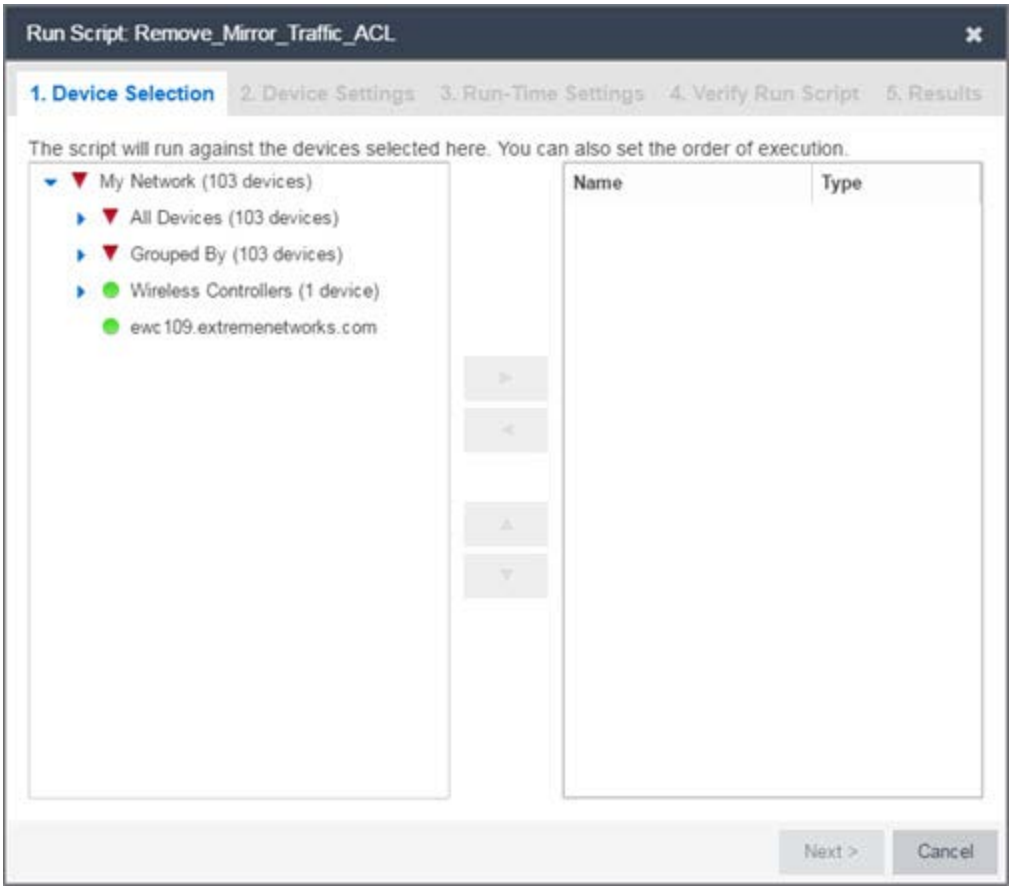
From the Tasks tab

1. Select **Scripts**.
2. On the **Scripts** tab, find the script in the list. If needed, filter the list by typing search terms in the **Search** field.
3. Select the script by selecting its row and then select **Run**. The Run Script window opens.

NOTE: Only select one script. The **Run** button is unavailable if two or more scripts are selected.

4. On the **Device Selection** tab, shown below, select the device or devices against which you want to run the script. Use the arrows to add/remove devices and to control the order of the

selected devices.



5. Select **Next**.
6. On the **Overview** tab of the **Device Settings** tab, set the configuration properties for the script. The options available on this tab vary depending on the script selected. If desired, select the **Description** tab to view the description defined for the script.
7. Select **Next**.
8. On the **Runtime Settings** tab, configure the runtime settings for the script.
    - **Timeout if script is not completed on each device (in seconds)** — Use to set a maximum amount of time for the script to run on each device (in seconds). This timeout value applies to each device independently.
    - **Run now, don't save as task** — Select to run the script immediately without saving the script as a task.
    - **Save as a task and run now** — Select to run the script immediately and save it as a task on the **Saved Tasks** tab. Type a name for the task in the **Task Name** field.
    - **Save as a task. I'll run later** — Select to save the script as a task you can run later. Type a name for the task in the **Task Name** field. The task appears on the **Saved Tasks** tab.

9. Select **Next**. On the **Verify Run Script** tab, verify your script selections, and then select **Run**.
10. On the **Results** tab, you see the results of the script including any errors.
11. Select **Close**.

View Script Results

When a script is run, results are stored in the `<install directory>/appdata/scripting/tmp` folder. The folder in which script results are stored cannot be configured.

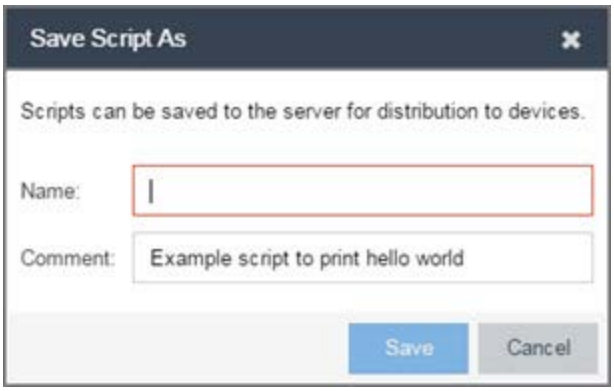
An event is stored in the console.log file in the `<install directory>/appdata/logs` folder each time a script is executed. The event in the log contains the location of the audit file. These audit logs reside in the tmp directory and remain for two weeks (per user), or until the next server restart, whichever comes first. The number of audit files written to the folder is limited to 1,000 files. When the number of files exceeds 1,000, the oldest 100 are deleted.

Edit a Script

To edit a script:

1. In the **Tasks** tab, select **Scripts**.
2. In the scripts table, select the script you want to edit. **Note:** Systems scripts that are packaged with ExtremeCloud IQ Site Engine cannot be edited. However, system scripts can be duplicated (using **Save As**) and the duplicated script can be edited. The systems scripts are labeled **system** in the **Modified By** field, but duplicated scripts show the last user name as Modified By.
3. Select the **Edit** button. The script opens in the **Edit Script** window, where you can edit the script.
4. Save the script:
    a. Select the **Save** button to save your changes to the script.
    b. Select **Save As** to save a copy of this script with a new name.

       The **Save Script As** window appears.



i. Type a name for the script file in the **Name** field and a comment about the script in the **Comment** field, if necessary.

ii. Select **Save**.

The script is saved.

Delete a Script

To delete a script:

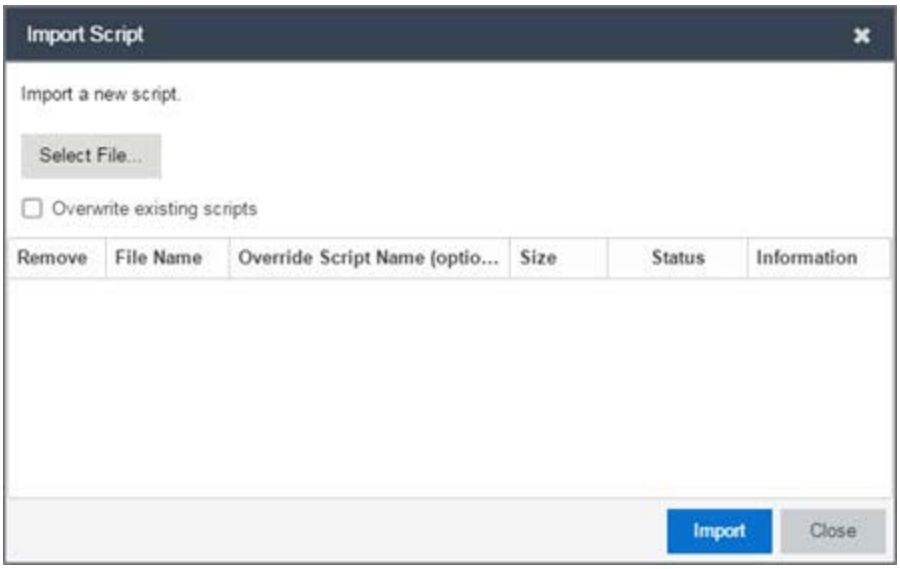
1. In the **Tasks** tab, select **Scripts**.
2. In the scripts table, select one or more scripts you want to delete.
3. Select the **Delete** button.
4. Select **Yes** to confirm the script deletion.

Import Scripts into ExtremeCloud IQ Site Engine

Import XML-formatted scripts into ExtremeCloud IQ Site Engine.

To import a script:

1. In the **Tasks** tab, select **Scripts**.
2. Select the **Import** button.



3. Select **Select File** to navigate to the location of the script. The script appears in the grid.
4. Enter a new Script Name in the **Override Script Name (optional)** field if you want to change the name of the script.
5. Select the **Overwrite existing scripts** checkbox, if necessary.
    - When **Overwrite existing scripts** is not selected and the script name displayed in the **File Name** field (if you did not use the **Override Script Name (optional)** field) or the **Override Script Name (optional)** field matches the name of a script in ExtremeCloud IQ Site Engine, the new script is not imported.
    - When **Overwrite existing scripts** is selected and the script name displayed in the **File Name** field (if you did not use the **Override Script Name (optional)** field) or the **Override Script Name (optional)** field matches the name of a script in ExtremeCloud IQ Site Engine, the new script is imported and overwrites the existing script.
6. Select **Import**.
7. Verify the script is imported and select **Close**.

NOTE: Exported EPICenter 6.0 telnet macros cannot be imported as XML scripts.

Export a Script

To export a script:

1. From the **Tasks** tab, select a script.
2. Select the **Export** button.

The script is exported in XML format to your browser download directory.

Save Script as a Task

When you run a script, you can save it as a task that appears in the Saved Tasks tab. This saves your device selections and runtime settings, and then allows you to manually run the script task at a later time or schedule it to run in the future either one time, or on a regular basis.

To save a script as a saved task:

1. Select a script.
2. Run the script and designate it as a task by selecting either **Save as a task and run now** or **Save as task. I'll run later** on the **Runtime Settings** tab.
3. Enter a new name for the task in the **Task Name** field.

ExtremeCloud IQ Site Engine saves the script to the Saved Tasks tab.

ExtremeCloud IQ Site Engine Script Reference

This section contains reference information for ExtremeCloud IQ Site Engine scripts. It contains the following topics:

- Metadata Tags
- ExtremeCloud IQ Site Engine-Specific Python Scripting Constructs
- ExtremeCloud IQ Site Engine-Specific TCL Scripting Constructs
- TCL Support in ExtremeCloud IQ Site Engine Scripts
- Entering Special Characters
- Line Continuation Character
- Case Sensitivity in ExtremeCloud IQ Site Engine Scripts
- Reserved Words in ExtremeCloud IQ Site Engine Scripts
- ExtremeXOS/Switch Engine CLI Scripting Commands Supported in ExtremeCloud IQ Site Engine Scripts
- ExtremeCloud IQ Site Engine-Specific System Variables

An ExtremeCloud IQ Site Engine script may contain a metadata section, which can serve as a usability aid in the script interface. The metadata section, if present, is the first section of an ExtremeCloud IQ Site Engine script, followed by the script logic section, which contains the CLI commands and control structures in the script. The metadata section is delimited between `#@MetaDataStart` and `#@MetaDataEnd` tags. A metadata section is optional in an ExtremeCloud IQ Site Engine script.

Use metadata tags to specify the description of the script, as well as parameters that the script user can input. The information specified by the metadata tags appears in the **Overview** tab for the script.

ExtremeCloud IQ Site Engine-Specific Python Scripting Constructs

Specifying the Wait Time Between Commands

After the script executes a command, the time.sleep command causes the script to wait a specified number of seconds before executing the next statement.

Syntax

```
time.sleep(10)
```

Example

```
# sleep for 10 seconds after executing a command

time.sleep(10)
```

Metadata Tags

#@MetaDataStart and #@MetaDataEnd

Indicates the beginning and end of the metadata section of the script. In order for description information and variable input fields to appear in the **Overview** tab for a script, the corresponding metadata tags must appear in the metadata section.

Example

```
#@MetaDataStart

#@SectionStart (description = "Protocol Configuration Section") Set var
protocolSelection eaps

#@SectionEnd

#@SectionStart (description = "vlan tag section") Set var vlanTag 100

#@MetaDataEnd
```

#@ScriptDescription

Specifies a one-line description of the script. The description specified with this tag cannot contain a newline character.

Example

```
#@ScriptDescription "This is a VLAN configuration script."
```

#@DetailDescriptionStart and #@DetailDescriptionEnd

Specifies the beginning and end of the detailed description of the script. The detailed description can be multiple lines or multiple paragraphs. The detailed description is shown in the **Script View** tab in the script editor window.

Example

```
#@DetailDescriptionStart

#This script performs configuration upload from ExtremeCloud IQ Site Engine to
the switch.

#The script only supports tftp.

#This script does not support third party devices.

#@DetailDescriptionEnd
```

#@SectionStart and #@SectionEnd

Specifies the beginning and end of a section within the metadata part of a script. You do not need to end with a `#@MetaDataEnd` tag, then the `#@SectionEnd` tag if this is the last section of the metadata. When a section starts with the `#@SectionStart` tag, the previous section automatically ends.

Example

```
#@SectionStart (description = "Protocol Configuration Section") Set var
protocolSelection eaps

#@SectionEnd
```

#@VariableFieldLabel

Defines user-input variables for the script. For each variable defined with the `#@VariableFieldLabel` tag, you specify the variable's description, scope, type, and whether it is required.

Description
Label that appears as the prompt for this parameter in the **Overview** tab.

Scope
Whether the parameter is global (uses the same value for all devices) or device-specific. Valid values: global, device. Default value is global.

Type
Parameter data type. This determines how the parameter input field is shown in the **Overview** tab. Valid value: String (the parameter input field on the **Overview** tab displays as a drop-down list if **validValues** are listed or as a text field if **validValues** are not listed).

readonly
Whether the parameter is read-only and cannot be modified by the user. Valid values: Yes, No. Default value is No.

validValues
Lists all possible values for a parameter. Separate each value using a comma and put into a square bracket.

Required

Indicates whether specifying the parameter is required to run the script. Valid values: Yes, No.

Example

```
#@VariableFieldLabel (description = "Partition:", scope = global,
#required = yes, validValue = [Primary,Secondary], readOnly=false)
set var partition ""
```

ExtremeCloud IQ Site Engine-Specific TCL Scripting Constructs

This section describes the TCL scripting constructs specific to ExtremeCloud IQ Site Engine:

- Specifying the Wait Time Between Commands
- Printing System Variables
- Configuring a Carriage Return Prompt Response
- Synchronizing the Device with ExtremeCloud IQ Site Engine
- Saving the Configuration on the Device Automatically
- Printing a String to the Output File

Specifying the Wait Time Between Commands

After the script executes a command, the sleep command causes the script to wait a specified number of seconds before executing the next statement.

Syntax

```
sleep 5
```

Example

```
# sleep for 5 seconds after executing a command
sleep 5
```

Printing System Variables

The printSystemVariables command prints the current values of the system variables. Specifically, values for the following variables are printed:

- deviceIP
- deviceName
- serverName
- deviceSoftwareVer
- serverIP
- serverPort

- date
- time
- abort_on_error
- CLI.OUT

Syntax

```
printSystemVariables
```

Example

```
# Display values for system variables

printSystemVariables
```

Configuring a Carriage Return Prompt Response

A special string within the script, `<cr>`, indicates a carriage return in response to a prompt for a command.

Syntax

```
<cr>
```

Example

```
# cancel download

download image 10.22.22.22 t.txt <cr>
```

Synchronizing the Device with ExtremeCloud IQ Site Engine

The PerformSync command manually initiates a synchronization for specified ExtremeCloud IQ Site Engine feature areas and scope.

Syntax

```
PerformSync [-device <ALL | deviceIp>] [-scope <EAPSDomain | VPLS> ]
```

If -device is not specified, the current device (indicated by the `$deviceIP` system variable) is assumed.

The PerformSync command is executed in an asynchronous manner so when the command is executed, ExtremeCloud IQ Site Engine moves on to the next command in the script without waiting for the PerformSync command to complete.

Examples

```
PerformSync -scope VPLS
```

Saving the Configuration on the Device Automatically

The run time settings for the script may include the option to issue the save command in the background after the script runs successfully on the device.

Printing a String to the Output File

Example

```
# Write Device IP address to file

ECHO "device ip is $deviceIP"
```

NOTE: The TCL `puts` and `ECHO` commands have the same function. However, the `ECHO` command is not case-sensitive (unless referenced inside another command), while the `puts` command is case-sensitive.

TCL Support in ExtremeCloud IQ Site Engine Scripts

The following TCL commands are supported in ExtremeCloud IQ Site Engine scripts:

after	concat	flush	info	lrange	puts	set	unset
append	continue	for	interp	lreplace	read	split	update
array	global	foreach	join	lsearch	regexp	string	uplevel
binary	eof	format	lappend	lsort	regsub	subst	upvar
break	error	gets	lindex	namespace	rename	switch	variable
catch	eval	history	linsert	open	return	tell	vwait
clock	expr	if	list	package	scan	time	while
close	fblocked	incr	llength	proc	seek	trace	

See www.tcl.tk/man/tcl8.2.3/TclCmd/contents.htm for syntax descriptions and usage information for these TCL commands.

Entering Special Characters

In an ExtremeCloud IQ Site Engine script, use the backslash character (\ ) as the escape character if you need to enter special characters, for example:

- quotation marks (" ")
- colon (:)
- dollar sign ($).

Example

```
set var value 100
set var dollar \$value
show var dollar >>> $value
```

NOTE: Do not place the backslash character at the end of a line in an ExtremeCloud IQ Site Engine script.

Line Continuation Character

The line continuation character is not supported in ExtremeCloud IQ Site Engine scripts. Place each command statement on a single line.

Case Sensitivity in ExtremeCloud IQ Site Engine Scripts

The commands and constructs in an ExtremeCloud IQ Site Engine script are not case-sensitive. However, if a command is referenced inside another command, the inner command is case-sensitive. In this instance, the inner command case matches how it appears in the ExtremeCloud IQ Site Engine documentation.

Example (Usage of the ExtremeCloud IQ Site Engine command ECHO)

```
echo hi (valid)
echo [echo hi] (error)
echo [ECHO hi] (valid)
```

Reserved Words in ExtremeCloud IQ Site Engine Scripts

The following words are reserved by ExtremeCloud IQ Site Engine and cannot be used as variable names in a script:

- Names of system variables (see ExtremeCloud IQ Site Engine-Specific System Variables)
- Names of ExtremeCloud IQ Site Engine command extensions (see ExtremeCloud IQ Site Engine-Specific Scripting Constructs)
- Names of ExtremeXOS/Switch Engine CLI commands
- Names of TCL functions

Also, do not use a period (.) within a variable name, use an underscore (_).

ExtremeXOS/Switch Engine CLI Scripting Commands Supported in ExtremeCloud IQ Site Engine Scripts

ExtremeCloud IQ Site Engine scripts support the CLI commands in this section.

- $VAREXISTS
- $TCL
- $UPPERCASE
- show var
- delete var
- configure cli mode scripting abort-on-error

$VAREXISTS

- Checks if a given variable is initialized.
- Switch Compatibility — Devices running ExtremeXOS/Switch Engine 12.1 and higher support this command.
- Example — `if ($VAREXISTS(foo)) then show var foo endif`

$TCL

- Evaluates a given TCL command. The following constructs support the $TCL command:
  - `set var if`
  - while
- See TCL Support in ExtremeCloud IQ Site Engine Scripts for a list of supported TCL commands.
- Switch Compatibility — Devices running ExtremeXOS/Switch Engine 11.6 and higher support this command.
- Example — `set var foo $TCL(expr 3+4) if ($TCL(expr 2+2) == 4) then`

$UPPERCASE

- Converts a given string to upper case.
- The following constructs support the $UPPERCASE command:
  - set var
  - if
  - while
- Switch Compatibility — Devices running ExtremeXOS/Switch Engine 11.6 and higher support this command.

NOTE: The $UPPERCASE command is deprecated in ExtremeXOS/Switch Engine 12.1 CLI scripting. Use the $TCL (string toupper <string>) command instead. Example: set var foo $TCL ("foo") .

show var

- Prints the current value of a specified variable.
- Switch Compatibility — Devices running ExtremeXOS/Switch Engine 11.6 and higher support this command.
- Example — `show var foo`

delete var

- Deletes a given variable. Only local variables can be deleted; system variables cannot be deleted.
- Switch Compatibility — Devices running ExtremeXOS/Switch Engine 11.6 and higher support this command.
- Example — `set var foo bar delete var foo if ($VAREXISTS(foo)) then ECHO "this should NOT be printed" else ECHO "Variable deleted." endif`

configure cli mode scripting abort-on-error

- Configures the script to halt when an error occurs. If there is a syntax error in the script constructs (set var / if ..then / do..while), execution stops even if the abort_on_error flag is not configured.
- Switch Compatibility — Devices running ExtremeXOS/Switch Engine 11.6 and higher support this command.
- Example — `enable cli scripting \$UPPERCASE uppercase # should not print show var abort_on_error`

ExtremeCloud IQ Site Engine-Specific System Variables

The following system variables can be set in ExtremeCloud IQ Site Engine scripts:

$abort_on_error
Whether the script terminates if a CLI error occurs: 1 aborts on error; 0 continues on error.

$CLI.OUT
The output of the last CLI command.

$CLI.SESSION_TYPE
The type of session for the connection to the device, either Telnet or SSH.

NOTE: Variables with TCL special characters must be enclosed in braces. For example, when using the system variables `$CLI.SESSION_TYPE` and `$CLI.OUT` in a script, they must be entered as `${CLI.SESSION_TYPE}` and `${CLI.OUT}`, respectively.

$date
The current date on the ExtremeCloud IQ Site Engine server.

$deviceIP
The IP address of the selected device.

$deviceLogin
The name of the login user for the selected device.

$deviceName
The DNS name of the selected device.

$deviceSoftwareVer
The version of ExtremeXOS/Switch Engine running on the selected device.

$deviceType
The product type of the selected device.

$netsightUser
The name of the ExtremeCloud IQ Site Engine user running the script.

$isExos
Indicates whether the device is an ExtremeXOS/Switch Engine device. Possible values are True or False.

$port
Selected port numbers, represented as a string. If the script is not associated with a port, this system variable is not supported.

$serverIP
The IP address of the ExtremeCloud IQ Site Engine server.

$serverName
The host name of the ExtremeCloud IQ Site Engine server.

$serverPort
The port number used by the ExtremeCloud IQ Site Engine web server; for example, 8080.

$STATUS
The execution status of the previously executed ExtremeXOS/Switch Engine command: 0 if the command executed successfully; non-zero otherwise.

$time
The current time on the ExtremeCloud IQ Site Engine server.

$vendor
Vendor name of the device; for example, Extreme.

FlexViews

FlexViews provide a convenient way for Operations people to view device data. These views are accessible from ExtremeCloud IQ Site Engine Devices and do not require the installation of any software (including ExtremeCloud IQ Site Engine) other than the browser itself.

You can also addadd your own custom FlexViews in ExtremeCloud IQ Site Engine.

Configure the options on the **Administration** > **Options** > FlexView tab to determine the behavior of FlexViews in ExtremeCloud IQ Site Engine.

To launch a FlexView, you must be a member of an authorization group that is assigned the OneView > FlexView > OneView FlexView Read Access capability. To launch and edit a FlexView, you must be a member of an authorization group that is assigned the OneView > FlexView > OneView FlexView Read/Write Access capability.

This Help topic provides information on the following topics:

- Browser Requirements
- Launching FlexViews
- Using FlexViews
    - Editing Writable Values
    - Exporting Table Data

Browser Requirements

The following web browsers are supported:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome

Enable JavaScript in your browser for the views to function. To avoid impaired functionality, enable cookies for your browser. This includes (but is not limited to) the ability to persist table configurations such as filters, sorting, and column selections.

Launching FlexViews

Use the following steps to launch and open a FlexView from the **Network** tab.

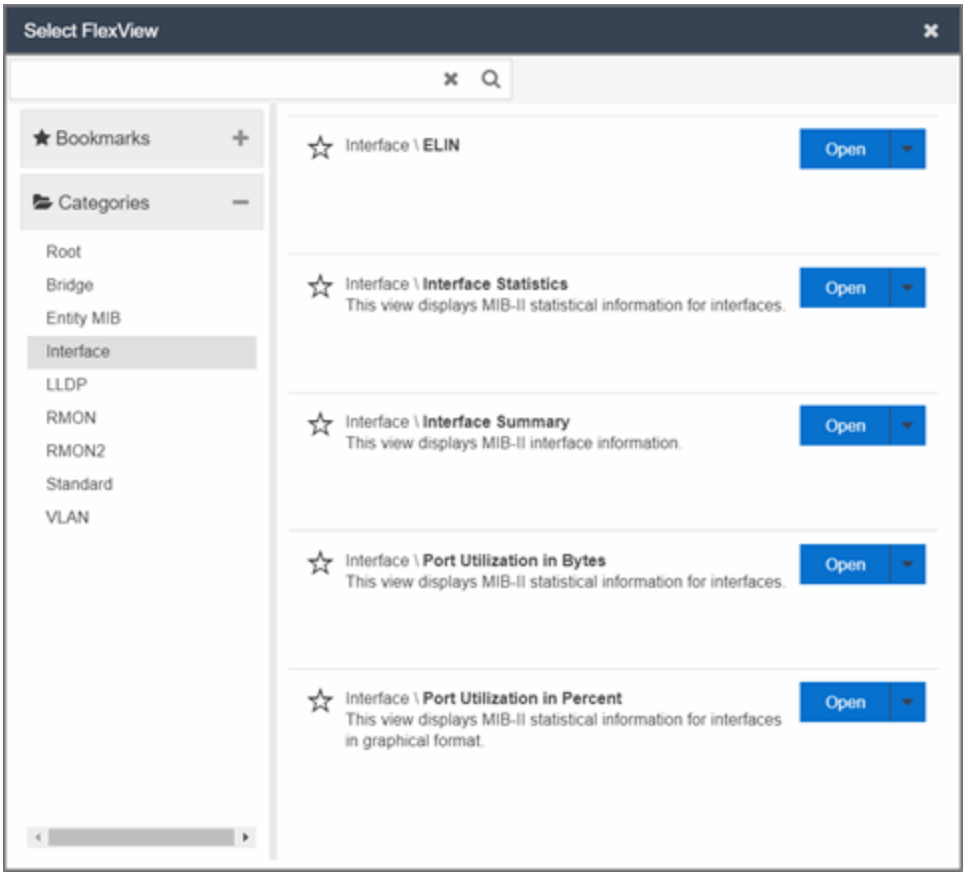
1. Launch ExtremeCloud IQ Site Engine and select **Network** > **Devices**.
2. Select one or more devices in the **Devices** tab left panel or from within the Devices list.

NOTE: When you select multiple devices, a FlexView may take additional time to populate with data, depending on the number of rows displayed in the particular view. Because of this, we recommend that, for interface-based FlexViews, you select five devices or fewer.

3. Select the **Menu** icon (☰) and select **View** > **FlexView** from the menu.

   The **Select FlexView** window opens.

NOTE: The location and availability of FlexViews in the **Select FlexView** window changes depending on the configuration of the options on the **Administration** > **Options** > **FlexView** tab.



4. Select a FlexView in one of the following ways:

   - Expand the Bookmarks folder in the left panel to view the FlexViews that are bookmarked.

- Expand the Categories folder in the left panel. Select a **Category** from the left panel, depending on the type of FlexView you want to open.

NOTE: ExtremeCloud IQ Site Engine saves user-created Custom FlexViews in the **My FlexViews** Category.

5. Locate a FlexView in the right panel.

NOTE: Select the **Star** icon next to a FlexView in the right panel and select the device types for which it is applicable to save it in the Bookmarks folder in the left panel of the **Select FlexViews** window. This allows you to quickly find frequently used FlexViews.

6. Select the **Open** drop-down list and select whether you want to open the FlexView in a new tab or window.

The FlexView opens in a new tab or window, depending on what you select.

Using FlexViews

FlexViews let you manipulate the table data in several ways to customize the view for your own needs:

- Select the column headings to sort column data in ascending or descending order.
- Hide or display different columns by selecting a column heading drop-down arrow and selecting the column options from the menu.
- Rearrange columns by dragging a column heading to the desired position.
- Use the **Search** field to filter on and search for specific FlexView data.
- Set a Refresh Interval, which automatically refreshes the data at the specified interval.
- Edit the values in FlexView table columns containing a writable MIB object.
- In the toolbar at the top of the window, select **Retrieve from Devices** ( ) to clear all data and retrieve data again from selected Devices.
- In the status bar at the bottom of the window, select **Refresh from Cache** ( ) to show any new data collected since the last FlexView Update.

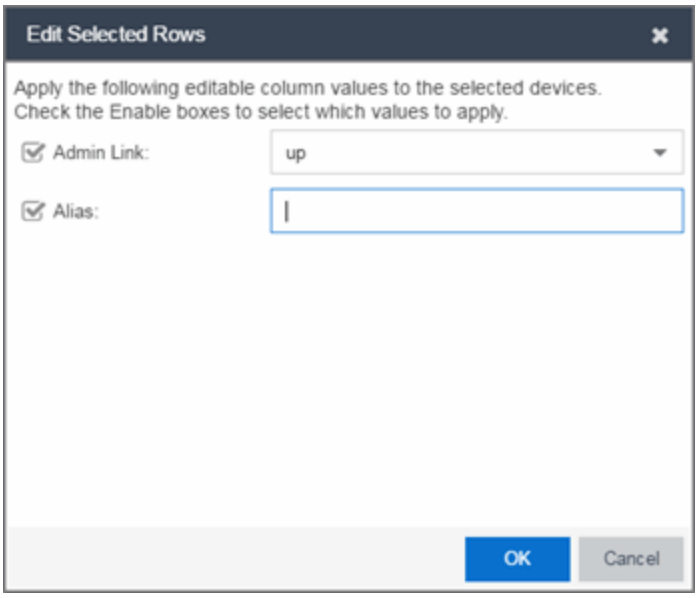
NOTE: Row creation and data exports are not currently supported in FlexViews.

Editing Writable Values

You can change the value in FlexView table columns that contain a writable MIB object.

1. Select one or more rows in the FlexView that contain columns with writable MIB objects, right-click and select **Edit Selected Rows**.

   The **Edit Selected Rows** window opens.



2. Select the writable objects you are changing and enter the appropriate values as needed.

   NOTE: Adding an alias to a port configures both ExtremeCloud IQ Site Engine and the CLI of the switch to display the character string.

3. Select **OK** to enter your changes into the selected rows. The new values are written directly to the device.

Bookmarking FlexViews

You can save frequently used FlexViews for each device type in the Bookmarks folder of the **Select FlexView** window. Bookmarks are shared among all ExtremeCloud IQ Site Engine users and provide your organization with the ability to select a FlexView without searching.

To add a FlexView to the Bookmarks folder, select the **Category** from the left panel and select the **Star** icon next to the appropriate FlexView in the right panel. Select the device types for which the FlexView is applicable and select **Save**. The FlexView is accessible from the Bookmarks folder when you access the Select FlexView window for a device that matches the device type configured for the FlexView.

Exporting Table Data

There are two methods of exporting the data in the table:

Export to CSV
Select to export all of the data in the table to a .CSV file. The exported data displays with any sorting, filtering, and searching applied.

Export Selected to CSV
Select to export the data in the currently selected row in the table to a .CSV file.

Add Custom FlexViews and MIBs

Use the instructions in this topic to add custom FlexViews and MIBs in ExtremeCloud IQ Site Engine.

To add a new FlexView to ExtremeCloud IQ Site Engine:

1. Create the following directory on the ExtremeCloud IQ Site Engine server: `/usr/local/Extreme_Networks/NetSight/appdata/VendorProfiles/Stage/MyVendorProfile/FlexViews/My FlexViews` if it does not already exist.
2. Add your custom FlexView files (.TPL) to the `/usr/local/Extreme_Networks/NetSight/appdata/VendorProfiles/Stage/MyVendorProfile/FlexViews/My FlexViews` directory on the ExtremeCloud IQ Site Engine server.
3. Add the MIB files that correspond to your custom FlexView files to the `/usr/local/Extreme_Networks/NetSight/appdata/VendorProfiles/Stage/MyVendorProfile/MIBs` directory on the ExtremeCloud IQ Site Engine server.
4. Log into the system shell (via the local console or SSH) on the ExtremeCloud IQ Site Engine server as root.
5. Restart the ExtremeCloud IQ Site Engine server:
    a. Enter `service nsserver stop`.
    b. Enter `service nsserver start`.

VLAN Concepts

The following concepts will assist you in configuring VLAN and port template definitions in ExtremeCloud IQ Site Engine.

Information on:

- Egress Rules (Transmitting Frames)
    - Dynamic Egress
        - GVRP
        - GARP Timers
- Enforcing
- Frame Types
- IGMP
    - Interface Robustness (Robustness Variable)
    - Last Member Query Interval

    - Query Interval
    - Query Response
- Ingress Filtering
- Priority Classification
    - Weighted Priority
- Verifying
- VLAN Identification
    - Port VLAN ID (PVID)
    - VLAN ID (VID)
- VLAN Model
- VLAN Learning

Egress Rules (Transmitting Frames)

A device determines which frames can be transmitted out a port based on the Egress List of the VLAN associated with it. Each VLAN has an Egress List that specifies the ports out of which frames can be forwarded, and specifies whether the frames will be transmitted as tagged or untagged frames. You can add or remove ports to or from a VLAN's Egress List, thereby controlling which VLAN's frames can be forwarded out which ports.

When a frame is transmitted out a port, the device first checks the Egress List. If the port is listed on the Egress List of the VLAN associated with it, the frame is then transmitted according to the priority assigned to the frame. The frame is transmitted as tagged or untagged according to the specification in the Egress List. If the port is not on the Egress List, or if the port is not operational, the frame is discarded.

Dynamic Egress

In ExtremeCloud IQ Site Engine, you can control whether or not Dynamic Egress is enabled for a VLAN in the VLAN Definitions table. When Dynamic Egress is enabled for a VLAN, any time a device tags a packet with that VLAN ID, the ingress port is automatically added to the VLAN's egress list, enabling the reply packet to be forwarded back to the source. This means that you do not need to add the ingress port to the VLAN's egress list manually. (See Example 1, below.)

Dynamic Egress affects only the egress lists for the source and destination ingress ports. You can enable GVRP (GARP VLAN Registration Protocol), which automatically adds the interswitch ingress ports to the egress lists of VLANs. (See Example 2, below.)

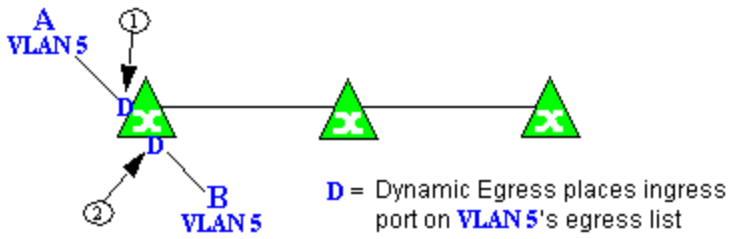
When you disable Dynamic Egress for a VLAN, the VLAN effectively becomes a discard VLAN. Since the destination port is not added to the egress list of the VLAN, the device discards the traffic. If you want a VLAN to act as a discard VLAN, disable Dynamic Egress for that VLAN. (See Example 3, below.)

If an endstation is talking to a "silent" endstation which does send responses, like a printer, you will need to add the silent endstation's ingress port to the VLAN's egress list manually with a tool like ExtremeCloud IQ Site Engine Device Manager, or local management. Dynamic Egress and GVRP take care of adding the other ingress ports to the VLAN's egress list. (See Example 4, below.)

CAUTION: If no packets are tagged with the applicable VLAN on a port within five minutes, Dynamic Egress list entries will time out. The result is that an endstation will appear "silent" if the VLAN has not been used within that time period. For example, if there is a "telnet" rule and two users (A & B) are on ports whose role includes a service containing the "telnet" rule, if User B has not utilized the "telnet" rule within the five minute time frame, User A will not be able to telnet to User B. For this reason, the best application of Dynamic Egress is for containing undirected traffic on "chatty" clients which utilize, for example, IPX, NetBIOS, AppleTalk, and/or broadcast/multicast protocols such as routing protocols.

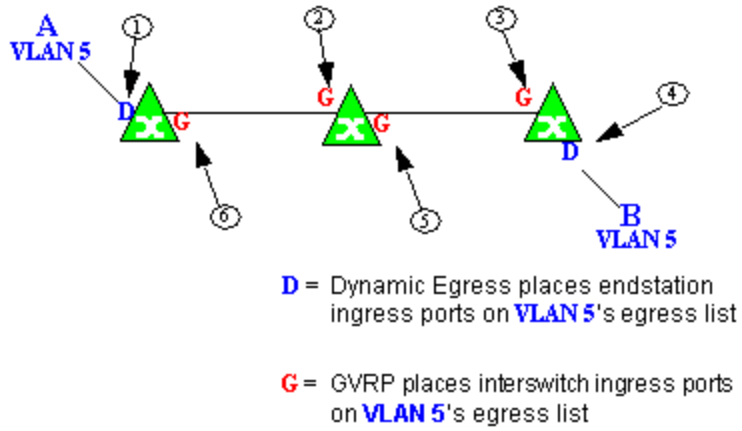
Example 1: Dynamic Egress Enabled

In this example, Dynamic Egress is enabled for VLAN 5. When source endstation A is tagged with VLAN 5, Dynamic Egress places A's ingress port (1) on VLAN 5's egress list. When destination endstation B's traffic is tagged with VLAN 5, Dynamic Egress places B's ingress port (2) on VLAN 5's egress list. The device can then forward traffic to both endstations.



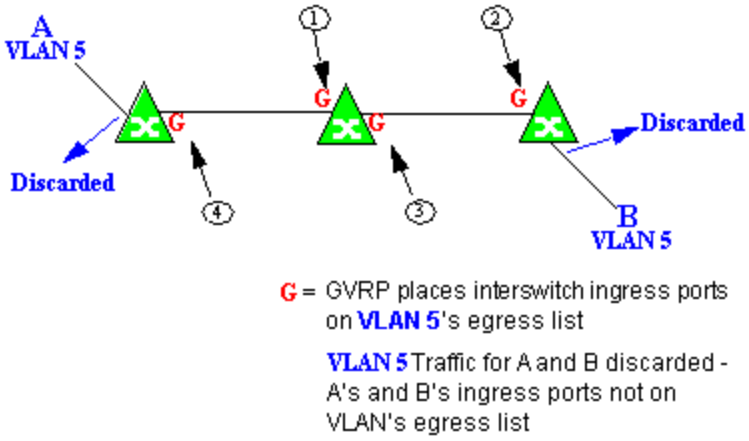
Example 2: Dynamic Egress + GVRP

In this example, Dynamic Egress is enabled for VLAN 5, and the destination endstation, B, is on a different device from the source endstation, A. When A is tagged with VLAN 5, Dynamic Egress places A's ingress port (1) on VLAN 5's egress list. GVRP then places interswitch ingress ports (2) and (3) on VLAN 5's egress list. When B's traffic is tagged with VLAN 5, Dynamic Egress places B's ingress port (4) on VLAN 5's egress list. GVRP then places interswitch ingress ports (5) and (6) on VLAN 5's egress list. The devices can then forward traffic to both endstations.



Example 3: Dynamic Egress Disabled

In this example, Dynamic Egress is disabled. When source endstation A is tagged with VLAN 5, A's ingress port is not placed on VLAN 5's egress list. GVRP places interswitch ingress ports (1) and (2) on VLAN 5's egress list. When B's traffic is tagged with VLAN 5, B's ingress port is not placed on VLAN5's egress list. GVRP places interswitch ingress ports (3) and (4) on VLAN 5's egress list. But VLAN 5 traffic for both A and B is discarded, because VLAN 5 is not aware of the ingress ports for A and B.



Example 4: Silent Endstation

In this example, Dynamic Egress is enabled for VLAN 5, but the destination endstation, B, is a "silent" endpoint, like a printer. Endstation B does not send responses, so the Administrator must place B's ingress port on VLAN 5's egress list manually (1). When A is tagged with VLAN 5, Dynamic Egress places A's ingress port (2) on VLAN 5's egress list. GVRP then places interswitch ingress ports (3) and (4), then (5) and (6) on VLAN 5's egress list. Endstation A is then able to communicate with the printer.

GVRP

GVRP (GARP VLAN Registration Protocol) dynamically adds interswitch ingress ports to the egress lists of VLANs across a domain.

NOTE: If you do not want GVRP enabled on your network, you can disable it, then manually configure the interswitch ports to do what GVRP does automatically, using MIB Tools or local management to set up your interswitch links as Q trunks. The trunk ports will be automatically added to the egress lists of all the VLANs at the time of trunk configuration.

GARP Timers

Set GARP timers on the device to control the timing of dynamic VLAN membership updates to connected devices. The timer values must be identical on all connected devices in order for GVRP to operate successfully.

- **Join Time** – Frequency of messages issued when a new port has been added to the VLAN. Possible values are 1 through 1488800 milliseconds.
- **Leave Time** – Frequency of messages issued when a single port no longer belongs to the VLAN. This value must be at least three times greater than the Join Time. Possible values are 1 through 1488800 milliseconds.
- **Leave All Time** – Frequency of messages issued when all ports no longer belong to the VLAN and the VLAN should be deleted. This value must be greater than the value for Leave Time. Possible values are 1 through 1488800 milliseconds.

Enforcing

When working with VLANs in ExtremeCloud IQ Site Engine, write the definitions in the VLAN model to selected devices or ports by selecting the **Enforce** button in the Configure Device window.

NOTE: On the X-Pedition router, enforcing will not overwrite the "System Static" VLAN (SYS_L3_Interface Name).

Frame Types

Incoming frames are processed according to ingress rules which determine the VLAN membership and transmission priority of a frame received on a port by checking for the presence of a VLAN tag. A VLAN tag is a field within a frame that identifies the frame's VLAN membership and priority.

Frames can be tagged or untagged. A tagged frame is a frame that contains a VLAN tag. An untagged frame does not have a VLAN tag, but will be tagged when it is received on a port. A tagged frame may have already been processed by an 802.1Q switch or originated at an endpoint capable of inserting a

VLAN tag into a frame. A VLAN tag may or may not contain a VLAN ID (VID), but it will always contain priority information. End systems are allowed to transmit frames with only a priority in the VLAN tag. When switches transmit a tagged frame, the VLAN tag will always include a VID along with the priority.

Tagged and untagged frames are assigned VLAN membership and transmission priority differently:

Untagged Frame - VLAN Membership
When an untagged frame is received on a port, if a VLAN Classification rule exists for the frame's classification type, the frame will gain membership in the associated VLAN. If not, the frame will be assigned to the VLAN identified as the port's VLAN ID (PVID).

Untagged Frame - Priority Assignment
When an untagged frame is received on a port, if a Priority Classification rule exists for the frame's classification type, the frame will be assigned the associated priority. If not, the frame will be assigned the port's default priority.

Tagged Frame - VLAN Membership
If a tagged frame includes a VID (VLAN ID), it will gain membership in the VLAN indicated by the VID. If not, and a VLAN Classification rule exists for the frame's classification type, the frame will be put into the associated VLAN. If there is no VID or classification rule, the frame will be put in the VLAN associated with the port's VLAN ID (PVID).

Tagged Frame - Priority Assignment
When a tagged frame is received on a port, it is assigned the priority contained in the VLAN tag.

You can set the acceptable frame type for a port in Ports.

IGMP

IGMP (Internet Group Management Protocol) is a protocol used by IP hosts and their immediate neighbor multicast agents to support the allocation of temporary group addresses and the addition and deletion of members of a VLAN. You can enable and disable IGMP in VLAN Definitions.

IGMP Intervals

You can control the following IGMP query settings in VLAN Definitions:

- **Query Interval** - Interval (in seconds) between general IGMP queries sent by the device to solicit VLAN membership information from other devices. By setting this interval, you can control the number of IGMP messages on a subnet. Larger values cause queries to be sent less often. The Query Interval must be greater than the Query Response interval. Valid values: 1 through 300 seconds.
- **Query Response** - Maximum amount of time allowed for responses to general IGMP queries. By setting this value, you can control the burstiness of IGMP messages on a subnet. Larger values result in less bursty traffic, because host responses are spread over a larger interval. This value must be less than the Query Interval. Valid values: 1 through 300.

- **Interface Robustness (Robustness Variable)** - Indicates the susceptibility of the subnet to lost packets. If a subnet is particularly susceptible to losses, you may wish to increase this value. IGMP is robust to (Robustness Variable-1) packet losses. The Interface Robustness value is used in the calculation of IGMP message intervals. Valid values are 2 thru 32767.
- **Last Member Query Interval** - Maximum amount of time (in seconds) between group-specific query messages, including those sent in response to leave-group messages. By setting this value, you can control the "leave latency" of the network. You might lower this interval to reduce the amount of time it takes the device to detect the loss of the last member of a group. Valid values: 10 through 32767 seconds.

Ingress Filtering

Ingress Filtering is a means of filtering out undesired traffic on a port. When Ingress Filtering is enabled, a port determines if a frame can be processed based on whether the port is on the Egress List of the VLAN associated with the frame. For example, if a tagged frame with membership in the Sales VLAN is received on a Port 1, and Ingress Filtering is enabled, the switch will determine if the port is on the Sales VLAN's Egress List. If it is, the frame can be processed. If it is not, the frame is dropped. You can set ingress filtering for a VLAN in Ports.

Priority Classification

Priority Classification is used to assign frames transmission priority over other frames. Priority is a value between 0 and 7 assigned to each frame as it is received on a port, with 7 being the highest priority. Frames assigned a higher priority will be transmitted before frames with a lower priority.

Each of the priorities is mapped into a specific transmit queue by the switch or router. The insertion of the priority value (0-7) allows all 802.1Q devices in the network to make intelligent forwarding decisions based on its own level of support for prioritization.

Frames can be assigned a transmission priority ;based on the default priority of the receiving switch port, regardless of the frame's classification type. However, with the addition of classification rules, frames can be assigned a priority based on the frame's classification type. Using priority classification rules, network administrators can classify a frame based on Layer 2/3/4 information to have higher or lower priority than other frames on a per port basis, allowing for better defined Class of Service configurations.

You can set the default priority for incoming frames in Ports.

Weighted Priority

Weighted priority, available on certain devices, is a way to further refine priority classification. You can control this setting in Ports.

Some devices support four transmit queues (0-3) per port. These queues can be serviced based on a strict method, meaning that all frames in Queue 3 will be transmitted before the frames in Queue 0, or

based on a fair weighted method. The weighted method allows the network administrator to give a certain percentage or weight to each queue, preventing a lower priority queue from being starved.

Forwarding priority can be tuned to allocate a percentage of a port's transmit resources to the each traffic queue. This lets you adjust a strict priority scheme to guarantee that some percentage of frames from lower priority queues will always be sent. Weighted priority settings divide each port's transmit resources into 16 equal parts, which can be allocated to traffic queues in increments of 6.25% (1/16th). The total resource allocation for a port must always add up to 100%.

To understand the effect of weighted priorities, consider a device port with strict priority settings. In this case, all of the frames from the highest priority traffic queue are sent before frames are sent from any of the lower priority queues. Now, assuming four traffic queues, assign weighted priorities for the port giving 50% of the transmit resources to Queue 3, 25% to Queue 2, and 25% to Queue 1 and 0% to Queue 0. With these settings, at least 50% of the frames will be transmitted from Queue 3, at least 25% from Queue 2, at least 25% from Queue 1 and frames will only be transmitted from Queue 0 when Queue 1, 2, and 3 are empty.

Verifying

Verifying retrieves the VLAN settings on the selected devices and compares them with the settings in the selected VLAN Definitions or Ports.

Differences are indicated by a red not-equals symbol ≠. A green exclamation point ! is displayed when you select a ≠ line in the table to the model setting that will be written to the device when you enforce. You can review the differences and make modifications to your model as needed, including updating the definitions in your model using the definitions from the selected devices.

VLAN Identification

VLAN identifiers include VLAN ID's and Port VLAN ID's.

VLAN ID (VID)

802.1Q VLANs are defined by VLAN IDs (VIDs) and VLAN names.

VID

A unique number between 1 and 4094 that identifies a particular VLAN. VID 1 is reserved for the Default VLAN.

VLAN Name

An alphanumeric name associated with a VLAN ID, used to make VLANs easier to identify and remember (up to 64 characters).

PVID (Port VLAN ID)

You can change a port's VLAN membership to reflect the specific needs of your network by assigning new VLAN membership to the port. When you assign VLAN membership to a port, that VLAN's ID (VID) becomes the Port VLAN ID (PVID) for the port and the port is added to the VLAN's Egress List.

PVID
The PVID (Port VLAN ID) represents a port's VLAN assignment. Possible values are 1 through 4094.

Egress List
The Egress List specifies which ports can transmit the frames associated with the VLAN.

NOTE: On the X-Pedition Router, you cannot assign a PVID to a port that has an interface assigned to it.

VLAN Model

In ExtremeCloud IQ Site Engine, you can create VLAN models and enforce them across multiple network devices. A VLAN model consists of at least one VLAN Definition and one VLAN Port Template.

ExtremeCloud IQ Site Engine provides you with one VLAN model (the Primary VLAN Model) which is pre-populated with a Default VLAN (VID 1). You can further define this VLAN model, and/or you can create other VLAN models. (The Default VLAN for a model cannot be deleted.)

Once a VLAN model has been created, you can utilize it in the following ways:

- Enforce the properties of a port template on selected devices. You can also make custom edits for selected ports.
- Perform a more detailed analysis of the differences between the definitions in the VLAN model and the VLAN settings on selected devices and their ports. Using these views in the Network > Device tab, you can review the differences and make modifications to your VLAN model and/or device or port VLAN configuration as required, including updating any or all of the definitions in the model with the settings on selected devices and their ports, and writing (enforcing) a model's VLAN definitions and/or VLAN port templates to selected devices or ports.

See Create and Edit a VLAN on a Device for more information.

VLAN Learning

VLAN learning allows the creation of groups of VLANs that will share Filtered Database information (MAC address, port, and VLAN ID) according to 802.1Q Shared Learning Constraints (IEEE Std 802.1Q-1998). This helps to speed MAC to port lookups and reduce flooding, because MAC addresses will be in the same Filtering Database.

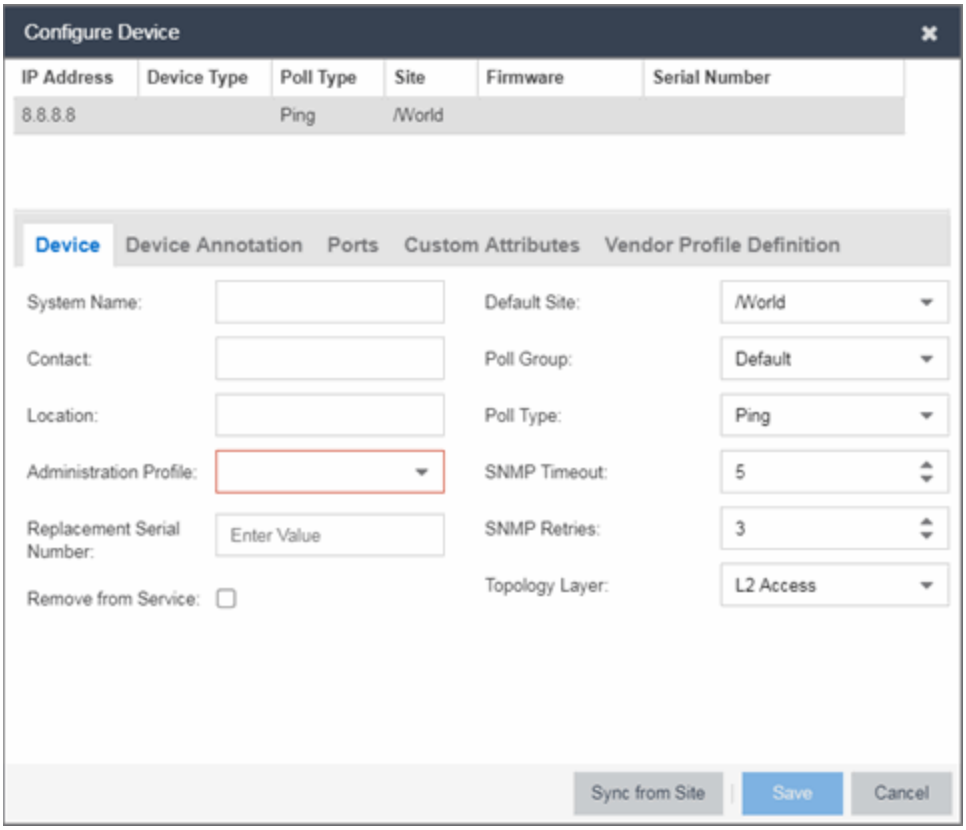
Create and Edit a VLAN on a Device

This section outlines how to create and edit a VLAN. From the Network tab, you can:

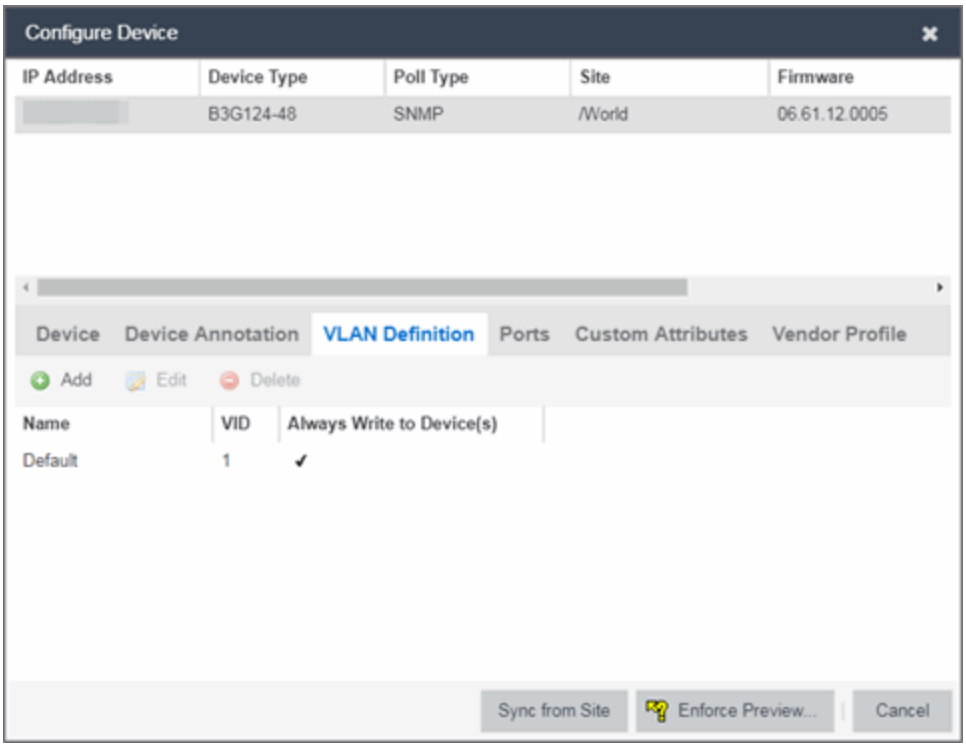
- Create a new VLAN
- Edit the ports of an existing VLAN
- Edit the name of an existing VLAN
- Remove devices from an existing VLAN

To create a new VLAN:

1. Launch ExtremeCloud IQ Site Engine.
2. Open the **Network > Devices** tab.
3. Select the device from the devices list. Right-click the device and select **Device > Configure Device**.
   The **Configure Device** window opens.

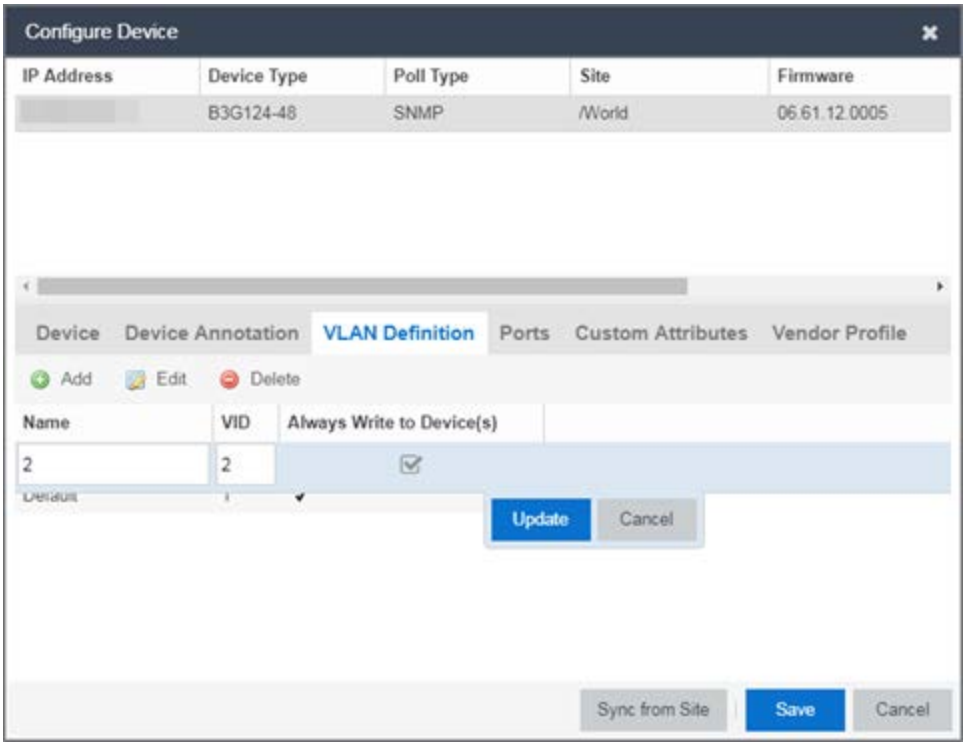


4. Select the **VLAN Definition** tab.



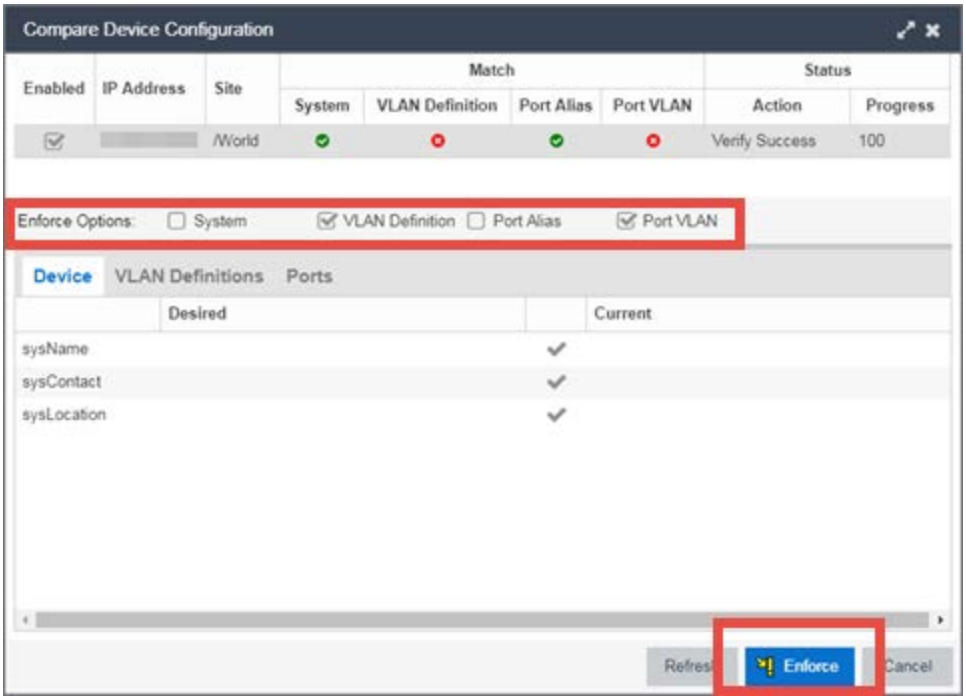
5. Select the **Add** button.

6. Enter the **Name** and the **VID** for the new VLAN.



7. Select **Update**.
   The new VLAN is added to the list.
8. Select **Enforce Preview**.

9. Under the Enforce Options, select the **VLAN Definition** checkbox and select **Enforce**.



NOTE:

By default, the checkboxes in the Enforce Options section of the window are not selected. To configure ExtremeCloud IQ Site Engine to select the checkboxes by default, open the `NSJBoss.properties` file and change **false** to **true** in the following lines:

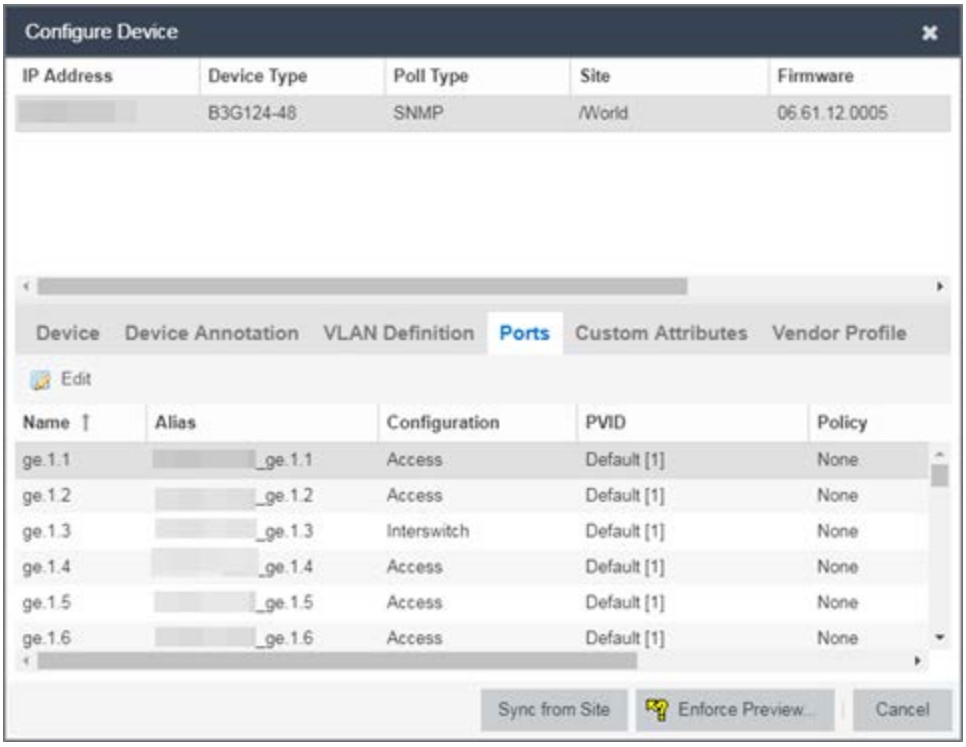
- `site.enforceOption.autoEnable.system=false`
- `site.enforceOption.autoEnable.vlanDefinition=false`
- `site.enforceOption.autoEnable.portAlias=false`
- `site.enforceOption.autoEnable.portVlan=false`

The VLAN is now created and assigned to the device.

To configure the VLAN(s) on the ports

1. Launch ExtremeCloud IQ Site Engine.
2. Open the **Network > Devices** tab.
3. Select the device from the devices list.
4. Right-click the device and select **Device > Configure Device**.
   The **Configure Device** window opens.

5. Select the **Ports** tab.



6. Select the Port on which you are configuring the VLAN.
7. Select **Edit**.
   The Port is now configurable.
8. Change the **PVID**, **Tagged**, and **Untagged** options to configure the VLAN onto the port.
9. Select **Enforce Preview**.
10. Under the Enforce Options, select the **Port VLAN** checkbox and select **Enforce**.

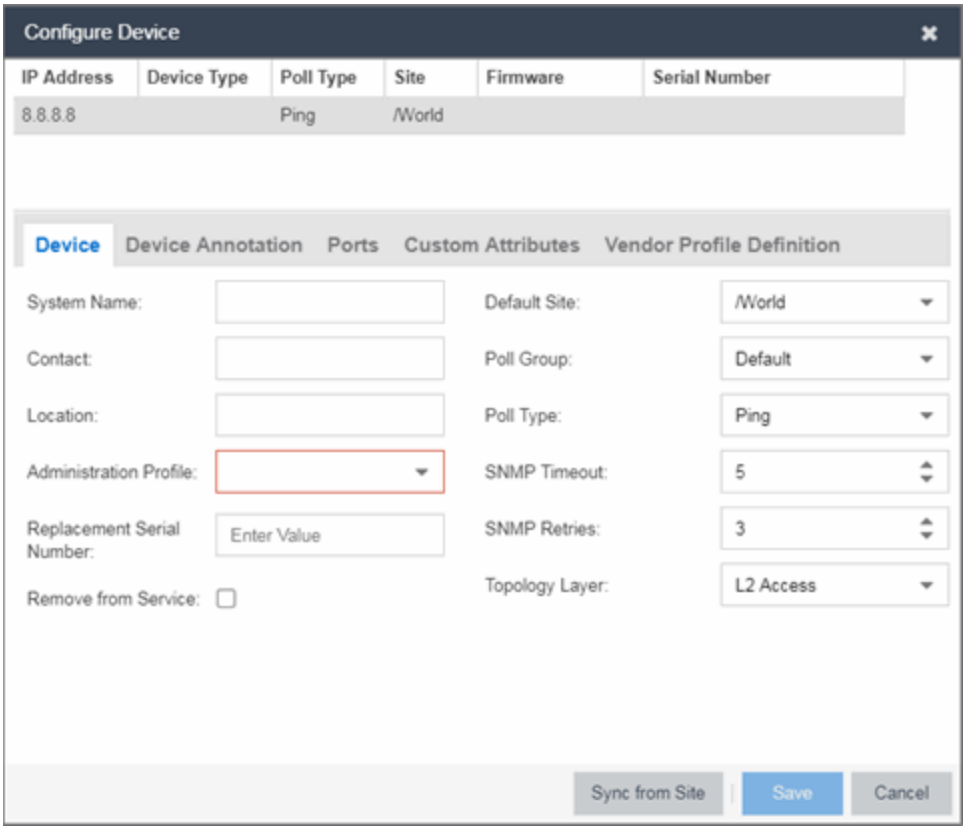
NOTE: By default, the checkboxes in the Enforce Options section of the window are not selected. To configure ExtremeCloud IQ Site Engine to select the checkboxes by default, open the `NSJBoss.properties` file and change **false** to **true** in the following lines:

- `site.enforceOption.autoEnable.system=false`
- `site.enforceOption.autoEnable.vlanDefinition=false`
- `site.enforceOption.autoEnable.portAlias=false`
- `site.enforceOption.autoEnable.portVlan=false`

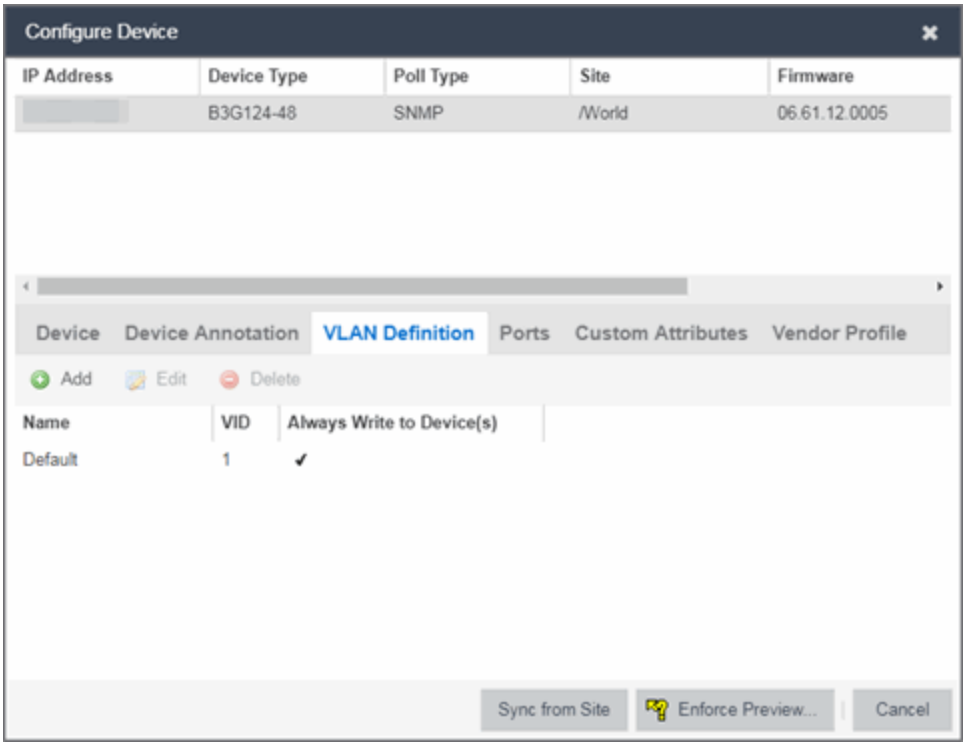
The VLAN is now configured to the Ports.

To edit the name of a VLAN:

1. Launch ExtremeCloud IQ Site Engine.
2. Open the **Network > Devices** tab.
3. Select the device from the devices list.
4. Right-click the device and select **Device > Configure Device**.
   The **Configure Device** window opens.



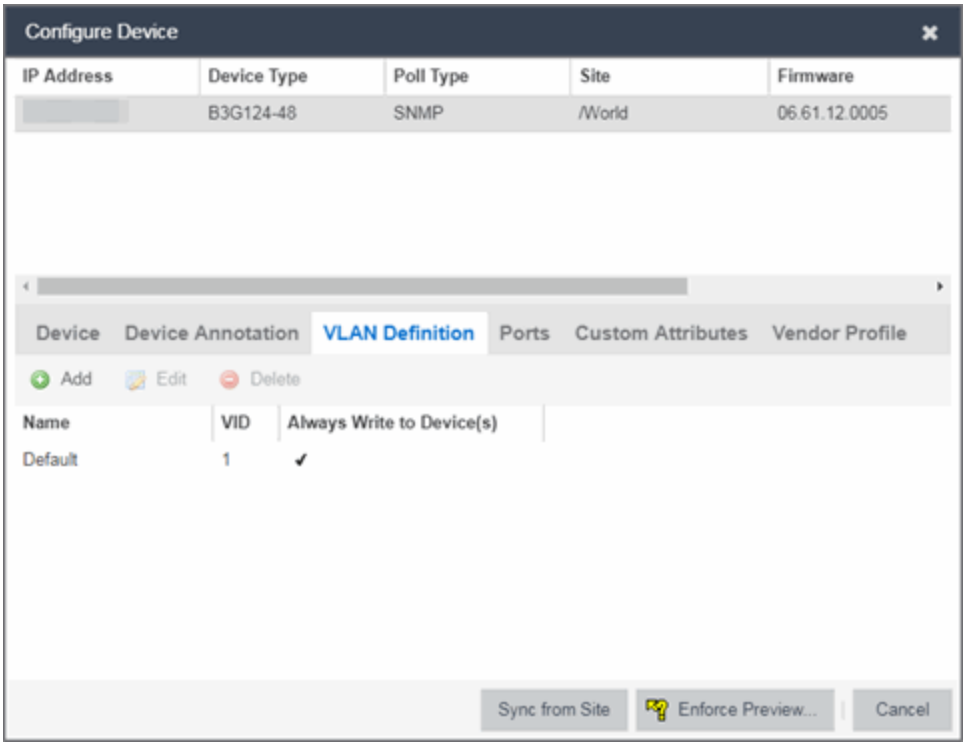
5. Select the **VLAN Definition** tab.



6. Select the VLAN to edit and then select the **Edit** button.
7. Enter the new name for the VLAN.
8. Select **Update**.
   The Edit pane closes.
9. Select **Save** to exit the VLAN Definition window. The VLAN is updated.

To remove devices from a VLAN:

1. Launch ExtremeCloud IQ Site Engine.
2. Open the **Network > Devices** tab.
3. Select the device from the devices list. Right-click the device and select **Device > Configure Device**.
   The **Configure Device** window opens.
4. Select the **VLAN Definition** tab.
   The VLAN Definition pane opens.



5. Select the VLAN and select **Delete**.

Discover Devices

ExtremeCloud IQ Site Engine allows you to discover the devices of your network and add them to the ExtremeCloud IQ Site Engine database.

NOTE: Before discovering devices, create the maps to which they belong. For additional information on creating maps, see How to Create and Edit Maps.
For a list of instructions outlining the initial setup of your network in ExtremeCloud IQ Site Engine, see ExtremeCloud IQ Site Engine Initial Configuration Checklist.

You can discover new devices based on the following criteria:

- Seed addresses for CDP, LLDP, EDP, or SONMP-compliant devices
- IP/Subnet masks
- IP Address Range

Discover automatically explores the defined network segment and creates a list of discovered devices. You can then save the discovered devices to the ExtremeCloud IQ Site Engine database, where they are displayed in the left-panel tree on the **Network** > **Devices** tab.

NOTE: When adding an ExtremeXOS/Switch Engine device in ExtremeCloud IQ Site Engine, enter the following commands in the device CLI:

```
configure snmpv3 add community "private" name "private" user "v1v2c_rw"
configure snmpv3 add community "public" name "public" user "v1v2c_rw"
enable snmp access
enable snmp access snmp-v1v2c
disable snmp access snmpv3
```

To discover devices, begin by using the Site tab to configure the default settings that apply to devices you add to ExtremeCloud IQ Site Engine and then configure individual devices and add them to the ExtremeCloud IQ Site Engine database via the Discovered tab.

NOTE: ZTP+ enabled devices use a different device discovery process. For additional information on discovering devices using ZTP+, see ZTP+ Device Configuration in ExtremeCloud IQ Site Engine.

Discovering Devices

1. Open the **Network** > **Devices** tab.
2. Select **Sites** from the left-panel drop-down list.
3. Select the site from the left panel to which you are adding the devices.
4. Select the **Site** tab in the right-panel.
5. Select the **Discover** tab.
6. Select the **Add** button in the Addresses list to open the Add Address window.
7. Select **Subnet**, **Seed Address**, or **Address Range** in the **Discover Type** drop-down list.
8. Enter the **Subnet**, **Seed Address**, or **Start Address** and **End Address**, depending on the **Discover Type** you select.
    - **Subnet** — Enter the IP address and subnet in the following format: *IP Address*/*Subnet Mask*
        - The *IP Address* must be one of the hosts in the subnet.
        - A **/** is required between the IP Address and Subnet Mask.
        - The *Subnet Mask* must use CIDR or dotted decimal notation.

          NOTE: When using dotted decimal notation, the network bits must be contiguous ones and the host bits must be contiguous zeros.
    - **Seed Address** — Enter the seed address for CDP, LLDP, EDP, SONMP-compliant devices.

- **Address Range** — Enter the **Start Address** and **End Address** for the IP addresses in the same address range.

NOTE: ExtremeCloud IQ Site Engine only allows a subnet search of a 16-bit mask or higher when discovering devices.

9. Select the **Add** button in the Profiles section of the window to open the Add Profile window. Select **New** in the drop-down list to create SNMP and CLI credentials for the profile and select the **Save** button.

   Profiles allow you to configure different sets of SNMP and CLI credentials for read access, write access, and maximum access. After you create profiles, assign them to devices to allow users appropriate access based on the credentials they use for a device.

10. Select the profiles you want the devices on your network to **Accept** or **Reject** using the **Profiles** list.
    For additional information about profiles, see **Profiles** tab.

11. Select the **Automatically Add Devices** checkbox to automatically add the devices to ExtremeCloud IQ Site Engine and configure any other appropriate actions for your devices in the Device Actions section of the window.

NOTE: When **Automatically Add Devices** is selected, devices are automatically added to ExtremeCloud IQ Site Engine and display in the Devices list on the Network > **Devices** tab. When **Automatically Add Devices** is not selected, devices are displayed on the Network > **Discovered** tab and require you to manually add them.

12. Repeat the process for all devices added to this site.
    For additional information about sites, see **Site** tab.

13. Select **Save**.

14. Select **Discover**.

15. Select the **Clock** icon in the Top menu to open the Operations table at the bottom of the ExtremeCloud IQ Site Engine window to monitor the progress of the device discovery.

16. Access the Network > **Discovered** tab.

NOTE: The devices displayed on this tab vary depending on whether you selected **Automatically Add Devices** in Step 11.

17. Configure and add any devices displayed to ExtremeCloud IQ Site Engine:

    - If you selected **Automatically Add Devices**, devices display on the **Discovered** tab only if they require additional attention (for example, devices are potential duplicates of another device). Configure the devices appropriately and add them to ExtremeCloud IQ Site Engine.

- If you did not select Automatically Add Devices, all devices are staged on the Discovered tab before being added to ExtremeCloud IQ Site Engine. Follow the steps in the Adding Devices section to complete the process of adding your devices to ExtremeCloud IQ Site Engine.

Adding Devices

If you did not select **Automatically Add Devices** in Step 11, use the **Discovered** tab to manually add the discovered devices to ExtremeCloud IQ Site Engine.

1. Open the **Network** > **Discovered** tab in ExtremeCloud IQ Site Engine.
2. Select the devices you want to add to the ExtremeCloud IQ Site Engine database and select the **Add Devices** button. The Add Devices window opens.
   The window is populated with the information you entered on the **Site** tab.
3. Enter any device-specific information, or change information that does not match the device defaults set on the **Site** tab.
4. Select the **Add** button.
   The devices are added to the ExtremeCloud IQ Site Engine database and move from the **Network** > **Discovered** tab to the **Network** > **Devices** tab.

Add Users

Users are given access to parts of ExtremeCloud IQ Site Engine based on the authorization group to which they are assigned. Assign a set of capabilities for each authorization group and then add users to each authorization group depending on the capabilities they require.

NOTE: This topic assumes devices are already added to the ExtremeCloud IQ Site Engine database. For additional information on discovering and adding devices, see Discover Devices in ExtremeCloud IQ Site Engine.

For a list of instructions outlining the initial setup of your network in ExtremeCloud IQ Site Engine, see ExtremeCloud IQ Site Engine Initial Configuration Checklist.

When you first log into ExtremeCloud IQ Site Engine the Administrator access through which you are currently logged in is the only set of user credentials.

This topic describes the process for adding users to ExtremeCloud IQ Site Engine, which is accomplished by performing the following steps:

1. Create Authorization Groups
2. Add Users to Authorization Groups
3. Select the Authentication Method

IMPORTANT: ExtremeCloud IQ Site Engine does not save passwords. Users you create are authenticated against the Operating System, the RADIUS server, the LDAP server, the TACACS+ server, or Okta SSO depending on the authentication method you select.

Create Authorization Groups

First, create authorization groups for each group of ExtremeCloud IQ Site Engine users.

1. Access the **Administration** > **Users** tab.
2. Select the **Acquire Lock** button in the Users/Groups Access section at the top of the tab. This button locks access to the tab for all other users and enables you to make changes to the authorization groups and authorized users.
3. Select the **Add** button in the Authorization Groups section at the bottom of the tab.
4. Enter the appropriate information for each authorization group using ExtremeCloud IQ Site Engine.
   The Capability section of the window enables you to expand each capability tree by selecting the arrow to the left of the checkbox to display more specific tasks. Select only those that apply to each user group. Additionally, you can search for a specific capability in the **Search** field above the tree.
5. Select the **Save** button to create the authorization group.
6. Repeat the process to create the necessary authorization groups.

Add Users to Authorization Groups

Next, use of the Administration > Users tab to create the users who require access to ExtremeCloud IQ Site Engine and add them to an authorization group depending on the level of access they require.

1. Select the **Add** button in the Authorized Users section.
2. Enter a User Name, a Domain/Host Name (if necessary), and select the Authorization Group with the appropriate level of access for the user.
3. Select the **Save** button to save the new user.
4. Repeat the process to add all ExtremeCloud IQ Site Engine users for each authorization group.

Select the Authentication Method

Finally, use Administration > Users tab to select the method by which users authenticate when accessing ExtremeCloud IQ Site Engine.

ExtremeCloud IQ Site Engine supports five different authentication methods to authenticate users: using the host Operating System, using an LDAP configuration, using RADIUS servers, using an TACACS+ configuration, or using an Okta SSO configuration.

1. Select the **Authentication Type** using the drop-down list in the Authentication Method section.
   The options change based on the **Authentication Type** selected.
2. Select the supplemental information based on the type selected.
3. Select the **Release Lock** button to enable other users to make changes.

The users you added now have access to the functionality you configured for their respective authorization group.

How to Integrate and Configure Okta SSO Authentication for ExtremeCloud IQ Site Engine Users

This help topic describes the steps for integrating Okta Single Sign-On (SSO) authentication for ExtremeCloud IQ Site Engine users. Users are given access to parts of ExtremeCloud IQ Site Engine based on the authorization group to which they are assigned.

When you first log into ExtremeCloud IQ Site Engine the Administrator access through which you are currently logged in is the only set of user credentials.

This topic describes the process for adding users to ExtremeCloud IQ Site Engine, which is accomplished by performing the following steps:

1. Requirements
2. Create the Application in Okta
3. Save the Values Required for the ExtremeCloud IQ Site Engine Configuration
4. Assign Users to the Okta Application
5. Configure the Okta Authentication Method in ExtremeCloud IQ Site Engine

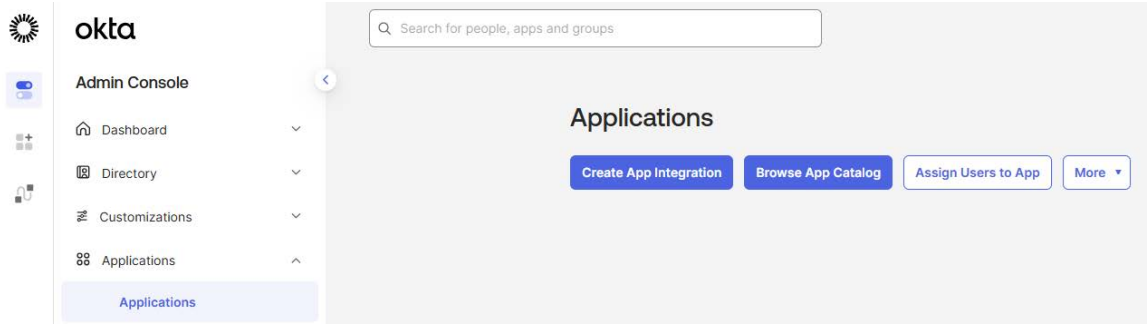
Requirements

- You must have access to the **Okta Admin Console**.
- You must have an **Okta Verify application** (provided by Okta).
- ExtremeCloud IQ Site Engine must have **network access to your Okta URL**.
- You must **refresh the Okta certificate periodically** before expiry. (Okta certificate is typically valid for 10 years).

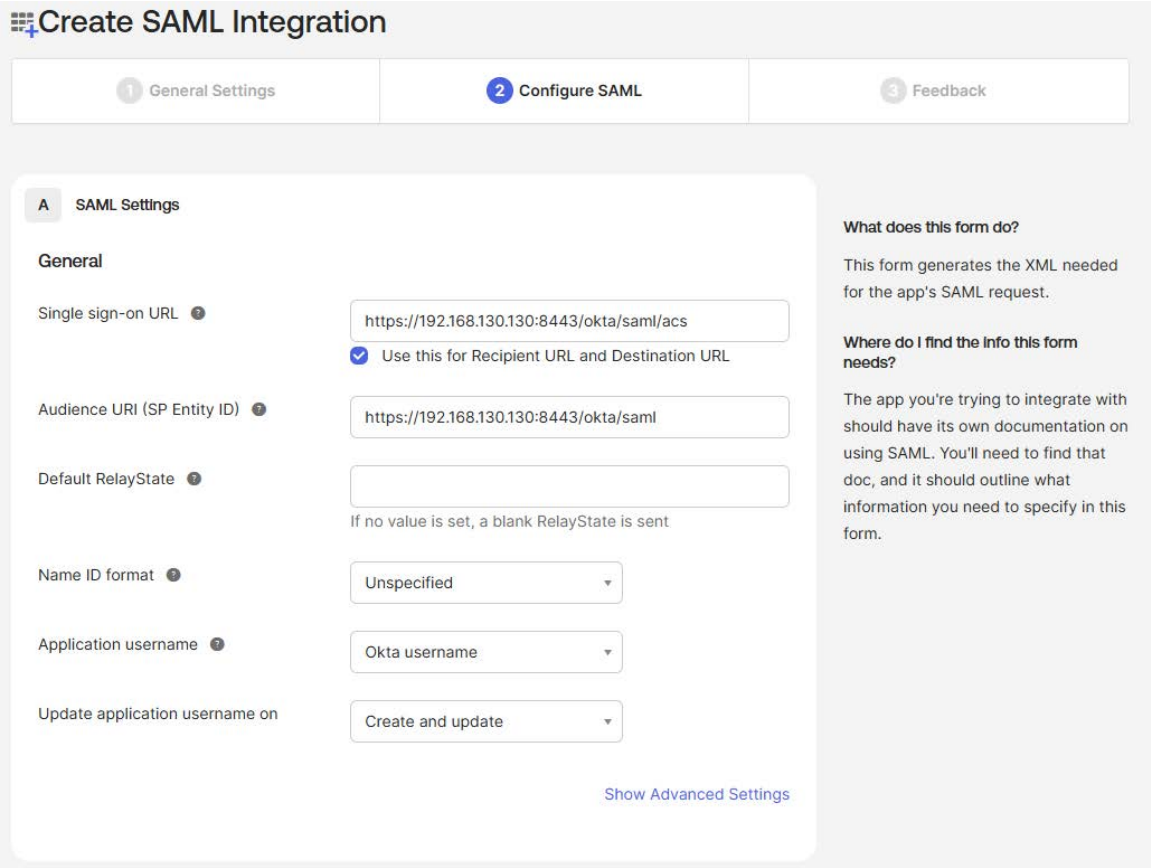
Create the Application in Okta

Use the following steps to create the application integration in Okta.

1. Log in to the **Okta Admin Console**.
2. Navigate to **Applications > Applications** and select **Create App Integration**.



3. Select **SAML 2.0** as the Sign-in method.
4. Select the **General Settings** tab and configure the following:
    a. Enter an application name in **App name.**
    b. (Optional) Upload an application logo in **App logo**.
5. Select the **Configure SAML** tab and configure the following:
    a. Enter `https://<ServerIP-or-FQDN>:8443/okta/saml/acs` for the **Single Sign-on URL.**
    b. Enter `https://<ServerIP-or-FQDN>:8443/okta/saml` for the **Audience URI (SP Entity ID)**.
    c. Keep the remaining settings as the default values

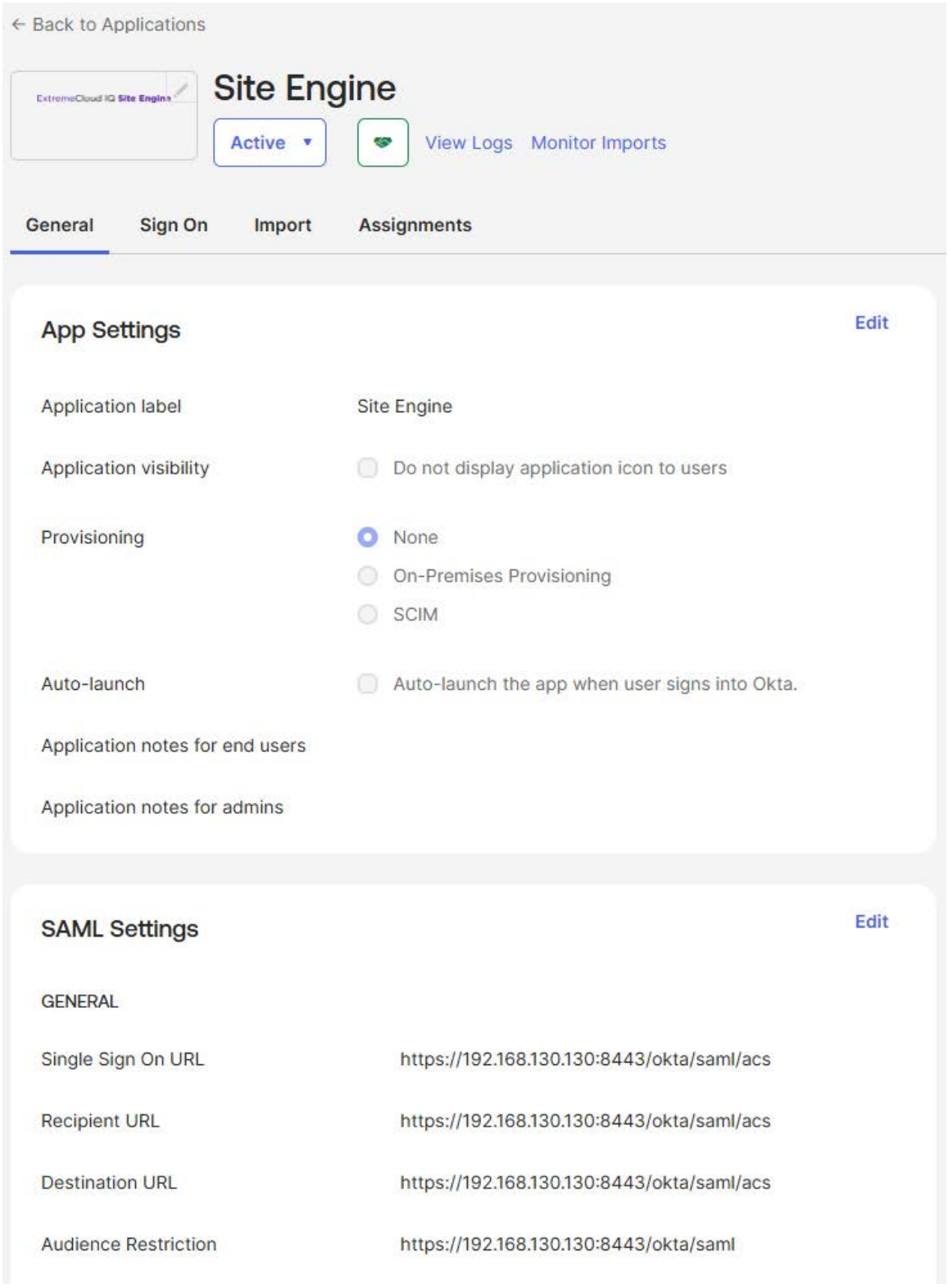


6. Select the **Feedback** tab and keep all as defaults.
7. Select **Finish**.

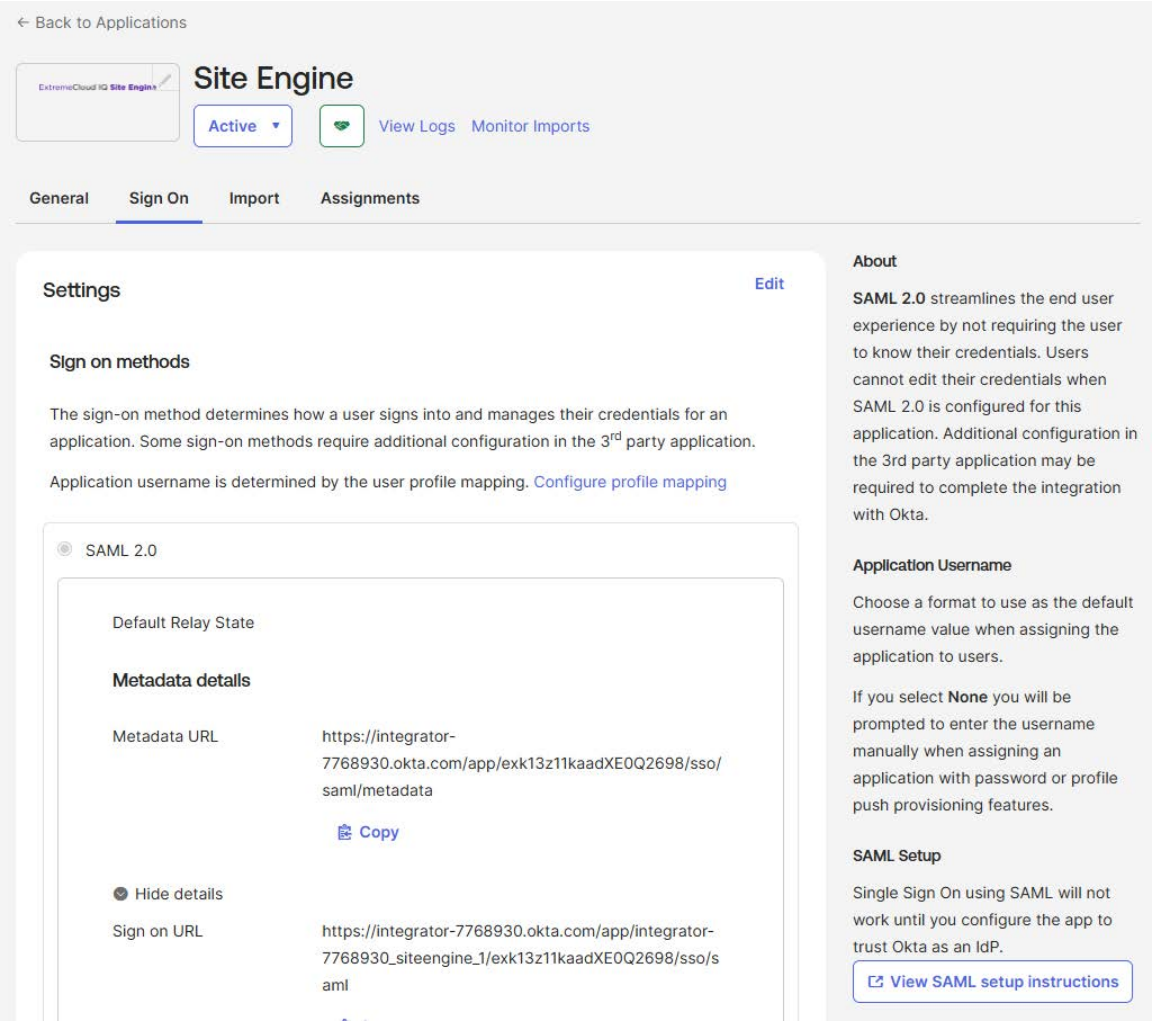
Save the Values Required for the ExtremeCloud IQ Site Engine Configuration

Use the following steps to copy and save the values required for the ExtremeCloud IQ Site Engine configuration.

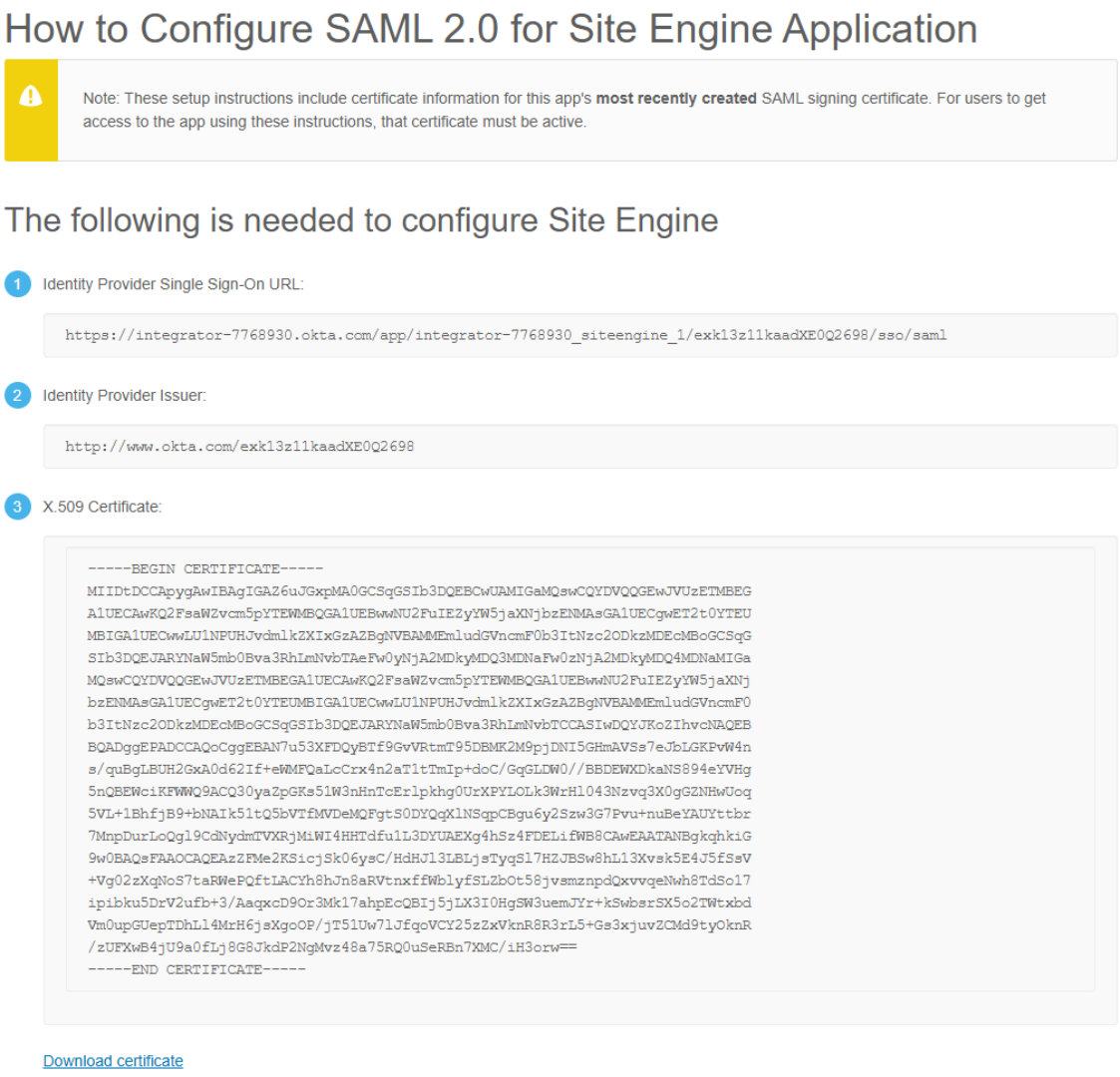
1. From the **Okta Admin Console**, navigate to the **General** tab.
2. Copy and save the **Audience Restriction** value (for the **SP Entity ID** in ExtremeCloud IQ Site Engine).


← Back to Applications
Site Engine
Active
View Logs
Monitor Imports
General
Sign On
Import
Assignments
App Settings
Edit
Application label
Site Engine
Application visibility
Do not display application icon to users
Provisioning
None
On-Premises Provisioning
SCIM
Auto-launch
Auto-launch the app when user signs into Okta.
Application notes for end users
Application notes for admins
SAML Settings
Edit
GENERAL
Single Sign On URL
https://192.168.130.130:8443/okta/saml/acs
Recipient URL
https://192.168.130.130:8443/okta/saml/acs
Destination URL
https://192.168.130.130:8443/okta/saml/acs
Audience Restriction
https://192.168.130.130:8443/okta/saml

3. Navigate to the **Sign On** tab, and select **View SAML setup instructions**.



4. Copy and save the **Identity Provider Single Sign-On URL** value (for the **IdP SSO URL** in ExtremeCloud IQ Site Engine).
5. Copy and save the **Identity Provider Issuer** value (for the **IdP Issue**r in ExtremeCloud IQ Site Engine).
6. Copy and save the **X.509 Certificate** value (for the **X.509 Certificate** in ExtremeCloud IQ Site Engine).



How to Configure SAML 2.0 for Site Engine Application

Note: These setup instructions include certificate information for this app's **most recently created** SAML signing certificate. For users to get access to the app using these instructions, that certificate must be active.

The following is needed to configure Site Engine

1. Identity Provider Single Sign-On URL:

```
https://integrator-7768930.okta.com/app/integrator-7768930_siteengine_1/exk13z11kaadXE0Q2698/sso/saml
```

2. Identity Provider Issuer:

```
http://www.okta.com/exk13z11kaadXE0Q2698
```

3. X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDtDCCApygAwIBAgIGAZ6uJGxpMA0GCSqGSIb3DQEBCwUAMIGaMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxGzAZBgNVBAMMEmludGVncmF0b3ItNzc2ODkzMDEcMBoGCSqG
SIb3DQEJARYNaW5mb0Bva3RhLmNvbTAeFw0yNjA2MDkyMDQ3MDNaFw0zNjA2MDkyMDQ4MDNaMIGa
MQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNj
bzENMAsGA1UECgwET2t0YTEUMBIGA1UECwwLU1NPUHJvdmlkZXIxGzAZBgNVBAMMEmludGVncmF0
b3ItNzc2ODkzMDEcMBoGCSqGSIb3DQEJARYNaW5mb0Bva3RhLmNvbTCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAN7u53XFDQyBTf9GvVRtmT95DBMK2M9pjDNI5GHmAVSs7eJbLGKPvW4n
s/quBgLBUH2GxA0d62If+eWMFQaLcCrx4n2aT1tTmIp+doC/GqGLDW0//BBDEWXDkaNS894eYVHg
5nQBEWciKFWWQ9ACQ30yaZpGKs51W3nHnTcErlpkhg0UrXPYLOLk3WrHl043Nzvq3X0gGZNHwUoq
5VL+1BhfjB9+bNAIk51tQ5bVTfMVDeMQFgtS0DYQqXlNSqpCBgu6y2Szw3G7Pvu+nuBeYAUYttbr
7MnpDurLoQgl9CdNydmTVXRjMiWI4HHTdfu1L3DYUAEXg4hSz4FDELifWB8CAwEAATANBgkqhkiG
9w0BAQsFAAOCAQEAzZFMe2KSicjSk06ysC/HdHJl3LBLjsTyqSl7HZJBSw8hL13Xvsk5E4J5fSsV
+Vg02zXqNoS7taRWePQftLACYh8hJn8aRVtnxffWblyfSLZbOt58jvsmznpdQxvvqeNwh8TdSo17
ipibku5DrV2ufb+3/AaqxcD9Or3Mk17ahpEcQBIj5jLX3I0HgSW3uemJYr+kSwbsrSX5o2TWtxbd
Vm0upGUepTDhLl4MrH6jsXgoOP/jT51Uw7lJfqoVCY25zZxVknR8R3rL5+Gs3xjuvZCMd9tyOknR
/zUFXwB4jU9a0fLj8G8JkdP2NgMvz48a75RQ0uSeRBn7XMC/iH3orw==
-----END CERTIFICATE-----
```

Download certificate

Assign Users to the Okta Application

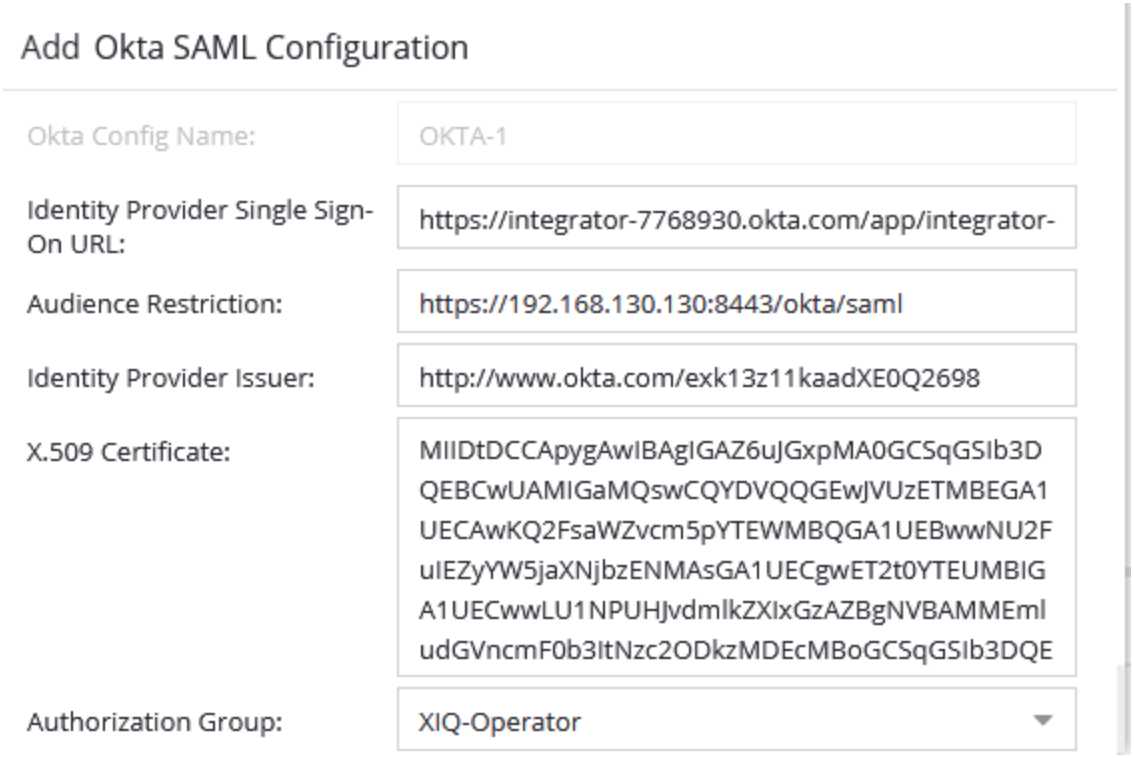
Use the following steps to assign people or groups that can use the Okta application to access ExtremeCloud IQ Site Engine with Okta SSO.

1. From the **Okta Admin Console**, navigate to the **Assignments** tab.
2. Select **Assign** and select people or a group, or both.
3. Repeat the previous step to assign all the people or groups required.

Configure the Okta Authentication Method in ExtremeCloud IQ Site Engine

After you have configured the Okta application, captured the required Okta values, and assigned Okta users, you can configure the Okta authorization method in ExtremeCloud IQ Site Engine.

1. From the ExtremeCloud IQ Site Engine, navigate to **Administration > Users**.
2. In the Authentication Method section **Authentication Type** dropdown, select **OKTA**.
3. From the **OKTA** dropdown, select **New**.
    a. Enter a name for the **OKTA Config Name**.
    b. Paste the Okta saved value for the **Identity Provider Single Sign-On URL**.
    c. Paste the Okta saved value for the **Audience Restriction**.
    d. Paste the Okta saved value for the **Identity Provider Issuer**.
    e. Paste the Okta saved value for the **X.509 Certificate**.
    f. (OPTIONAL) Select the **Authorization Group** drop down to specify a default authorization group for Okta authenticated new users without a pre-defined record in **Authorized Users**.
    g. Select **Save** to save the configuration.



   h. Select **Yes** to confirm.

4. In the **Authorized Users** section, in the table select **Add...**
   a. Select the **User Name** and mapping to an **Authorization Group**.
   b. Select **Save** to confirm.
5. (Optional) Select the **Authenticate to OS on Failure to Authorization Group** option. Enabling allows an Okta user access to GUI even if the configuration is incorrect, or Okta connectivity is lost.

The best practice is to now test the Okta SSO integration with an authorized user before you logout or close the User Administration window.

NOTE: The **Authorized Users** configuration has priority over the **Authorized Group** configuration. If you add a record for a user in **Authorized Users,** the **Authorized Group** value in the OKTA SAML Configuration is ignored for that user. If the user has no record in **Authorized Users**, a new record is created during login, and the **Authorized Group** value is applied.

If neither options are configured (user not added to **Authorized User** and **Authorized Group** left blank), the user authorization is declined with the error message "Not Authorized, contact Administrator".

- Users
- Administration
- Add Users

Compare Device Configurations

You can compare archived device configurations in ExtremeCloud IQ Site Engine by using either the **Network** > **Devices** tab or the Archive Details Report available in the **Network** > **Reports** tab.

In order to perform the compare configuration operation, you must be a member of an authorization group with the Inventory Manager > Configuration Archive Management > View/Compare Configurations capability.

This Help topic provides the following information:

- Selecting the Files to Compare
- Comparing the Files

Selecting the Files to Compare

Select the files to compare using either the **Network** tab or the **Reports** tab.

From the Network tab:

Use the **Network** tab to compare the last two archived configuration files for a device.

Select a device in the table and use either the **Menu** icon (☰) or the right-click menu off the device to select **More Actions** > **Compare Last Configurations**.

From the Reports tab:

Use the **Reports** tab to compare two configuration files selected from all archived files for the device.

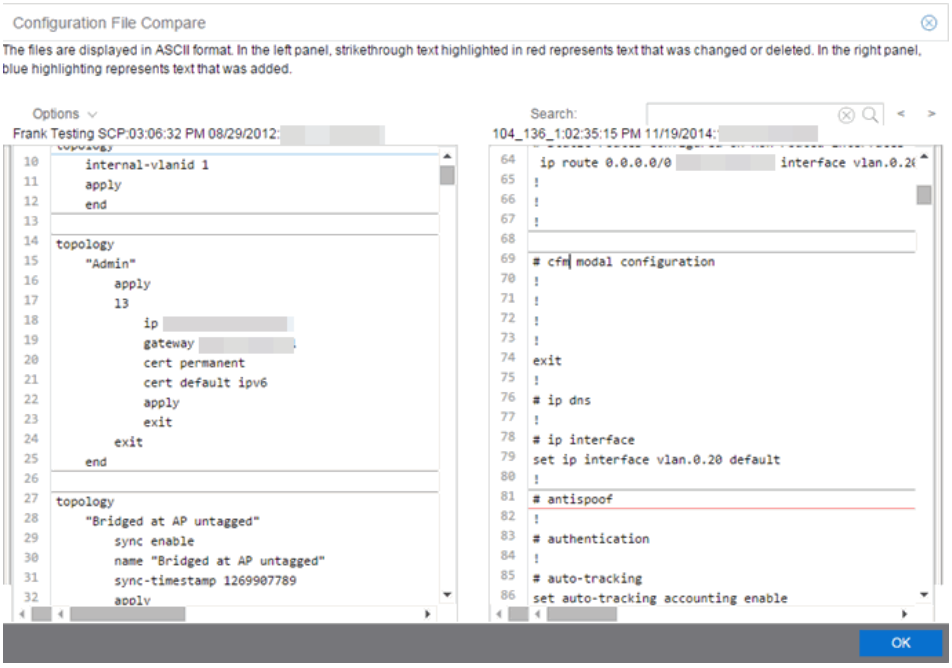
Select the Device > Device Archives report. Select the **Archive Details** tab in the right panel and then select the **Archives by Device** sub-tab.

The tab displays all the ExtremeCloud IQ Site Engine archives by device IP address. Select two files to compare and select **Compare Configuration**.

Comparing the Files

The Configuration File Compare window displays the files in two panels. Titles over each file show the archive name that contains the configuration file, the date, and the IP address of the device from which you create the configuration file.

Scroll through the two files to view file differences. Typically, the newer file displays in the right panel. You can use the "Swap sides" option to swap the files. In the left panel, strikethrough text highlighted in red represents text that is changed or deleted. In the right panel, blue highlighting represents text that is added.



Use the toolbar Options menu to control the look of the display window:

- Enable line numbers displays line numbers alongside the text.
- Wrap lines shows all the text in the column and removes the horizontal scroll bars.
- Enable side bars shows where the text differences are in the whole file.
- Swap sides swaps the files contained in the left and right panels.

TIP: Removing line numbers and side bars may speed up the display of larger files.

Use the **Search** field in the toolbar to perform a search in the panel side that is selected by the cursor. Use the forward and back arrows to search for the next or previous instance of the search term.

Device View

Device View is an ExtremeCloud IQ Site Engine component that provides a wide range of analysis and troubleshooting information for your network wired and wireless devices, including a device summary, FlexViews, and ExtremeCloud IQ Site Engine reports.

The primary launch point for Device View is from the **Network** tab. Device View can also be launched from other locations in ExtremeCloud IQ Site Engine.

This Help topic provides the following Device View information:

- Requirements
    - Access Requirements
    - Data Collection Requirements
- Device View Reports
    - Left-Panel Device Summary
- Launching Device View

Requirements

Access Requirements

Access to Device View reports is determined by the user's membership in an ExtremeCloud IQ Site Engine authorization group and the group's assigned capabilities. The following list shows the capabilities required for full access to all the Device View reports.

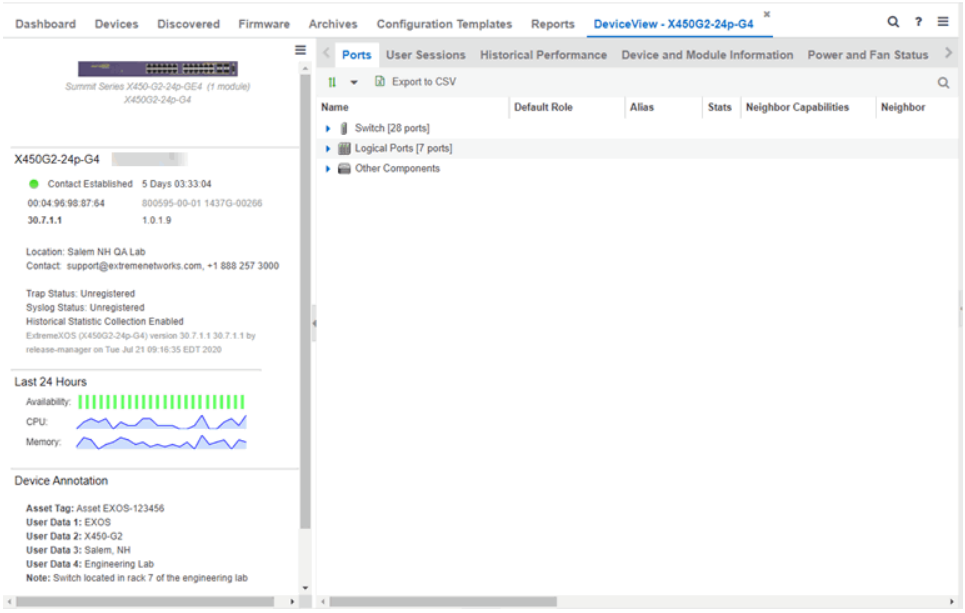
- XIQ-SE OneView > Access OneView
- XIQ-SE OneView > Access OneView Reports
- XIQ-SE OneView > Events and Alarms > OneView Event Log Access
- XIQ-SE OneView > FlexView > OneView FlexView Read Access

Data Collection Requirements

Device View reports require that historical data collection is enabled for the device. For information on configuring data collection, see Collect Device Statistics in the Devices section of the ExtremeCloud IQ Site Engine User Guide.

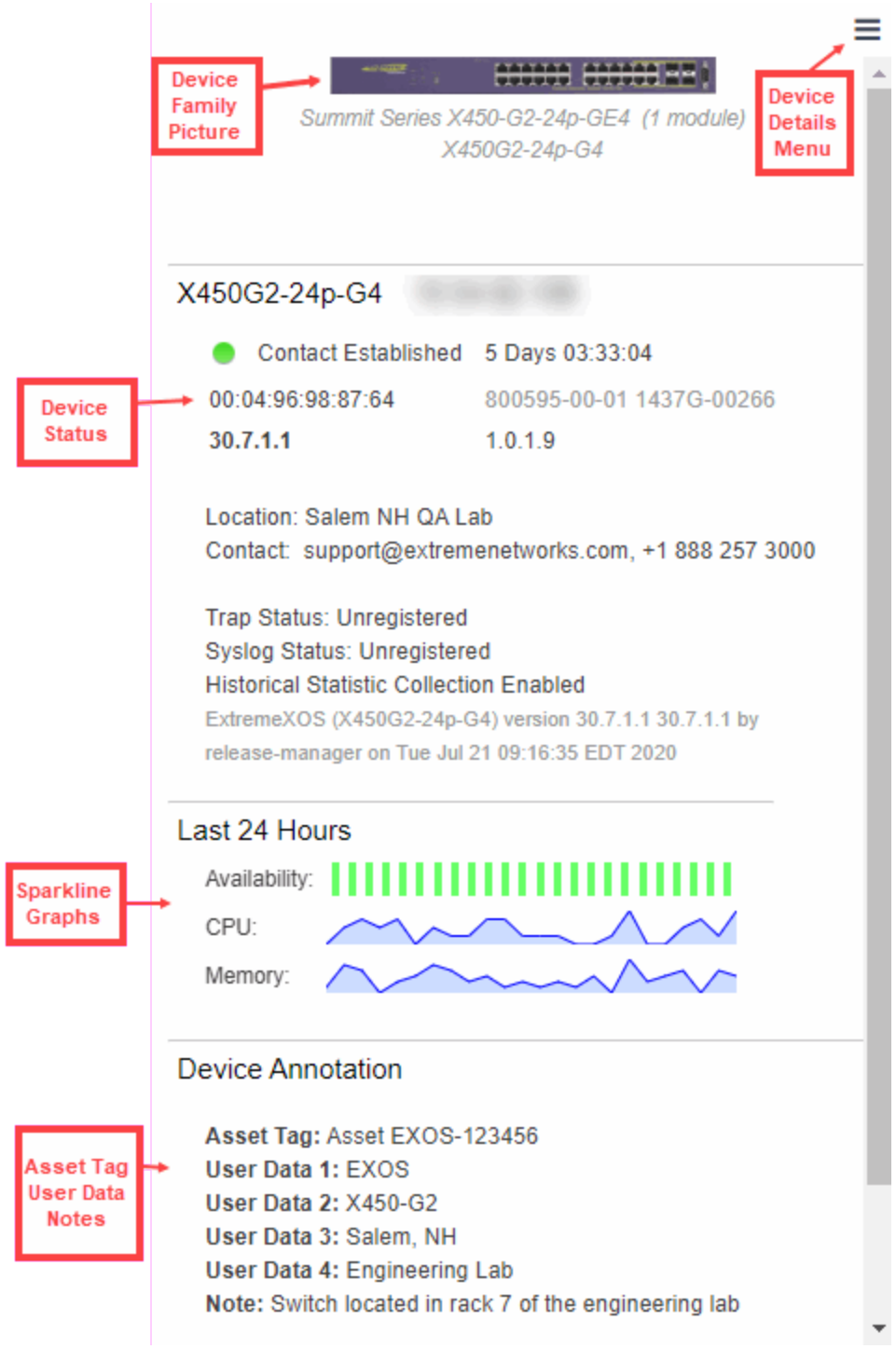
Device View Panels

The Device View is comprised of a left-panel device summary, and a selection of tabbed panels that display FlexViews and reports based on the device family.



Left-Panel Device Summary

The left-panel device summary view (shown below) is displayed in each Device View report.



Each device summary view includes:

- **Device Family Picture** — A generic device family picture for the device.

- **Device Status** — Indicates the alarm/device status for the device. The icon color indicates the severity of the most severe alarm on the device. A red icon indicates a critical alarm or the device is down. A green icon indicates that there are no alarms and the device is up.
- **Sparkline Graphs** — Provides network trends in dense, succinct charts that present report data in an easy to read, condensed format. You must have Historical Statistic Collection enabled in order to see the Sparkline graphs and other report data. If Historical Statistic Collection is not enabled, you will see a line that says, "Historical Statistic Collection Disabled." For information on configuring data collection, see Collect Device Statistics in the Devices section of the ExtremeCloud IQ Site Engine User Guide.
- **Asset Tag, User Data, Notes** - Displays the Asset Tag, User Data and notes about the device. This data is only displayed if you have configured these values in ExtremeCloud IQ Site Engine.
- **Device Details Menu** — Select the **Menu** icon (☰) in the upper right corner to access additional device reports.

Right-Panel Device Summary

The following tabs and reports are available in the Device View. The reports displayed in a Device View vary according to the selected device. For most reports, right-click a device in the table to export the table details or details about the selected device to a .csv report.

Ports

 Refreshes the status of all ports.

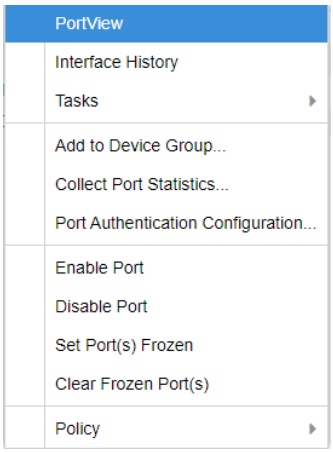
 Rediscovers all the device data.

Use the Ports report to view details about the ports and other components associated with the Device Family. The following columns are included in the Ports report:

- Name - The name assigned to the port
- Default Role - The policy role assigned to the selected port.
- Alias - An alternate name for the port.
- Stats - Displays whether statistics collection is enabled or disabled on the port. A black check indicates that historical collection is enabled, and a blue check indicates that threshold alarms collection (formerly monitor collection) is enabled.
- Neighbor Capabilities - Displays capabilities for neighbor ports.
- Neighbor - Displays neighbor details from CDP/EDP/LLDP. Place your mouse over the column to see the protocol type.
- Port Speed - Displays the speed of the port
- PVID - The port's VLAN ID.
- VLANs - Displays the name of the VLAN.

- Description - A description of the port.
- Port Type Details - Displays the port type and other information about the port type.
- Serial Number - Displays the port's serial number.

  Select an entry in the table, expand to display a port, and right-click to open the following drop-down list:



  - PortView - Access PortView for that port.
  - Interface History - view interface history including interface utilization, availability, and bandwidth/packets/flows statistics (Flow stats display only for S/K series and PF-FC-180 devices).
  - Add to Device Group - Use to select a Device Group to which you will add the port.

    NOTES:

    Right-clicking ports and selecting Add to Device Group opens the Add to Device Group window, which allows you to select a device group to which to add the selected ports.

    Right-click a port and select the **Application Telemetry** menu to view the Interface Top Applications Treemap or Top Clients by Interface report for the port. If Application Telemetry is not enabled on the device, the Application Telemetry menu does not display.

    Only VLANs to which ports are assigned are displayed in this report. Additionally, VLAN reports for ExtremeXOS/Switch Engine devices may display duplicate VLANs as VLANs are assigned by slot.

- Collect Port Statistics - Opens a window from which you can select your statistics collection mode (Historical, Threshold Alarms), or disable statistics collection.
    - In **Historical mode**, port statistics are saved to the database and aggregated over time, for use in reports. The statistics are also used for threshold alarms configured in the Console Alarms Manager. In the Active Threshold Alarm Summary box, you can see all active threshold alarms configured in the Console Alarms Manager that use these statistics.

      NOTE: Enabling Historical Statistics Collection may use substantial disk space.

    - In **Threshold Alarms (formerly Monitor) mode**, port statistics are saved for one hour and then dropped. You can use these statistics for threshold alarms, but not for ExtremeCloud IQ Site Engine reporting. In the Active Threshold Alarm Summary box, you can see all active threshold alarms configured in the **Alarms and Events** tab that use these statistics. (Note that you do not see the Threshold Alarms mode option if you have disabled threshold alarms collection in the OneView Collector Advanced Settings in **Administration** > **Options**.)
    - **Disable** — Select this check box to disable statistic collection mode.
- Port Authentication Configuration - Access the Authentication Configuration for the port.
- Enable Port - Enables the port for the device.
- Disable Port - Disables the port for the device.
- Set Port(s) Frozen - Select to freeze the selected port.
- Clear Frozen Port(s) - Select to clear the selected frozen port.
- Policy - Use to create policy profiles, called roles, that are assigned to the ports in your network.

- MAC Addresses
- Device Logs
- Alarms
- Events
- Archives
- User Sessions
- Historical Performance
- Switch Resources
- Device and Module Information
- Controller History
- Power and Fan Status

- Active Access Points
- Storage Utilization
- Process Utilization
- WLAN Services
- CPU and Process Utilization
- VLAN
- Active Clients
- IP Traffic Summary
- MLAG
- Alarms and Events
- VPLS

Launching Device View

Device View can be launched from a variety of locations in ExtremeCloud IQ Site Engine.

Network Tab

The primary launch point for Device View is from the **Network** tab.

1. Open the **Network** > **Devices** tab.
2. Place your mouse over the first column and select the Device View icon .
3. The Device View opens as a separate tab.

Control Tab

Use the following steps to launch Device View from the **Control** tab.

1. Open the **Control** > **Dashboard** tab.
2. Select the **System** view.
3. In the Engine Information report, select an engine IP address to open a Device View for the engine.

ExtremeCloud IQ Site Engine Maps

Use the following steps to launch Device View from a map.

1. Open ExtremeCloud IQ Site Engine Maps and select a map.
2. In the map, right-click on a device icon and select Device View.

Search

Use the following steps to launch Device View from the **Search** tab.

1. Open **Search** and search for a device.
2. In the Overview, right-click on the device icon and select Device View.

Upgrade Firmware

Use ExtremeCloud IQ Site Engine to upgrade device firmware for your Extreme Networks devices.

NOTE: Prior to upgrading firmware, you must access the Extreme Networks website to obtain information about the latest Extreme Networks firmware releases available for download.

You can upgrade firmware in one of three ways:

- For a particular device on your network
- For all devices of a device type
- For a Fabric Manager

You must be a member of an authorization group that includes Inventory Manager > Firmware/Boot PROM Management > Firmware/Boot PROM Upgrade Wizard capability to see this menu option.

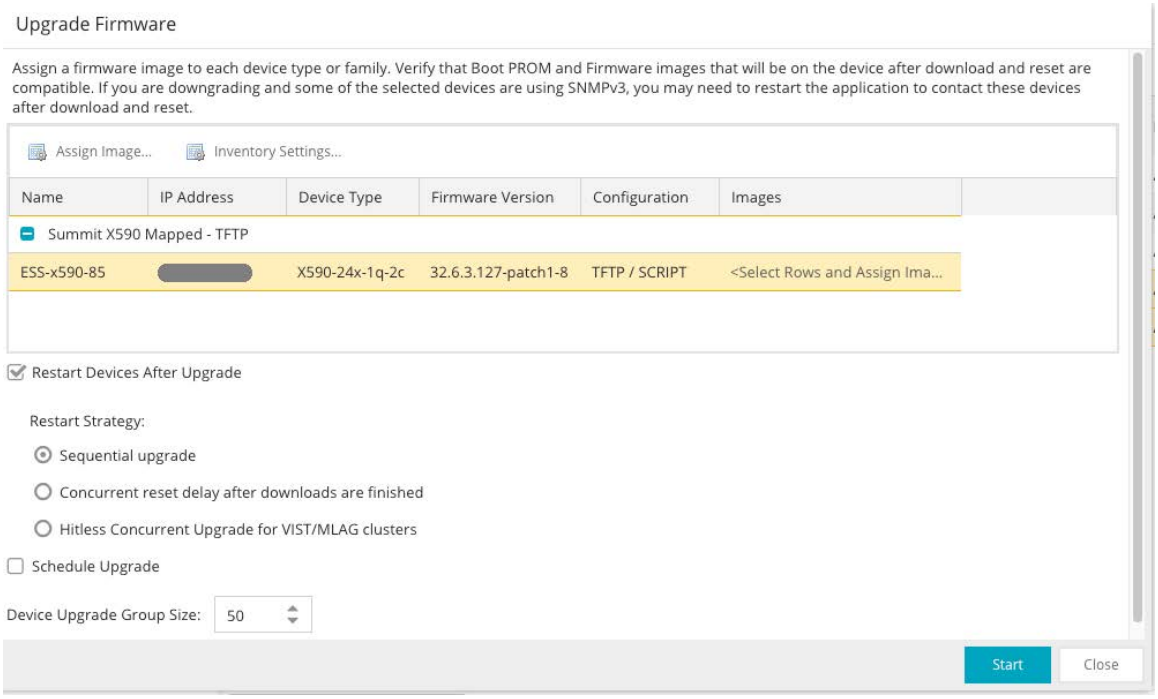
Upgrading for a Device

To upgrade firmware for a particular device:

1. Open the **Network** tab.
2. Select the **Devices** tab.
3. Select **All Devices** from the left-panel drop-down list, or select a **Map** or **Site**, depending on the location of the device you are upgrading.
4. Select the **Devices** tab in the right-panel.
5. Select the devices for which you are upgrading firmware in the Devices table in the right-hand panel.
6. Select the **Menu** icon (☰) or right-click in the Devices list.
7. Select **Upgrade Firmware**.

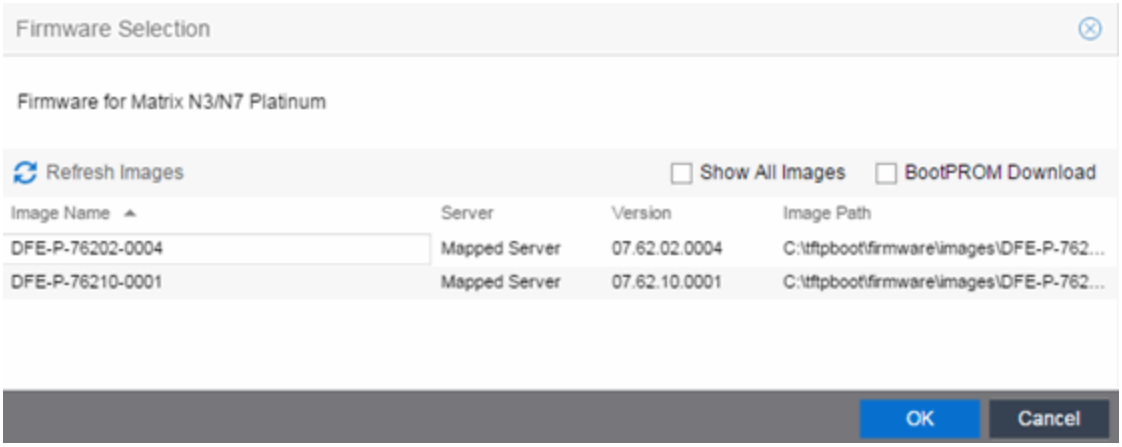
   NOTE: You can also right-click a single device in the left-panel and select **Upgrade Firmware**.

   The Upgrade Firmware window opens, displaying the devices you selected grouped by device family.



8. Select one or more devices and select **Assign Image**.

   The Firmware Selection window opens, displaying the firmware versions compatible with the device type.



9. Select the **Show All Images** checkbox to show all available firmware images.
10. Select the firmware image to download to the device.
11. After the upgrade operation completes, verify the boot PROM and firmware images on the device are compatible. Refer to the boot PROM and firmware release notes for more information. To upgrade the boot PROM, select the **BootPROM Download** checkbox in the

Firmware Selection window. This clears any images already assigned and only displays boot PROM images for selection.

12. Select **OK**.
13. Repeat the process for all of the devices in the Upgrade Firmware window.

NOTE: Right-click the device in the **Upgrade Firmware** window to configure how the firmware is downloaded and installed on the device (e.g. to change the server from which the firmware image is downloaded, the file transfer method, or the MIB or script used to download the firmware image).

---

14. Select the **Restart Devices After Upgrade** checkbox to automatically restart devices that support restarting immediately after upgrading the firmware image.

NOTES: Selecting the **Restart Devices After Upgrade** checkbox displays the Supports Restart column in the **Upgrade Firmware** window. A check mark indicates devices that support this functionality.

You can also restart a device manually in the **Restart Devices** window, accessible from the **Network** tab in ExtremeCloud IQ Site Engine by right-clicking the device and selecting **More Actions** > **Restart Device** option.

---

15. Select an **Upgrade Method**.
    - **Sequential Upgrade** — Each device restarts after the firmware transfer is done sequentially, one by one.
    - **Concurrent reset delay after downloads are finished** — Each device restarts at the same time after the all the firmware transfers are done.
    - **Hitless Concurrent Upgrade for VIST/MLAG Clusters** — The devices restart in three batches after the firmware transfers are done:
        1. The first batch concurrently restarts half of every VIST/MLAG cluster.
        2. The second batch concurrently restarts the remaining half of the VIST/MLAG cluster.
        3. The third batch sequentially restarts devices that are not part of the VIST/MLAG cluster, one by one.
16. Select the **Schedule Upgrade** checkbox to run the firmware image upgrade at a future date. Selecting this checkbox displays additional fields where you can configure the scheduled upgrade.
    - **Name** — The name for the scheduled upgrade. The default name automatically populates with the creation date and time of the firmware upgrade.
    - **Select Date** — The date and time the upgrade automatically runs. Enter a date in the mm-dd-yyyy format or select the **Calendar** icon to open a monthly calendar from

which you can select the date of the upgrade. Enter the time for the scheduled upgrade or select the drop-down arrow to select the time from a drop-down list.

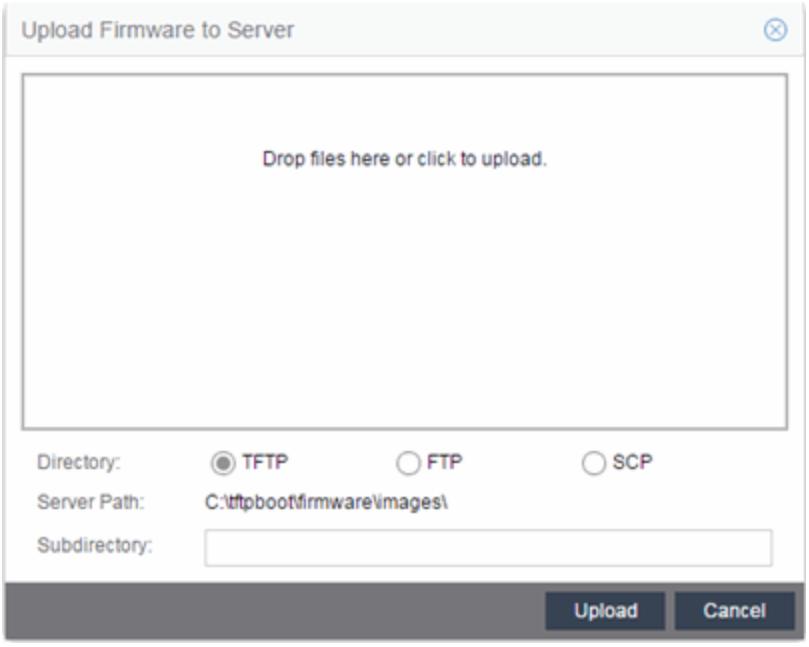
- **Abort on Failure** — Selecting this checkbox causes the upgrade to terminate in the event it is not successful.

17. Enter the number of downloads upgraded simultaneously in the **Device Upgrade Group Size** field. Enter a value of **1** to have the downloads performed serially (one device at a time).
18. Select **Start** if you are upgrading the firmware immediately or **Schedule** if the upgrade is scheduled for a future date.
    Note: To view or cancel a scheduled firmware upgrade, select **Tasks > Scheduled Tasks**.
19. If upgrading the firmware image immediately, a progress column appears on the **Upgrade Firmware** window. When the upgrade is complete, a Status section appears, displaying whether the upgrade occurred successfully.
20. Select **Close**.

Upgrading for a Device Type

To upgrade the firmware for all devices of a particular device type:

1. Open the **Network** tab.
2. Select the **Firmware** tab.
3. Select the device type from the Firmware tree in the left panel.
4. Upload the firmware or boot PROM image, if necessary.
    a. Select the **Upload** button to open the Upload Firmware to Server window from which you can save image files to the ExtremeCloud IQ Site Engine server.



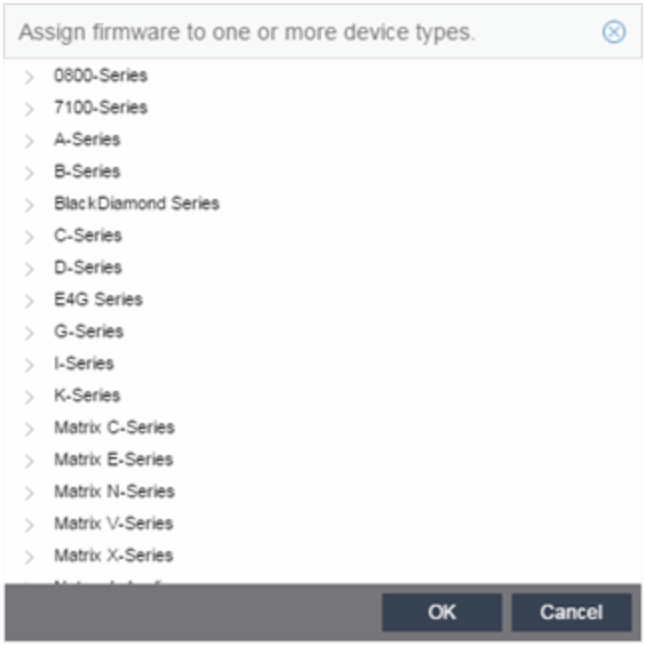
b. Drag the file or files into the box in the main part of the window or select the box to open a window from which you can navigate to the appropriate directory.

c. Select **TFTP**, **FTP**, or **SCP** to indicate whether you are upgrading the firmware or boot PROM image using a TFTP, FTP, or SCP server, respectively.

d. Type the Subdirectory within the Server Path where the firmware or boot PROM images are uploaded.

e. Select the **Upload** button.
A status bar displays over the file icon and a check mark indicates when the upload is complete. Anyone with access to ExtremeCloud IQ Site Engine is now able to download the image file to a device.

5. Right-click the firmware or boot PROM image from the Device Type Images section of the window and select **Assign Firmware** from the menu.
The Assign Firmware to One or More Device Types window appears.



6. Select the device type on which you are assigning the firmware or boot PROM image.
7. Select **OK**.

If you did not select **Restart Devices After Upgrade**, restart your devices.

Upgrading for Fabric Manager

To upgrade the firmware image for Fabric Manager, follow the instructions in Upgrading Fabric Manager.

How to Restart a Device

Use the **Devices** tab to restart a single device or multiple devices. The tab lets you restart devices that support Timed Restart as well as those devices that do not. Timed Restart lets you configure your restart operation with a time delay, so that the actual device restarts take place at a later time.

To restart a device:

1. Access the **Network** > **Devices** tab.
2. Use the left-panel drop-down list to select **All Devices**, **Maps**, or **Sites**, depending on the devices you are restarting. You can also use the drop-down list to select how the devices are organized (e.g. by IP address, by Device Type).
3. Select the **Devices** tab in the right-panel.
4. Select the device or devices you want to restart (using the **Ctrl** or **Shift** keys).
5. Select the **Menu** icon (☰) or right-click in the Devices list.

6. Select **More Actions** > **Restart Device**.

   NOTE: You can also right-click a single device in the left-panel and select **More Actions** > **Restart Device**.

   The **Restart Devices** window displays.
7. Select the devices you want to restart by selecting the checkbox in the **Selected** column.

   NOTE: The **Restart Devices** window contains additional fields for devices that support timed restart.
8. Select the date and time you want to restart the device for devices that support timed restart using the **Restart Time** fields. This field defaults to the current date and time, so to restart the devices now, do not change this field.
9. Select **Start** to initiate the device restarts or to schedule a future device restart. **Elapsed Time** displays the elapsed time since beginning the restart process.
10. Select **Finish** to close the window.

Add a New Regime in ExtremeCloud IQ Site Engine (Legacy)

The Compliance tab provides you with regimes that include predefined audit tests. You can also create your own regimes, composed of audit tests you can copy from existing regimes, or configure yourself.

To create a new regime:

1. Open the **Compliance** > **Audit Tests** tab.
2. Select the **Menu** icon (☰) and select **Add** > **Regime**.

   The Create Regime window displays.
3. Enter a **Regime Name**, describing the overarching standard or regulation against which you are testing compliance.
4. Enter a **Description** for the regime, if necessary.
5. Select **Test Wireless Events** to include wireless events in the ExtremeCompliance audit.

NOTE: Because of the number of wireless events potentially stored by ExtremeCloud IQ Site Engine, wireless events are not included in an ExtremeCompliance audit the first time it is run. When the audit is run the first time, older wireless events are moved, so older events are not included in the results.

6. Select **Save**.
7. Copy existing audit tests to the new regime, if necessary.
    a. Right-click the audit test in left-panel and selecting **Copy Audit Test**.

       The **Copy Audit Test** window displays.
    b. Enter a new name for the audit test, if necessary.
    c. Select the new regime in the **Regime** drop-down list.
    d. Select the device type to which the audit test applies in the **Device Type** drop-down list.
    e. Select **Copy**.
8. Create your own audit tests.
    a. Select the **Menu** icon (☰) and select **Add** > **Audit Test**.
    b. Complete the fields in the **Audit Test Editor** tab to test for a device configuration.
    c. Complete the fields in the **Dependent Tests** tab, if necessary.
    d. Select **Save**.

ZTP+ Device Configuration

Using Extreme Networks' ZTP+ (Zero Touch Provisioning Plus) functionality, you can quickly add new ZTP+-enabled devices to your network and configure them in ExtremeCloud IQ Site Engine.

Typically, when adding a new device to the network, a network administrator connects a console cable to the device to access the local console and manually configure the device.

IMPORTANT: Stacked ExtremeXOS/Switch Engine systems must be running ExtremeXOS/Switch Engine version 30.3 or later to support ZTP+ configuration.

In ExtremeCloud IQ Site Engine, new devices are automatically discovered on the network the moment they are connected. ZTP+-enabled devices send information to ExtremeCloud IQ Site Engine automatically, including the serial number, the number and speed of the ports, and the firmware version. When a ZTP+-enabled device is connected, you can add it to ExtremeCloud IQ Site Engine with minimal server configuration. In addition, the latest updates are automatically downloaded to the new device. This process minimizes the amount of time needed to configure a new device and deploy it on the network.

Prerequisites

Before connecting your devices, configure the following:

- Select the Reference Firmware Image Location
- Default Device Configuration in ExtremeCloud IQ Site Engine
- Download XMODs (ExtremeXOS/Switch Engine devices only)
- General Network Configuration
- NOS Persona Change from Switch Engine to Fabric Engine

Select the Reference Firmware Image Location

You can configure ExtremeCloud IQ Site Engine to automatically update your device's firmware and application versions. When upgrading the firmware image on your device, access the appropriate firmware image for your version from ExtremeNetworks.com and save it on your server to a directory you configure in ExtremeCloud IQ Site Engine. After the firmware image is saved on the ExtremeCloud IQ Site Engine server, it is available in ExtremeCloud IQ Site Engine and can be downloaded to the device.

For the device to recognize a new version is available, the firmware image must be downloaded from ExtremeNetworks.com to your server and saved in a directory you configure in ExtremeCloud IQ Site Engine.

To configure the file transfer directory:

1. Access the **Options** tab.
2. Select **Inventory Manager** in the left panel.
3. Enter the **Firmware Directory Path** in either the FTP Server Properties, SCP Server Properties, or TFTP Properties section of the right panel, depending on the file transfer settings used.
4. Download the latest firmware image for your device from ExtremeNetworks.com and save it in the specified directory.

When you download the firmware image from ExtremeNetworks.com and save it on the ExtremeCloud IQ Site Engine server, use the **Firmware** tab in ExtremeCloud IQ Site Engine to download the image from the ExtremeCloud IQ Site Engine server to the device.

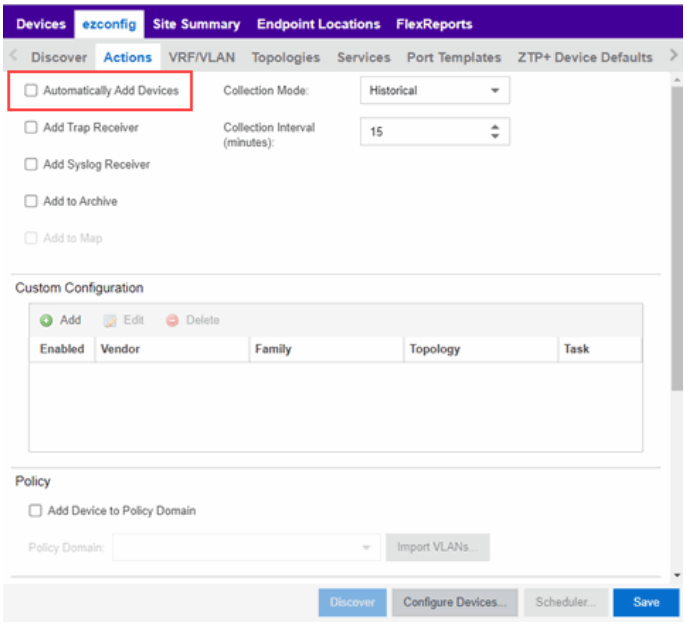
1. Access the **Network** > **Firmware** tab.
2. Expand the **Device Type** navigation tree in the left-panel for the device family you are configuring and select the folder for the type of device.
3. Right-click the firmware file you downloaded (specified in the section above) and select **Set as Reference Image**.

   Your device automatically updates with this firmware image when it restarts and is logged in the Event log with a **Category** of **Inventory**.

Default Device Configuration in ExtremeCloud IQ Site Engine

Before connecting your devices, you can configure the default settings that ExtremeCloud IQ Site Engine applies to all devices you add to the network. This is accomplished using the Site tab.

1. Access the **Devices** tab in ExtremeCloud IQ Site Engine.
2. Expand the World Site navigation tree and select the map in the left panel into which you are adding the devices.
3. Select the **Site** tab in the right panel.
4. Select the **Automatically Add Devices** checkbox in the Discovered Device Actions section and any other actions you want to occur on your devices discovered in ExtremeCloud IQ Site Engine.



5. Use the Custom Configuration section to automatically run a script on devices being added to the site, if necessary.

CAUTION:	If the script or workflow task selected for the Custom Configuration restarts the device, other actions selected to execute during discovery might not execute (for example, Add Trap Receiver).

6. Select **Add Device to Policy Domain** or **Add Device to Access Control Engine Group** to automatically add devices being added to the site to a Policy Domain or Access Control engine group.
7. Add the VLANs that are used on your devices on the **VLAN Definition** tab by selecting the **Add** button and entering the **Name** and **VID**.
8. Use the **Port Templates** tab to create a port configuration, if necessary.
9. Enter the **Gateway Address**, **Domain Name**, and **DNS Server** address on the **ZTP+ Device Defaults** tab. Additionally, you can configure the NTP Server address and select the protocols to enable on your devices, if necessary.
10. Select **Save**.

    The default configuration for this site is complete and any devices you discover with this site selected use this criteria.

Download XMODs (ExtremeXOS/Switch Engine devices only)

XMODs are files that work in conjunction with firmware image upgrades to enhance ZTP+ functionality on ExtremeXOS/Switch Engine devices as well as provide bug fixes for existing features. Like firmware

image upgrades, they are posted by Extreme Networks on github and ExtremeNetworks.com. Save XMODs in the directory you specify in the **Firmware Directory Path** field. Do not set an XMOD as the reference image.

IMPORTANT: ExtremeXOS devices running version 21.1.1.4 require an update to the CloudConnector XMOD for ZTP+ to function properly. Save the most recent XMOD in the **Firmware Directory Path** specified above to update the device, allowing ZTP+ to function as intended. Recent ExtremeXOS/Switch Engine firmware images already include the CloudConnector XMOD, and no updates are required for ZTP+ functionality.

If multiple CloudConnector XMOD files exist in the same directory on the ExtremeCloud IQ Site Engine server as the reference image, ExtremeCloud IQ Site Engine downloads the XMOD file with the higher version number on the device.

General Network Configuration

In order for the switch to communicate to the ExtremeCloud IQ Site Engine server:

- The DHCP Server needs to return a DNS Server and Domain Name to the ZTP+ device.
- The DNS Server needs to map the name **extremecontrol.<*domain-name*>** to the IP address of the ExtremeCloud IQ Site Engine server.

NOS Persona Change from Switch Engine to Fabric Engine

You can configure the ExtremeCloud IQ Site Engine to change the persona of a switch from Switch Engine to Fabric Engine during the ZTP+ process. For the persona change to occur, you must:

- Upload the Fabric Engine firmware to both the TFTP and SFTP directories (Network > Firmware > Upload...)
- Configure the Fabric Engine firmware in the SFTP directory as a reference image
- Configure the NOS Persona Change field as **To Fabric Engine** for a specific site, or manually during the ZTP+ process

Adding the Device to the ExtremeCloud IQ Site Engine Database

Now that the default criteria is configured for devices added to the World Site and you set up the DHCP and DNS servers allowing the device to communicate with the ExtremeCloud IQ Site Engine database, connect the device and add it to ExtremeCloud IQ Site Engine.

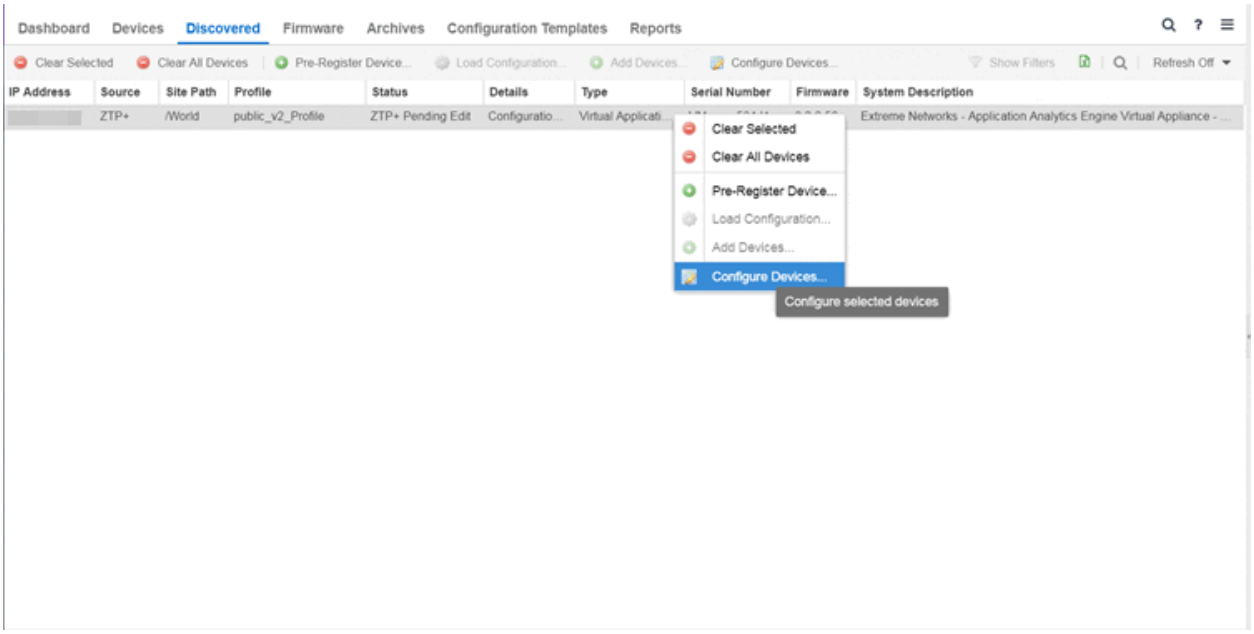
1. Connect the device to your network.

   ZTP+ enabled devices communicate with ExtremeCloud IQ Site Engine securely via an HTTPS

connection and transmit information to ExtremeCloud IQ Site Engine, including the serial number, firmware version, MAC address, operating system, and port information. ExtremeCloud IQ Site Engine determines the status of devices and if new updates are available in the **Firmware** tab and set as Reference images, they are automatically installed.

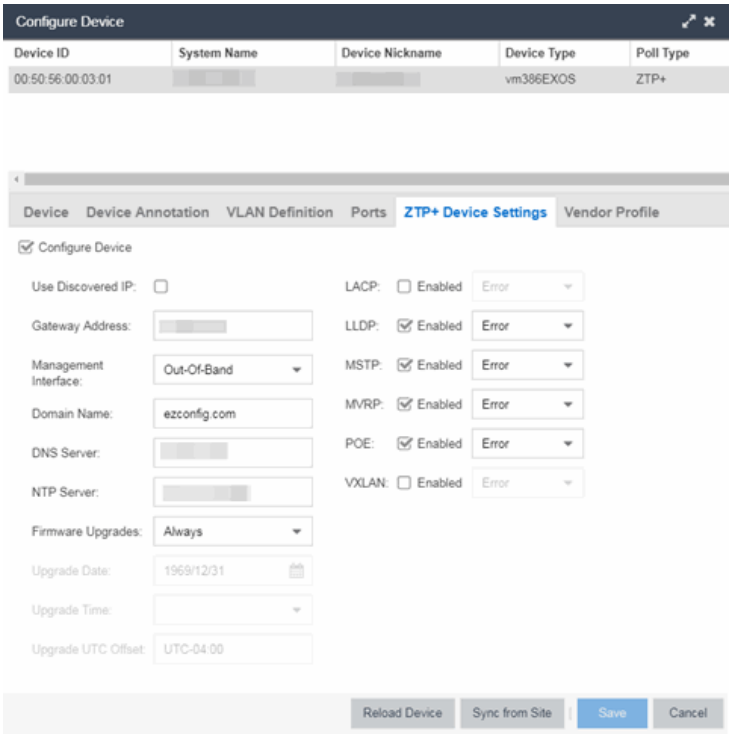
2. Open the Discovered tab in ExtremeCloud IQ Site Engine.

   The device is listed with a **Status** of **ZTP+ Pending Edit**, indicating the device configuration needs to be edited before adding it to the ExtremeCloud IQ Site Engine server.



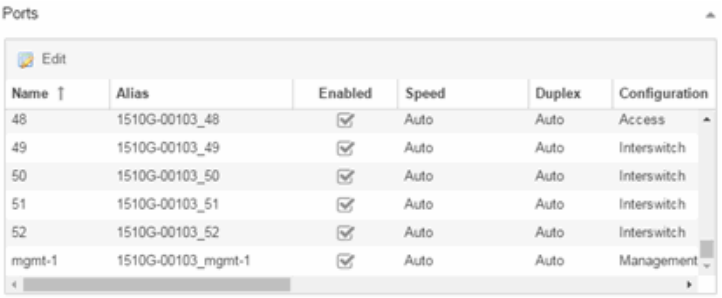
3. Select the device and select the **Configure Devices** button.

   The Configure Device window opens.



4. Select the **Default Site** for the device.
5. Select the **Poll Group** for the device, which indicates the frequency with which ExtremeCloud IQ Site Engine checks for new configurations or updates.
6. Select the appropriate **Poll Type**, which determines how devices are managed on your network:
    - **ZTP Plus** — Devices are polled using ZTP+ functionality.
    - **SNMP** — After devices are added to ExtremeCloud IQ Site Engine via ZTP+, devices are polled using SNMP and are managed manually.
7. Open the **ZTP+ Device Settings** tab.
8. Configure the fields on the **ZTP+ Device Settings** tab to determine how the device is managed by ExtremeCloud IQ Site Engine using ZTP+ functionality.
9. Open the Ports section of the window by selecting the section heading.

   The Ports section opens, displaying the ports transmitted by the device to ExtremeCloud IQ Site Engine when connected to the network.



10. Select a port in the list to configure the port Name, Alias, Configuration, or port VLAN ID.

    You can also add and delete ports by selecting the **Add** and **Delete** buttons, respectively:

    a. Enter the port **Alias**.

    b. Select the port **Configuration**, which is its role or purpose for the device.

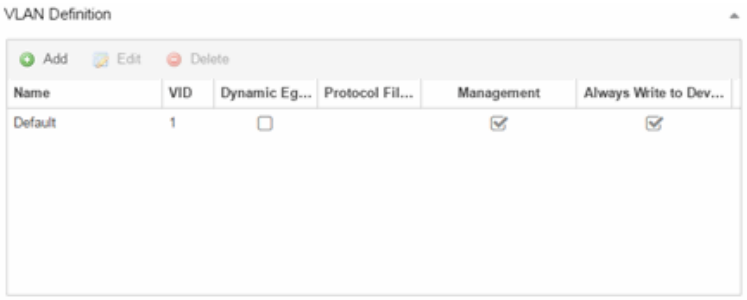
    - **Access** — The port provides access to end-systems.
    - **Interswitch** — The port connects the switch to another switch.
    - **Management** — The port is used to manage the network via ExtremeCloud IQ Site Engine.

    c. Enter a VLAN ID for the port in the **PVID** field.

    d. Configure the port **Speed** and **Duplex**.

11. Open the ZTP+ VLAN Definition section of the window by selecting the section heading.

    The ZTP+ VLAN definition section opens, containing any VLANs you configured on the **Site** tab.



12. Add any device-specific VLANs to those already included in the list by selecting the **Add** button.
13. Change any incorrect fields in the Device, Device Annotation, or Discovered Device Actions sections.
14. Select **Save** at the bottom of the window.

The device is added to the ExtremeCloud IQ Site Engine database and moves from the **Discovered** tab to the **Devices** tab.

NOTES: If you did not select **Automatically Add Devices** on the **Site** tab, the device remains on the **Discovered** tab with a **Status** of **ZTP+ Complete**. Select the device, select the **Add Devices** button (the **Add Device** window appears), and select the **Add** button to add the device to the ExtremeCloud IQ Site Engine database.

In the event a configuration is not correctly transmitted to the switch or if connectivity is lost during any part of this process, the device resets and allows the process to restart.

The device **Status** (displayed on the Discovered tab) is now **ZTP+ Staged**, indicating ExtremeCloud IQ Site Engine will push the configuration to the device the next time the device contacts ExtremeCloud IQ Site Engine.

When ExtremeCloud IQ Site Engine pushes the configuration to the device, the device **Status** is **ZTP+ Complete**.

ExtremeCloud IQ Site Engine generates an event indicating it is upgrading a device image, when the device image is upgraded to the latest version, and when a configuration is sent to a device.

ExtremeAnalyticsEngine ZTP+ Configuration

Using Extreme Networks' ZTP+ (Zero Touch Provisioning Plus) functionality, you can quickly add new ExtremeAnalyticsengines to your network and configure them in ExtremeCloud IQ Site Engine.

IMPORTANT: Logging in to the engine and running the initial engine configuration script will result in the ZTP+ configuration process being shutdown.

Once ZTP+ enabled devices are configured and connected in ExtremeCloud IQ Site Engine, you can view important data and flow collector information on the **ExtremeAnalytics** tab.

General Network Configuration

In order for the engine to communicate with the ExtremeCloud IQ Site Engine server:

- The DHCP Server needs to return a DNS Server and Domain Name to the ZTP+ device.
- The DNS Server needs to map the name **extremecontrol.<*domain-name*>** to the IP address of the ExtremeCloud IQ Site Engine server.

Once ExtremeCloud IQ Site Engine and the ZTP+ device are pre-configured, you can add the site definition to the ExtremeCloud IQ Site Engine database.

Adding the Device to the ExtremeCloud IQ Site Engine Database

When the default criteria is configured for devices added to the World Site and you set up the DHCP and DNS servers allowing the device to communicate with the ExtremeCloud IQ Site Engine database, connect the device and add it to the Discovered tab.

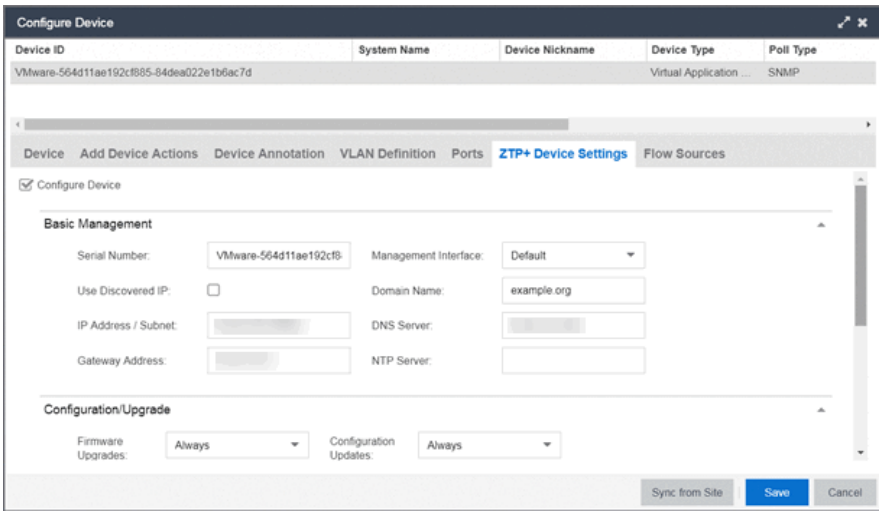
1. Open the **Discovered** tab in ExtremeCloud IQ Site Engine.

   The device is listed with a **Status** of **ZTP+ Pending Edit**, indicating the device configuration needs to be edited before adding it to the ExtremeCloud IQ Site Engine server. Add the ZTP device settings and the flow source information.

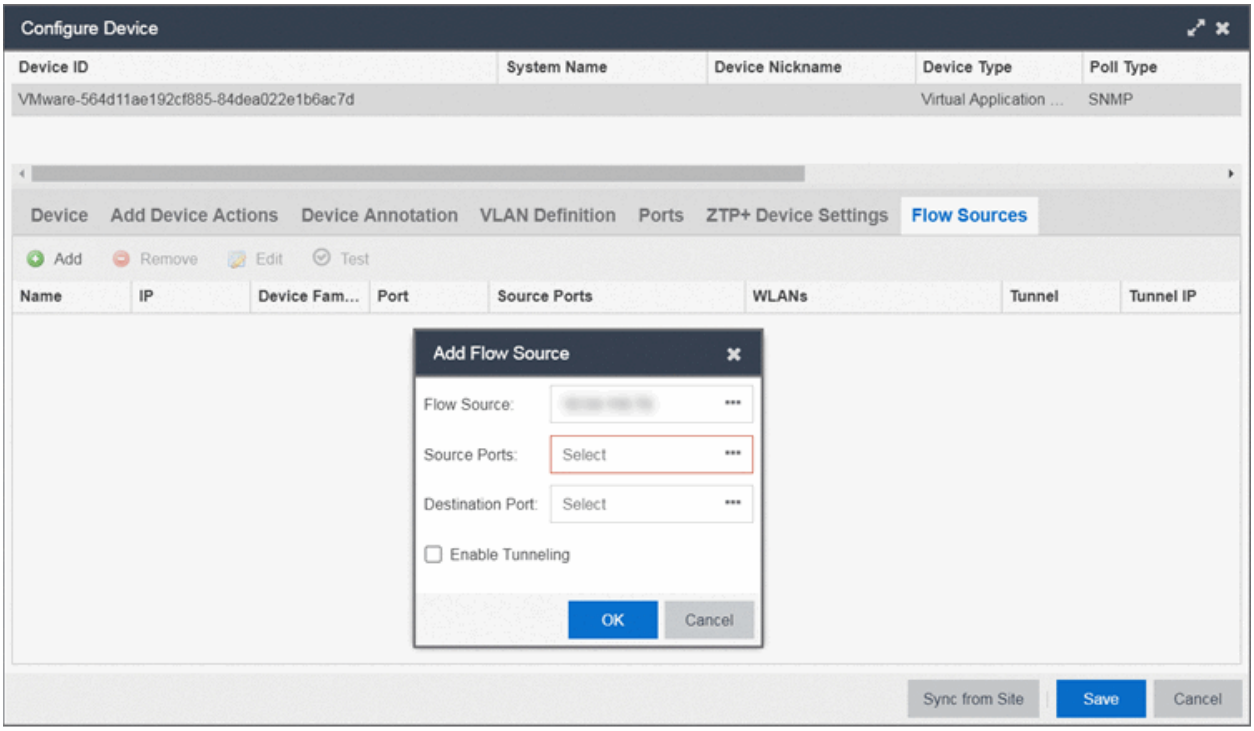
2. Right-click the device and select **Configure Devices** tab from the drop-down list.

   The **Configure Device** window opens.

3. Select the **ZTP+ Device Settings** tab.

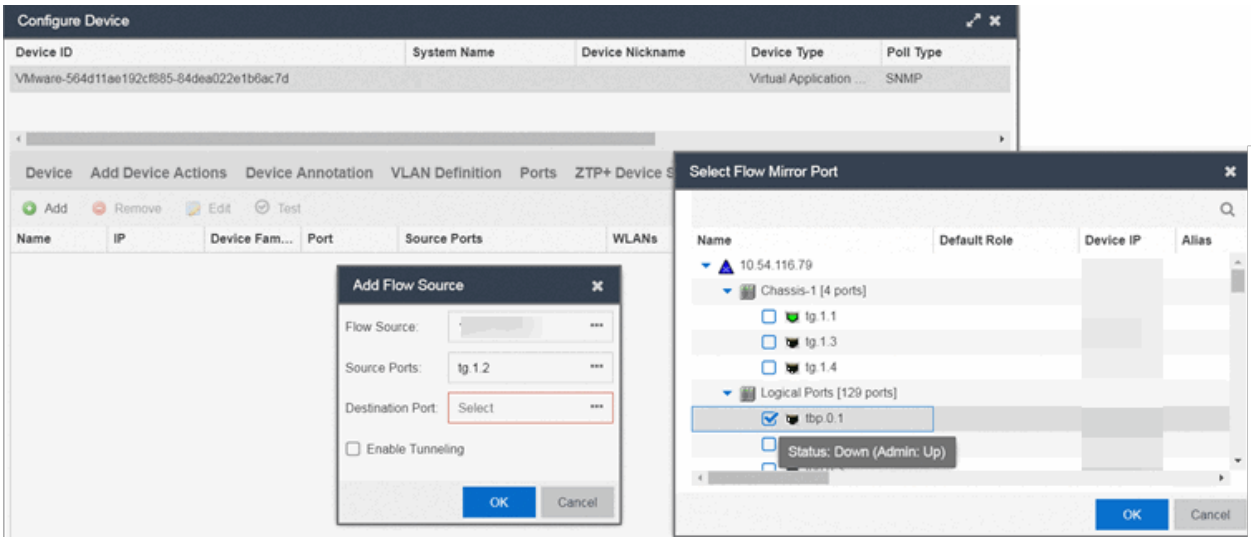


4. Configure the fields on the **ZTP+ Device Settings** tab to determine how the ExtremeAnalyticsengine is managed by ExtremeCloud IQ Site Engine using ZTP+ functionality.
5. Select the **Flow Sources** tab in the **Configure Device** window.



6. Select the ExtremeAnalyticsengine flow information.
    1. Select the **Add** ( ) button.

       The **Add Flow Source** window displays.
    2. Select **FC-180** from the **Flow Source** drop-down list.
    3. Select the **Source Ports** from the drop-down list.
    4. Select the **Destination Port** from the drop-down list.



5. Select the **Enable Tunneling** checkbox.
6. Select the **Tunnel IP** address from the drop-down list.
7. Select **OK** to complete the Flow Source configuration.

NOTES: If you did not select **Automatically Add Devices** on the **Site** tab, the ExtremeAnalyticsengine remains on the **Discovered** tab with a **Status** of **ZTP+ Complete**. Select the engine, select the **Add Devices** button (the **Add Device** window appears), and select the **Add** button to add the engine to the ExtremeCloud IQ Site Engine database.

In the event a configuration is not correctly transmitted to the switch or if connectivity is lost during any part of this process, the engine resets and allows the process to restart.

Completing Configuration and Enforcing the Engine in ExtremeAnalytics

The engine**Status** (displayed on the Discovered tab) is now **ZTP+ Staged**, indicating ExtremeCloud IQ Site Engine will push the configuration to the device the next time the device contacts ExtremeCloud IQ Site Engine.

Open the Configuration tab. The engine is configured with the ZTP+ enabled device and is displayed in the **Overview** window. Enforce the engine to complete the process.

PortView

PortView is an ExtremeCloud IQ Site Engine component that provides port analysis and troubleshooting information including NetFlow data and ExtremeControl end-system details, for your network wired and wireless devices.

The primary launch point for PortView is from the ExtremeCloud IQ Site Engine Search. Depending on the type of item you are searching for, one or more PortView tabs display with information pertaining to your search item. You can also launch PortView from other locations in ExtremeCloud IQ Site Engine.

PortView lets you:

- View a topological display of device relationships.
- Analyze flow details, applications, senders, and receivers.
- Analyze real-time status, utilization, errors, and packets for a port.
- View the map of devices to which the end-system is connected.
- Analyze historical utilization and availability for a port.
- View all end-systems attached to a port and critical end-system information.

This Help topic provides the following PortView information:

- Requirements
  - License and Data Collection Requirements
  - Access Requirements
- Launching PortView
  - Launching from ExtremeCloud IQ Site Engine
  - Launching from Console
  - Launching from NAC Manager

Requirements

License and Data Collection Requirements

The information provided in each report depends on the selected switch and the report data collections you configure. For information on configuring data collection, see Enable Report Data Collection.

The following chart describes the complete set of PortView reports and provides the data collection requirements for each report (if applicable). Some of these reports are available as PortView tabs, others are launched from the right-click menu in the graphical Overview report.

PortView Report	Description	Requirements
Overview	Topological display of device relationships.	
Application Summary	View reports that present a summary of application information.	
Details	The tabs within the report contain the following information: Access Profile — Displays an interactive fingerprint containing information about the end-system. Select an icon to open additional details. End-System — View information about the end-system. End-System Events — View the Access Control Dashboard end-system events table filtered to display all events for the end-system based on the MAC address. Health Results — Displays risk information for the selected end-system.	Switch must have Access Control authentication enabled.
Map	Displays the map containing the device to which the end-system is connected.	
Sessions	The tabs within the report contain the following information: Interface History — Historical interface utilization and availability. Client History — Historical statistics for wired or wireless clients. End-System Events — View the Access Control Dashboard end-system events table filtered to display all events for the end-system based on the MAC address. NetFlow — NetFlow data for the selected port.	Requires active interface statistics collection. Client statistics collection must be enabled. Switch must have Access Control authentication enabled. The switch must support NetFlow and flow collection must be enabled on the port.
Network Information	The tabs within the report contain the following information: Wireless Details — Presents controller, AP, or client information, depending on your search. Interface Details — Real-time interface status, utilization, and errors. AP History — Contains historical data for your APs. Switch Resources — Switch CPU and memory utilization statistics. Device Resources — Device CPU and memory utilization statistics.	Requires active device statistics collection. Requires active device statistics collection.

Access Requirements

Access to PortView reports is determined by the user's membership in an ExtremeCloud IQ Site Engine authorization group and the group's assigned capabilities. The following table lists the capabilities required for access to the different PortView reports.

PortView Report	Required Capability
Network Information Interface History Client History Client Event History Switch History Controller History	XIQ-SE OneView > Access OneView or XIQ-SE OneView > Access OneView and Access OneView Administration
Sessions > NetFlow	XIQ-SE OneView > NetFlow Read Access
Modify Flow Collection	XIQ-SE OneView > NetFlow Read/Write Access
Map	XIQ-SE OneView > Maps > Maps Read Access or Maps Read/Write Access
Details Sessions > End-System Events	XIQ-SE OneView > Access Control > OneView End-Systems Read Access or XIQ-SE OneView > Access Control > OneView End-Systems Read/Write Access

Launching PortView

You can launch PortView from a variety of locations in ExtremeCloud IQ Site Engine. By default, you can have five active PortView searches displayed in ExtremeCloud IQ Site Engine at one time. You can change this display limit in the **Maximum PortViews Displayable** field in Site Engine - General (Administration > Options > Site Engine - General > Session Limits).

NOTE: A single PortView search returns a maximum of five matching results. If the number of matching results exceeds five, an error message appears asking you to refine the search term and try again.

Launching from ExtremeCloud IQ Site Engine

ExtremeCloud IQ Site Engine Search Tab

The primary launch point for PortView is from ExtremeCloud IQ Site Engine Search. The Search page provides a search field where you can enter a MAC address, IP address, host name, AP serial number, or Access Control custom field information to begin searching. Depending on the type of item for which you are searching, the search results return one or more PortView tabs, with information pertaining to your search item. You can right-click on the different devices in the topology results to launch additional reports.

1. Open the **Search** tab.
2. Enter a MAC address, IP address, host name, AP serial number, or Identity and Access custom field information, and press **Enter** to begin the search. You can copy the IP or MAC address from another source and enter it into the **Search** field. For example, you can copy an end-system MAC address from the **Control** tab End-Systems view, and then paste the MAC address into the search field and press **Enter**.

3. Depending on the type of item for which you are searching, the secondary navigation bar displays one or more PortView tabs, with information pertaining to your search item, similar to the search results shown below.

ExtremeCloud IQ Site Engine Interface Summary FlexView

Use the following steps to launch PortView from an ExtremeCloud IQ Site Engine Interface Summary FlexView.

1. On the **Network** tab, select on the device Name link to open the Interface Summary FlexView.
2. In the Interface Summary, select the interface Name or Alias link to open PortView.

Launching from Console

You can launch PortView from Console using any of the following methods:

- In the **Port Properties** tab, right-click on one or more ports and select **Port Tools** > **PortView**.
- In the Compass Results table, right-click on up to four entries and select **Port Tools** > **PortView**.
- In the Interface Summary FlexView, right-click on one or more ports and select **Port Tools** > **PortView**.

Launching from NAC Manager

You can launch the PortView Access Control reports from NAC Manager using either of the following two methods:

- In the **End-Systems** tab, right-click on an end-system in the table and select **PortView** from the menu.
- On the **Control** tab's End-Systems view, right-click the entry with the desired switch port and select **PortView** from the menu.

AP Wireless Real Capture

Real Capture allows real-time collection of Access Point (AP) wireless traffic for troubleshooting and problem resolution. Real Capture collects traces on the AP wireless interface and transmits them to Wireshark running on a local Windows client. It allows Wireshark to capture RF/wireless traffic as if it were running directly on the AP, providing visibility into network connectivity and performance issues. All Wireshark features are supported, including filters and I/O graphs.

NOTE: APs must be running firmware version 8.x or later. The AP2600 series of Access Points does not support the Real Capture feature.

Real Capture can be enabled for each AP individually from PortView in the ExtremeCloud IQ Site Engine. When it is enabled, Real Capture runs a daemon on the AP that allows it to interface with Wireshark using port 2002 or 2003. The AP then captures all the wireless traffic (except for management traffic) originating from the AP and sends it to Wireshark for analysis.

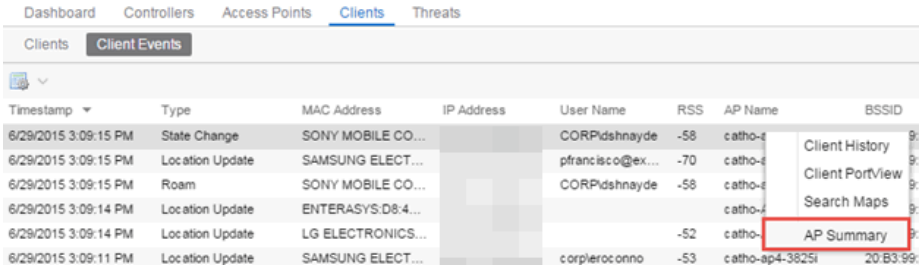
In addition to capturing network traffic for analysis in Wireshark, the AP also collects RF information. The RADIOTAP header format delivers RF information. You must use Wireshark 1.6 or later to read the full RADIOTAP header information. For troubleshooting features like TxBF/STBC, you can enable capturing the 802.11n preamble header using the AP CLI commands.

NOTE: When capturing client traffic on the AP, if the topology is bridged at AP, client traffic is captured and can be analyzed in the resultant trace. However, if the topology is bridged at controller, only WASSP traffic is captured as the AP tunnels this communication back to the controller. This traffic must be sent to the Extreme Networks Support for analysis because it needs to be decoded. In this scenario, it may be better to mirror the switch port where the controller connects to the LAN.

Configure and Use Real Capture

Use the following steps to configure and use the Real Capture feature.

1. Launch ExtremeCloud IQ Site Engine.
2. Launch PortView for the AP from the Wireless Client Event History report.
    a. Select the **Wireless** tab and then select the **Clients** tab and the **Client Events** sub-tab. Right-click on the AP Name and select **AP Summary** from the menu.

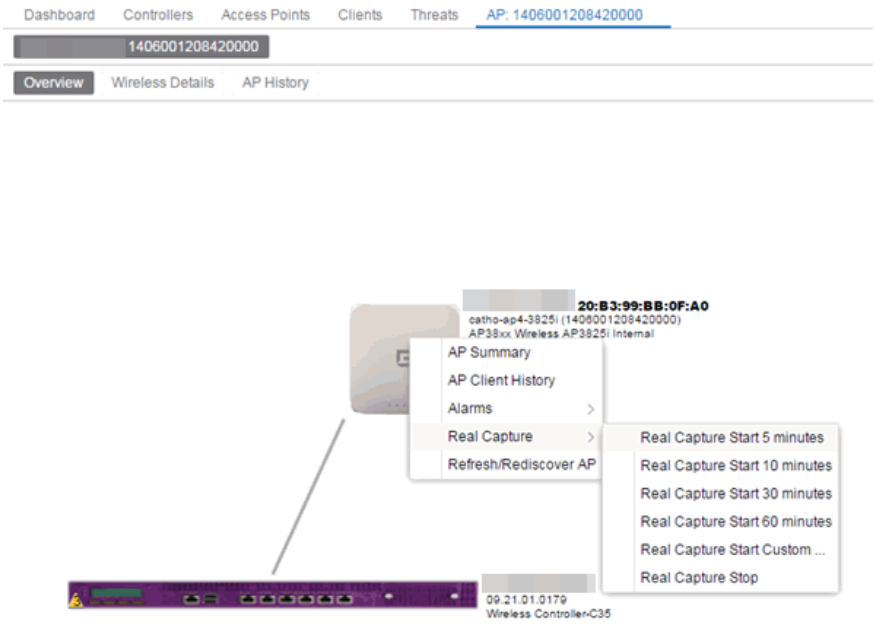


b. The AP PortView opens.

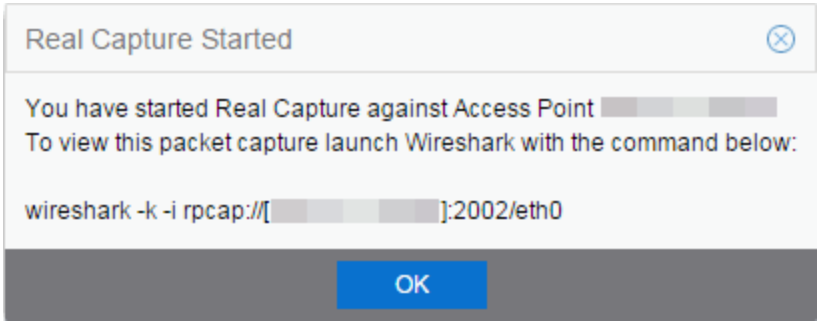


NOTE: You can also launch PortView for the AP using the **Search** tab. Open the **Search** tab, enter the search criteria (MAC, IP, hostname, or AP serial number) and press **Enter** to display the AP PortView.

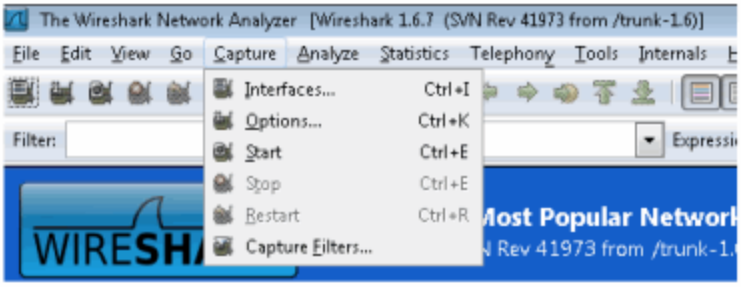
3. Right-click on the AP in the PortView topology display and select **Real Capture** > **Real Capture Start xx minutes**. Select the desired amount of time to run the capture or create a custom capture duration value. If you need to, you can stop the Real Capture by selecting **Real Capture Stop**.



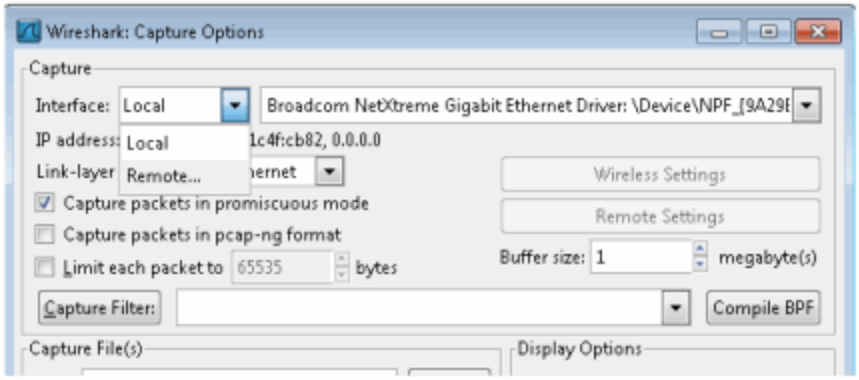
4. A message appears to inform you Real Capture has started, and provides a CLI command you can use on a client on which Wireshark is installed, to launch Wireshark against the AP and view the captured traffic.



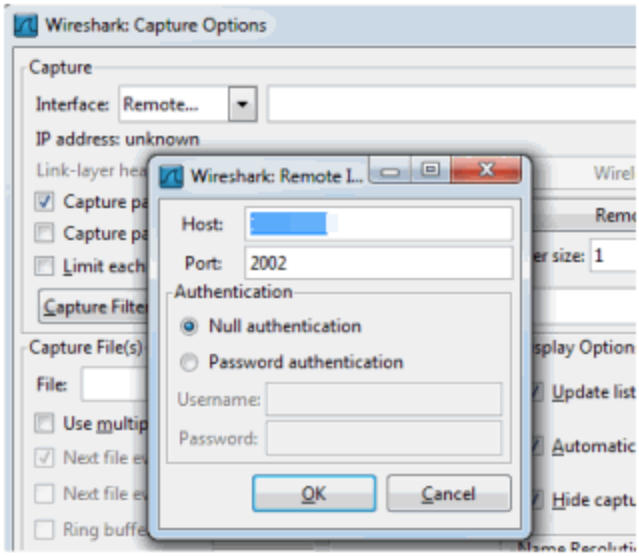
5. You can also access the captured traffic in Wireshark using the following steps:
   a. In Wireshark, select **Capture** > **Options** from the menu bar.



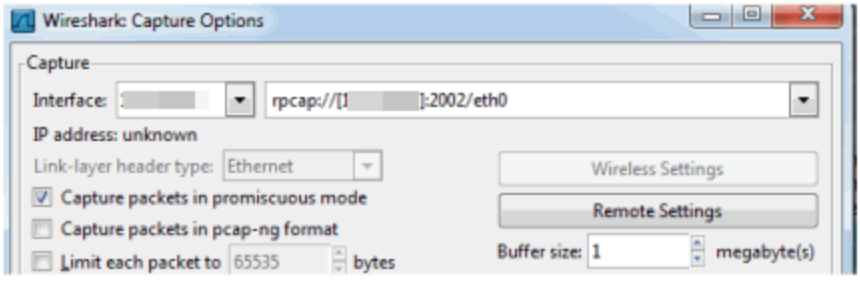
b. In the Capture Options window, set the **Interface** value to **Remote**.



c. The Remote Interface window appears. Enter the AP's IP address in the **Host** field, and the port number (2002 or 2003) in the **Port** field (you can see this information in the CLI command message described in step 4). In the Authentication section, select **Null authentication**. Select **OK**.



d. Wireshark adds the command information to the Capture options.



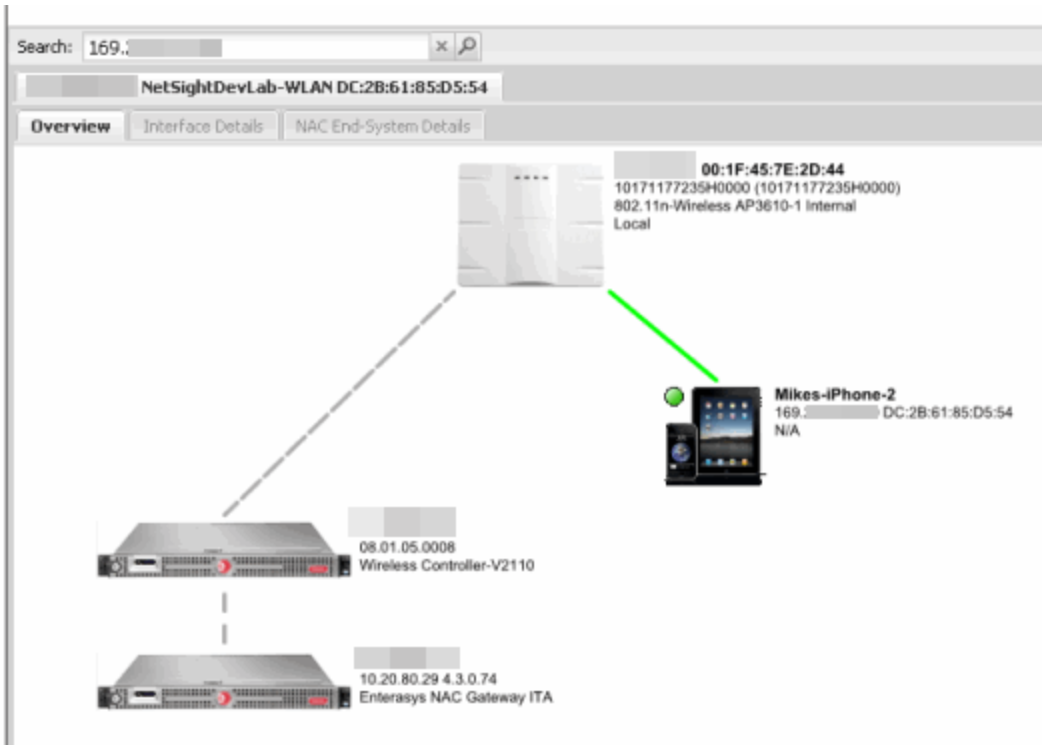
e. Select **OK** in the Capture Options window to begin viewing the captured traffic in Wireshark. When you have the data you need, you can stop the capture and save it to a file for further diagnosis and troubleshooting.

Real Capture Example

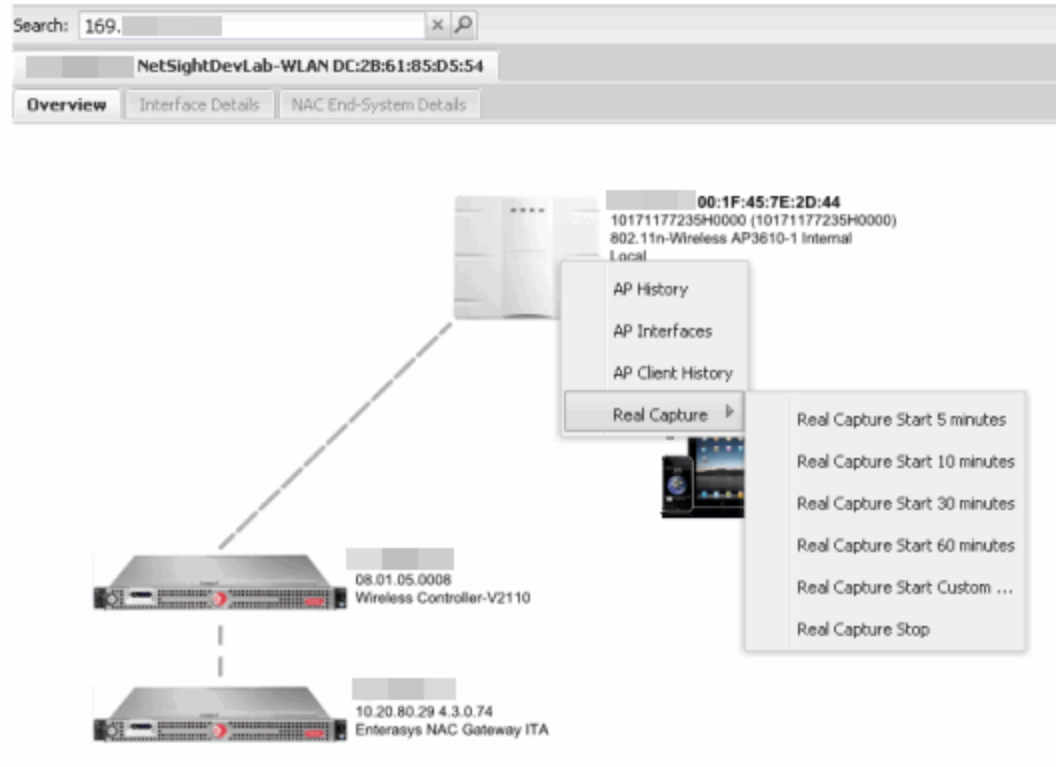
The following example shows how to use Real Capture to diagnose an end-system connection problem in ExtremeCloud IQ Site Engine.

The problem starts when an end-system in ExtremeCloud IQ Site Engine is not able to obtain an IP address.

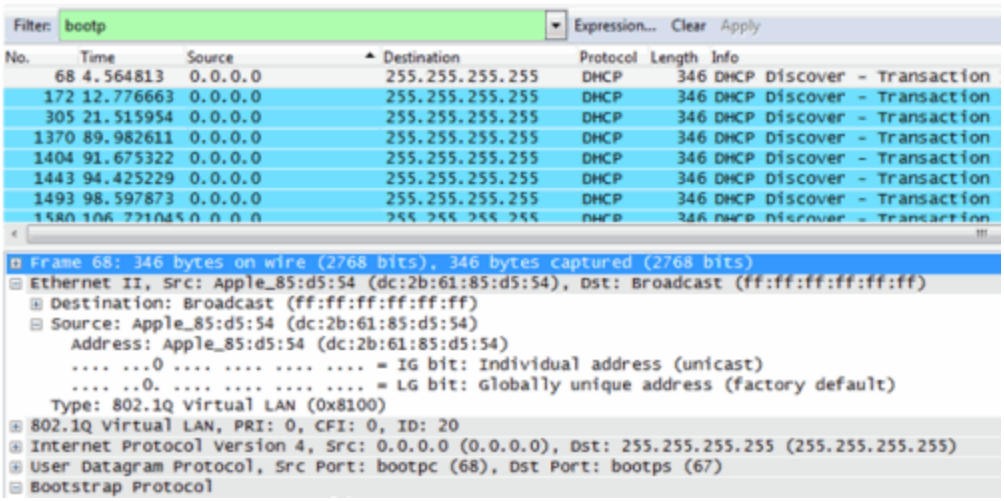
A search is performed on the 169.x.x.x IP address.



The traffic capture is started on the AP to which the end-system is connected.



The resulting trace in Wireshark shows the end-system sending out DHCP Discover packets with no response, perhaps indicating a VLAN or network-related issue.



Restoring the Database Using the CLI

Use the instructions in this topic to restore an ExtremeCloud IQ Site Engine database backup using the CLI (command line). Restoring a database using the CLI may be necessary after making significant

unwanted configuration changes.

NOTE: For ExtremeCloud IQ Site Engine 24.2 and earlier, a database backup created by the Backup/Restore procedure, with **Back Up Alarm**, **End-System Event**, and **Reporting Database** enabled, is required prior to running the following database restore procedure. This procedure does not work if **Back Up Alarm**, **End-System Event**, and **Reporting Database** are disabled.

In release 24.2 and earlier, the backup script is `mysqlbackup_restore.sh`

The restore runs using the `backup_restore` script in the *<install directory>*`/scripts` directory.

To restore the backup from another instance of ExtremeCloud IQ Site Engine, the backup needs to be transferred first. The content of `<install directory>/backup>` including subdirectories should be transferred to the new instance. To restore the ExtremeCloud IQ Site Engine database backup:

1. Ensure you are running the **same version** of ExtremeCloud IQ Site Engine used when creating the database backup on the ExtremeCloud IQ Site Engine server.
2. Log into the system shell (via the local console or SSH) on the ExtremeCloud IQ Site Engine server as root.
3. Navigate to the scripts directory:
   - Enter `cd` *<install directory>*`/scripts`.
4. Run the backup_restore script:
   - Enter `./backup_restore.sh` *<full backup directory structure configured on Backup/Restore tab, including path>*

     (for example, `./backup_restore.sh /usr/local/Extreme_Networks/NetSight/backup/xiqse_03302021/`).

NOTE: If you restore a backup for troubleshooting purposes, disable the connection to ExtremeCloud IQ to prevent influencing the production statistics. The restoration script will offer you the option to disable the connection to ExtremeCloud IQ.

For air gap deployment mode, the option to disable the ExtremeCloud IQ connection is not relevant.

The database backup is restored. Devices onboarded to ExtremeCloud IQ after the backup was created become orphaned when the database restore is finished. Manual deletion of orphaned devices in ExtremeCloud IQ might be needed.

IMPORTANT:

The deployment mode (connected or air gap) is part of the database backup. Restoring from the backup will not change the deployment mode. The serial number is part of the database backup. Restoring the backup also restores the serial number. The air gap license file is bound to the serial number. Neither license keys nor license files are part of the database backup.

In Connected deployment mode, the following sequence is recommended:

1. Delete ExtremeCloud IQ Site Engine from ExtremeCloud IQ
2. Wait for all devices managed byExtremeCloud IQ Site Engine to disappear from ExtremeCloud IQ
3. Restore the backup of ExtremeCloud IQ Site Engine
4. Onboard ExtremeCloud IQ Site Engine to ExtremeCloud IQ

If you are restoring the backup to a clean installation, license files and license keys should be inserted into ExtremeCloud IQ Site Engine after the restore.

- Database Backup Options

Restore Device Configuration

On the **Network** tab, you can easily restore a device configuration to an active network device using a "cloned" configuration from an existing network device or a configuration template created on the **Network** > **Devices** tab. In addition, you also have the ability to download the latest firmware on the active device.

This Help topic provides the following information:

- Preliminary Steps
  - Required Capabilities
  - Device Firmware
- Restoring a Configuration
  - Using a Configuration Template
  - Cloning a Device Configuration

Preliminary Steps

Required Capabilities

In order to perform the restore configuration operation, you must be a member of an authorization group with the following capabilities.

Required Capability
Inventory Manager > Firmware/Boot PROM Management > Firmware/Boot PROM Upgrade Wizard
Inventory Manager > Configuration Archive Management > Archive Restore Wizard
Inventory Manager > Configuration Templates Management > Configuration Templates Download Wizard
XIQ-SE Suite > Devices > Add, Discover, and Import

Device Firmware

If you are updating the device's firmware, you must first add the new firmware version to the left-panel Firmware folder on the **Network** > **Firmware** tab. It is then available when configuring the device.

For information on obtaining firmware, contact your Extreme Networks representative, or access the firmware download library at: https://extremeportal.force.com/.

1. Place your new firmware in your firmware directory. ExtremeCloud IQ Site Engine uses the default tftpboot\firmware\images directory for storing your firmware.

2. In the left-panel Firmware folder, select the **Refresh** icon (Refresh). ExtremeCloud IQ Site Engine automatically adds your new firmware to the appropriate firmware groups in the left-panel Firmware folder.

The new firmware version is available when configuring the device in ExtremeCloud IQ Site Engine.

Restoring a Configuration

When restoring a configuration to an active device, there are two options for selecting a configuration to use. One option is to "clone" an existing device on the network for a configuration. Another option is to use a Configuration Template you create.

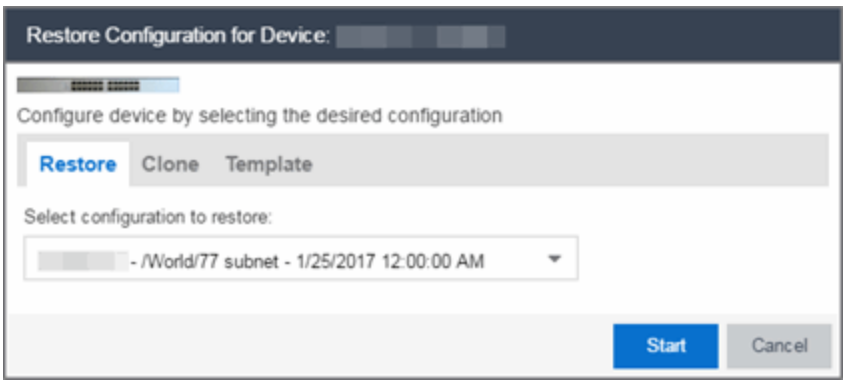
Cloning a device configuration is useful when you want to use the exact same configuration on another device. If you are cloning a device configuration, you must have an existing configuration for that device archived.

Using a configuration template allows you to restore a complete or partial configuration to the device with variables you can define specifically for that device. If you are going to use a configuration template for your device, you must create the Configuration Template to use as the source configuration for a device.

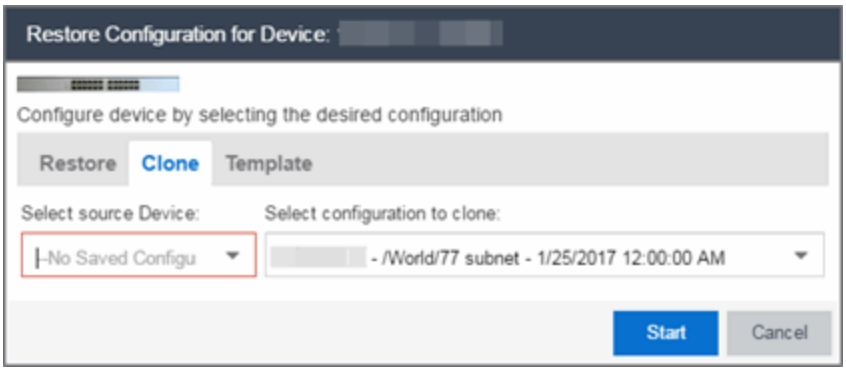
Cloning a Device Configuration

When cloning a device configuration, use an existing configuration of a network device archived in ExtremeCloud IQ Site Engine. The cloned device (the archived device you are using) must **not** be active on the network to prevent two devices from having the same IP address on the network.

1. Launch ExtremeCloud IQ Site Engine. On the **Network** > **Devices** tab, right-click on the active device and select **More Actions > Restore Configuration**. The Restore Configuration window opens.



2. Select the **Clone** tab.

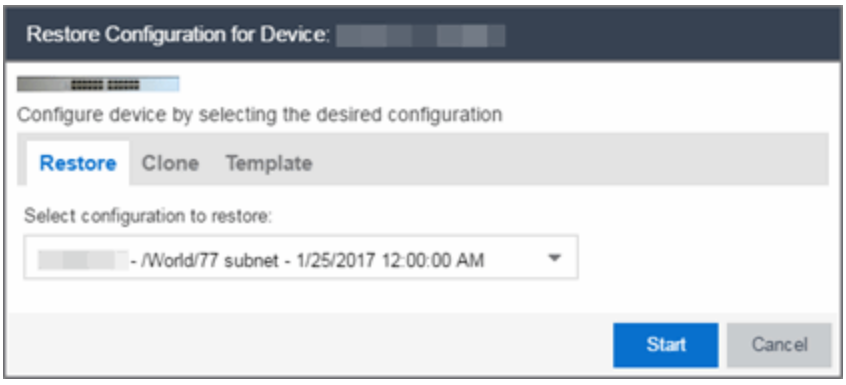


3. If desired, select a new version of firmware to download to the device. (You must add the new firmware version to ExtremeCloud IQ Site Engine. For more information; see "Device Firmware".)
4. Select the Device option as the Configuration Source.
5. Select the source device for the configuration. The selected device must be Inactive on the network or you cannot perform the restore operation. This prevents two devices from having the same IP address on the network.
6. Select the archived device configuration to clone.
7. Select **Start**. First, the firmware is updated (if that option is selected) and then the configuration is loaded and the device is restarted.

Using a Configuration Template

The following steps describe how to use a configuration template as the source configuration for a device.

1. Launch ExtremeCloud IQ Site Engine. On the **Network** > **Devices** tab, right-click on the active device and select **More Actions > Restore Configuration**. The Restore Configuration window opens.



2. Select the Template option as the Configuration Source.

3. Select the appropriate template from the **Template** drop-down list and enter the required variables.
4. Select the **Profile** for the new device from the drop-down list.
5. Select **Start**. The configuration is loaded and the device is restarted.

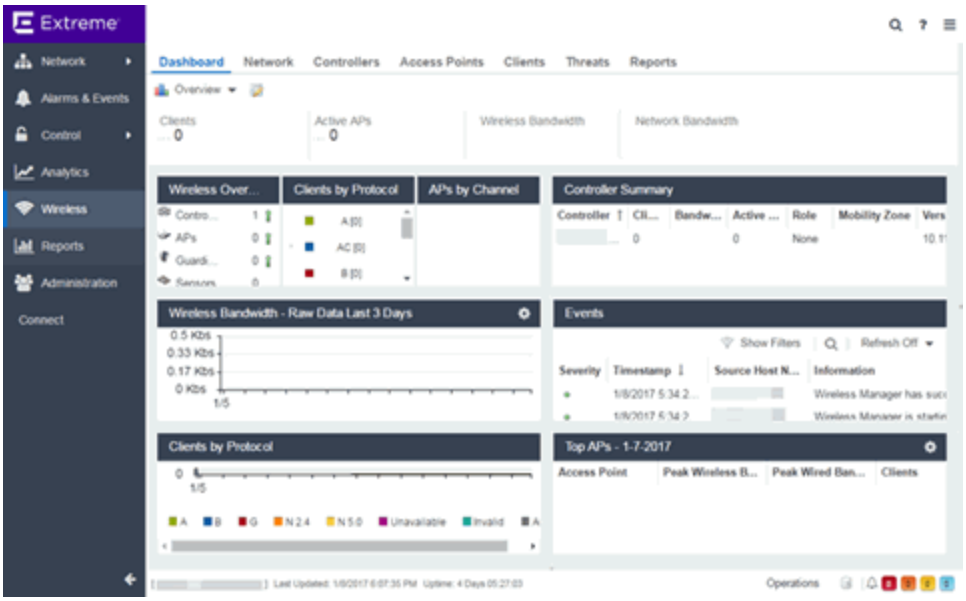
Configuring Enhanced Netflow for Extreme Analytics and Extreme Wireless Controller Version 10.21

When adding a Wireless Controller as a flow source in ExtremeCloud IQ Site Engine, a mirror port is automatically created. Wireless Controllers on which a firmware version of 10.21 or higher is installed use IPFIX, so the mirror port is unnecessary.

NOTE: Wireless Controllers on which a firmware version lower than 10.21 is installed still require the mirror port be configured.

To remove a mirror port on a Wireless Controller running version 10.21:

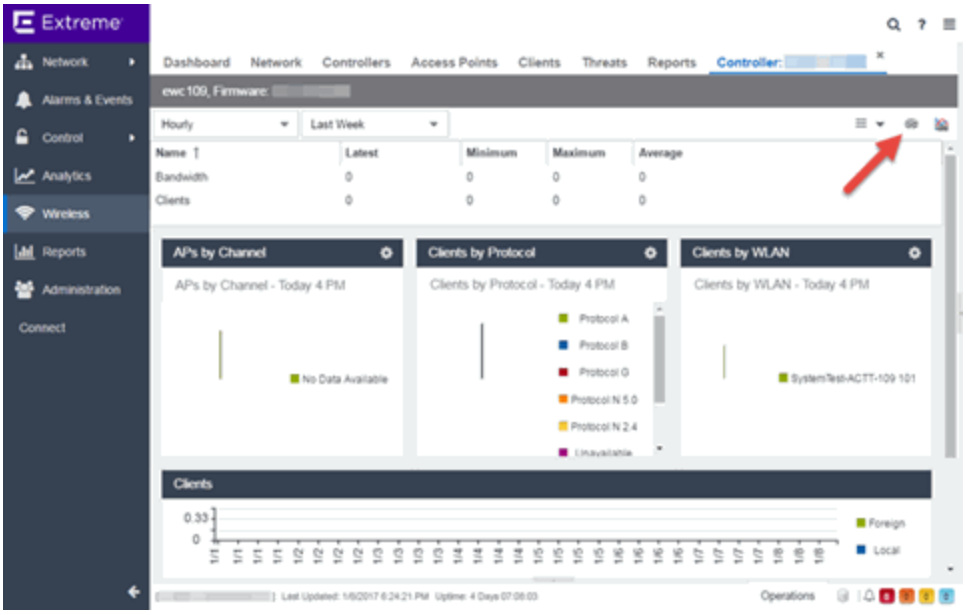
1. Access the **Wireless** tab in ExtremeCloud IQ Site Engine.
   The **Wireless** tab opens.



2. Select the **Controllers** tab.
   The **Controllers** tab opens.

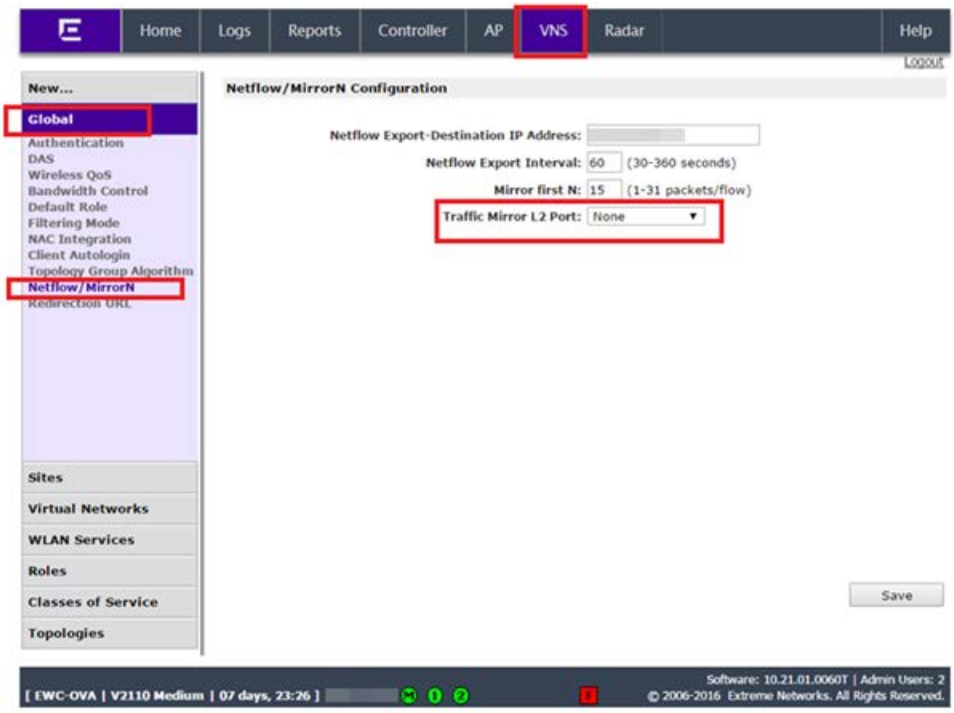


3. Select the **IP address** for the controller, located in the **Controller** column.
   The Wireless Controller Summary page opens.



4. Select the **WebView** icon ( ) at the top right of the Wireless Controller Summary page.
   The WebView opens for the controller.

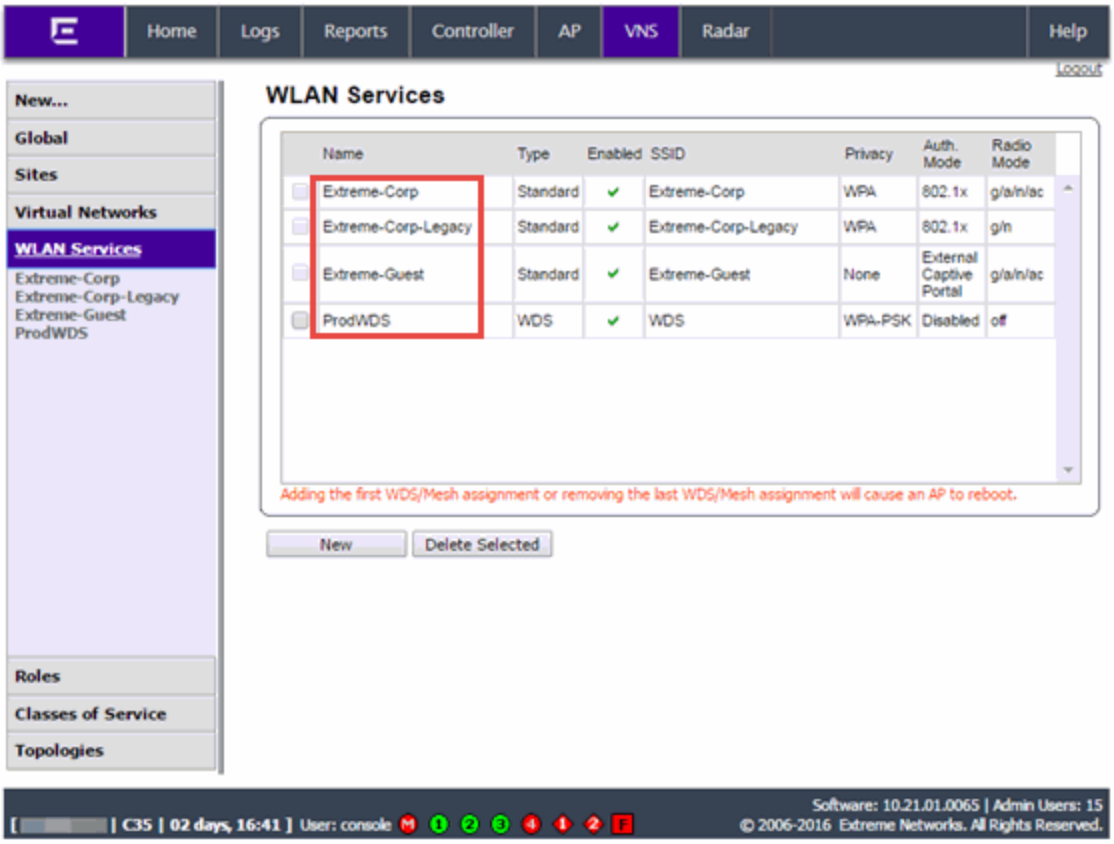
5. Select the **VNS** tab.
   The **VNS** tab opens.



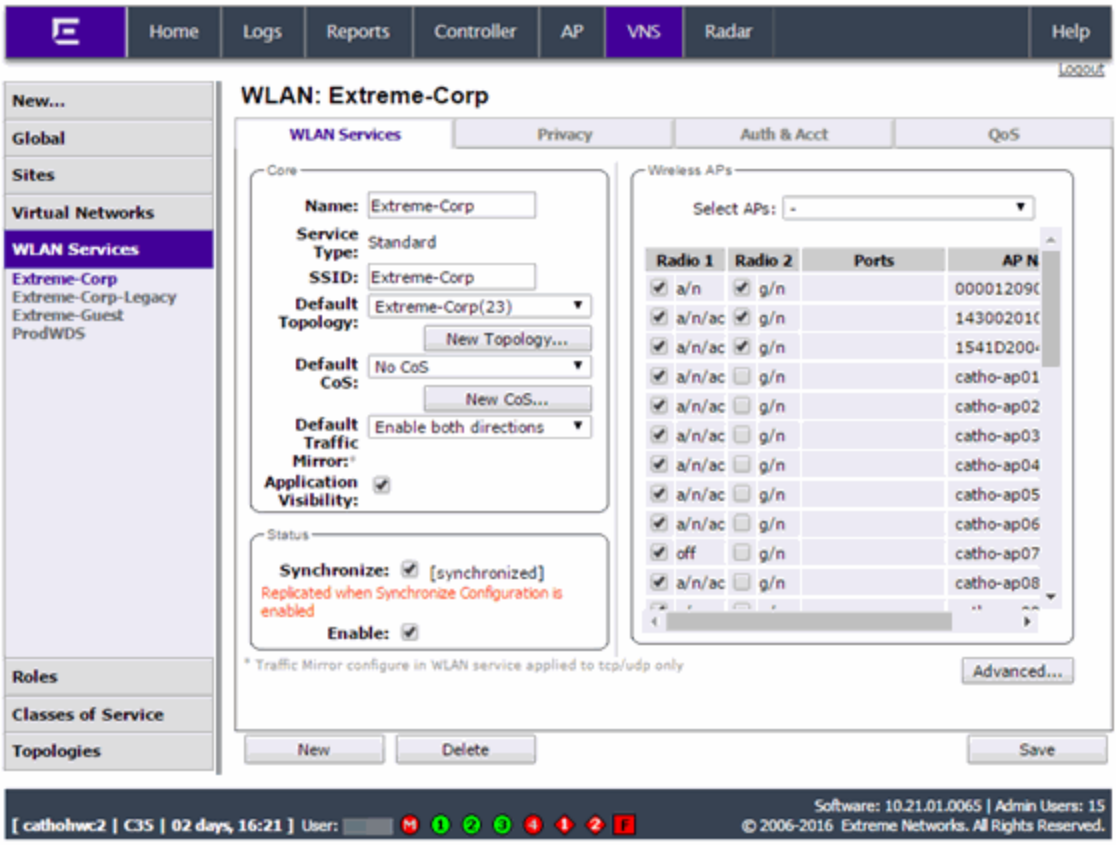
6. Select **Netflow/MirrorN** from the left-panel.
   The Netflow/MirrorN Configuration page opens.
7. Select **None** from the **Traffic Mirror L2 Port** drop-down list.
8. Select the **Save** button.

NOTE: The Mirror Port in the Wireless Control Flow Sources section of the **Analytics** > **Configuration** > **Configuration** tab is not available when the **Traffic Mirror L2 Port** is disabled.

9. Select **WLAN Services** from the left-panel.
   The WLAN Services page opens.

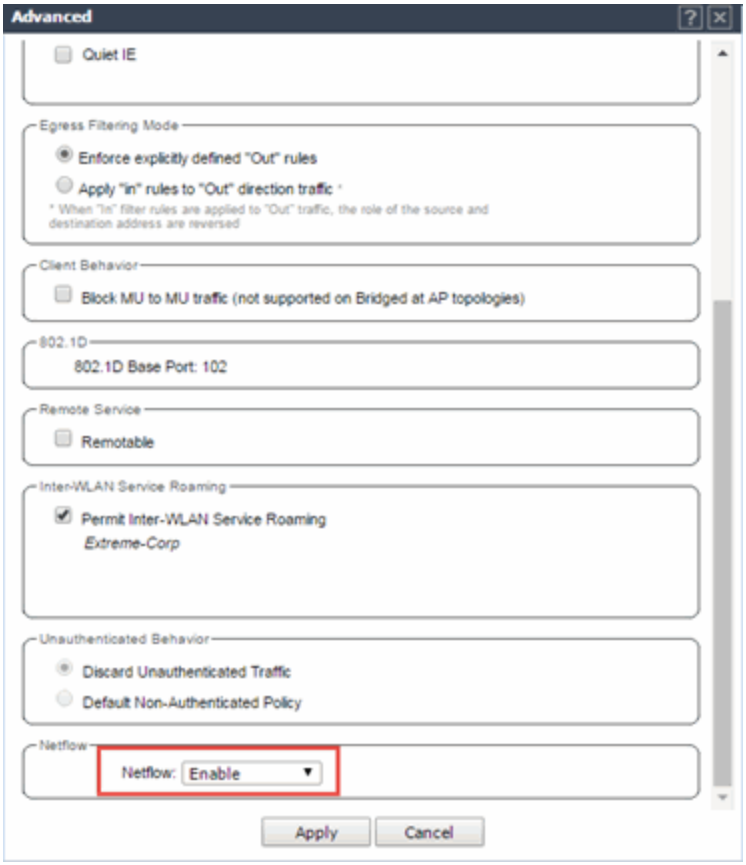

Home
Logs
Reports
Controller
AP
VNS
Radar
Help
Logout
New...
Global
Sites
Virtual Networks
WLAN Services
Extreme-Corp
Extreme-Corp-Legacy
Extreme-Guest
ProdWDS
Roles
Classes of Service
Topologies
WLAN Services
Name
Type
Enabled
SSID
Privacy
Auth. Mode
Radio Mode
Extreme-Corp
Standard
Extreme-Corp
WPA
802.1x
g/a/n/ac
Extreme-Corp-Legacy
Standard
Extreme-Corp-Legacy
WPA
802.1x
g/n
Extreme-Guest
Standard
Extreme-Guest
None
External Captive Portal
g/a/n/ac
ProdWDS
WDS
WDS
WPA-PSK
Disabled
off
Adding the first WDS/Mesh assignment or removing the last WDS/Mesh assignment will cause an AP to reboot.
New
Delete Selected
C35 | 02 days, 16:41] User: console
Software: 10.21.01.0065 | Admin Users: 15
© 2006-2016 Extreme Networks. All Rights Reserved.

10. Select a wireless LAN in the table.
    The WLAN page opens for the selected wireless LAN.



11. Select the **Advanced** button.
    The **Advanced** window opens.

12. Scroll to the bottom of the window and ensure the **Netflow** drop-down list is set to **Enable**.



13. Select the **Apply** button.

The wireless controller is now configured.

NOTE: **Rx Packets** and **Rx Bytes** can incorrectly be **0** when flow data is gathered via a wireless controller running version 10.21 or higher. Additionally, application response times and some meta data can be blank. This is a known issue and will be addressed in a future release.

Configure ExtremeXOS/Switch Engine Identity Manager to Send Events to ExtremeCloud IQ Site Engine

This chapter describes how to use the Identity Management — Configuration script on a Summit series or Black Diamond series switch to send events to ExtremeCloud IQ Site Engine.

In order to run the Identity Management — Configuration script on a device, you must be a member of an authorization group assigned the ExtremeCloud IQ Site Engine Suite > Common Web Services > Web Services APIs Read/Write Access capability.

To run the Identity Management — Configuration script on a device:

1. Open the **Network** > **Devices** tab in ExtremeCloud IQ Site Engine.
2. Right-click a Summit series or Black Diamond series switch in the Devices table or in the Device Groups left-hand panel.
3. Select the Identity Management — Configuration script in the Scripts > Access Control menu. The Run Script window opens.
4. On the **Device Selection** tab, the selected device is automatically included. Use the arrows to add additional devices or remove devices and to control the order of the selected devices.
5. Select **Next**.
6. On the **Overview** tab of the **Device Settings** tab, set the configuration properties for the script. If desired, select the **Description** tab to view the description defined for the script.
    - Stop on error? — Indicates whether the script stops if an error occurs.
    - Target Server IP Address — The IP address to which notifications are sent.
        - Entering a value of $serverIP automatically enters the IP address of the ExtremeCloud IQ Site Engine server IP.
        - Enter the IP address of the Access Control engine if using the Extreme Networks ExtremeControl solution.
    - Target Server Type — Selecting netsight monitors the IP, username, and port of the user accessing the device. Users with the Extreme Networks ExtremeControl solution can select nac, which provides you with the ability to run Kerberos authentication (if enabled) on the device.

      NOTE: In order to give elevated access to users when using the Kerberos authentication type on the device, the Target Server Type must be **nac** to allow the Access Control engine to learn the Kerberos traffic.

    - Target Server Username — The username of the user to which the web service request is made.
    - Target Server Password — The password of the user to which the web service request is made.
    - Target Server HTTPs Port — The port that the ExtremeCloud IQ Site Engine server or Access Control engine uses for HTTPS communication. The default port is 8443, but if the port was changed when configuring the ExtremeCloud IQ Site Engine server or Access Control engine, enter the custom port used.
    - XML Target Name — The name of the targets on the switch to which IDM events are sent. Using the default predefined XML Target Name creates a unique name for each server.
    - Choose Action — The action that occurs on the device when the script is run.
        - Enable ID Monitoring — This option sets up the XML notification, configures ports for Identity Management (if specified), and enables or disables ports for devices

you can use with Identity Management.

- Manage Ports — This option only configures ports for Identity Management (if specified).

7. On the Run-Time Settings tab, set the run-time settings for the script (for more information about defining run-time variables when creating a script, see Specifying Run-Time Settings for a Script).
    - Save configuration in the background after running script successfully — Device configuration is saved after the script is run.
    - Timeout if script is not completed on each device (in seconds) — The amount of time in seconds before a timeout occurs if a device does not respond.
    - Run now, don't save as a task — Select to run the script now and do not save the script as a task.
    - Save as a task and run now — Select to run the script now and save it as a task. Type a name for the task in the Task Name box below. The task appears on the Script Tasks tab (see "Save Script as a Task").
    - Save as task. I'll run later — Select to save running the script as a task. The script does not run at this time. Type a name for the task in the Task Name box below. The task appears on the Script Tasks tab (see "Save Script as a Task").
8. Select **Next**. On the Verify Run Script tab, verify your script selections, and then select **Next**.
9. Select **Next**.
10. On the Results tab, you see the results of the script including any errors.
11. Select **Close**.

Schedule Tasks

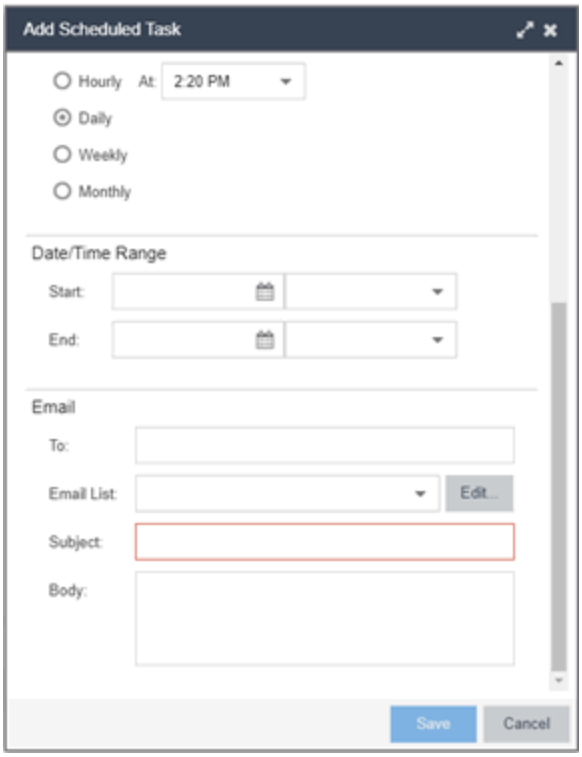
The Scheduled Task tab allows you to configure ExtremeCloud IQ Site Engine to automatically perform the following tasks:

- Generate a subset of available reports in PDF format
- Run a script or workflow
- Set SMTP Email Server Options to use when the scheduled task sends an email notification.
- Discover newly added devices

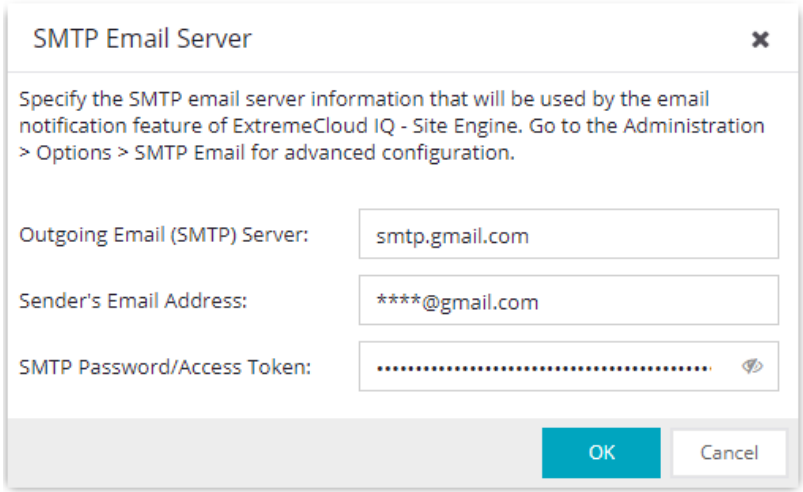
Create a New Scheduled Task

1. Launch ExtremeCloud IQ Site Engine.
2. Select **Tasks** and select the **Scheduled Tasks** tab.

3. Select the **Add** button. The Add Scheduled Task window opens.



If no SMTP email settings are configured, the SMTP Email Server window also opens, where you can define the SMTP email settings. You can also configure the SMTP email settings in SMTP Email Options.



4. Enter the outgoing SMTP email settings, if necessary, and select **OK**.

5. Select the type of task from the **Type** drop-down list in the Add Scheduled Task window:
    - **Device Export** — Exports the list of devices on your network from the **Network** > **Devices** tab.
    - **Disable Alarms** — Disables enabled alarms for the amount of time you define on a scheduled basis. Use this task to avoid alarms during times you reserve for network maintenance activity. You can manually ignore enabled alarms in Alarm Configuration .
    - **FlexReports** — Creates a FlexReport for the devices you select on a scheduled basis.
    - **FlexViews** — Creates a FlexView for the devices you select on a scheduled basis.
    - **Compliance** — Emails the most recently run ExtremeCompliance report on a scheduled basis in PDF format.
    - **Port Usage** — Creates a Port Usage report for the devices you select on a scheduled basis.
    - **Port Usage Details** — Creates a Port Usage Details report for the devices you select on a scheduled basis.
    - **Reporting** — Emails a report you select (see Report Designer) on a scheduled basis.
    - **Scripting Task** — Runs a script saved on the Saved Tasks on a scheduled basis.
    - **Support** — Emails debugging data on a scheduled basis that provides information to Extreme Networks Support in the event of an issue with your network. ***Only select this option if instructed to do so by Extreme Networks Support.***
    - **Site** — Runs a device discover for a site (created on the Site) on a scheduled basis.
    - **Workflow Task** — Runs a workflow saved on the Saved Tasks on a scheduled basis.
6. Select the report, saved task, support task, or site you want to schedule in the **Report Name**, **Saved Task Name**, **Support Task Name**, or **Site to Discover** drop-down list, respectively. Depending on what you select, you may need to make other selections such as specifying the source engine or controller.
7. Edit the task name and description, if desired.
8. Select or deselect the **Enabled** checkbox to enable or disable the task, respectively. A disabled task is not performed.
9. Select whether you want the task to occur on an hourly, daily, weekly, or monthly basis.
    - **Hourly** — specify the minute each hour you want the task performed.
    - **Daily** — specify the time each day you want the task performed.
    - **Weekly** — specify the day or days of the week and the time you want the task performed.
    - **Monthly** — specify the day of the month and the time you want the task performed.
10. Specify a start and end date and time for the task, if desired.

11. Enter an email address or list of email addresses (separated by semicolons) to which generated PDF reports are sent in the **To** field, if desired.
12. Select a list of email addresses to which PDF reports are sent in the **Email List** field, if desired.

    Select the **Edit** button to create a new email list or edit an existing email list.
13. Enter the subject line and body text for the email, if desired.
14. Select **Save**.

    The task appears in the Scheduled Tasks table.

    Additionally, use the toolbar buttons to edit, copy, or delete the task. The **Refresh** button updates the Scheduled Tasks table to display any recent changes. Selecting the **Disable** button causes a task not to run without deleting it from the Scheduled Tasks table.

    Select the **Run** button to run the scheduled task immediately, if desired.

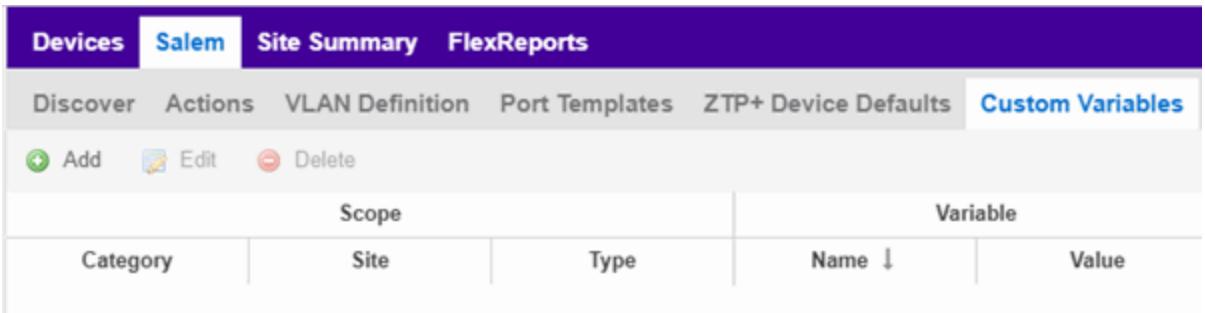
    Select the **SMTP** button to open the SMTP Email Server window to edit your outgoing email options.

Create a Variable

Use the Custom Variables tab on the Sites tab to configure variables. Variables you create serve as a placeholder for a specific value. Use variables you create in a configuration template, script or workflow, in a CLI command, or in a third-party application via the Northbound Interface.

To create a variable:

1. Access the **Network** > **Devices** tab.
2. Use the left-panel drop-down list and select **Sites**.
3. Select the site in which you are adding the variable.
4. Select the tab displaying the site name in the right-panel.
5. Select the **Custom Variables** tab.



6. Select **Add** to add a new row to the table.
7. Select a **Category**, **Site**, and **Type** in the Scope section of the table.
8. Enter a **Name**, select a **Type**, and enter a **Value** in the Variable section of the table.
9. Select **Update** to save the new variable to the table.
10. Select **Save** to save the new variable to the site.

Creating Scripts

This chapter describes the scripting functionality built into ExtremeCloud IQ Site Engine and describes how to use ExtremeCloud IQ Site Engine to create scripts.

ExtremeCloud IQ Site Engine Scripts Overview

ExtremeCloud IQ Site Engine scripts are files containing CLI commands, control structures, and data manipulation functions. ExtremeCloud IQ Site Engine scripts can be executed on one or more devices or ports: simultaneously on multiple devices or ports, or on one device or port at a time.

ExtremeCloud IQ Site Engine allows you to create ExtremeCloud IQ Site Engine tasks, which run a script on specified devices or ports at specified times, either on a one-time or recurring basis. Tasks execute the script according to a schedule you configure.

In general, ExtremeCloud IQ Site Engine scripts support syntax and constructs from the following sources:

- **Python scripting language** — Create scripts using the Python syntax. The script can access ExtremeCloud IQ Site Engine data through API and NBI calls, and can use variables from the **Custom Variables** tab. Python scripts can be saved as tasks, and then run from the **Tasks** menu or run as scheduled tasks.

  To execute a Python script on a device using an ExtremeXOS/Switch Engine operating system, use `Type= JSON-RPC-Python`. For other device operating systems, use `Type=Python`.
- **TCL scripting language version 8.1** — Create scripts using TCL syntax. The script can send CLI commands to devices in ExtremeCloud IQ Site Engine and the resulting responses can be use by the script in ExtremeCloud IQ Site Engine. TCL scripts can be saved as tasks, and then run from the **Tasks** menu or run as scheduled tasks.

  To execute TCL scripts on a device using an ExtremeXOS/Switch Engine operating system, abbreviated commands (such as `sh vlan` instead of `show vlan`) can be used in the script if the commands use the prefix `CLI`.

  Example: `CLI sh vlan`

  To copy the whole script to an ExtremeXOS/Switch Engine device, use `Type=JSON-RPC-CLI`,

the script will be executed in the `enable cli scripting` session. For other device operating systems, use `Type=TCL`.

For general information about the TCL scripting language, see www.tcl.tk. For more information about using CLI scripting, see the *ExtremeXOS/Switch Engine User Guide*.

- **ExtremeXOS/Switch Engine CLI commands** — ExtremeXOS/Switch Engine CLI commands can be combined into a script to execute in sequence using `Type=CLI`. The CLI script is saved and executed in the **Scripts** tab. However, if the sequence of command needs to be accessed or scheduled as a task, then `Type=TCL` should be used as the script type instead. An ExtremeCloud IQ Site Engine script is sent to the device or port and the response can be used by the script.

  CLI commands can also be executed for selected devices using the CLI Commands feature on the **Tasks** menu for devices. The commands are executed sequentially and can be saved to a script but not saved to a task.

  Abbreviated ExtremeXOS/Switch Engine commands do not work unless you prefix the shortened command with CLI. For example, to abbreviate `show vlan`, type `CLI sh vlan`.

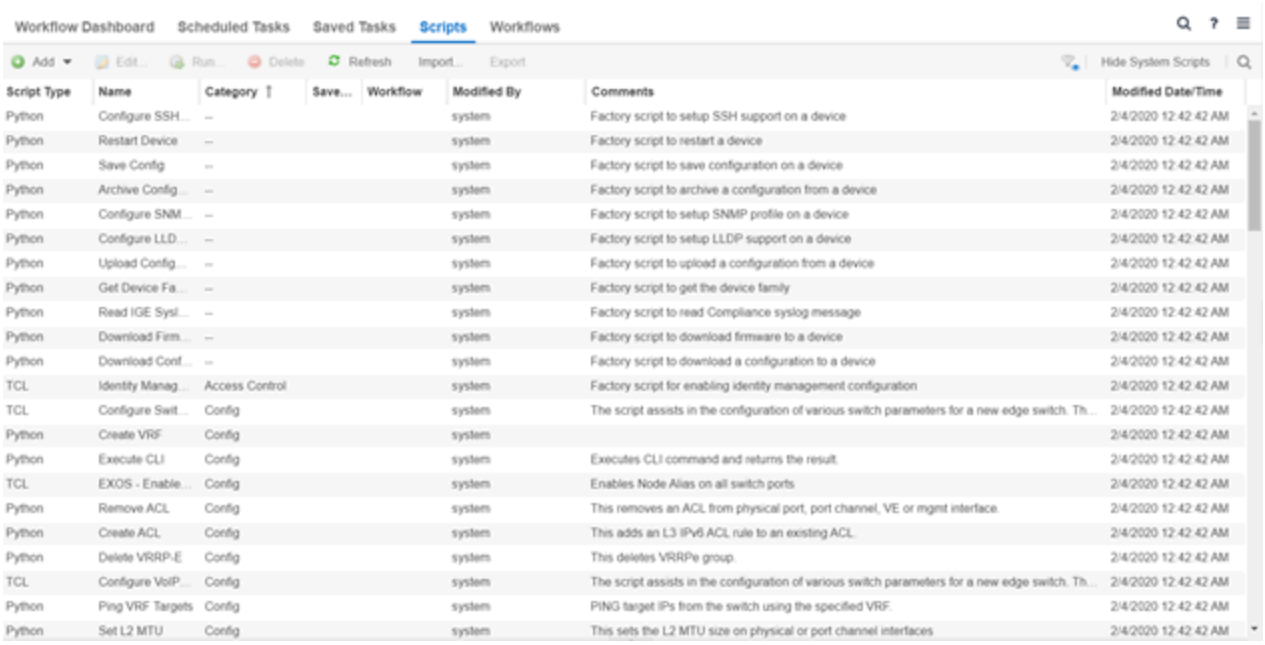
Bundled ExtremeCloud IQ Site Engine Scripts

ExtremeCloud IQ Site Engine includes a number of sample scripts you can use as templates for your own ExtremeCloud IQ Site Engine scripts. These scripts perform such tasks as enable/disable ports, apply ACLs, restart engines, and configure VLANs.

The sample scripts included with ExtremeCloud IQ Site Engine are available to users with an Administrator role. The XML source files for the scripts are located at `<install directory>\appdata\scripting\bundled_scripts`.

The ExtremeCloud IQ Site Engine Script Interface

To display the scripts configured in ExtremeCloud IQ Site Engine, select the **Tasks** tab, then select the **Scripts** tab.

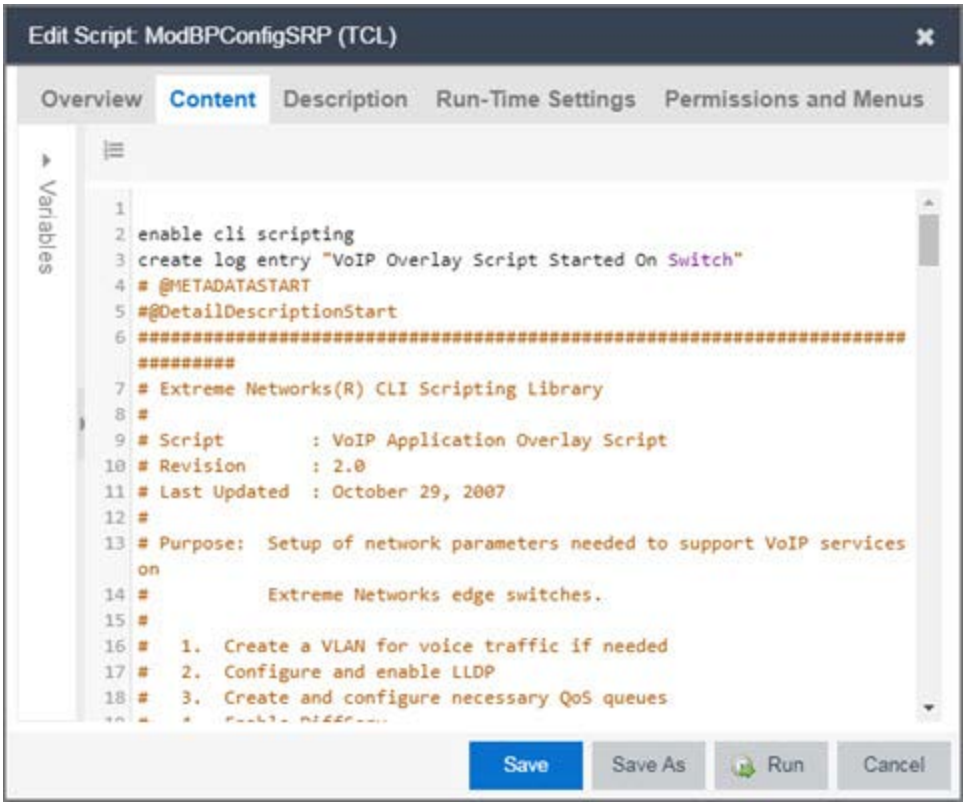


Script Type	Name	Category	Save...	Workflow	Modified By	Comments	Modified Date/Time
Python	Configure SSH...	--			system	Factory script to setup SSH support on a device	2/4/2020 12:42:42 AM
Python	Restart Device	--			system	Factory script to restart a device	2/4/2020 12:42:42 AM
Python	Save Config	--			system	Factory script to save configuration on a device	2/4/2020 12:42:42 AM
Python	Archive Config...	--			system	Factory script to archive a configuration from a device	2/4/2020 12:42:42 AM
Python	Configure SNM...	--			system	Factory script to setup SNMP profile on a device	2/4/2020 12:42:42 AM
Python	Configure LLD...	--			system	Factory script to setup LLDP support on a device	2/4/2020 12:42:42 AM
Python	Upload Config...	--			system	Factory script to upload a configuration from a device	2/4/2020 12:42:42 AM
Python	Get Device Fa...	--			system	Factory script to get the device family	2/4/2020 12:42:42 AM
Python	Read IGE Sysl...	--			system	Factory script to read Compliance syslog message	2/4/2020 12:42:42 AM
Python	Download Firm...	--			system	Factory script to download firmware to a device	2/4/2020 12:42:42 AM
Python	Download Conf...	--			system	Factory script to download a configuration to a device	2/4/2020 12:42:42 AM
TCL	Identity Manag...	Access Control			system	Factory script for enabling identity management configuration	2/4/2020 12:42:42 AM
TCL	Configure Swit...	Config			system	The script assists in the configuration of various switch parameters for a new edge switch. Th...	2/4/2020 12:42:42 AM
Python	Create VRF	Config			system		2/4/2020 12:42:42 AM
Python	Execute CLI	Config			system	Executes CLI command and returns the result.	2/4/2020 12:42:42 AM
TCL	EXOS - Enable...	Config			system	Enables Node Alias on all switch ports	2/4/2020 12:42:42 AM
Python	Remove ACL	Config			system	This removes an ACL from physical port, port channel, VE or mgmt interface.	2/4/2020 12:42:42 AM
Python	Create ACL	Config			system	This adds an L3 IPv6 ACL rule to an existing ACL.	2/4/2020 12:42:42 AM
Python	Delete VRRP-E	Config			system	This deletes VRRPe group.	2/4/2020 12:42:42 AM
TCL	Configure VoIP...	Config			system	The script assists in the configuration of various switch parameters for a new edge switch. Th...	2/4/2020 12:42:42 AM
Python	Ping VRF Targets	Config			system	PING target IPs from the switch using the specified VRF.	2/4/2020 12:42:42 AM
Python	Set L2 MTU	Config			system	This sets the L2 MTU size on physical or port channel interfaces	2/4/2020 12:42:42 AM

The Scripts tab contains the following information:

- **Script Type** — The language in which the script is written.
- **Name** — The name of the script. The script **Name** is defined when adding the script and can not be edited.
- **Category** — The script category, if configured.
- **Saved Tasks** — Indicates whether the script is configured as a saved task and is available on the **Saved Tasks** tab.
- **Workflow** — Indicates if the script is included in a workflow.
- **Modified By** — The name of the last user to modify the script. System scripts that are packaged with ExtremeCloud IQ Site Engine are indicated as **system**.
- **Comments** — Comments or a description of the script.
- **Modified Date/Time** — The date and time the script was last modified.

To view a script, double-click it. Note: Systems scripts cannot be edited. However, system scripts can be duplicated (using Save As) and the duplicated script can be edited. The duplicated script shows the last user to edit the script in the Modified By field.



The ExtremeCloud IQ Site Engine **Edit Script** window allows you to add content to a script, set values for parameters, specify run time settings, and specify the ExtremeCloud IQ Site Engine users with permission to run the script.

Depending on the type of script you are editing, the following tabs may appear in the ExtremeCloud IQ Site Engine **Script Editor** window:

- **Overview** — Displays fields to enter script parameters. The contents of this tab are derived from the metadata specified in the script.
- **Content** — Displays the script in a text editor window, where you can modify it directly.
- **Description** — Contains descriptive information about the script. The script description is specified in the metadata section of the script.
- **Runtime Settings** — Specifies script settings applied when the script is run.
- **Permissions and Menus** — Specifies ExtremeCloud IQ Site Engine user roles with the ability to run the script, and whether or not, and where, the option to run the script appears in the ExtremeCloud IQ Site Engine interface, such as on a menu or in a shortcut menu.
- **Network OS** — Allows you to select the Network Operating Systems that support the script. The script is available on a device's Tasks submenu when the device's Network OS matches one of the Network Operating Systems defined for the script.

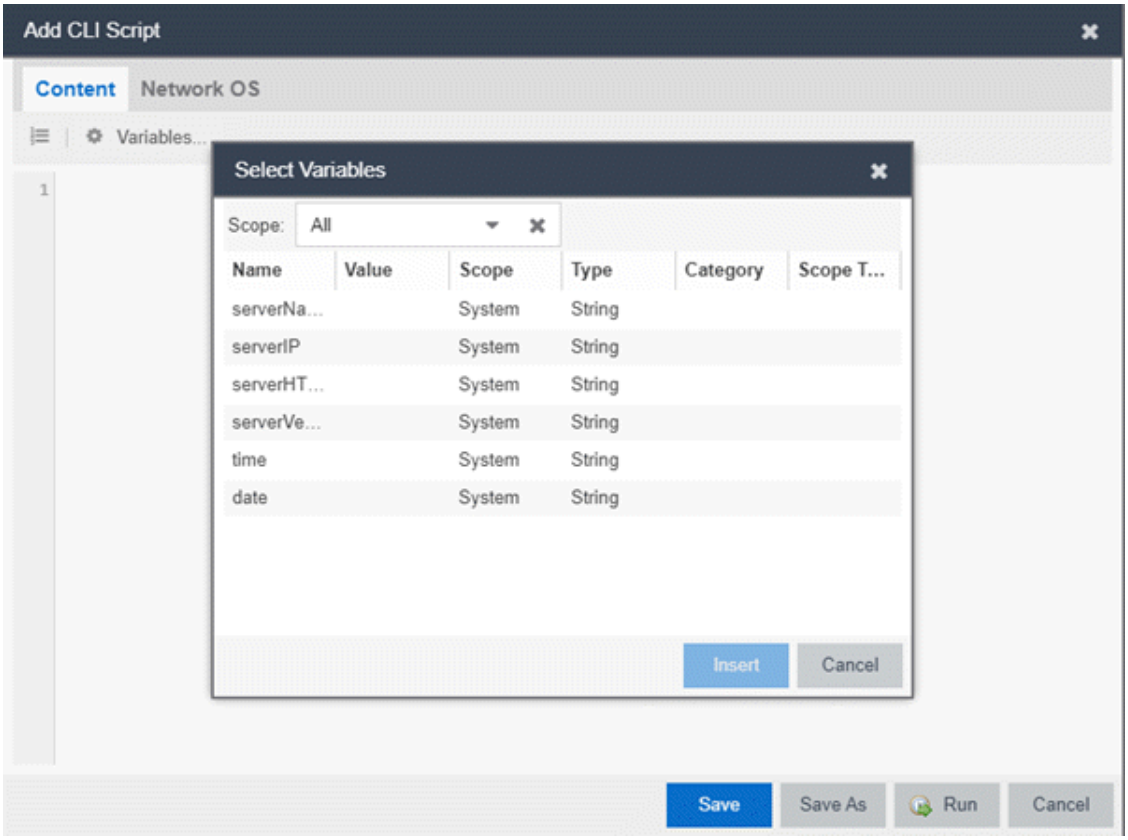
Managing ExtremeCloud IQ Site Engine Scripts

With scripting, you can:

- Create an ExtremeCloud IQ Site Engine Script
- Specify Runtime Settings for a Script
- Specify Permissions and Run Locations for Scripts
- Run a Script
- View Script Results
- Edit a Script
- Delete a Script
- Import Scripts into ExtremeCloud IQ Site Engine
- Export a Script
- Save Script as a Task

Create an ExtremeCloud IQ Site Engine Script

1. Select **Scripts** on the **Tasks** tab.
2. Select the **Add** button.
3. Select the type of script you are creating:
    - **TCL** — A Tool Command Language script. Use TCL instead of CLI if you need to use the script in a task. Proceed to step 5.
    - **Python** — A Python script. Proceed to step 5.
    - **JSON-RPC-Python** — Machine to Machine Interface (used to send a Python script to an ExtremeXOS/Switch Engine device). Proceed to step 5.
    - **JSON-RPC-CLI** — Machine to Machine Interface (used to send CLI commands to an ExtremeXOS/Switch Engine device). Proceed to step 5.
    - **CLI** — A CLI command script. Use CLI instead of TCL if you do not need to use the script in a task. Proceed to step 4.
4. When selecting **CLI** from the **Add** drop-down list, the **Add Script** window opens, where you can enter the CLI commands for the script. Select **Variables** to open the **Select Variables** window, from which you can select variables you define on the **Custom Variables** tab.



Use the **Scope** drop-down list to select either **All**, **Custom**, or **System** from the drop-down list, depending on how you configured the variable you are inserting. Select **Insert** to add the variable to your script.

Select **Save** to save the CLI script on the **Scripts** tab or select **Save As** to save the script to the ExtremeCloud IQ Site Engine server.

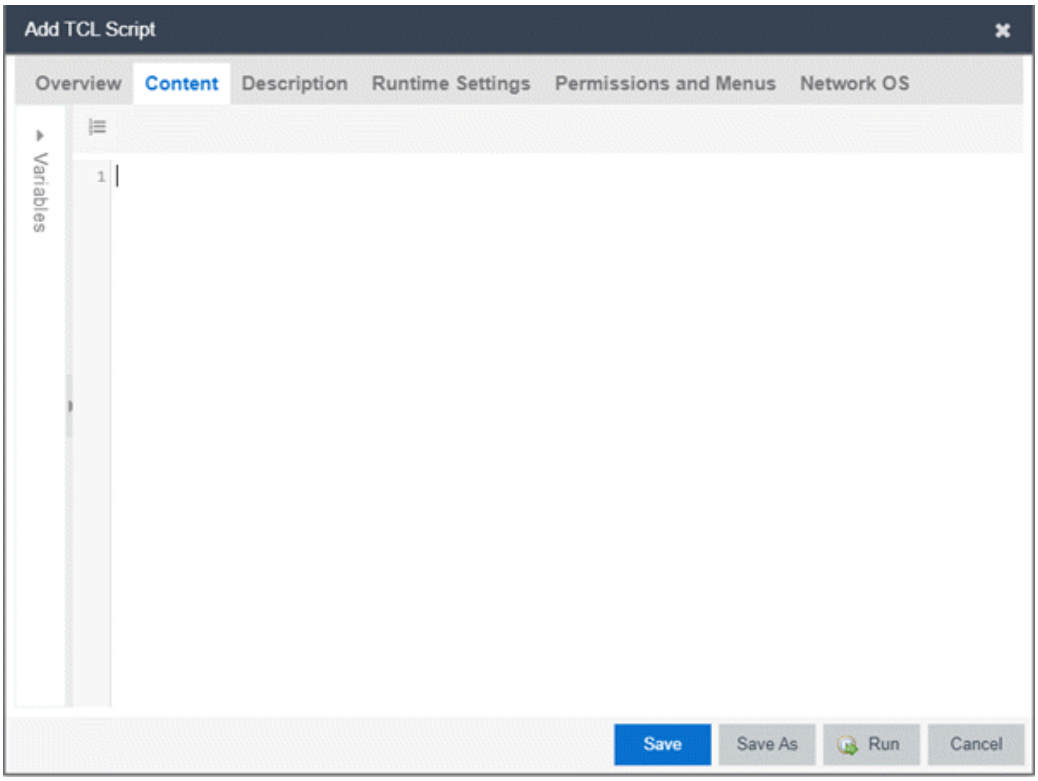
Select **Run** to run the CLI script immediately.

5. When selecting the **TCL**, **Python**, J**SON-RPC-Python**, and **JSON-RPC-CLI** script types, the **Add Script** window also opens, but contains the following tabs:
    - **Overview** — Use to enter script parameters. The contents of this tab are derived from the metadata specified in the script.
    - **Content** — Use to modify the script directly in a text editor window.
    - **Description** — Add descriptive information about the script. The script description is specified in the metadata section of the script.
    - **Runtime Settings** — Specify script settings applied when the script is run.
    - **Permissions and Menus** — Specify ExtremeCloud IQ Site Engine user roles with the ability to run the script, and whether or not, and where, the option to run the script

appears in the ExtremeCloud IQ Site Engine interface, such as on a menu or in a shortcut menu.

- Select the **Network OS** tab to select the select the Network Operating Systems that support the script.

NOTE: Select **Unknown** when creating scripts or workflows that include devices before their Network OS has been determined (e.g. onboarding new devices).



6. Type the metadata tags `#@DetailDescriptionStart` and `#@DetailDescriptionEnd` between the tags `#@MetaDataStart` and `#@MetaDataEnd`, and then type a detailed description between these detailed description tags. This description appears on the **Description** tab.
7. Place variable definition statements in the metadata section (between `#@MetaDataStart` and `#@MetaDataEnd` tags).

   Select a variable by expanding the Variables menu on the left of the **Content** tab. A list of system variables appears under Variables. To add a variable to the script, double-click the variable.
8. Enter script commands after the metadata section of the script.

   The following are examples of types of script commands supported in ExtremeCloud IQ Site

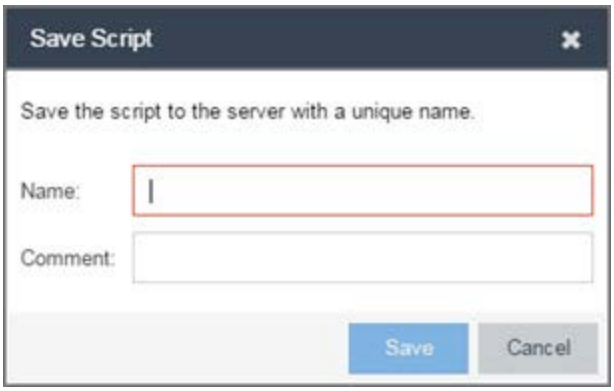
Engine:

- ExtremeXOS/Switch Engine 12.1 and later CLI scripting commands
- TCL commands
- Constructs

9. Select the **Runtime Settings** tab to specify runtime settings.
10. Select the **Permissions And Menus** tab to specify which ExtremeCloud IQ Site Engine user roles have permission to run the script, and whether or not, and where, the script appears in the menu or in a shortcut menu.
11. Select the **Network OS** tab to select the select the Network Operating Systems that support the script.

NOTE: Select **Unknown** when creating scripts or workflows that include devices before their Network OS has been determined (e.g. onboarding new devices).

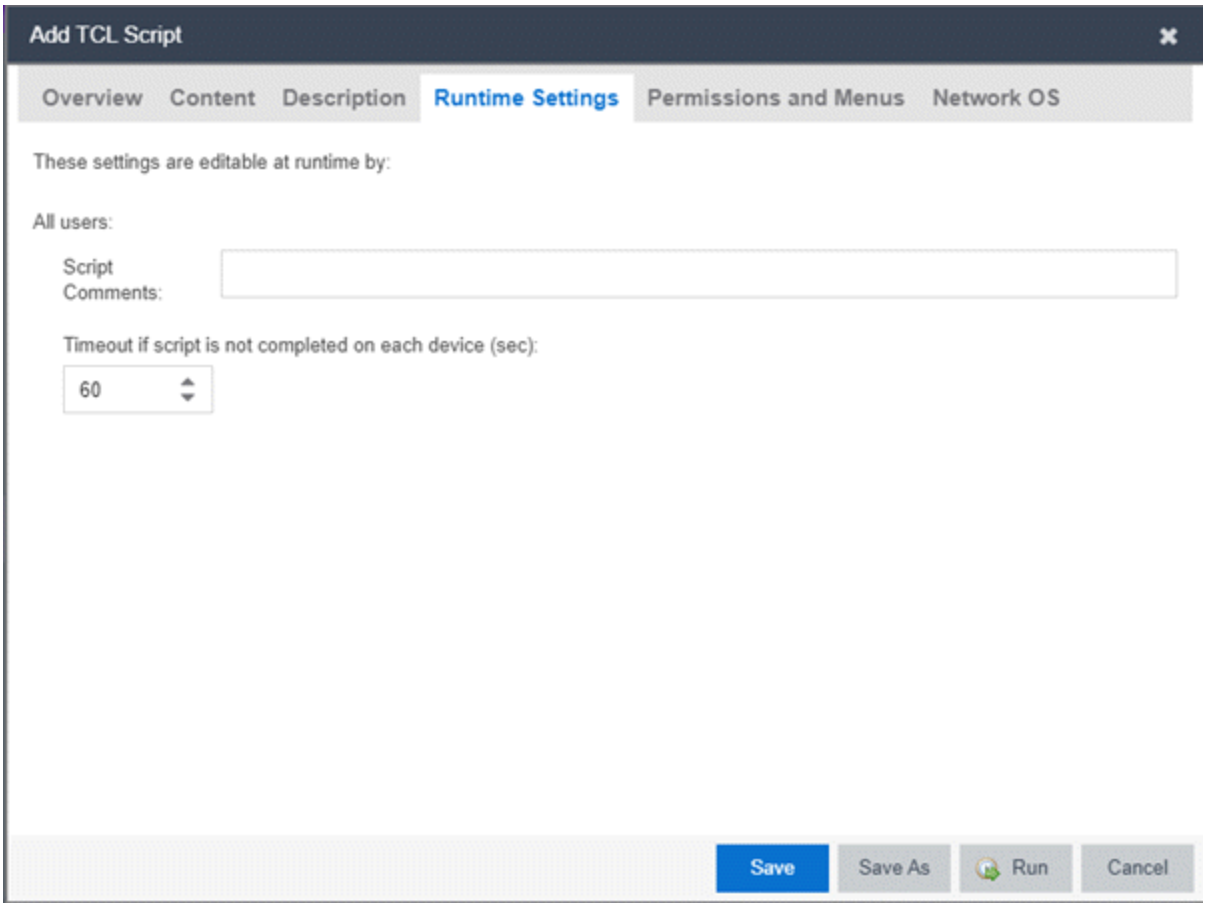
12. Select **Save**. The **Save Script** window appears.



13. Type a name for the script file in the **Name** field and a comment about the script in the **Comment** field, if necessary.
14. Select **Save**.
15. Select **Run** to run the script now or **Cancel** to run the script at a later time.

Specify Runtime Settings for a Script

To specify the runtime settings for a script, select the **Runtime Settings** tab.



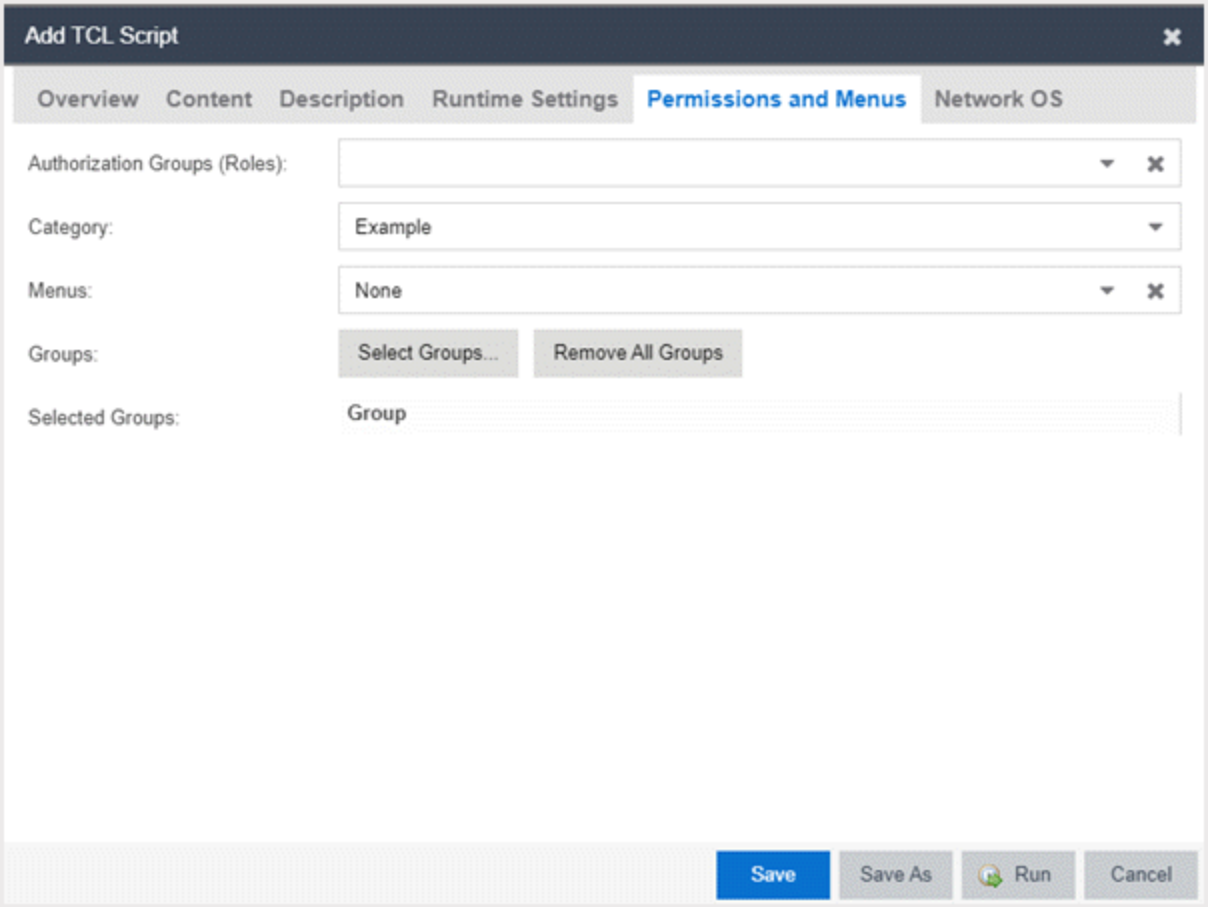
Use this tab to specify the following settings:

- **Script Comments** — Use this field to enter comments or a description of the script.
- **Timeout if script is not completed on each device (in seconds)** — Select the maximum length of time the script runs on each device or port (in seconds) before the process ends. This timeout value applies to each device or port independently.

Specify Permissions and Run Locations for Scripts

Specify which ExtremeCloud IQ Site Engine user roles have permission to run the script, and whether or not, and where, the script appears in the menu or in a shortcut menu.

Select the **Permissions and Menus** tab to set permissions and menu locations for the script.



Authorization Group (Roles)
: Select the Authorization Group credentials required to execute the script from the drop-down list.

Category
: Select the **Category** group from the drop-down list, which defines the Tasks submenu in which the script is grouped throughout ExtremeCloud IQ Site Engine. The default category is Example.

Menus
: Select the Tasks submenus in ExtremeCloud IQ Site Engine in which you want the script to display from the drop-down list. Select **Multi-Device** for User Device Group scripts.

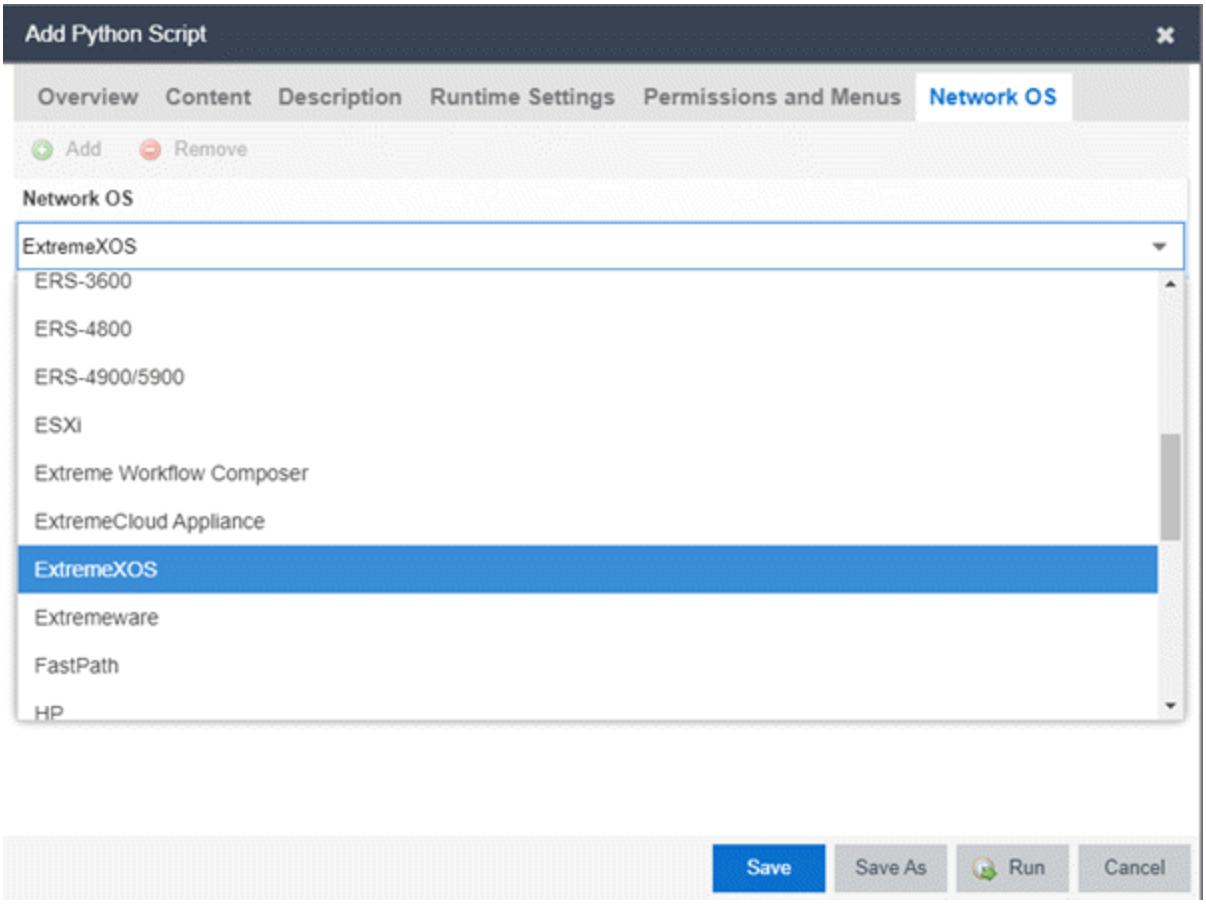
Groups
: Select the **Select Groups** to select the device groups on which the script displays.

Selected Groups
: Displays the Groups in which the script is included.

Specify Network Operating System

Select the **Network OS** tab to select the Network Operating Systems that support the script.

NOTE: Select **Unknown** when creating scripts or workflows that include devices before their Network OS has been determined (e.g. onboarding new devices).



Run a Script

From the **Network** tab

NOTE: The **Runtime Settings** tab is unavailable for scripts run via the **Network** tab. To save a script as a saved task or configure a timeout when running the script, run the script via the **Tasks** tab.

1. Right-click the device in the Devices table or in the Device Groups left-hand panel on the **Devices** tab.
2. Select a script in the Tasks menu. The Run Script window opens.
3. On the **Device Selection** tab, select the device or devices against which you want to run the script. Use the arrows to add/remove devices and to control the order of the selected devices.
4. Select **Next**.

5. On the **Overview** tab of the **Device Settings** tab, set the configuration properties for the script. The options available on this tab vary depending on the script selected. If desired, select the **Description** tab to view the description defined for the script.
6. Select **Next**.

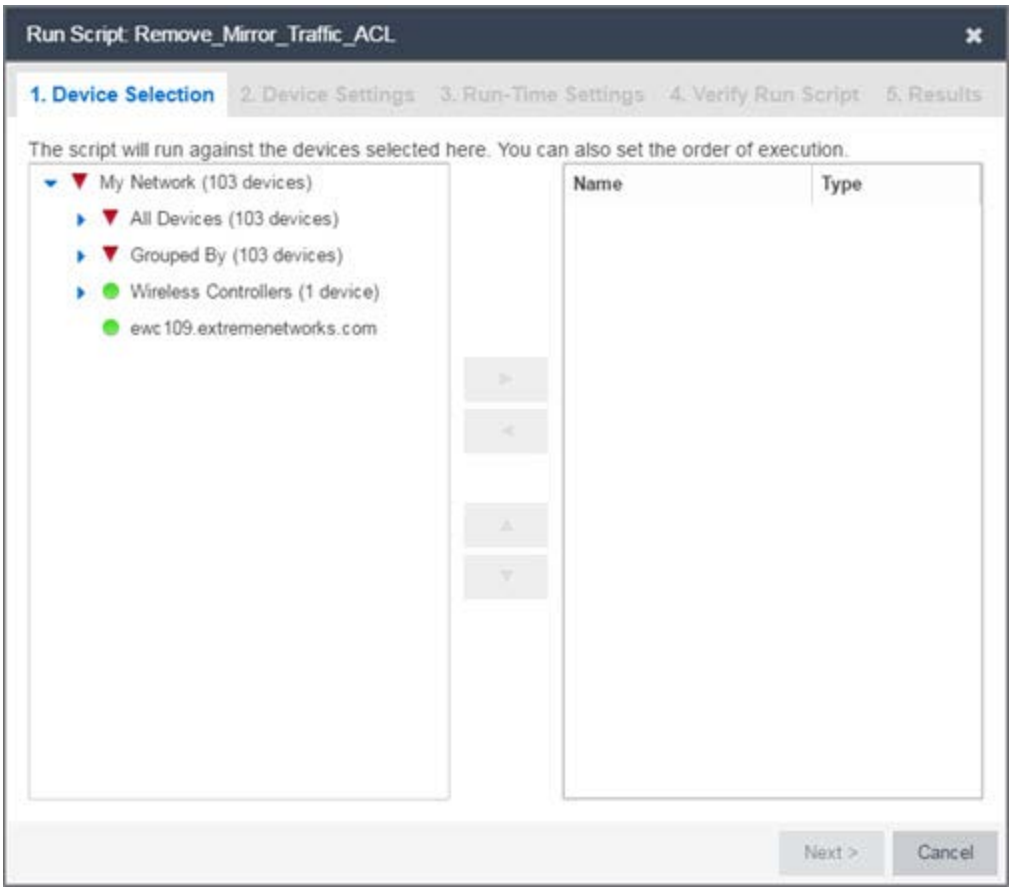
   The **Verify Run Script** tab opens.
7. Verify your script selections, and then select **Run**.
8. On the **Results** tab, you see the results of the script including any errors.
9. Select **Close**.

From the Tasks tab

1. Select **Scripts**.
2. On the **Scripts** tab, find the script in the list. If needed, filter the list by typing search terms in the **Search** field.
3. Select the script by selecting its row and then select **Run**. The Run Script window opens.

NOTE: Only select one script. The **Run** button is unavailable if two or more scripts are selected.

4. On the **Device Selection** tab, shown below, select the device or devices against which you want to run the script. Use the arrows to add/remove devices and to control the order of the selected devices.



5. Select **Next**.
6. On the **Overview** tab of the **Device Settings** tab, set the configuration properties for the script. The options available on this tab vary depending on the script selected. If desired, select the **Description** tab to view the description defined for the script.
7. Select **Next**.
8. On the **Runtime Settings** tab, configure the runtime settings for the script.
    - **Timeout if script is not completed on each device (in seconds)** — Use to set a maximum amount of time for the script to run on each device (in seconds). This timeout value applies to each device independently.
    - **Run now, don't save as task** — Select to run the script immediately without saving the script as a task.
    - **Save as a task and run now** — Select to run the script immediately and save it as a task on the **Saved Tasks** tab. Type a name for the task in the **Task Name** field.
    - **Save as a task. I'll run later** — Select to save the script as a task you can run later. Type a name for the task in the **Task Name** field. The task appears on the **Saved Tasks** tab.
9. Select **Next**. On the **Verify Run Script** tab, verify your script selections, and then select **Run**.

10. On the **Results** tab, you see the results of the script including any errors.
11. Select **Close**.

View Script Results

When a script is run, results are stored in the `<install directory>/appdata/scripting/tmp` folder. The folder in which script results are stored cannot be configured.

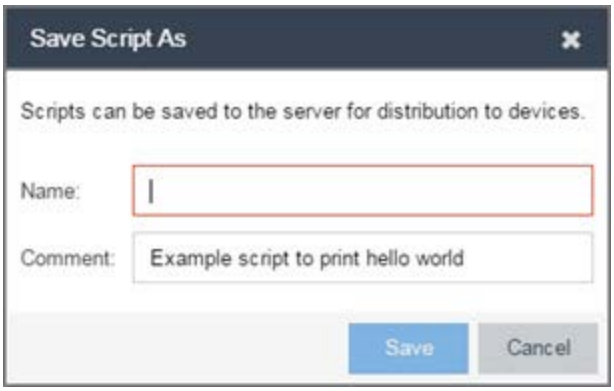
An event is stored in the console.log file in the `<install directory>/appdata/logs` folder each time a script is executed. The event in the log contains the location of the audit file. These audit logs reside in the tmp directory and remain for two weeks (per user), or until the next server restart, whichever comes first. The number of audit files written to the folder is limited to 1,000 files. When the number of files exceeds 1,000, the oldest 100 are deleted.

Edit a Script

To edit a script:

1. In the **Tasks** tab, select **Scripts**.
2. In the scripts table, select the script you want to edit. **Note:** Systems scripts that are packaged with ExtremeCloud IQ Site Engine cannot be edited. However, system scripts can be duplicated (using **Save As**) and the duplicated script can be edited. The systems scripts are labeled **system** in the **Modified By** field, but duplicated scripts show the last user name as Modified By.
3. Select the **Edit** button. The script opens in the **Edit Script** window, where you can edit the script.
4. Save the script:
    a. Select the **Save** button to save your changes to the script.
    b. Select **Save As** to save a copy of this script with a new name.

    The **Save Script As** window appears.



i. Type a name for the script file in the **Name** field and a comment about the script in the **Comment** field, if necessary.

ii. Select **Save**.

The script is saved.

Delete a Script

To delete a script:

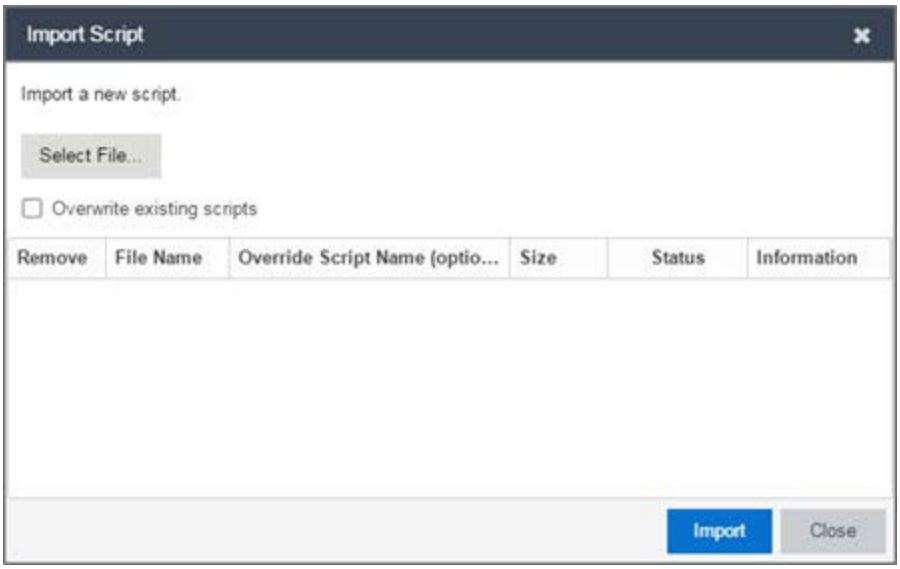
1. In the **Tasks** tab, select **Scripts**.
2. In the scripts table, select one or more scripts you want to delete.
3. Select the **Delete** button.
4. Select **Yes** to confirm the script deletion.

Import Scripts into ExtremeCloud IQ Site Engine

Import XML-formatted scripts into ExtremeCloud IQ Site Engine.

To import a script:

1. In the **Tasks** tab, select **Scripts**.
2. Select the **Import** button.



3. Select **Select File** to navigate to the location of the script. The script appears in the grid.
4. Enter a new Script Name in the **Override Script Name (optional)** field if you want to change the name of the script.
5. Select the **Overwrite existing scripts** checkbox, if necessary.
    - When **Overwrite existing scripts** is not selected and the script name displayed in the **File Name** field (if you did not use the **Override Script Name (optional)** field) or the **Override Script Name (optional)** field matches the name of a script in ExtremeCloud IQ Site Engine, the new script is not imported.
    - When **Overwrite existing scripts** is selected and the script name displayed in the **File Name** field (if you did not use the **Override Script Name (optional)** field) or the **Override Script Name (optional)** field matches the name of a script in ExtremeCloud IQ Site Engine, the new script is imported and overwrites the existing script.
6. Select **Import**.
7. Verify the script is imported and select **Close**.

NOTE: Exported EPICenter 6.0 telnet macros cannot be imported as XML scripts.

Export a Script

To export a script:

1. From the **Tasks** tab, select a script.
2. Select the **Export** button.

The script is exported in XML format to your browser download directory.

Save Script as a Task

When you run a script, you can save it as a task that appears in the **Saved Tasks** tab. This saves your device selections and runtime settings, and then allows you to manually run the script task at a later time or schedule it to run in the future either one time, or on a regular basis.

To save a script as a saved task:

1. Select a script.
2. Run the script and designate it as a task by selecting either **Save as a task and run now** or **Save as task. I'll run later** on the **Runtime Settings** tab.
3. Enter a new name for the task in the **Task Name** field.

ExtremeCloud IQ Site Engine saves the script to the **Saved Tasks** tab.

ExtremeCloud IQ Site Engine Script Reference

This section contains reference information for ExtremeCloud IQ Site Engine scripts. It contains the following topics:

- Metadata Tags
- ExtremeCloud IQ Site Engine-Specific Python Scripting Constructs
- ExtremeCloud IQ Site Engine-Specific TCL Scripting Constructs
- TCL Support in ExtremeCloud IQ Site Engine Scripts
- Entering Special Characters
- Line Continuation Character
- Case Sensitivity in ExtremeCloud IQ Site Engine Scripts
- Reserved Words in ExtremeCloud IQ Site Engine Scripts
- ExtremeXOS/Switch Engine CLI Scripting Commands Supported in ExtremeCloud IQ Site Engine Scripts
- ExtremeCloud IQ Site Engine-Specific System Variables

An ExtremeCloud IQ Site Engine script may contain a metadata section, which can serve as a usability aid in the script interface. The metadata section, if present, is the first section of an ExtremeCloud IQ Site Engine script, followed by the script logic section, which contains the CLI commands and control structures in the script. The metadata section is delimited between `#@MetaDataStart` and `#@MetaDataEnd` tags. A metadata section is optional in an ExtremeCloud IQ Site Engine script.

Use metadata tags to specify the description of the script, as well as parameters that the script user can input. The information specified by the metadata tags appears in the **Overview** tab for the script.

ExtremeCloud IQ Site Engine-Specific Python Scripting Constructs

Specifying the Wait Time Between Commands

After the script executes a command, the time.sleep command causes the script to wait a specified number of seconds before executing the next statement.

Syntax

```
time.sleep(10)
```

Example

```
# sleep for 10 seconds after executing a command

time.sleep(10)
```

Metadata Tags

#@MetaDataStart and #@MetaDataEnd

Indicates the beginning and end of the metadata section of the script. In order for description information and variable input fields to appear in the **Overview** tab for a script, the corresponding metadata tags must appear in the metadata section.

Example

```
#@MetaDataStart

#@SectionStart (description = "Protocol Configuration Section") Set var
protocolSelection eaps

#@SectionEnd

#@SectionStart (description = "vlan tag section") Set var vlanTag 100

#@MetaDataEnd
```

#@ScriptDescription

Specifies a one-line description of the script. The description specified with this tag cannot contain a newline character.

Example

```
#@ScriptDescription "This is a VLAN configuration script."
```

#@DetailDescriptionStart and #@DetailDescriptionEnd

Specifies the beginning and end of the detailed description of the script. The detailed description can be multiple lines or multiple paragraphs. The detailed description is shown in the **Script View** tab in the script editor window.

Example

```
#@DetailDescriptionStart

#This script performs configuration upload from ExtremeCloud IQ Site Engine to
the switch.

#The script only supports tftp.

#This script does not support third party devices.

#@DetailDescriptionEnd
```

#@SectionStart and #@SectionEnd

Specifies the beginning and end of a section within the metadata part of a script. You do not need to end with a `#@MetaDataEnd` tag, then the `#@SectionEnd` tag if this is the last section of the metadata. When a section starts with the `#@SectionStart` tag, the previous section automatically ends.

Example

```
#@SectionStart (description = "Protocol Configuration Section") Set var
protocolSelection eaps

#@SectionEnd
```

#@VariableFieldLabel

Defines user-input variables for the script. For each variable defined with the `#@VariableFieldLabel` tag, you specify the variable's description, scope, type, and whether it is required.

Description
Label that appears as the prompt for this parameter in the **Overview** tab.

Scope
Whether the parameter is global (uses the same value for all devices) or device-specific. Valid values: global, device. Default value is global.

Type
Parameter data type. This determines how the parameter input field is shown in the **Overview** tab. Valid value: String (the parameter input field on the **Overview** tab displays as a drop-down list if **validValues** are listed or as a text field if **validValues** are not listed).

readonly
Whether the parameter is read-only and cannot be modified by the user. Valid values: Yes, No. Default value is No.

validValues
Lists all possible values for a parameter. Separate each value using a comma and put into a square bracket.

Required

Indicates whether specifying the parameter is required to run the script. Valid values: Yes, No.

Example

```
#@VariableFieldLabel (description = "Partition:", scope = global,
#required = yes, validValue = [Primary,Secondary], readOnly=false)
set var partition ""
```

ExtremeCloud IQ Site Engine-Specific TCL Scripting Constructs

This section describes the TCL scripting constructs specific to ExtremeCloud IQ Site Engine:

- Specifying the Wait Time Between Commands
- Printing System Variables
- Configuring a Carriage Return Prompt Response
- Synchronizing the Device with ExtremeCloud IQ Site Engine
- Saving the Configuration on the Device Automatically
- Printing a String to the Output File

Specifying the Wait Time Between Commands

After the script executes a command, the sleep command causes the script to wait a specified number of seconds before executing the next statement.

Syntax

```
sleep 5
```

Example

```
# sleep for 5 seconds after executing a command
sleep 5
```

Printing System Variables

The printSystemVariables command prints the current values of the system variables. Specifically, values for the following variables are printed:

- deviceIP
- deviceName
- serverName
- deviceSoftwareVer
- serverIP
- serverPort

- date
- time
- abort_on_error
- CLI.OUT

Syntax

```
printSystemVariables
```

Example

```
# Display values for system variables

printSystemVariables
```

Configuring a Carriage Return Prompt Response

A special string within the script, `<cr>`, indicates a carriage return in response to a prompt for a command.

Syntax

```
<cr>
```

Example

```
# cancel download

download image 10.22.22.22 t.txt <cr>
```

Synchronizing the Device with ExtremeCloud IQ Site Engine

The PerformSync command manually initiates a synchronization for specified ExtremeCloud IQ Site Engine feature areas and scope.

Syntax

```
PerformSync [-device <ALL | deviceIp>] [-scope <EAPSDomain | VPLS> ]
```

If -device is not specified, the current device (indicated by the `$deviceIP` system variable) is assumed.

The PerformSync command is executed in an asynchronous manner so when the command is executed, ExtremeCloud IQ Site Engine moves on to the next command in the script without waiting for the PerformSync command to complete.

Examples

```
PerformSync -scope VPLS
```

Printing a String to the Output File

Example

```
# Write Device IP address to file

ECHO "device ip is $deviceIP"
```

NOTE: The TCL `puts` and `ECHO` commands have the same function. However, the `ECHO` command is not case-sensitive (unless referenced inside another command), while the `puts` command is case-sensitive.

TCL Support in ExtremeCloud IQ Site Engine Scripts

The following TCL commands are supported in ExtremeCloud IQ Site Engine scripts:

after	concat	flush	info	lrange	puts	set	unset
append	continue	for	interp	lreplace	read	split	update
array	global	foreach	join	lsearch	regexp	string	uplevel
binary	eof	format	lappend	lsort	regsub	subst	upvar
break	error	gets	lindex	namespace	rename	switch	variable
catch	eval	history	linsert	open	return	tell	vwait
clock	expr	if	list	package	scan	time	while
close	fblocked	incr	llength	proc	seek	trace	

See www.tcl.tk/man/tcl8.2.3/TclCmd/contents.htm for syntax descriptions and usage information for these TCL commands.

Entering Special Characters

In an ExtremeCloud IQ Site Engine script, use the backslash character (\ ) as the escape character if you need to enter special characters, for example:

- quotation marks (" ")
- colon (:)
- dollar sign ($).

Example

```
set var value 100

set var dollar \$value

show var dollar >>> $value
```

NOTE: Do not place the backslash character at the end of a line in an ExtremeCloud IQ Site Engine script.

Line Continuation Character

The line continuation character is not supported in ExtremeCloud IQ Site Engine scripts. Place each command statement on a single line.

Case Sensitivity in ExtremeCloud IQ Site Engine Scripts

The commands and constructs in an ExtremeCloud IQ Site Engine script are not case-sensitive. However, if a command is referenced inside another command, the inner command is case-sensitive. In this instance, the inner command case matches how it appears in the ExtremeCloud IQ Site Engine documentation.

Example (Usage of the ExtremeCloud IQ Site Engine command ECHO)

```
echo hi (valid)

echo [echo hi] (error)

echo [ECHO hi] (valid)
```

Reserved Words in ExtremeCloud IQ Site Engine Scripts

The following words are reserved by ExtremeCloud IQ Site Engine and cannot be used as variable names in a script:

- Names of system variables (see ExtremeCloud IQ Site Engine-Specific System Variables)
- Names of ExtremeCloud IQ Site Engine command extensions (see ExtremeCloud IQ Site Engine-Specific Scripting Constructs)
- Names of ExtremeXOS/Switch Engine CLI commands
- Names of TCL functions

Also, do not use a period (.) within a variable name, use an underscore (_).

ExtremeXOS/Switch Engine CLI Scripting Commands Supported in ExtremeCloud IQ Site Engine Scripts

ExtremeCloud IQ Site Engine scripts support the CLI commands in this section.

- $VAREXISTS
- $TCL
- $UPPERCASE
- show var
- delete var
- configure cli mode scripting abort-on-error

$VAREXISTS

- Checks if a given variable is initialized.
- Switch Compatibility — Devices running ExtremeXOS/Switch Engine 12.1 and higher support this command.
- Example — `if ($VAREXISTS(foo)) then show var foo endif`

$TCL

- Evaluates a given TCL command. The following constructs support the $TCL command:
  - `set var if`
  - while
- See TCL Support in ExtremeCloud IQ Site Engine Scripts for a list of supported TCL commands.
- Switch Compatibility — Devices running ExtremeXOS/Switch Engine 11.6 and higher support this command.
- Example — `set var foo $TCL(expr 3+4) if ($TCL(expr 2+2) == 4) then`

$UPPERCASE

- Converts a given string to upper case.
- The following constructs support the $UPPERCASE command:
  - set var
  - if
  - while
- Switch Compatibility — Devices running ExtremeXOS/Switch Engine 11.6 and higher support this command.

NOTE: The $UPPERCASE command is deprecated in ExtremeXOS/Switch Engine 12.1 CLI scripting. Use the $TCL (string toupper <string>) command instead. Example: set var foo $TCL ("foo") .

---

show var

- Prints the current value of a specified variable.
- Switch Compatibility — Devices running ExtremeXOS/Switch Engine 11.6 and higher support this command.
- Example — `show var foo`

delete var

- Deletes a given variable. Only local variables can be deleted; system variables cannot be deleted.

- Switch Compatibility — Devices running ExtremeXOS/Switch Engine 11.6 and higher support this command.
- Example — `set var foo bar delete var foo if ($VAREXISTS(foo)) then ECHO "this should NOT be printed" else ECHO "Variable deleted." endif`

configure cli mode scripting abort-on-error

- Configures the script to halt when an error occurs. If there is a syntax error in the script constructs (set var / if ..then / do..while), execution stops even if the abort_on_error flag is not configured.
- Switch Compatibility — Devices running ExtremeXOS/Switch Engine 11.6 and higher support this command.
- Example — `enable cli scripting \$UPPERCASE uppercase # should not print show var abort_on_error`

ExtremeCloud IQ Site Engine-Specific System Variables

The following system variables can be set in ExtremeCloud IQ Site Engine scripts:

$abort_on_error
Whether the script terminates if a CLI error occurs: 1 aborts on error; 0 continues on error.

$CLI.OUT
The output of the last CLI command.

$CLI.SESSION_TYPE
The type of session for the connection to the device, either Telnet or SSH.

NOTE: Variables with TCL special characters must be enclosed in braces. For example, when using the system variables `$CLI.SESSION_TYPE` and `$CLI.OUT` in a script, they must be entered as `${CLI.SESSION_TYPE}` and `${CLI.OUT}`, respectively.

$date
The current date on the ExtremeCloud IQ Site Engine server.

$deviceIP
The IP address of the selected device.

$deviceLogin
The name of the login user for the selected device.

$deviceName
The DNS name of the selected device.

$deviceSoftwareVer
The version of ExtremeXOS/Switch Engine running on the selected device.

$deviceType
The product type of the selected device.

$netsightUser
The name of the ExtremeCloud IQ Site Engine user running the script.

$isExos
Indicates whether the device is an ExtremeXOS/Switch Engine device. Possible values are True or False.

$port
Selected port numbers, represented as a string. If the script is not associated with a port, this system variable is not supported.

$serverIP
The IP address of the ExtremeCloud IQ Site Engine server.

$serverName
The host name of the ExtremeCloud IQ Site Engine server.

$serverPort
The port number used by the ExtremeCloud IQ Site Engine web server; for example, 8080.

$STATUS
The execution status of the previously executed ExtremeXOS/Switch Engine command: 0 if the command executed successfully; non-zero otherwise.

$time
The current time on the ExtremeCloud IQ Site Engine server.

$vendor
Vendor name of the device; for example, Extreme.

FlexViews

FlexViews provide a convenient way for Operations people to view device data. These views are accessible from ExtremeCloud IQ Site Engine Devices and do not require the installation of any software (including ExtremeCloud IQ Site Engine) other than the browser itself.

You can also add your own custom FlexViews in ExtremeCloud IQ Site Engine.

Configure the options on the **Administration** > **Options** > FlexView tab to determine the behavior of FlexViews in ExtremeCloud IQ Site Engine.

To launch a FlexView, you must be a member of an authorization group that is assigned the OneView > FlexView > OneView FlexView Read Access capability. To launch and edit a FlexView, you must be a member of an authorization group that is assigned the OneView > FlexView > OneView FlexView Read/Write Access capability.

This Help topic provides information on the following topics:

- Browser Requirements
- Launching FlexViews
- Using FlexViews
    - Editing Writable Values
    - Exporting Table Data

Browser Requirements

The following web browsers are supported:

- Microsoft Edge
- Mozilla Firefox 34 and later
- Google Chrome 33.0 and later

Enable JavaScript in your browser for the views to function. To avoid impaired functionality, enable cookies for your browser. This includes (but is not limited to) the ability to persist table configurations such as filters, sorting, and column selections.

Launching FlexViews

Use the following steps to launch and open a FlexView from the **Network** tab.

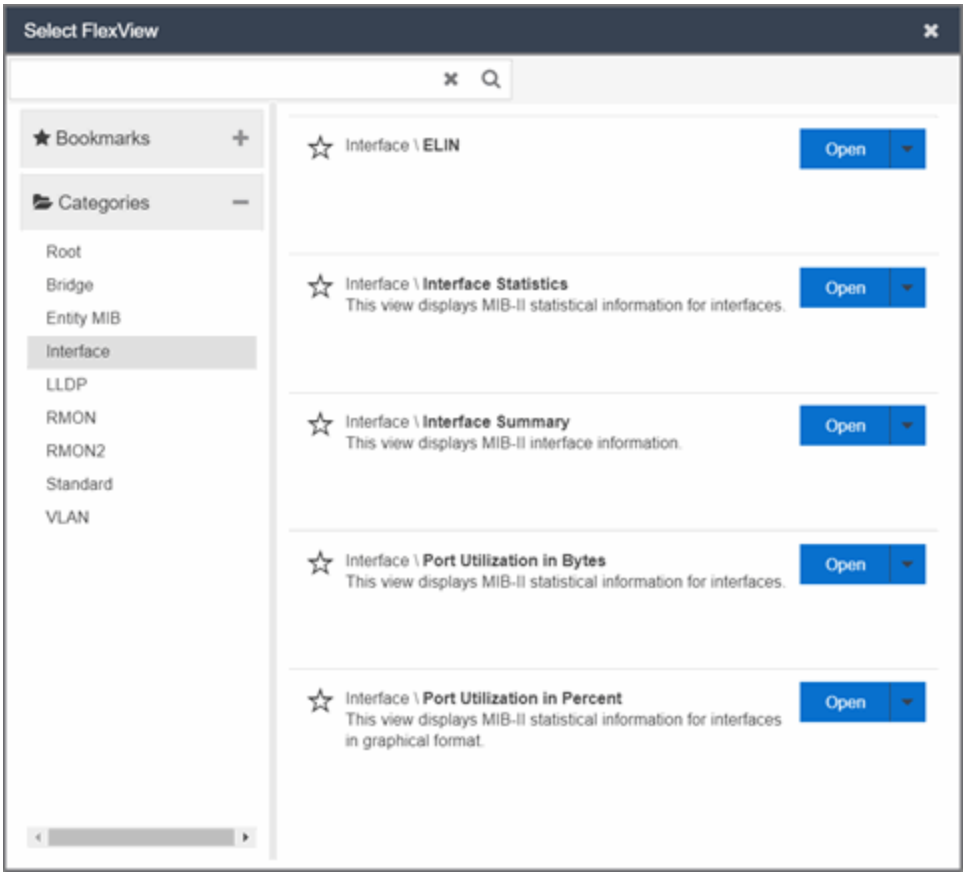
1. Launch ExtremeCloud IQ Site Engine and select **Network** > **Devices**.
2. Select one or more devices in the **Devices** tab left panel or from within the Devices list.

NOTE: When you select multiple devices, a FlexView may take additional time to populate with data, depending on the number of rows displayed in the particular view. Because of this, we recommend that, for interface-based FlexViews, you select five devices or fewer.

3. Select the **Menu** icon (☰) and select **View** > **FlexView** from the menu.

   The **Select FlexView** window opens.

NOTE: The location and availability of FlexViews in the **Select FlexView** window changes depending on the configuration of the options on the **Administration** > **Options** > **FlexView** tab.



4. Select a FlexView in one of the following ways:

   - Expand the Bookmarks folder in the left panel to view the FlexViews that are bookmarked.

- Expand the Categories folder in the left panel. Select a **Category** from the left panel, depending on the type of FlexView you want to open.

NOTE: ExtremeCloud IQ Site Engine saves user-created Custom FlexViews in the **My FlexViews** Category.

5. Locate a FlexView in the right panel.

NOTE: Select the **Star** icon next to a FlexView in the right panel and select the device types for which it is applicable to save it in the Bookmarks folder in the left panel of the **Select FlexViews** window. This allows you to quickly find frequently used FlexViews.

6. Select the **Open** drop-down list and select whether you want to open the FlexView in a new tab or window.

The FlexView opens in a new tab or window, depending on what you select.

Using FlexViews

FlexViews let you manipulate the table data in several ways to customize the view for your own needs:

- Select the column headings to sort column data in ascending or descending order.
- Hide or display different columns by selecting a column heading drop-down arrow and selecting the column options from the menu.
- Rearrange columns by dragging a column heading to the desired position.
- Use the **Search** field to filter on and search for specific FlexView data.
- Set a Refresh Interval, which automatically refreshes the data at the specified interval.
- Edit the values in FlexView table columns containing a writable MIB object.
- In the toolbar at the top of the window, select **Retrieve from Devices** ( ) to clear all data and retrieve data again from selected Devices.
- In the status bar at the bottom of the window, select **Refresh from Cache** ( ) to show any new data collected since the last FlexView Update.

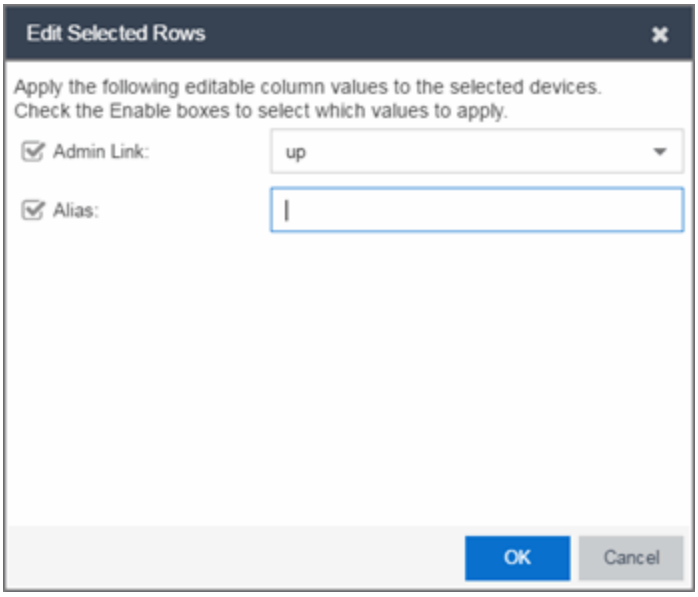
NOTE: Row creation and data exports are not currently supported in FlexViews.

Editing Writable Values

You can change the value in FlexView table columns that contain a writable MIB object.

1. Select one or more rows in the FlexView that contain columns with writable MIB objects, right-click and select **Edit Selected Rows**.

   The **Edit Selected Rows** window opens.



2. Select the writable objects you are changing and enter the appropriate values as needed.

   NOTE: Adding an alias to a port configures both ExtremeCloud IQ Site Engine and the CLI of the switch to display the character string.

3. Select **OK** to enter your changes into the selected rows. The new values are written directly to the device.

Bookmarking FlexViews

You can save frequently used FlexViews for each device type in the Bookmarks folder of the **Select FlexView** window. Bookmarks are shared among all ExtremeCloud IQ Site Engine users and provide your organization with the ability to select a FlexView without searching.

To add a FlexView to the Bookmarks folder, select the **Category** from the left panel and select the **Star** icon next to the appropriate FlexView in the right panel. Select the device types for which the FlexView is applicable and select **Save**. The FlexView is accessible from the Bookmarks folder when you access the Select FlexView window for a device that matches the device type configured for the FlexView.

Exporting Table Data

There are two methods of exporting the data in the table:

Export to CSV
Select to export all of the data in the table to a .CSV file. The exported data displays with any sorting, filtering, and searching applied.

Export Selected to CSV
Select to export the data in the currently selected row in the table to a .CSV file.

Add Custom FlexViews and MIBs

Use the instructions in this topic to add custom FlexViews and MIBs in ExtremeCloud IQ Site Engine.

To add a new FlexView to ExtremeCloud IQ Site Engine:

1. Create the following directory on the ExtremeCloud IQ Site Engine server: `/usr/local/Extreme_Networks/NetSight/appdata/VendorProfiles/Stage/MyVendorProfile/FlexViews/My FlexViews` if it does not already exist.
2. Add your custom FlexView files (.TPL) to the `/usr/local/Extreme_Networks/NetSight/appdata/VendorProfiles/Stage/MyVendorProfile/FlexViews/My FlexViews` directory on the ExtremeCloud IQ Site Engine server.
3. Add the MIB files that correspond to your custom FlexView files to the `/usr/local/Extreme_Networks/NetSight/appdata/VendorProfiles/Stage/MyVendorProfile/MIBs` directory on the ExtremeCloud IQ Site Engine server.
4. Log into the system shell (via the local console or SSH) on the ExtremeCloud IQ Site Engine server as root.
5. Restart the ExtremeCloud IQ Site Engine server:
    a. Enter `service nsserver stop`.
    b. Enter `service nsserver start`.

VLAN Concepts

The following concepts will assist you in configuring VLAN and port template definitions in ExtremeCloud IQ Site Engine.

Information on:

- Egress Rules (Transmitting Frames)
    - Dynamic Egress
        - GVRP
        - GARP Timers
- Enforcing
- Frame Types
- IGMP
    - Interface Robustness (Robustness Variable)
    - Last Member Query Interval

    - Query Interval
    - Query Response
- Ingress Filtering
- Priority Classification
    - Weighted Priority
- Verifying
- VLAN Identification
    - Port VLAN ID (PVID)
    - VLAN ID (VID)
- VLAN Model
- VLAN Learning

Egress Rules (Transmitting Frames)

A device determines which frames can be transmitted out a port based on the Egress List of the VLAN associated with it. Each VLAN has an Egress List that specifies the ports out of which frames can be forwarded, and specifies whether the frames will be transmitted as tagged or untagged frames. You can add or remove ports to or from a VLAN's Egress List, thereby controlling which VLAN's frames can be forwarded out which ports.

When a frame is transmitted out a port, the device first checks the Egress List. If the port is listed on the Egress List of the VLAN associated with it, the frame is then transmitted according to the priority assigned to the frame. The frame is transmitted as tagged or untagged according to the specification in the Egress List. If the port is not on the Egress List, or if the port is not operational, the frame is discarded.

Dynamic Egress

In ExtremeCloud IQ Site Engine, you can control whether or not Dynamic Egress is enabled for a VLAN in the VLAN Definitions table. When Dynamic Egress is enabled for a VLAN, any time a device tags a packet with that VLAN ID, the ingress port is automatically added to the VLAN's egress list, enabling the reply packet to be forwarded back to the source. This means that you do not need to add the ingress port to the VLAN's egress list manually. (See Example 1, below.)

Dynamic Egress affects only the egress lists for the source and destination ingress ports. You can enable GVRP (GARP VLAN Registration Protocol), which automatically adds the interswitch ingress ports to the egress lists of VLANs. (See Example 2, below.)

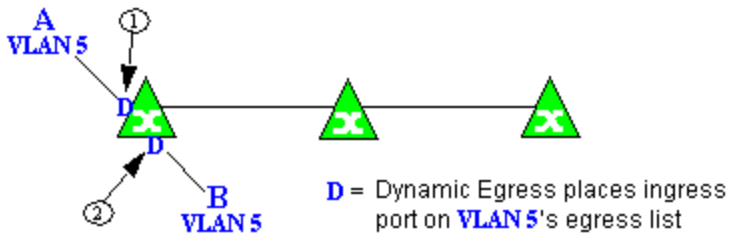
When you disable Dynamic Egress for a VLAN, the VLAN effectively becomes a discard VLAN. Since the destination port is not added to the egress list of the VLAN, the device discards the traffic. If you want a VLAN to act as a discard VLAN, disable Dynamic Egress for that VLAN. (See Example 3, below.)

If an endstation is talking to a "silent" endstation which does send responses, like a printer, you will need to add the silent endstation's ingress port to the VLAN's egress list manually with a tool like ExtremeCloud IQ Site Engine Device Manager, or local management. Dynamic Egress and GVRP take care of adding the other ingress ports to the VLAN's egress list. (See Example 4, below.)

CAUTION: If no packets are tagged with the applicable VLAN on a port within five minutes, Dynamic Egress list entries will time out. The result is that an endstation will appear "silent" if the VLAN has not been used within that time period. For example, if there is a "telnet" rule and two users (A & B) are on ports whose role includes a service containing the "telnet" rule, if User B has not utilized the "telnet" rule within the five minute time frame, User A will not be able to telnet to User B. For this reason, the best application of Dynamic Egress is for containing undirected traffic on "chatty" clients which utilize, for example, IPX, NetBIOS, AppleTalk, and/or broadcast/multicast protocols such as routing protocols.

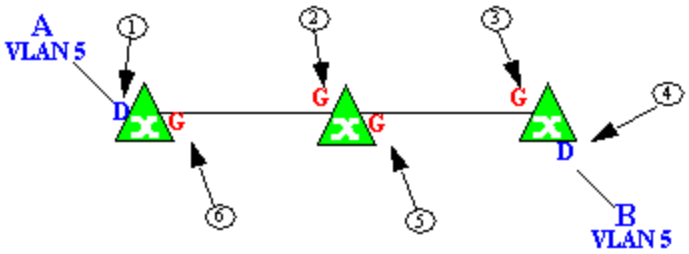
Example 1: Dynamic Egress Enabled

In this example, Dynamic Egress is enabled for VLAN 5. When source endstation A is tagged with VLAN 5, Dynamic Egress places A's ingress port (1) on VLAN 5's egress list. When destination endstation B's traffic is tagged with VLAN 5, Dynamic Egress places B's ingress port (2) on VLAN 5's egress list. The device can then forward traffic to both endstations.



Example 2: Dynamic Egress + GVRP

In this example, Dynamic Egress is enabled for VLAN 5, and the destination endstation, B, is on a different device from the source endstation, A. When A is tagged with VLAN 5, Dynamic Egress places A's ingress port (1) on VLAN 5's egress list. GVRP then places interswitch ingress ports (2) and (3) on VLAN 5's egress list. When B's traffic is tagged with VLAN 5, Dynamic Egress places B's ingress port (4) on VLAN 5's egress list. GVRP then places interswitch ingress ports (5) and (6) on VLAN 5's egress list. The devices can then forward traffic to both endstations.

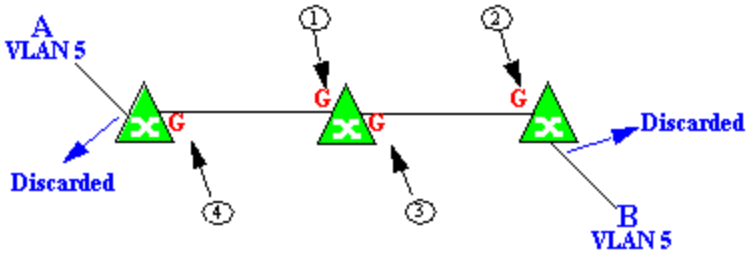


D = Dynamic Egress places endstation ingress ports on **VLAN 5**'s egress list

G = GVRP places interswitch ingress ports on **VLAN 5**'s egress list

Example 3: Dynamic Egress Disabled

In this example, Dynamic Egress is disabled. When source endstation A is tagged with VLAN 5, A's ingress port is not placed on VLAN 5's egress list. GVRP places interswitch ingress ports (1) and (2) on VLAN 5's egress list. When B's traffic is tagged with VLAN 5, B's ingress port is not placed on VLAN5's egress list. GVRP places interswitch ingress ports (3) and (4) on VLAN 5's egress list. But VLAN 5 traffic for both A and B is discarded, because VLAN 5 is not aware of the ingress ports for A and B.



G = GVRP places interswitch ingress ports on **VLAN 5**'s egress list

VLAN 5 Traffic for A and B discarded - A's and B's ingress ports not on VLAN's egress list

Example 4: Silent Endstation

In this example, Dynamic Egress is enabled for VLAN 5, but the destination endstation, B, is a "silent" endpoint, like a printer. Endstation B does not send responses, so the Administrator must place B's ingress port on VLAN 5's egress list manually (1). When A is tagged with VLAN 5, Dynamic Egress places A's ingress port (2) on VLAN 5's egress list. GVRP then places interswitch ingress ports (3) and (4), then (5) and (6) on VLAN 5's egress list. Endstation A is then able to communicate with the printer.

GVRP

GVRP (GARP VLAN Registration Protocol) dynamically adds interswitch ingress ports to the egress lists of VLANs across a domain.

NOTE: If you do not want GVRP enabled on your network, you can disable it, then manually configure the interswitch ports to do what GVRP does automatically, using MIB Tools or local management to set up your interswitch links as Q trunks. The trunk ports will be automatically added to the egress lists of all the VLANs at the time of trunk configuration.

GARP Timers

Set GARP timers on the device to control the timing of dynamic VLAN membership updates to connected devices. The timer values must be identical on all connected devices in order for GVRP to operate successfully.

- **Join Time** - Frequency of messages issued when a new port has been added to the VLAN. Possible values are 1 through 1488800 milliseconds.
- **Leave Time** - Frequency of messages issued when a single port no longer belongs to the VLAN. This value must be at least three times greater than the Join Time. Possible values are 1 through 1488800 milliseconds.
- **Leave All Time** - Frequency of messages issued when all ports no longer belong to the VLAN and the VLAN should be deleted. This value must be greater than the value for Leave Time. Possible values are 1 through 1488800 milliseconds.

Enforcing

When working with VLANs in ExtremeCloud IQ Site Engine, write the definitions in the VLAN model to selected devices or ports by selecting the **Enforce** button in the Configure Device window.

NOTE: On the X-Pedition router, enforcing will not overwrite the "System Static" VLAN (SYS_L3_ Interface Name).

Frame Types

Incoming frames are processed according to ingress rules which determine the VLAN membership and transmission priority of a frame received on a port by checking for the presence of a VLAN tag. A VLAN tag is a field within a frame that identifies the frame's VLAN membership and priority.

Frames can be tagged or untagged. A tagged frame is a frame that contains a VLAN tag. An untagged frame does not have a VLAN tag, but will be tagged when it is received on a port. A tagged frame may have already been processed by an 802.1Q switch or originated at an endpoint capable of inserting a

VLAN tag into a frame. A VLAN tag may or may not contain a VLAN ID (VID), but it will always contain priority information. End systems are allowed to transmit frames with only a priority in the VLAN tag. When switches transmit a tagged frame, the VLAN tag will always include a VID along with the priority.

Tagged and untagged frames are assigned VLAN membership and transmission priority differently:

Untagged Frame - VLAN Membership
When an untagged frame is received on a port, if a VLAN Classification rule exists for the frame's classification type, the frame will gain membership in the associated VLAN. If not, the frame will be assigned to the VLAN identified as the port's VLAN ID (PVID).

Untagged Frame - Priority Assignment
When an untagged frame is received on a port, if a Priority Classification rule exists for the frame's classification type, the frame will be assigned the associated priority. If not, the frame will be assigned the port's default priority.

Tagged Frame - VLAN Membership
If a tagged frame includes a VID (VLAN ID), it will gain membership in the VLAN indicated by the VID. If not, and a VLAN Classification rule exists for the frame's classification type, the frame will be put into the associated VLAN. If there is no VID or classification rule, the frame will be put in the VLAN associated with the port's VLAN ID (PVID).

Tagged Frame - Priority Assignment
When a tagged frame is received on a port, it is assigned the priority contained in the VLAN tag.

You can set the acceptable frame type for a port in Ports.

IGMP

IGMP (Internet Group Management Protocol) is a protocol used by IP hosts and their immediate neighbor multicast agents to support the allocation of temporary group addresses and the addition and deletion of members of a VLAN. You can enable and disable IGMP in VLAN Definitions.

IGMP Intervals

You can control the following IGMP query settings in VLAN Definitions:

- **Query Interval** - Interval (in seconds) between general IGMP queries sent by the device to solicit VLAN membership information from other devices. By setting this interval, you can control the number of IGMP messages on a subnet. Larger values cause queries to be sent less often. The Query Interval must be greater than the Query Response interval. Valid values: 1 through 300 seconds.
- **Query Response** - Maximum amount of time allowed for responses to general IGMP queries. By setting this value, you can control the burstiness of IGMP messages on a subnet. Larger values result in less bursty traffic, because host responses are spread over a larger interval. This value must be less than the Query Interval. Valid values: 1 through 300.

- **Interface Robustness (Robustness Variable)** - Indicates the susceptibility of the subnet to lost packets. If a subnet is particularly susceptible to losses, you may wish to increase this value. IGMP is robust to (Robustness Variable-1) packet losses. The Interface Robustness value is used in the calculation of IGMP message intervals. Valid values are 2 thru 32767.
- **Last Member Query Interval** - Maximum amount of time (in seconds) between group-specific query messages, including those sent in response to leave-group messages. By setting this value, you can control the "leave latency" of the network. You might lower this interval to reduce the amount of time it takes the device to detect the loss of the last member of a group. Valid values: 10 through 32767 seconds.

Ingress Filtering

Ingress Filtering is a means of filtering out undesired traffic on a port. When Ingress Filtering is enabled, a port determines if a frame can be processed based on whether the port is on the Egress List of the VLAN associated with the frame. For example, if a tagged frame with membership in the Sales VLAN is received on a Port 1, and Ingress Filtering is enabled, the switch will determine if the port is on the Sales VLAN's Egress List. If it is, the frame can be processed. If it is not, the frame is dropped. You can set ingress filtering for a VLAN in Ports.

Priority Classification

Priority Classification is used to assign frames transmission priority over other frames. Priority is a value between 0 and 7 assigned to each frame as it is received on a port, with 7 being the highest priority. Frames assigned a higher priority will be transmitted before frames with a lower priority.

Each of the priorities is mapped into a specific transmit queue by the switch or router. The insertion of the priority value (0-7) allows all 802.1Q devices in the network to make intelligent forwarding decisions based on its own level of support for prioritization.

Frames can be assigned a transmission priority ;based on the default priority of the receiving switch port, regardless of the frame's classification type. However, with the addition of classification rules, frames can be assigned a priority based on the frame's classification type. Using priority classification rules, network administrators can classify a frame based on Layer 2/3/4 information to have higher or lower priority than other frames on a per port basis, allowing for better defined Class of Service configurations.

You can set the default priority for incoming frames in Ports.

Weighted Priority

Weighted priority, available on certain devices, is a way to further refine priority classification. You can control this setting in Ports.

Some devices support four transmit queues (0-3) per port. These queues can be serviced based on a strict method, meaning that all frames in Queue 3 will be transmitted before the frames in Queue 0, or

based on a fair weighted method. The weighted method allows the network administrator to give a certain percentage or weight to each queue, preventing a lower priority queue from being starved.

Forwarding priority can be tuned to allocate a percentage of a port's transmit resources to the each traffic queue. This lets you adjust a strict priority scheme to guarantee that some percentage of frames from lower priority queues will always be sent. Weighted priority settings divide each port's transmit resources into 16 equal parts, which can be allocated to traffic queues in increments of 6.25% (1/16th). The total resource allocation for a port must always add up to 100%.

To understand the effect of weighted priorities, consider a device port with strict priority settings. In this case, all of the frames from the highest priority traffic queue are sent before frames are sent from any of the lower priority queues. Now, assuming four traffic queues, assign weighted priorities for the port giving 50% of the transmit resources to Queue 3, 25% to Queue 2, and 25% to Queue 1 and 0% to Queue 0. With these settings, at least 50% of the frames will be transmitted from Queue 3, at least 25% from Queue 2, at least 25% from Queue 1 and frames will only be transmitted from Queue 0 when Queue 1, 2, and 3 are empty.

Verifying

Verifying retrieves the VLAN settings on the selected devices and compares them with the settings in the selected VLAN Definitions or Ports.

Differences are indicated by a red not-equals symbol ≠. A green exclamation point ! is displayed when you select a ≠ line in the table to the model setting that will be written to the device when you enforce. You can review the differences and make modifications to your model as needed, including updating the definitions in your model using the definitions from the selected devices.

VLAN Identification

VLAN identifiers include VLAN ID's and Port VLAN ID's.

VLAN ID (VID)

802.1Q VLANs are defined by VLAN IDs (VIDs) and VLAN names.

VID

A unique number between 1 and 4094 that identifies a particular VLAN. VID 1 is reserved for the Default VLAN.

VLAN Name

An alphanumeric name associated with a VLAN ID, used to make VLANs easier to identify and remember (up to 64 characters).

PVID (Port VLAN ID)

You can change a port's VLAN membership to reflect the specific needs of your network by assigning new VLAN membership to the port. When you assign VLAN membership to a port, that VLAN's ID (VID) becomes the Port VLAN ID (PVID) for the port and the port is added to the VLAN's Egress List.

PVID
The PVID (Port VLAN ID) represents a port's VLAN assignment. Possible values are 0 through 4094.

NOTE: The PVID value 0 means incoming untagged traffic is not assigned to any VLAN.

Egress List
The Egress List specifies which ports can transmit the frames associated with the VLAN.

NOTE: On the X-Pedition Router, you cannot assign a PVID to a port that has an interface assigned to it.

VLAN Model

In ExtremeCloud IQ Site Engine, you can create VLAN models and enforce them across multiple network devices. A VLAN model consists of at least one VLAN Definition and one VLAN Port Template.

ExtremeCloud IQ Site Engine provides you with one VLAN model (the Primary VLAN Model) which is pre-populated with a Default VLAN (VID 1). You can further define this VLAN model, and/or you can create other VLAN models. (The Default VLAN for a model cannot be deleted.)

Once a VLAN model has been created, you can utilize it in the following ways:

- Enforce the properties of a port template on selected devices. You can also make custom edits for selected ports.
- Perform a more detailed analysis of the differences between the definitions in the VLAN model and the VLAN settings on selected devices and their ports. Using these views in the Network > Device tab, you can review the differences and make modifications to your VLAN model and/or device or port VLAN configuration as required, including updating any or all of the definitions in the model with the settings on selected devices and their ports, and writing (enforcing) a model's VLAN definitions and/or VLAN port templates to selected devices or ports.

See Create and Edit a VLAN on a Device for more information.

VLAN Learning

VLAN learning allows the creation of groups of VLANs that will share Filtered Database information (MAC address, port, and VLAN ID) according to 802.1Q Shared Learning Constraints (IEEE Std 802.1Q-

1998). This helps to speed MAC to port lookups and reduce flooding, because MAC addresses will be in the same Filtering Database.

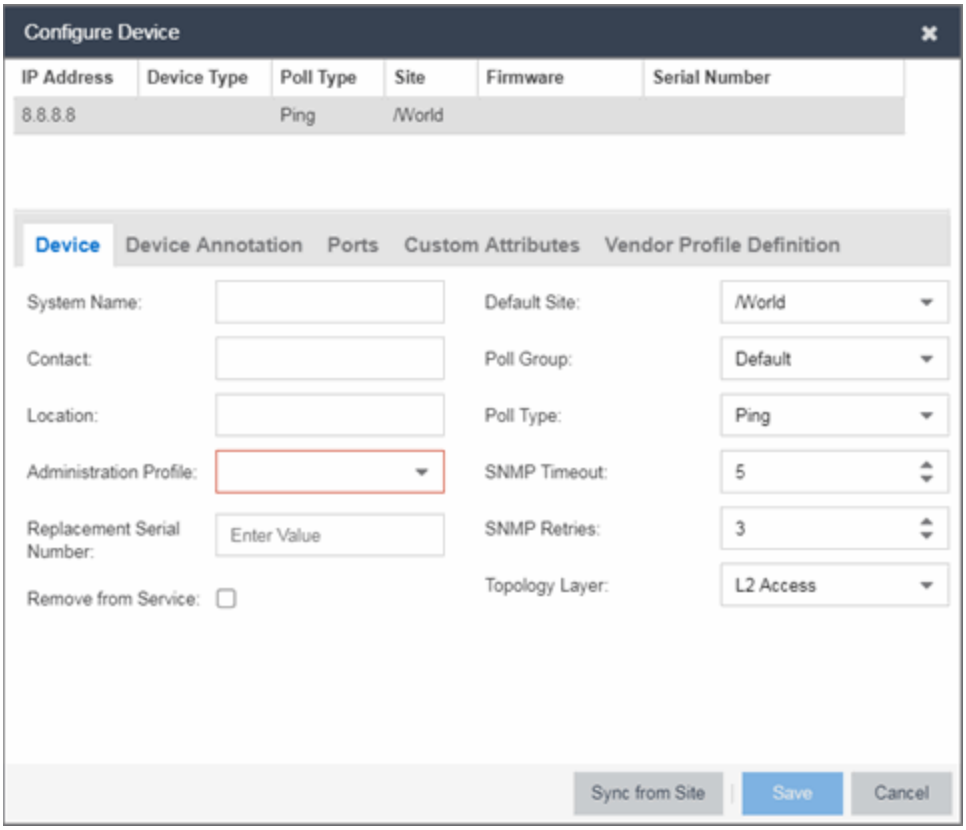
Create and Edit a VLAN on a Device

This section outlines how to create and edit a VLAN. From the Network tab, you can:

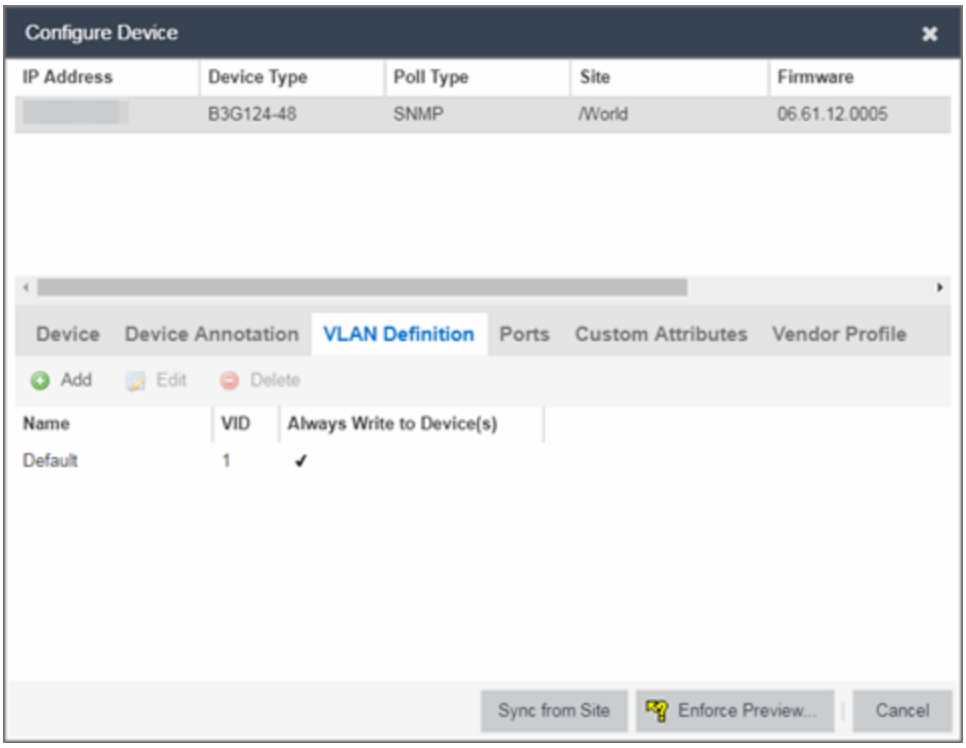
- Create a new VLAN
- Edit the ports of an existing VLAN
- Edit the name of an existing VLAN
- Remove devices from an existing VLAN

To create a new VLAN:

1. Launch ExtremeCloud IQ Site Engine.
2. Open the **Network > Devices** tab.
3. Select the device from the devices list. Right-click the device and select **Device > Configure Device**.
   The **Configure Device** window opens.

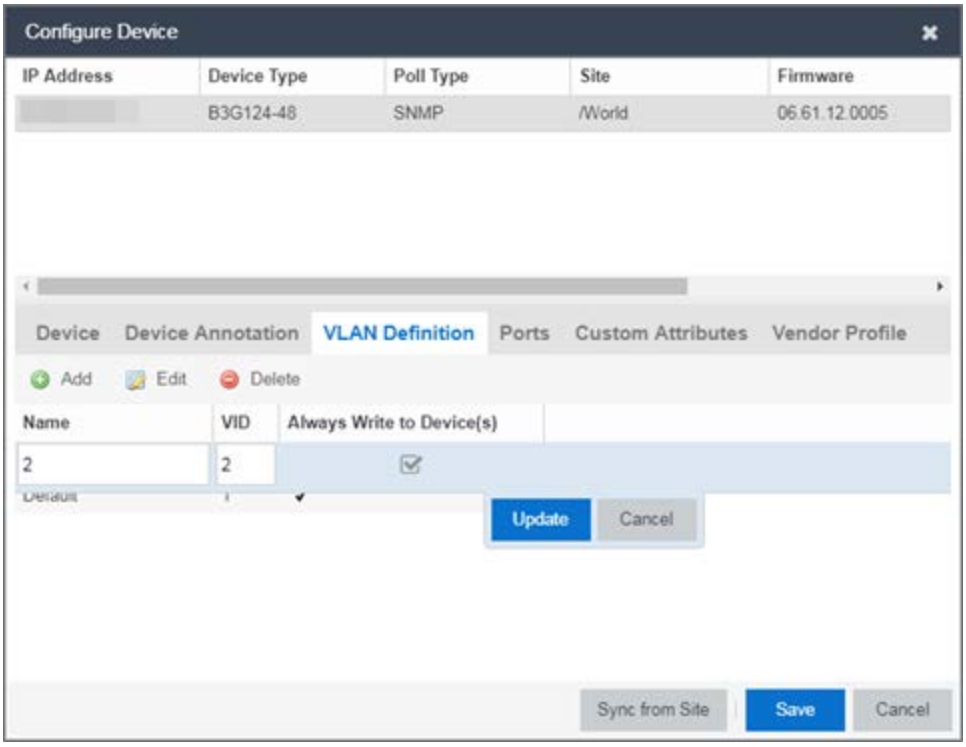

Configure Device
IP Address
Device Type
Poll Type
Site
Firmware
Serial Number
8.8.8.8
Ping
/World
Device
Device Annotation
Ports
Custom Attributes
Vendor Profile Definition
System Name:
Contact:
Location:
Administration Profile:
Replacement Serial Number:
Enter Value
Remove from Service:
Default Site:
/World
Poll Group:
Default
Poll Type:
Ping
SNMP Timeout:
5
SNMP Retries:
3
Topology Layer:
L2 Access
Sync from Site
Save
Cancel

4. Select the **VLAN Definition** tab.



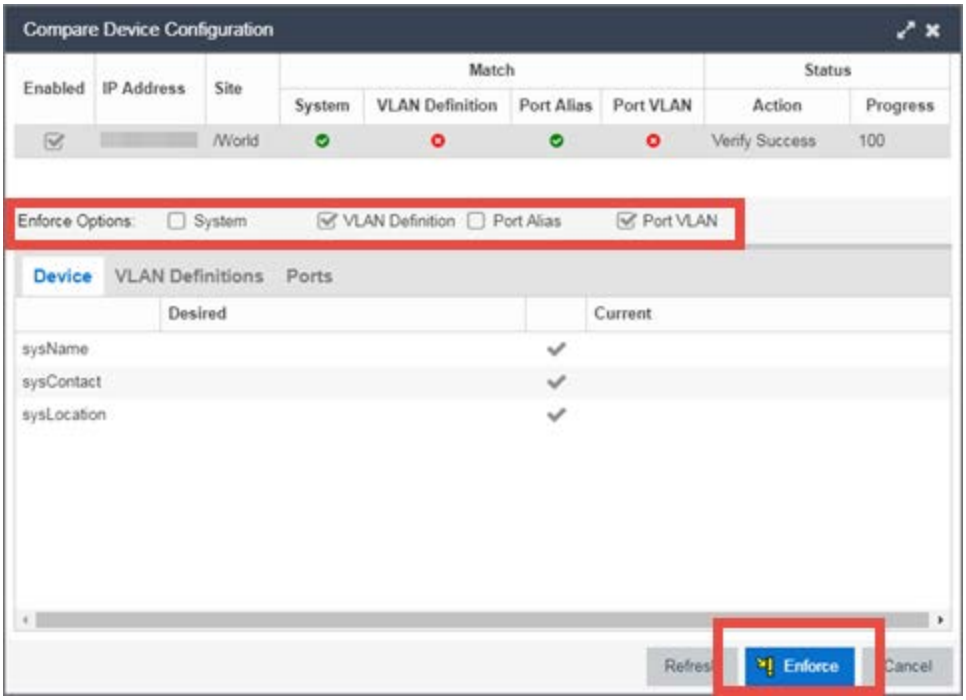
5. Select the **Add** button.

6. Enter the **Name** and the **VID** for the new VLAN.



7. Select **Update**.
   The new VLAN is added to the list.
8. Select **Enforce Preview**.

9. Under the Enforce Options, select the **VLAN Definition** checkbox and select **Enforce**.



NOTE: By default, the checkboxes in the Enforce Options section of the window are not selected. To configure ExtremeCloud IQ Site Engine to select the checkboxes by default, open the `NSJBoss.properties` file and change **false** to **true** in the following lines:

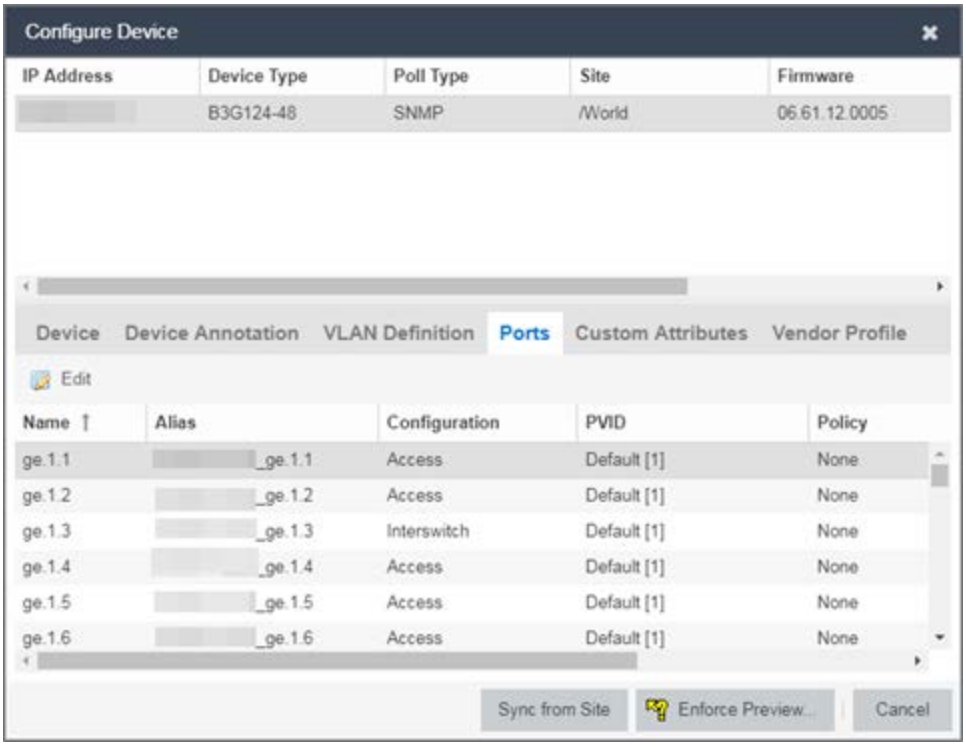
- `site.enforceOption.autoEnable.system=false`
- `site.enforceOption.autoEnable.vlanDefinition=false`
- `site.enforceOption.autoEnable.portAlias=false`
- `site.enforceOption.autoEnable.portVlan=false`

The VLAN is now created and assigned to the device.

To configure the VLAN(s) on the ports

1. Launch ExtremeCloud IQ Site Engine.
2. Open the **Network > Devices** tab.
3. Select the device from the devices list.
4. Right-click the device and select **Device > Configure Device**.
   The **Configure Device** window opens.

5. Select the **Ports** tab.



6. Select the Port on which you are configuring the VLAN.
7. Select **Edit**.
   The Port is now configurable.
8. Change the **PVID**, **Tagged**, and **Untagged** options to configure the VLAN onto the port.
9. Select **Enforce Preview**.
10. Under the Enforce Options, select the **Port VLAN** checkbox and select **Enforce**.

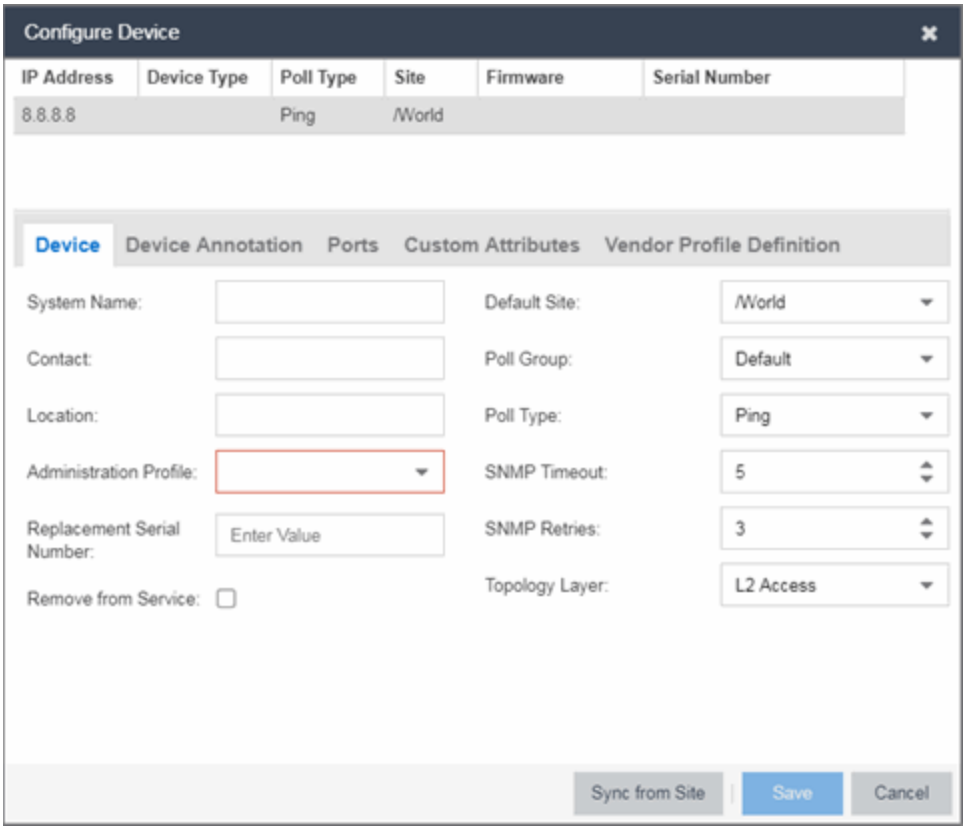
NOTE: By default, the checkboxes in the Enforce Options section of the window are not selected. To configure ExtremeCloud IQ Site Engine to select the checkboxes by default, open the `NSJBoss.properties` file and change **false** to **true** in the following lines:

- `site.enforceOption.autoEnable.system=false`
- `site.enforceOption.autoEnable.vlanDefinition=false`
- `site.enforceOption.autoEnable.portAlias=false`
- `site.enforceOption.autoEnable.portVlan=false`

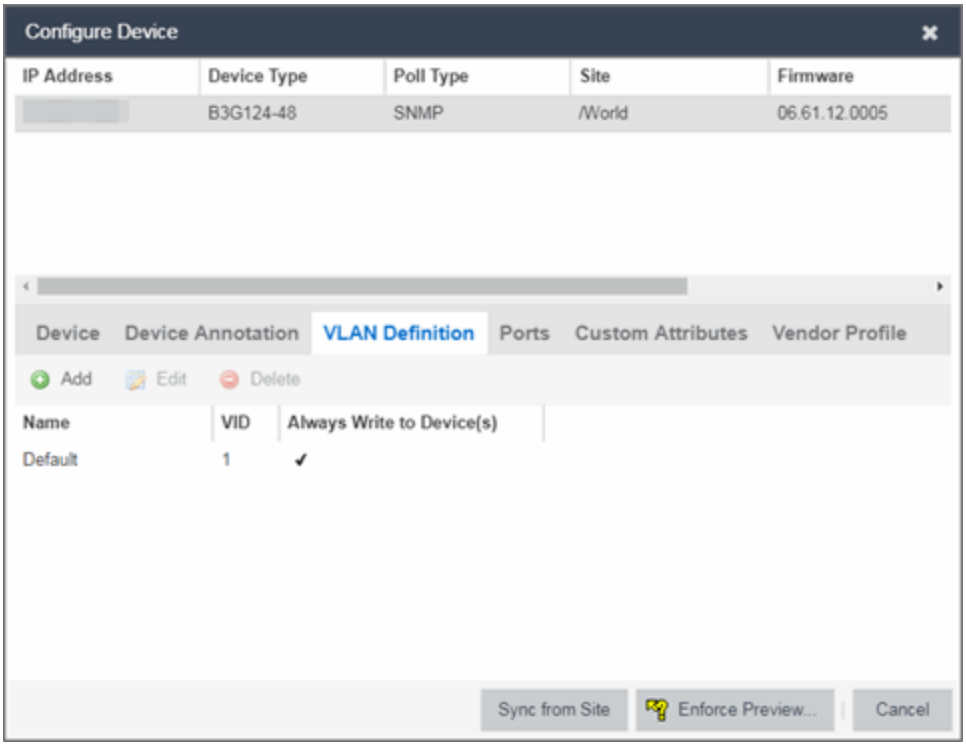
The VLAN is now configured to the Ports.

To edit the name of a VLAN:

1. Launch ExtremeCloud IQ Site Engine.
2. Open the **Network > Devices** tab.
3. Select the device from the devices list.
4. Right-click the device and select **Device > Configure Device**.
   The **Configure Device** window opens.



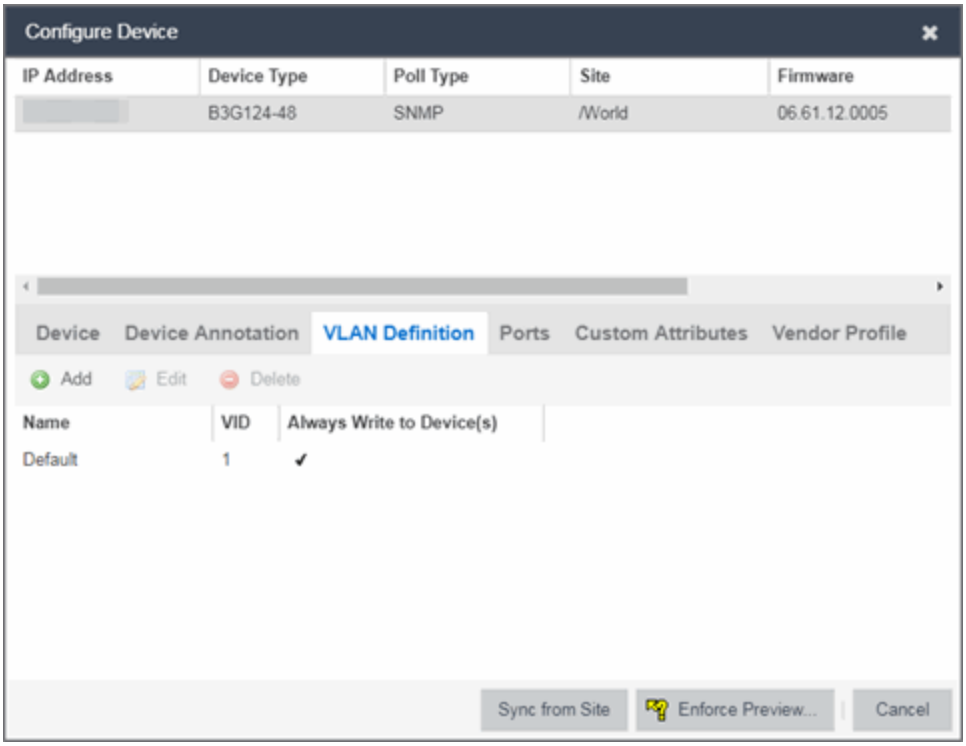
5. Select the **VLAN Definition** tab.



6. Select the VLAN to edit and then select the **Edit** button.
7. Enter the new name for the VLAN.
8. Select **Update**.
   The Edit pane closes.
9. Select **Save** to exit the VLAN Definition window. The VLAN is updated.

To remove devices from a VLAN:

1. Launch ExtremeCloud IQ Site Engine.
2. Open the **Network > Devices** tab.
3. Select the device from the devices list. Right-click the device and select **Device > Configure Device**.
   The **Configure Device** window opens.
4. Select the **VLAN Definition** tab.
   The VLAN Definition pane opens.



5. Select the VLAN and select **Delete**.

Troubleshooting

This troubleshooting guide provides a list of items to check when ExtremeCloud IQ Site Engine functionality is failing to perform correctly. Locate a problem in the left column and then review the troubleshooting information in the right column.

Problem	Troubleshooting Steps
Error contacting a wireless controller. The controller shows a Warning icon. 	1. Verify that the Configuration password in the CLI Credential used for this device is properly configured. a. From ExtremeCloud IQ Site Engine, access **Administration** > **Profiles** tab. b. Select the **CLI Credentials** subtab. c. Select the CLI Credential being used by the controller's Profile, and select **Edit**. d. Verify the user name and password used in the credential. For wireless controllers, add the Login password to the Configuration password field instead of the Login password field. The username and Configuration password specified here must match the username and Login password configured on the controller. e. Verify the SSH connection type is selected. f. Select **OK**. g. Use this CLI Credential in the controller's Profile. **NOTE:** When configuring profiles for ExtremeWireless Controllers, you must ensure that controllers are discovered using an SNMPv2c or SNMPv3 profile. The profile must also contain SSH CLI credentials for the controller. Wireless Manager uses the controller's CLI to retrieve required information and to configure managed controllers. 2. Verify that the following ports are accessible through firewalls for the ExtremeCloud IQ Site Engine Server and Wireless Controllers to communicate: SSH: 22 SNMP: 161, 162 Langley: 20506