ExtremeCloud™ IQ - Site Engine Guide
Version 21.11.10

12/2021
9037286-00

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

Help

ExtremeCloud IQ - Site Engine provides access to web-based reporting, network analysis, troubleshooting, and helpdesk tools. ExtremeCloud IQ - Site Engine includes wired/wireless dashboards, reports, end-system information and policy, interactive topology maps, application identification, web-based FlexViews, device views, and event logs. NetFlow diagnostics enable assessment of network issues and performance. Search functionality enables you to search for end-systems by MAC address, IP address, end-system name, or user name.

Contact your sales representative for information on obtaining an ExtremeCloud IQ - Site Engine license.

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.

Additionally, for information about using this help system, please see Using the Help System.

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 helpdesk 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.
- **Governance**—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.
- **Administration**—ExtremeCloud IQ - Site Engine administration tools to monitor and maintain the ExtremeCloud IQ - Site Engine application and its components.
- —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.

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

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.	NetSight OneView > Access OneView
View ExtremeCloud IQ - Site Engine Reports. Adds the ability to view reporting data.	NetSight OneView > Access OneView Reports
View ExtremeCloud IQ - Site Engine Maps. Adds the ability to view maps.	NetSight OneView > Maps > Maps Read Access
View and Configure ExtremeCloud IQ - Site Engine Maps. Adds the ability to view and configure maps.	NetSight OneView > Maps > Maps Read/ Write Access
View ExtremeCloud IQ - Site Engine Wireless. Adds the ability to view wireless data.	NetSight 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.	NetSight OneView > Access OneView Administration
View ExtremeCloud IQ - Site Engine Search. Adds the ability to use the ExtremeCloud IQ - Site Engine Search functionality.	NetSight 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.	NetSight 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.	NetSight 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.	NetSight 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.	NetSight 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.	NetSight OneView > Identity and Access > OneView End-Systems Read Access

ExtremeCloud IQ - Site Engine Access Options and Features	Required Capabilities
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 and changing an end-system's group membership.	NetSight OneView > Identity and Access > OneView End-Systems Read/Write Access
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.	NetSight 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, and delete groups.	NetSight 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.	NetSight 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.	NetSight 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.	NetSight 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.	NetSight 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.	NetSight 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.	NetSight Suite > NetSight 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.	NetSight Policy Manager > Read/Write capabilities for Policy Enforcement and Management
Add Devices. Adds the ability to add devices in the ExtremeCloud IQ - Site Engine **Network** tab.	NetSight Suite > Devices > Add, Discover and Import
Delete Devices. Adds the ability to delete devices in the ExtremeCloud IQ - Site Engine **Network** tab.	NetSight 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:

- NetSight OneView > Access OneView
- NetSight OneView > Access OneView Reports
- NetSight OneView > Access OneView Search
- NetSight OneView > Access OneView Administration
- NetSight OneView > NetFlow Read/Write Access
- NetSight OneView > Maps > Maps Read/Write Access
- NetSight Console > Wireless Manager > Launch
- NetSight OneView > Events and Alarms > OneView Event Log Access
- NetSight OneView > Events and Alarms > OneView Alarms Read/Write Access
- NetSight OneView > FlexView > OneView FlexView Read/Write Access
- NetSight OneView > Identity and Access > Access OneView Identity and Access Reports
- NetSight OneView > Identity and Access > OneView End-Systems Read/Write Access
- NetSight OneView > Identity and Access > OneView Group Read/Write Access
- NetSight Policy Manager > Read/Write capabilities for Policy Enforcement and Management
- NetSight Suite > Device Local Management WebView > Auto Login to Web Local Management for ExtremeWireless Wireless Controllers
- NetSight Suite > NetSight All User Options > Request and Configure ExtremeNetworks.com Support
- NetSight Suite > Devices > Add, Discover and Import
- NetSight 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:

- NetSight OneView > Access OneView
- NetSight OneView > Access OneView Reports
- NetSight OneView > Access OneView Search
- NetSight OneView > NetFlow Read Access

- NetSight OneView > Maps > Maps Read Access
- NetSight Console > Wireless Manager > Launch
- NetSight OneView > Events and Alarms > OneView Event Log Access
- NetSight OneView > Events and Alarms > OneView Alarms Read Access
- NetSight OneView > FlexView > OneView FlexView Read Access
- NetSight OneView > Identity and Access > Access OneView Identity and Access Reports
- NetSight OneView > Identity and Access > OneView End-Systems Read Access
- NetSight 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:

- NetSight OneView > Access OneView
- NetSight OneView > Access OneView Reports
- NetSight 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:

- NetSight OneView > Access OneView
- NetSight 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:

- NetSight OneView > Access OneView
- NetSight 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 NetSight OneView > Access NetSight 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.

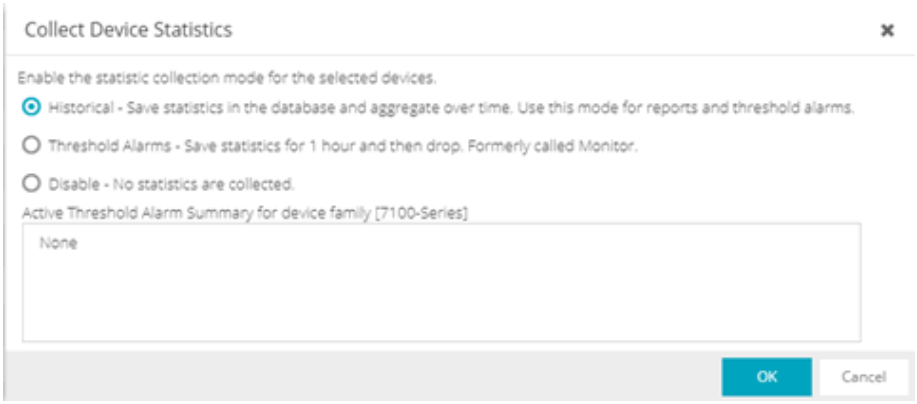
If you are enabling statistics collection on an ExtremeControl engine, Application Detection engine, or ExtremeWireless Controller, read through the following notes:

- **ExtremeControl Engine**
  When collecting statistics on an ExtremeControl 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 ExtremeControl 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.)

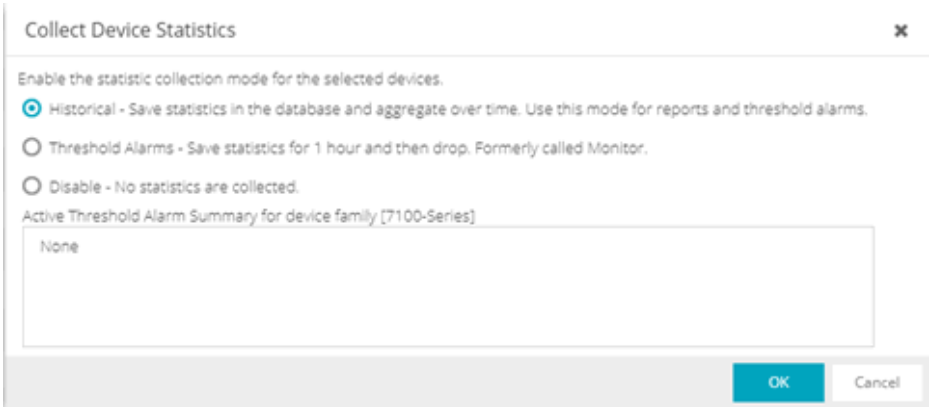
Enabling Interface Statistics Collection

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

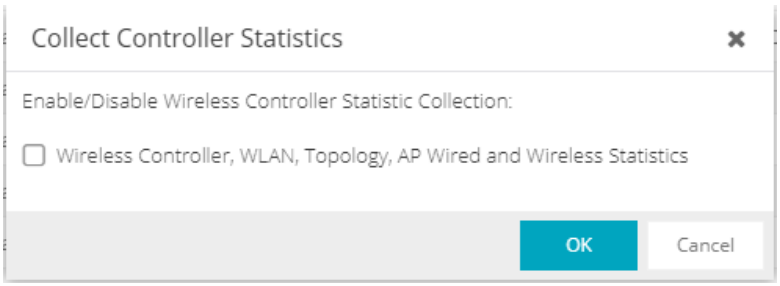
Wireless Controller statistics collection is configured separately from other devices. When you enable Wireless Controller statistics collection, it includes Wireless Controller, WLAN, Topology, and AP wired and wireless statistics, and you also have the option to collect wireless client statistics.

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 devices support application telemetry flow collection. You must be a member of an authorization group assigned the NetSight OneView > NetFlow Read/Write Access capability to view NetFlow data or the NetSight 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

Variables		Scenario 1	Scenario 2
Devices	Wireless Controllers	5	10
	Wireless APs	1000	2000
	Advanced Switch/ Routers	150	50
	Advanced Interfaces	1000	200
	Servers	150	50
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 ExtremeAnalyticsvirtual engine deployment requirements and how to deploy a virtual engine on a VMware®and Hyper-V server.

Upgrading Fabric Manager

Use the following procedure to upgrade your version Fabric Manager.

Prerequisites

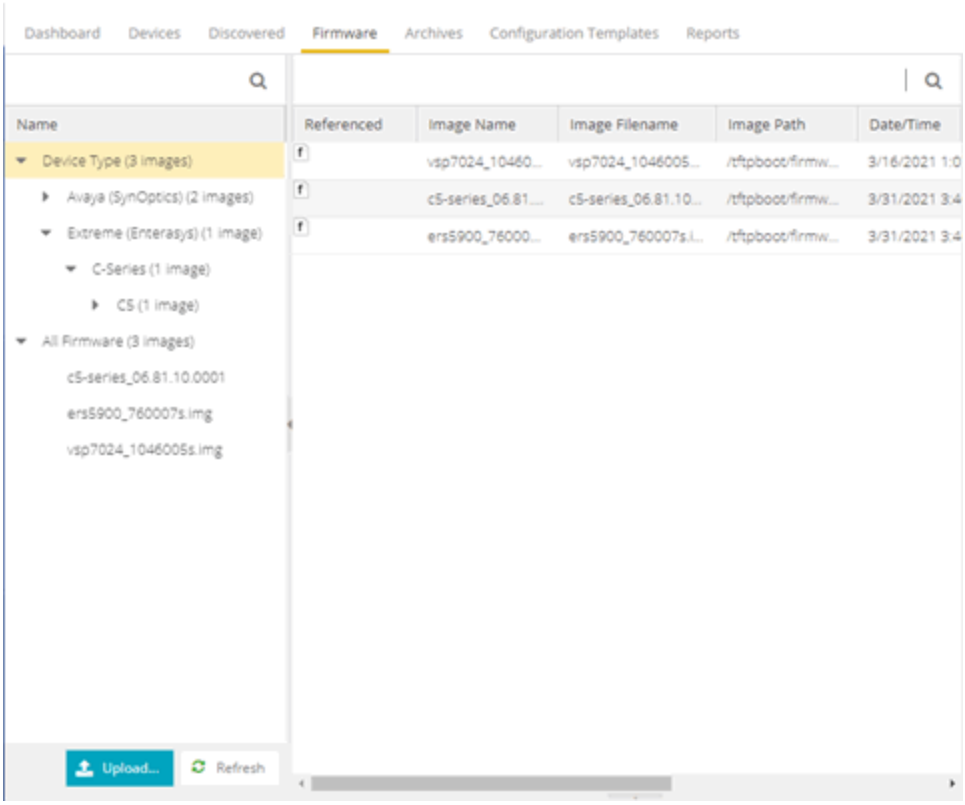
- Upgrade ExtremeCloud IQ - Site Engine to the later version before you upgrade Fabric Manager to the corresponding build number.
- Ensure that both the current and target ExtremeCloud IQ - Site Engine and Fabric Manager build numbers are the same.
- Download the latest upgrade bundle from the Extreme 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.

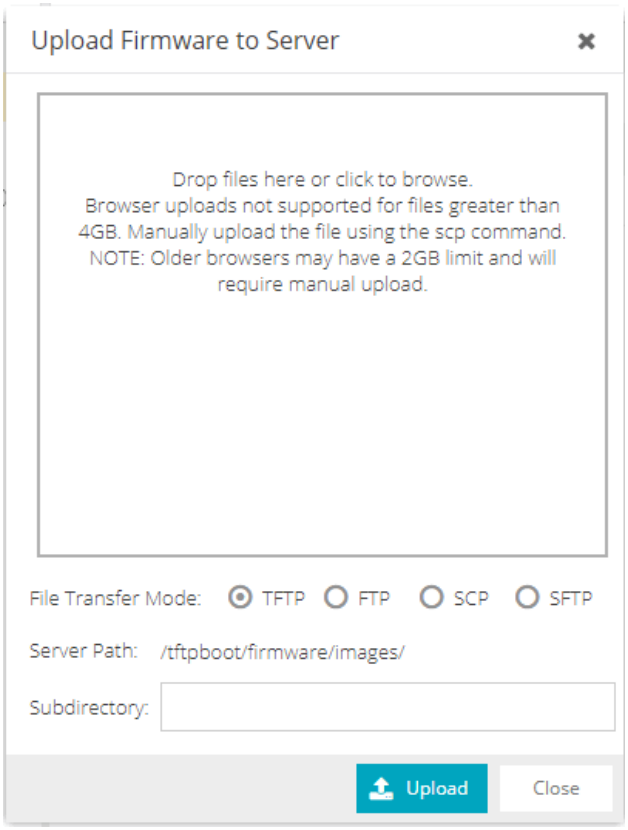
NOTE: After you deploy Fabric Manager and then register with ExtremeCloud IQ - Site Engine, only the user credential associated with the Fabric Manager profile has SSH login access.

Upgrade Procedure

1. Open the **Network** tab in ExtremeCloud IQ - Site Engine.
2. Select the **Firmware** tab.

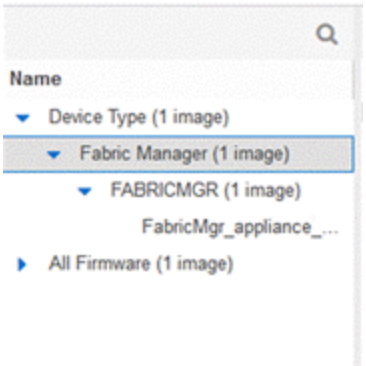


3. On the left panel, select **Upload**  .
4. In the Directory field, select the **SCP** radio button and select **Upload**.

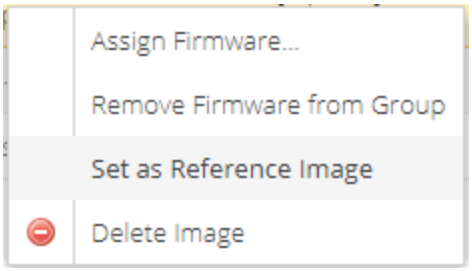


5. Select on **Drop files here or select to browse** and select the previously downloaded upgrade bundle.
6. Select the **Upload** button to initiate the bundle upload to the ExtremeCloud IQ - Site Engine server.

   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.

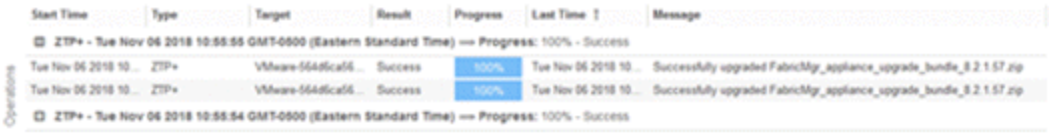


7. Navigate through the newly added Device type until you see the bundle image listed.
8. Right-click the bundle listed on the main panel and select **Set as Reference Image**.

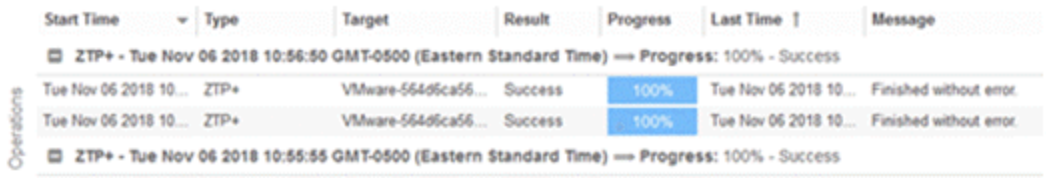


This step sets this image bundle as the Reference upgrade image for Fabric Manager. The upgrade process to get triggered by default can take **up to five minutes** depending on the poll interval set on ExtremeCloud IQ - Site Engine.

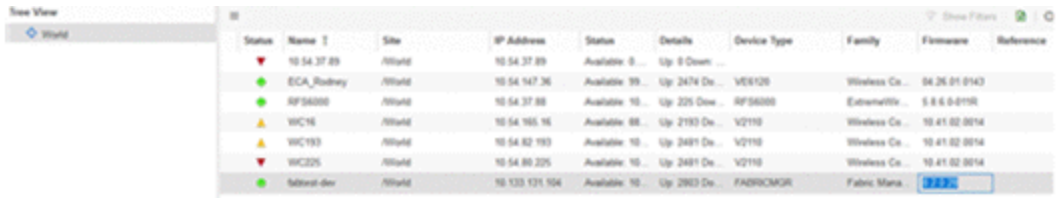
9. Open the **Operations** log on ExtremeCloud IQ - Site Engine and wait until a log of type 'ZTP+' with the message `Successfully upgraded FabricMgr_appliance_upgrade_bundle_<version_number>.zip` appears.



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**.

Related Information

- ExtremeCloud IQ - Site Engine Fabric
- Fabric Connect

ExtremeCloud IQ - Site Engine Port List

ExtremeCloud IQ - Site Engine 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 (redirects to port 8443) ExtremeControl and ExtremeAnalytics engine communication
TCP	8443	HTTPS	Web browser access to ExtremeCloud IQ - Site Engine user interface Northbound Interface (NBI) ExtremeControl, ExtremeAnalytics, and Fabric Manager communication
TCP	8444	HTTPS	ExtremeControl engine communication

Type	Port	Description	Purpose
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
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
UDP	6343	SFlow	SFlow for ExtremeAnalytics / Application Telemetry

ExtremeCloud IQ - Site Engine 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	49	TACACS+	Required when using TACACS+ for user authentication

Type	Port	Description	Purpose
TCP	80	HTTP	Internet for ExtremeControl Assessment Agent updates (extremenetworks.com) Virtual sensor communication
TCP	389	LDAP	Required when using LDAP for user authentication
TCP	443	HTTPS	Allows ExtremeCloud IQ - Site Engine to connect to ExtremeCloud IQ (extremecloudiq.com) ExtremeAnalytics Fingerprint updates (services.enterasys.com)
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	20505	ExtremeWireless Protocol	ExtremeWireless Controller communication
UDP	53	DNS	
UDP	123	NTP	
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.
UDP	162	SNMP Trap	Send SNMP traps to external trap receivers
UDP	514	Syslog	Send syslog messages to external syslog receivers

Type	Port	Description	Purpose
UDP	1812	RADIUS authentication	Required when using RADIUS for user authentication

ExtremeControl 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
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	
UDP	161	SNMP	SNMP agent managed by ExtremeCloud IQ - Site Engine

Type	Port	Description	Purpose
UDP	1812	RADIUS authentication	ExtremeControl RADIUS server
UDP	1813	RADIUS accounting	ExtremeControl RADIUS server

ExtremeControl Remote Ports

Type	Port	Description	Purpose
TCP	389	LDAP	User-based network authentication and directory services
TCP	80/443	HTTPS	CRL verification
TCP	636	LDAPs	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	123	NTP	
UDP	162	SNMP Trap	SNMP traps sent to ExtremeCloud IQ - Site Engine
UDP	1700	RADIUS CoA	ExtremeControl RADIUS server to authenticators

Type	Port	Description	Purpose
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 IP Protocols

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

ExtremeAnalytics 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	
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	ExtremeXOS IPFIX collector
UDP	2095	NetFlow	ExtremeWireless NetFlow collector
UDP	4739	IPFIX	VTAP IPFIX collector from Virtual Sensor
UDP	6343	SFlow	SFlow for ExtremeAnalytics Application Telemetry

ExtremeAnalytics Remote Ports

Type	Port	Description	Purpose
TCP	80	HTTP	Virtual Sensor configuration
TCP	443	HTTPS	Virtual Sensor configuration

Type	Port	Description	Purpose
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

Internet Connectivity

Type	Port	Description	Purpose
TCP	443	HTTPS	ExtremeAnalytics Fingerprint updates (services.enterasys.com)
TCP	443	HTTPS	Allows ExtremeCloud IQ - Site Engine to connect to ExtremeCloud IQ (*.extremecloudiq.com)
TCP	80	HTTP	ExtremeControl Assessment Agent download (extremenetworks.com)

Fabric Manager 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 Local Ports

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

Ephemeral Ports

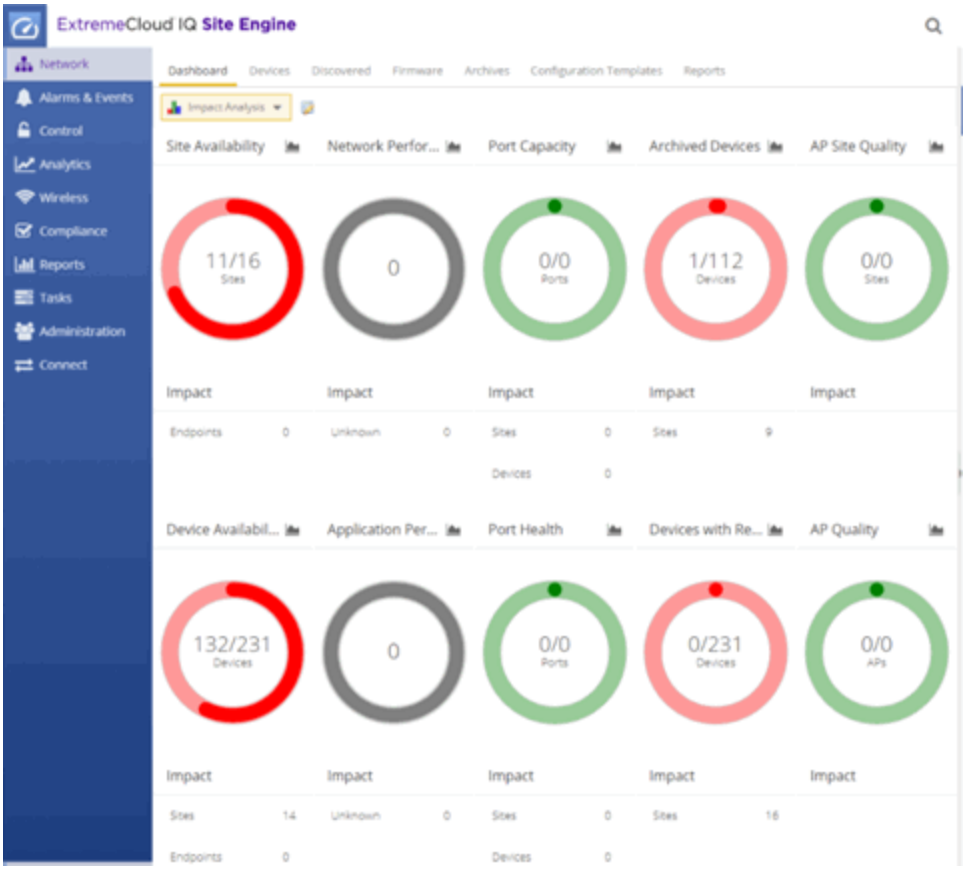
The port range 32768 to 61000 is reserved for dynamically allocated port numbers used by most TCP and UDP based protocols, such as TFTP and FTP.

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 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.

Related Information

For information on related topics:

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

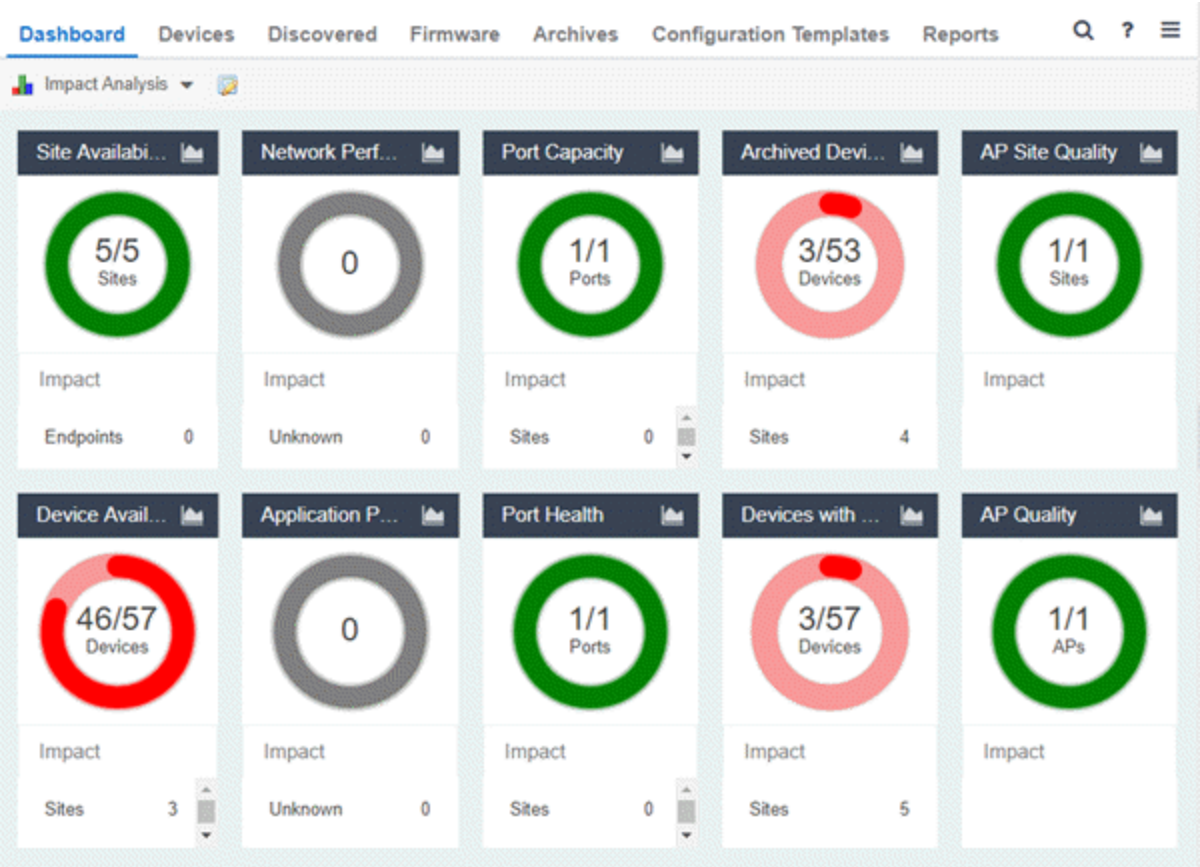
For information on related tasks:

- 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: Enable Dynamic Thresholding to allow ExtremeCloud IQ - Site Engine to automatically determine the expected response times based on previously observed response times. If you do not use ExtremeAnalytics or do not want to enable Dynamic Thresholding, 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: Enable Dynamic Thresholding to allow ExtremeCloud IQ - Site Engine to automatically determine the expected response times based on previously observed response times. If you do not use ExtremeAnalytics or do not want to enable Dynamic Thresholding, 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.

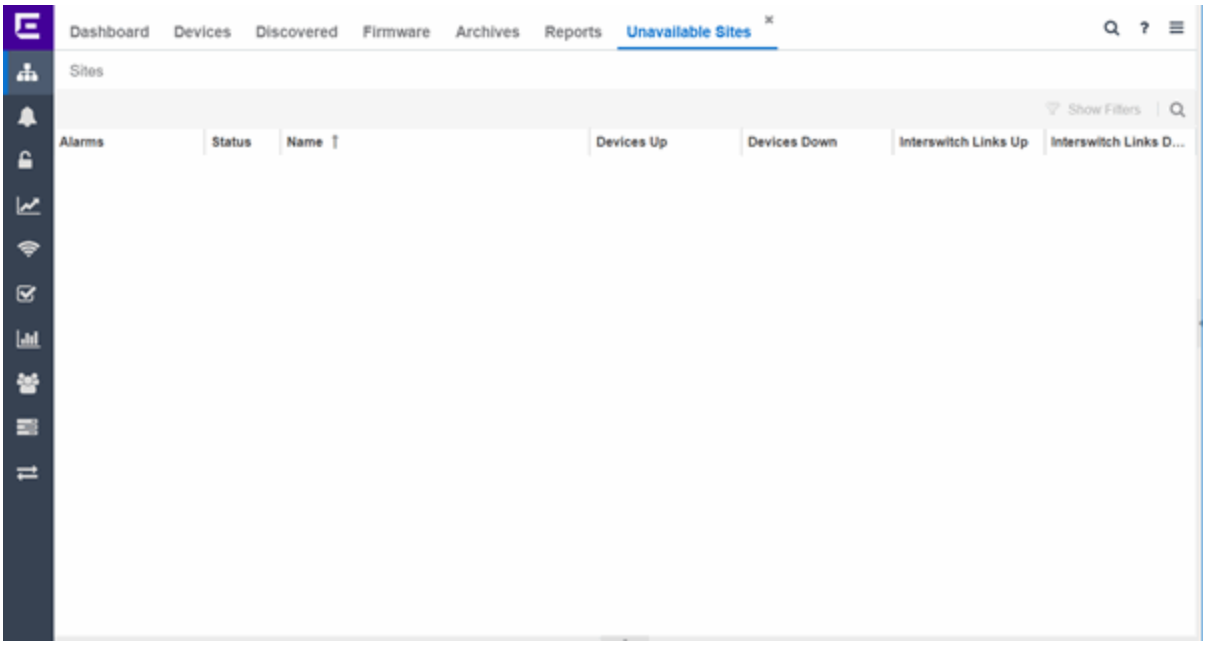
- Select the ring chart to open the **APs with Low Quality** report that displays details about APs experiencing low quality.
- Select **Impact** in the Impact Summary beneath the ring chart to open the **APs Impacted by Low Quality** report that provides a list of the APs experiencing low quality.
-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

Related Information

- 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.

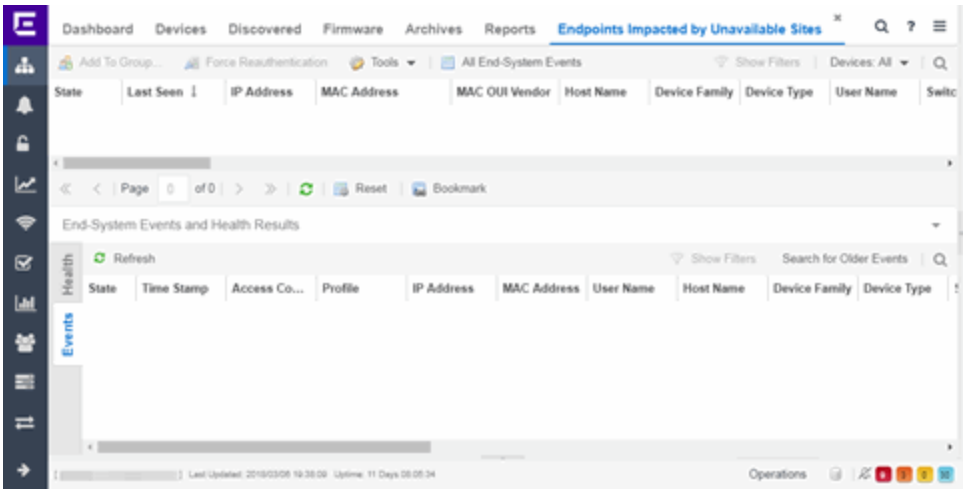
Interswitch Links Down
This column indicates the number of Interswitch Links with a **Status** of **Down** in the site.

Related Information

- 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

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 ID Manager —An Extreme switch running ExtremeXOS with the Identify Manager feature configured to send events to NetSight.
- 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 ID Manager —An Extreme switch running ExtremeXOS with the Identify Manager feature configured to send events to NetSight.
- 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: http://www.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.

Related Information

- 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.

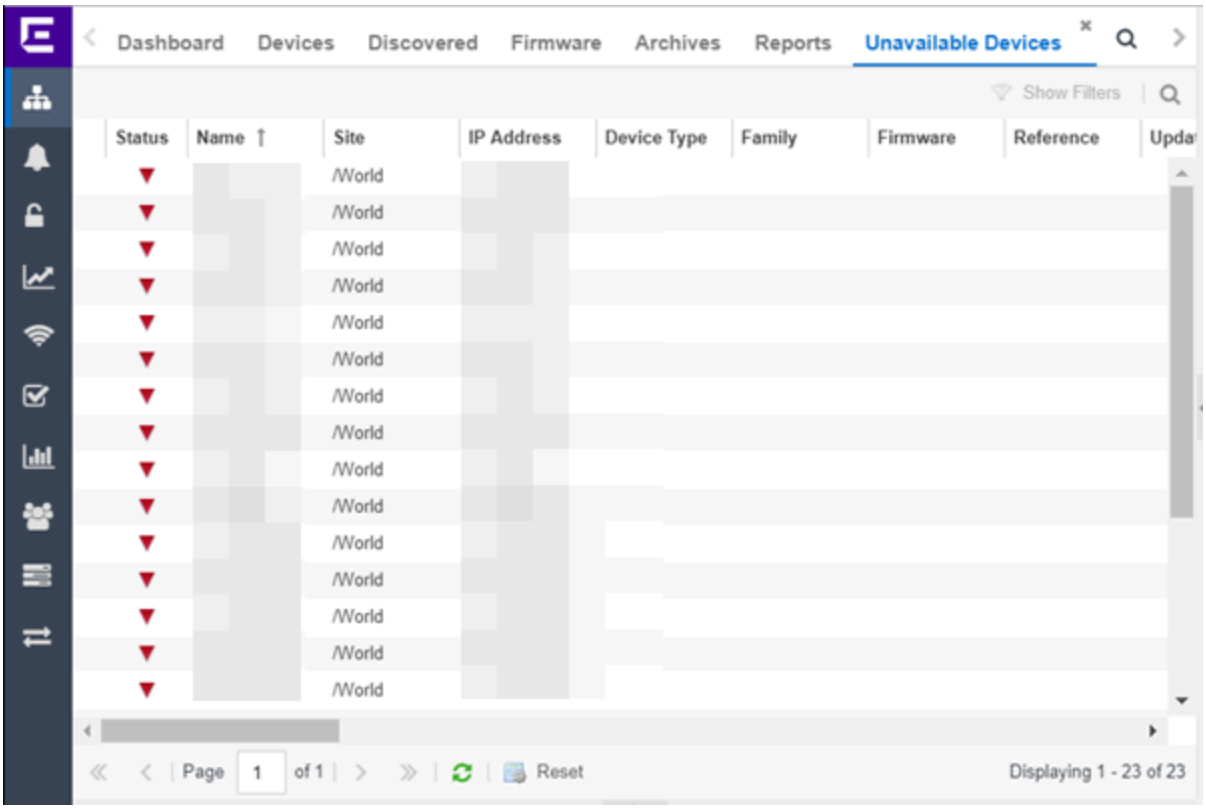
Select the time span for which the report displays from the time span drop-down list. Available options are **Last 24 Hours**, **Yesterday**, **Last 3 Days**, **Last Week**, **Last 2 Weeks**, **Last Month**.

Related Information

- 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.

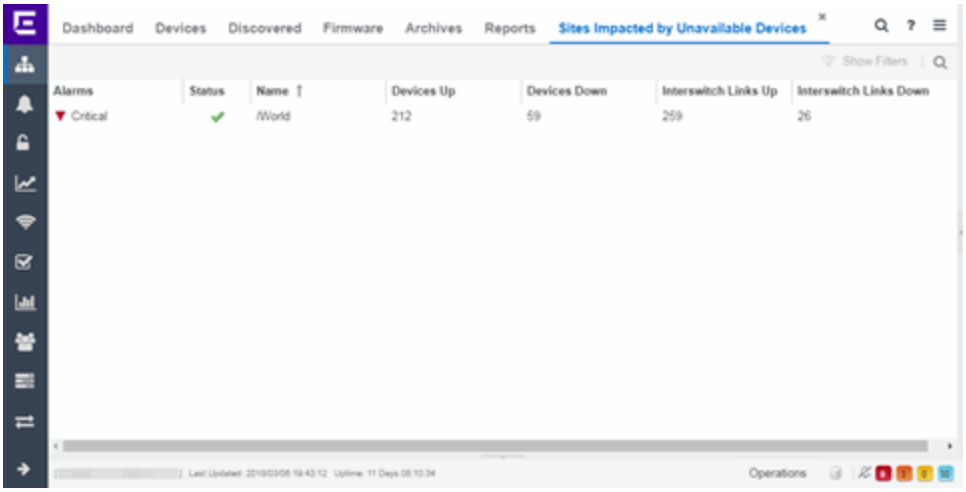
User Data 1-4, Notes
These columns can provide additional information about the device.

Related Information

- 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.

Related Information

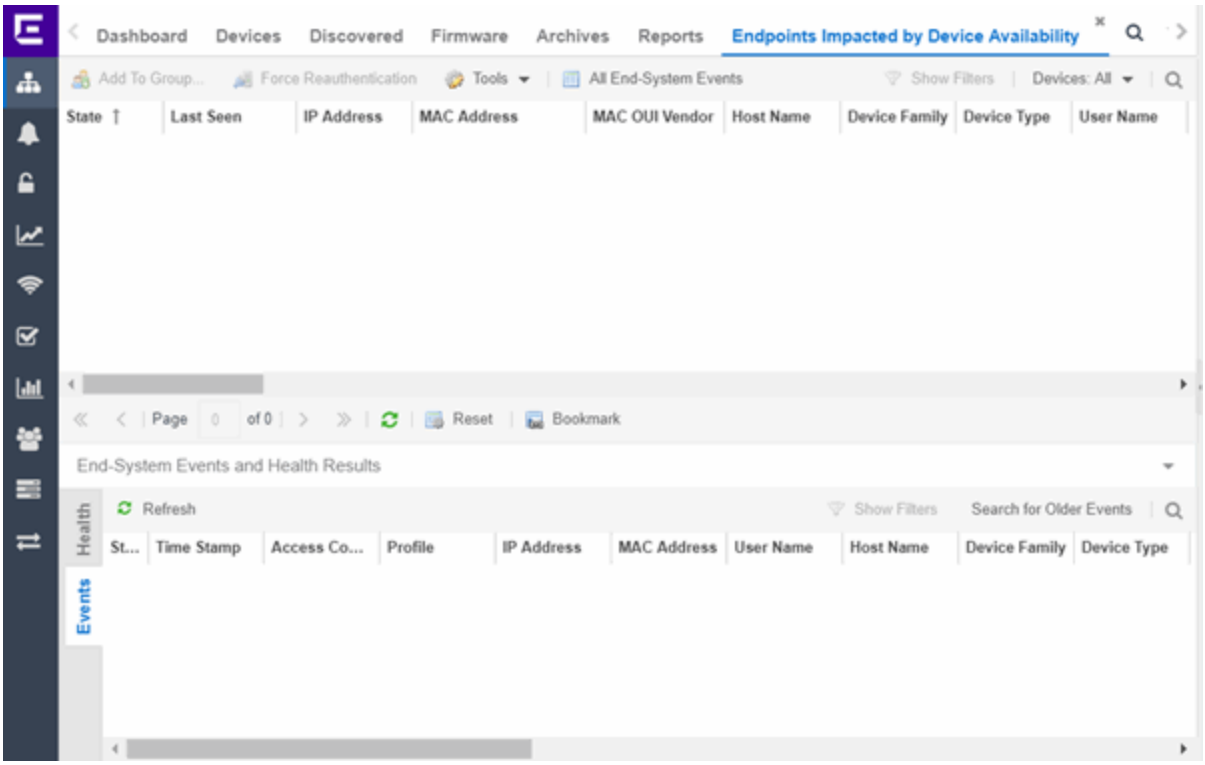
- Impact Analysis Dashboard Overview

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 ID Manager —An Extreme switch running ExtremeXOS with the Identify Manager feature configured to send events to NetSight.
- 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 ID Manager —An Extreme switch running ExtremeXOS with the Identify Manager feature configured to send events to NetSight.
- 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: http://www.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.

Related Information

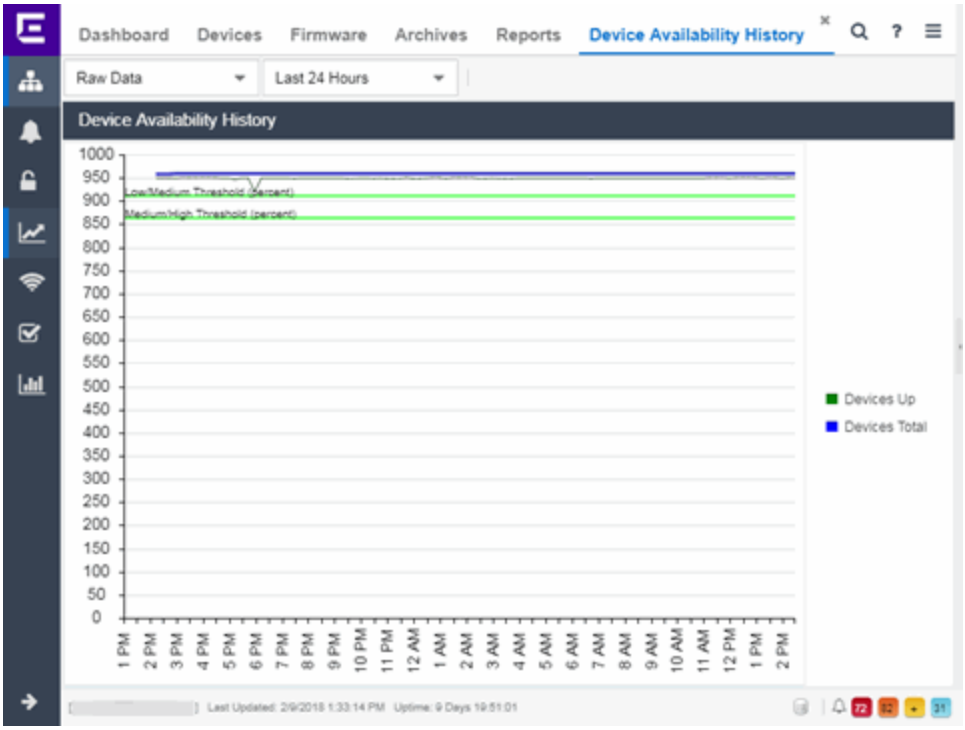
- Impact Analysis Dashboard Overview

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**.



Related Information

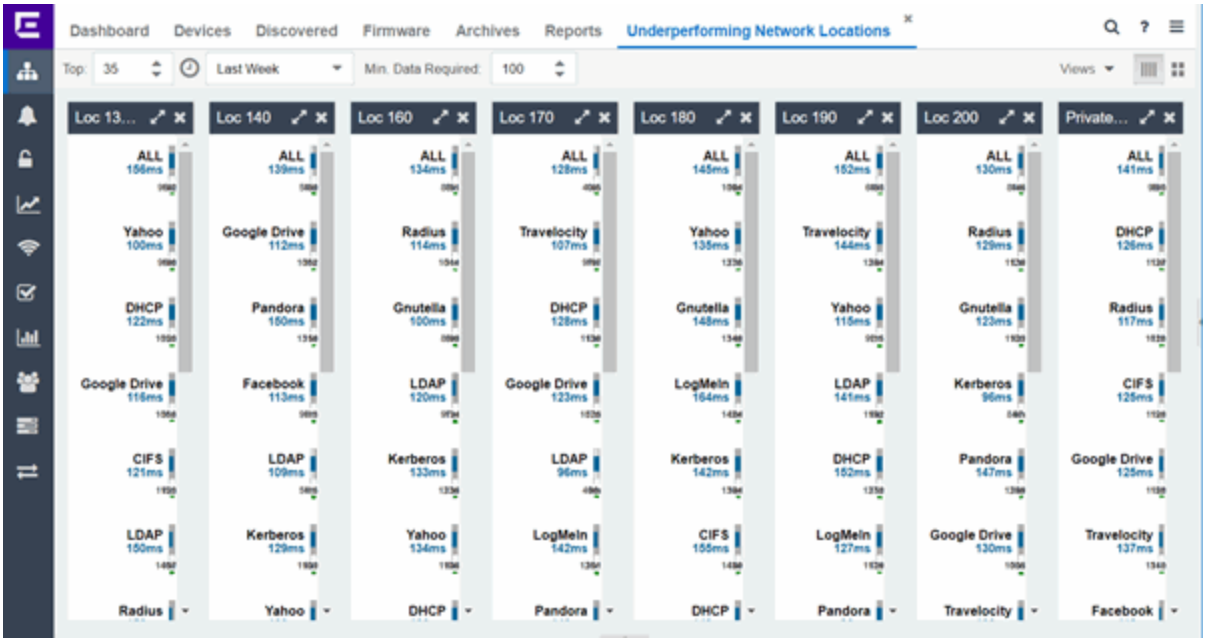
- Impact Analysis Dashboard Overview

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.

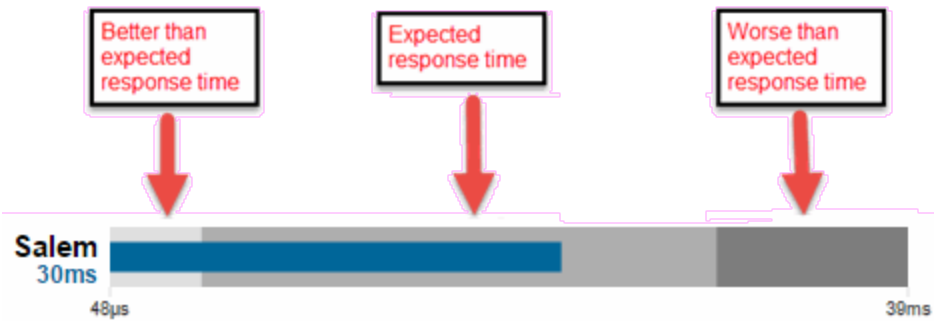
The report contains two types of graphs:

- 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.

Related Information

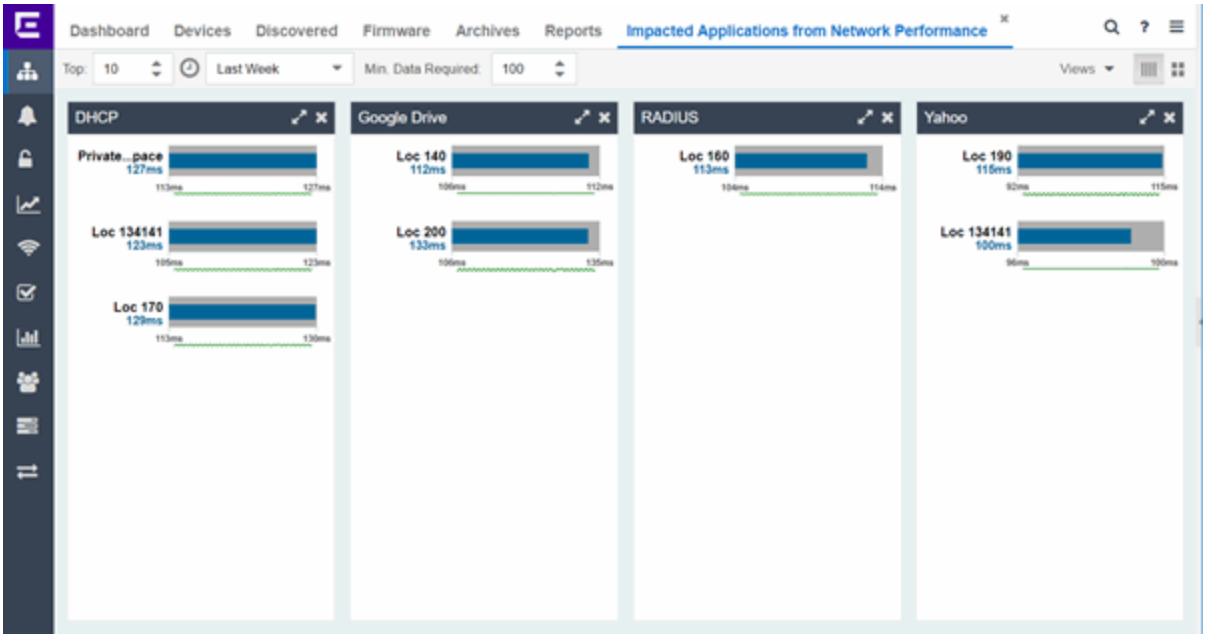
- Impact Analysis Dashboard Overview

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.

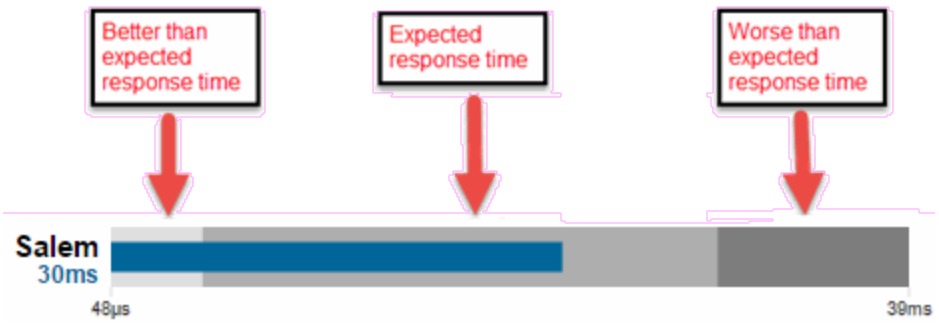
The report contains two graphs:

- 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.

Related Information

- Impact Analysis Dashboard Overview

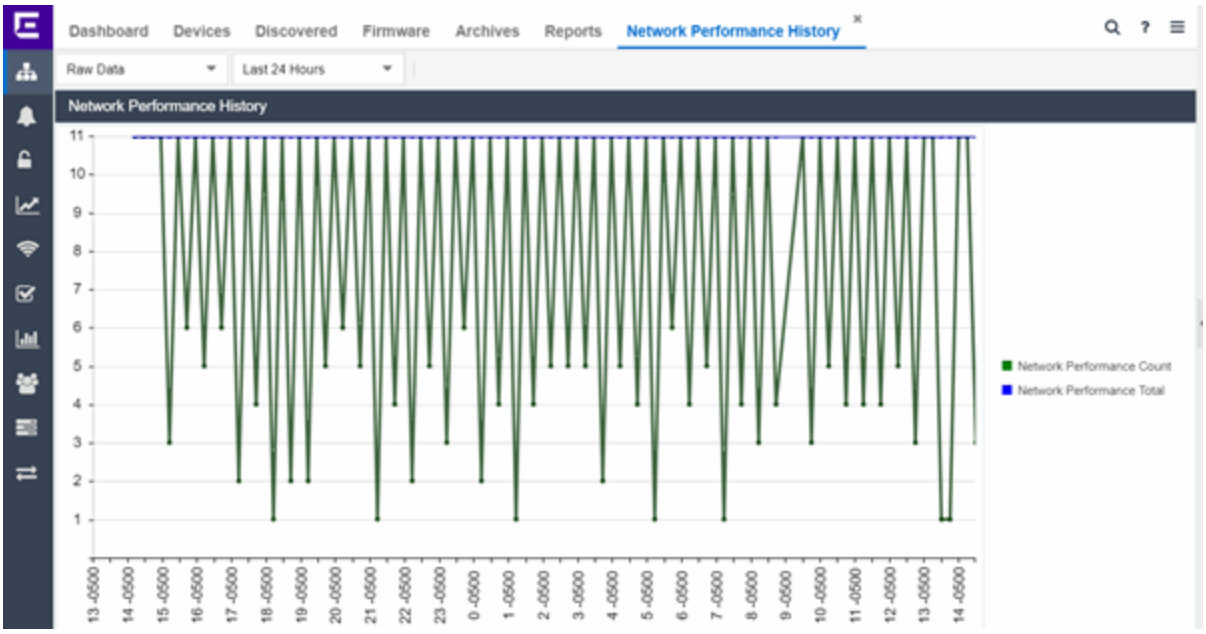
Network Performance History Report

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**.

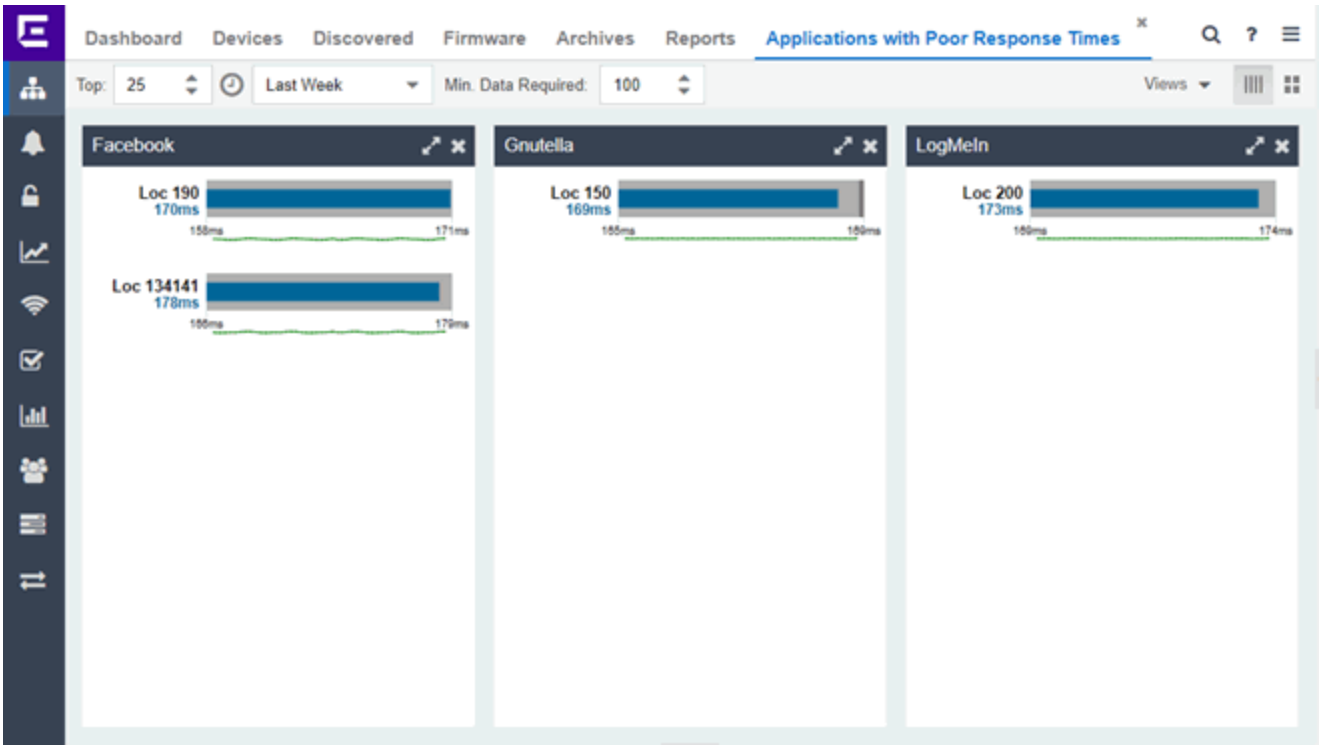


Related Information

- 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.

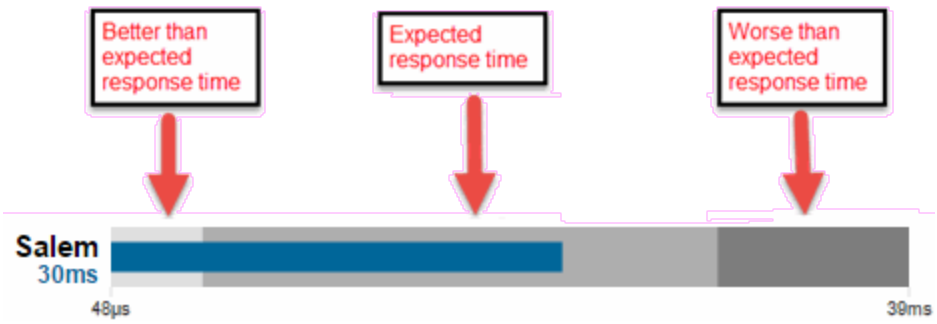
The report contains two types of graphs:

- 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.

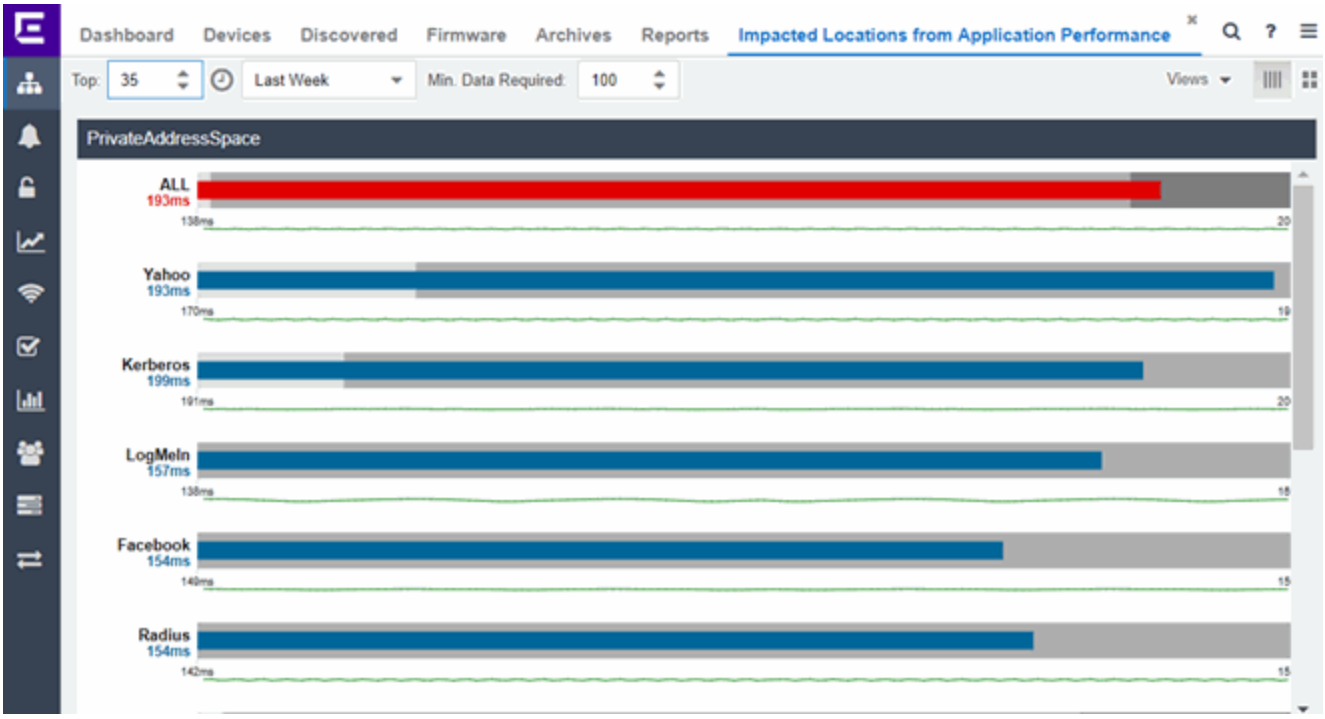
Related Information

- 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.

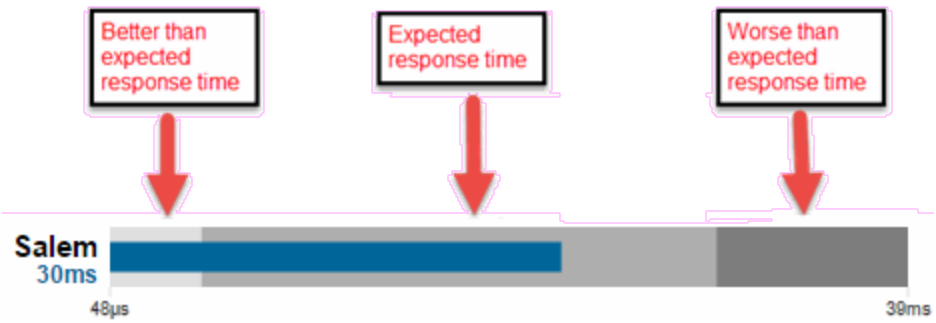
The report contains two types of graphs:

- 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.

Related Information

- Impact Analysis Dashboard Overview

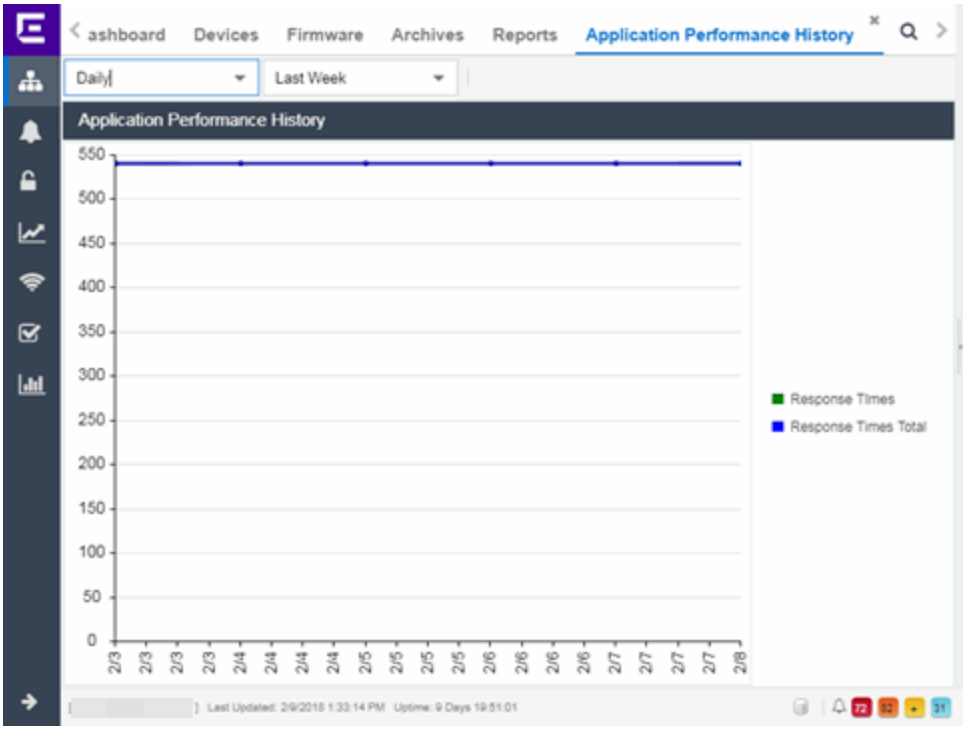
Application Performance History Report

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**.



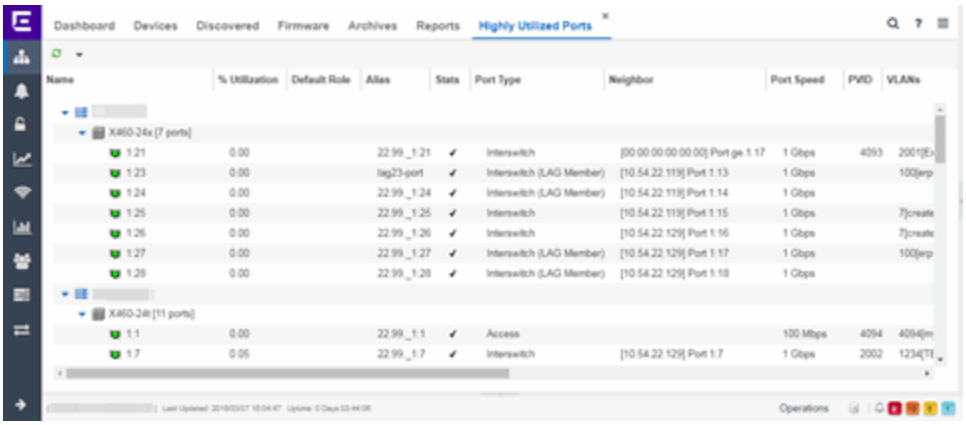
Related Information

- 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 1Backplane, 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.

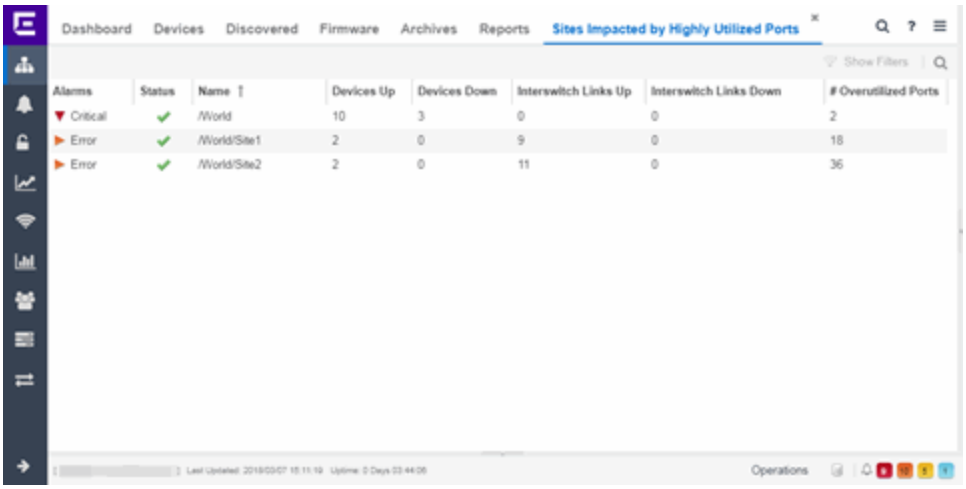
Related Information

- 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

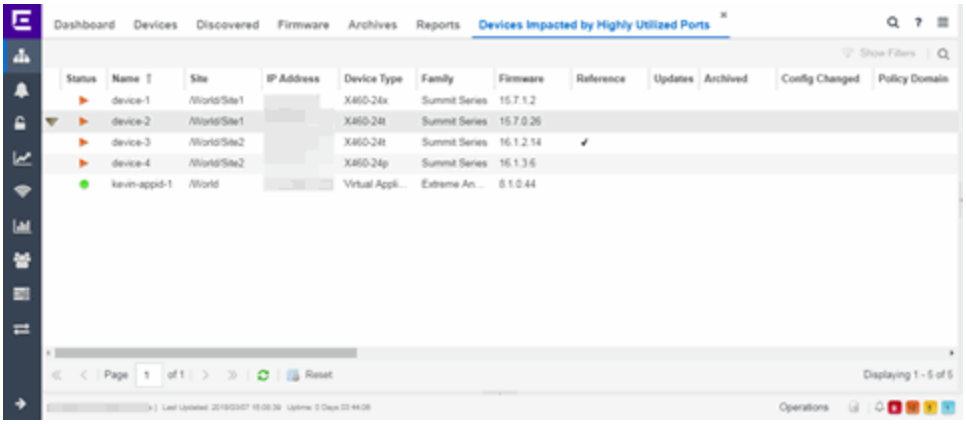
Related Information

- 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.

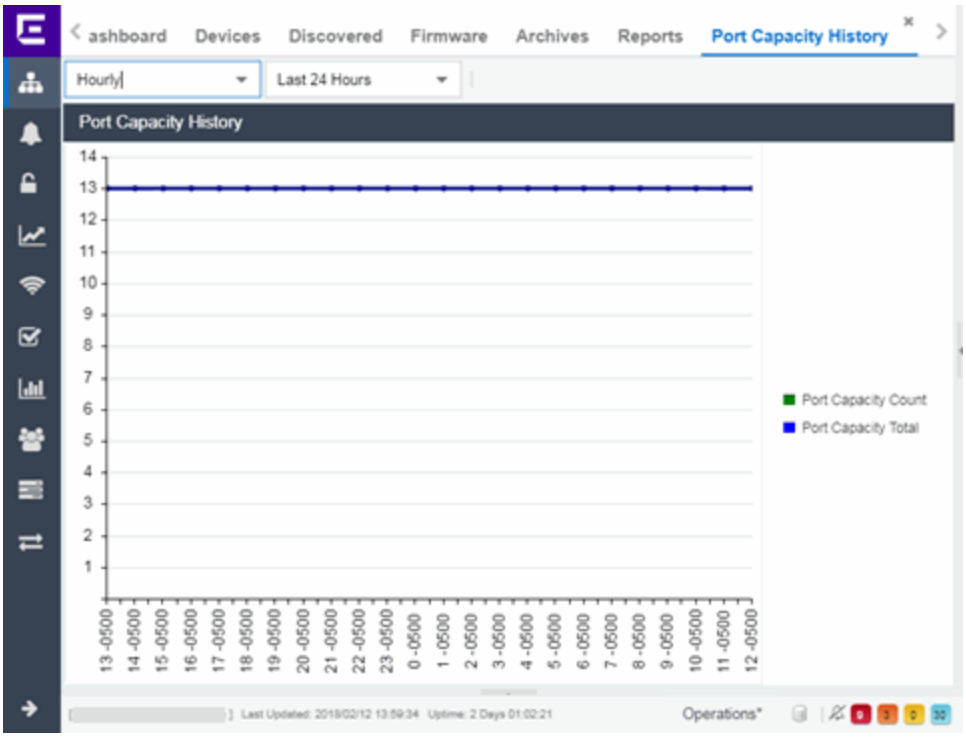
Related Information

- 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}

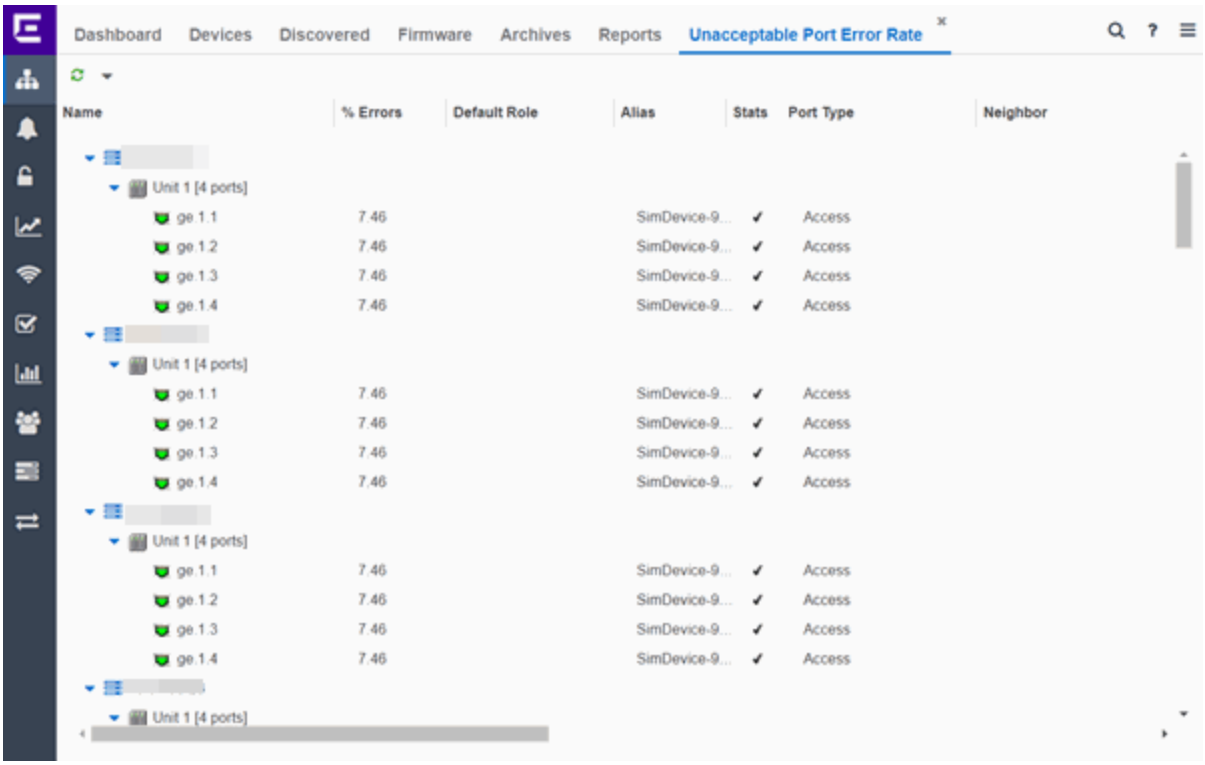
Related Information

- 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 1Backplane, 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.

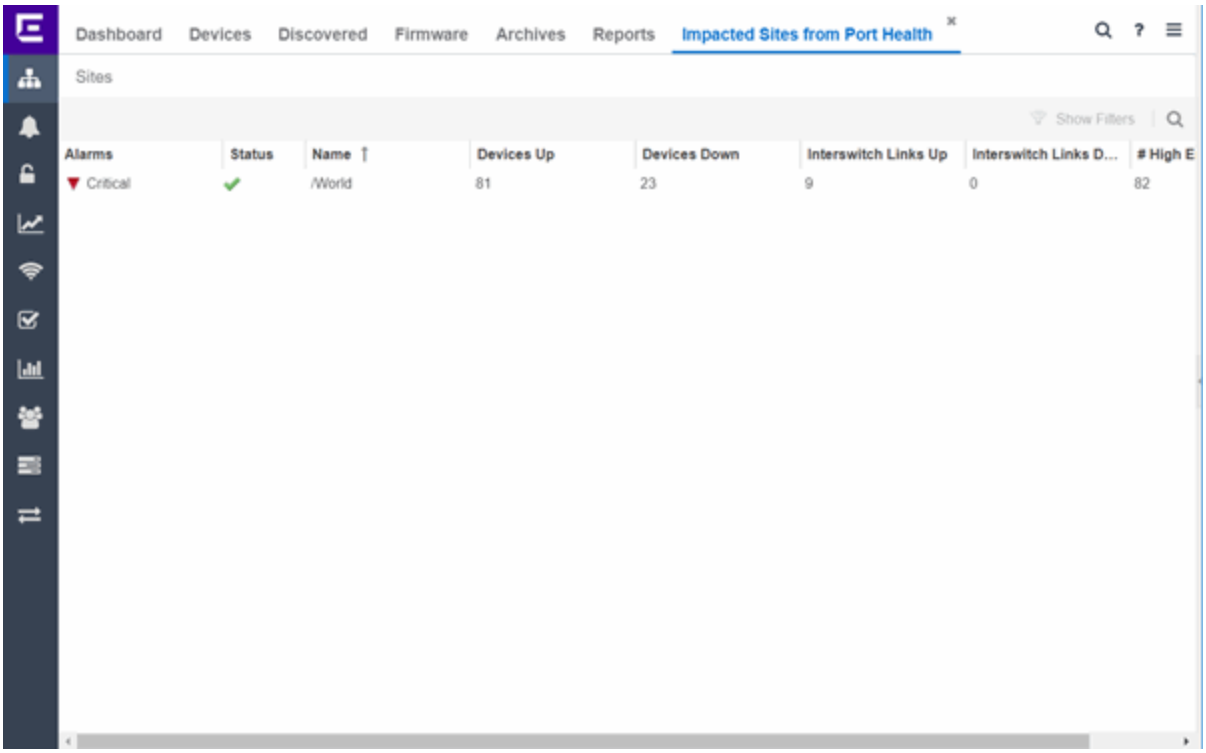
Related Information

- 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.

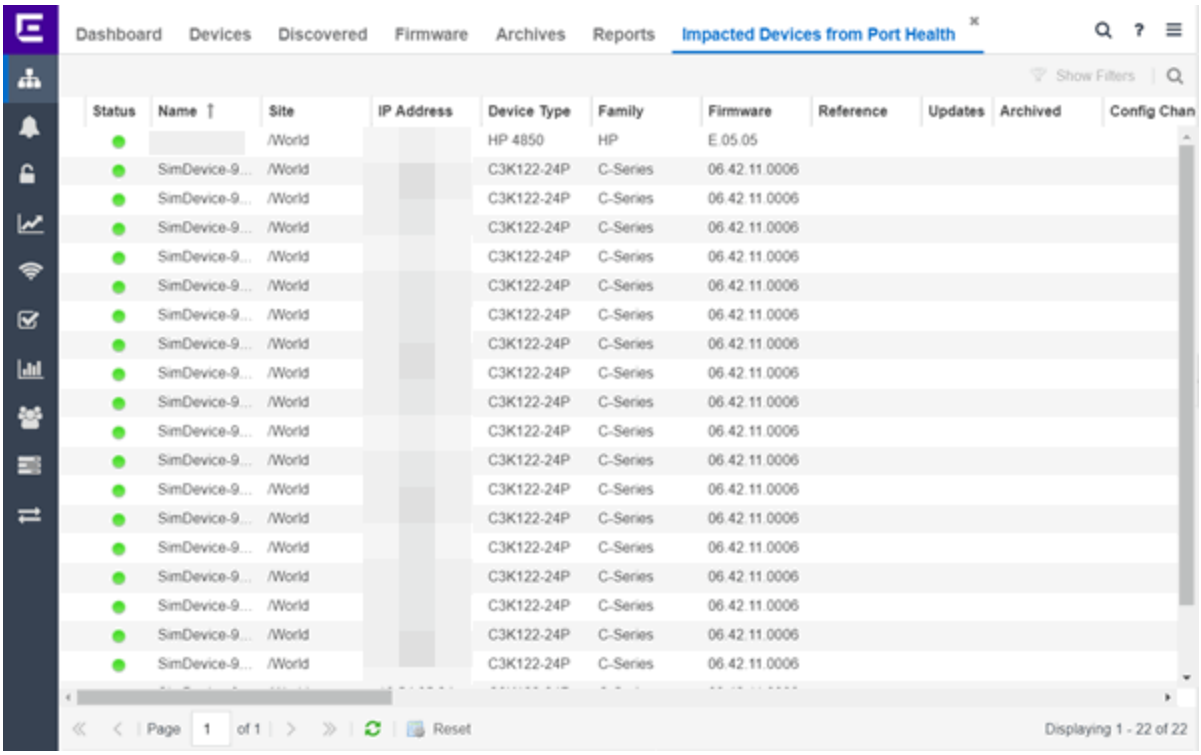
Related Information

- 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.

Related Information

- Impact Analysis Dashboard Overview

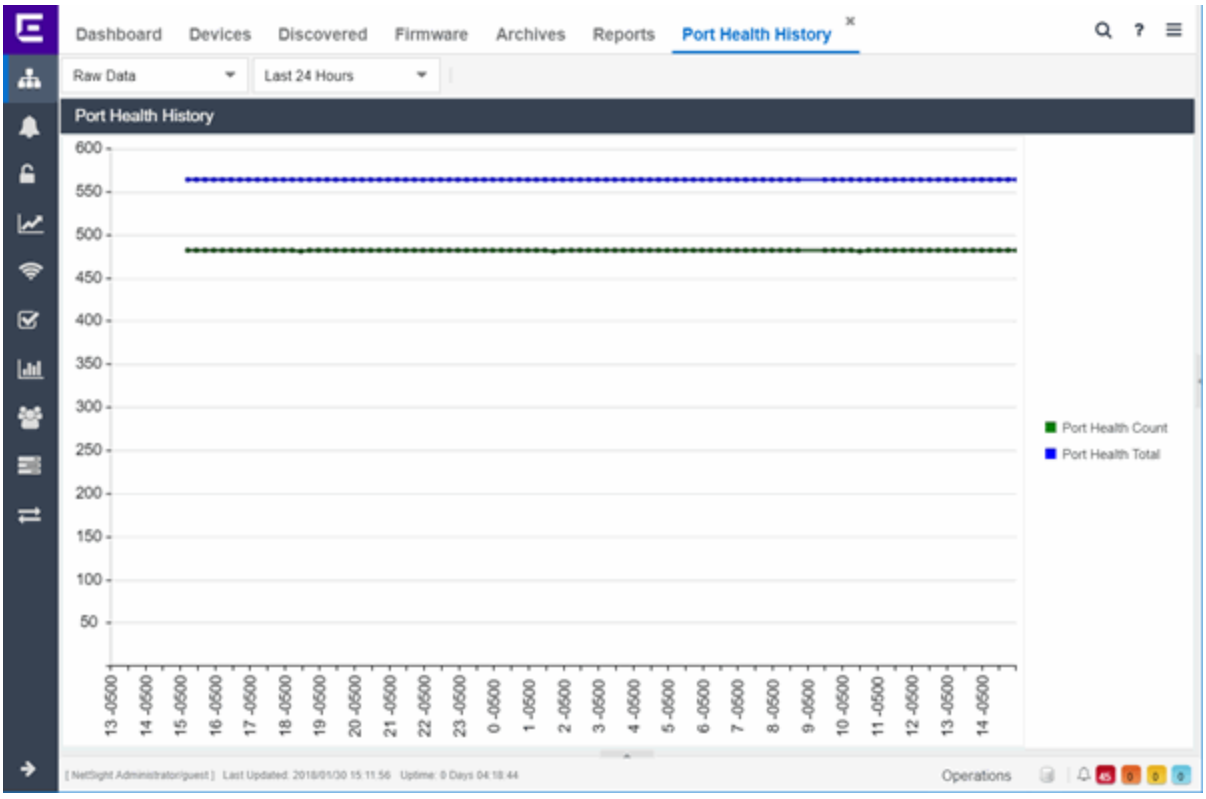
Port Health History Report

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**.

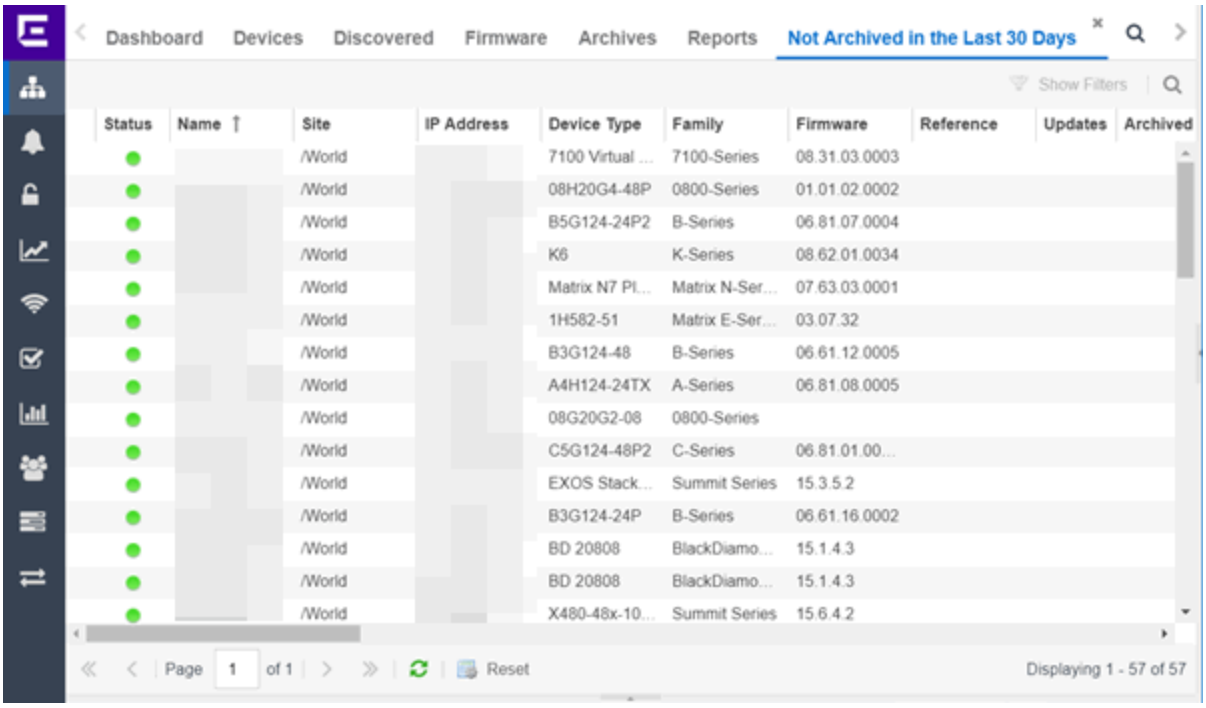


Related Information

- 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.

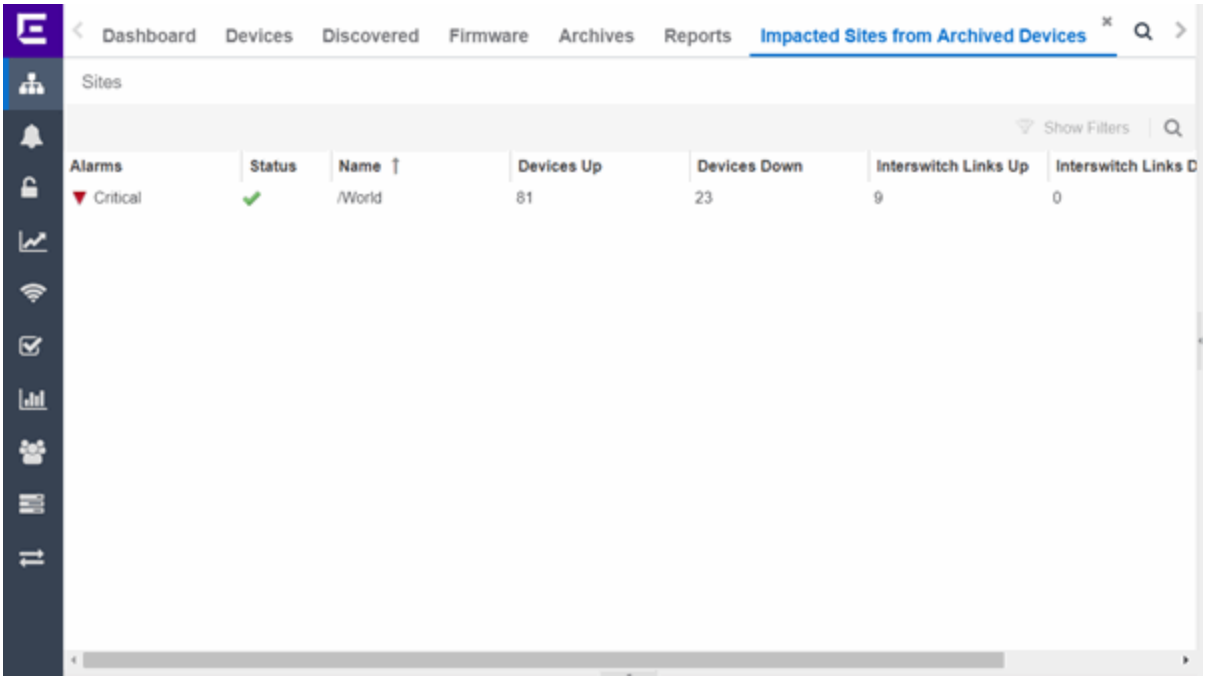
Asset Tag
A unique asset number assigned to the module or component for inventory tracking purposes.

Related Information

- 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.

Related Information

- 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.

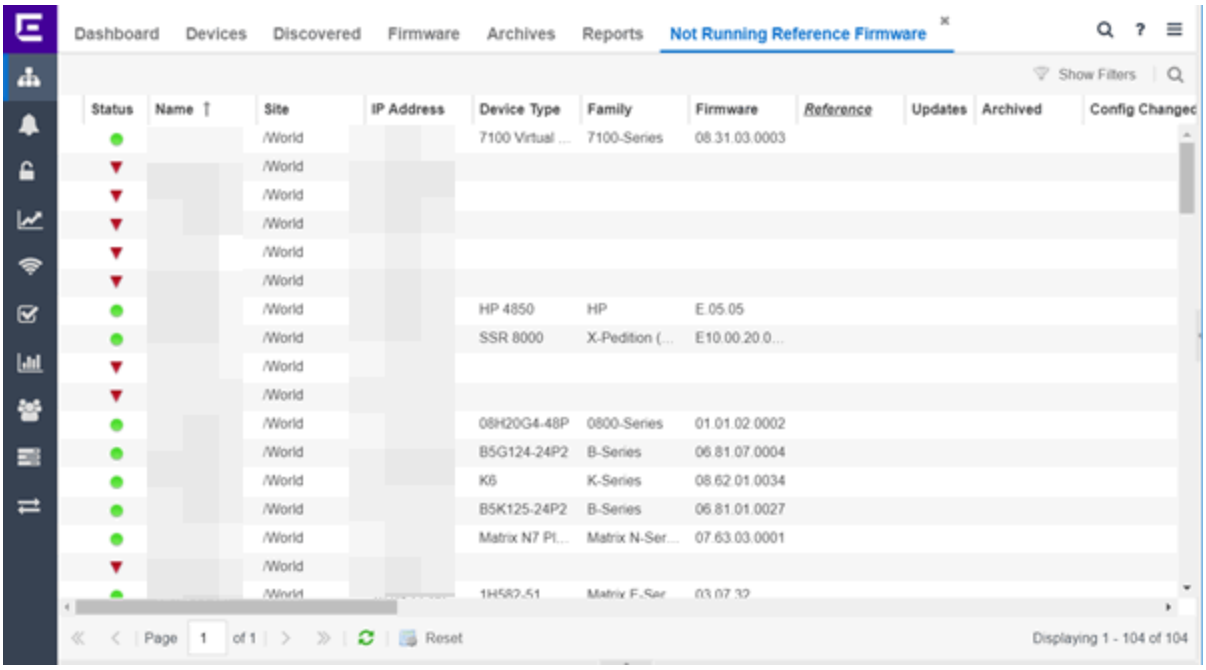
Select the time span for which the report displays from the time span drop-down list. Available options are **Last 24 Hours**, **Yesterday**, **Last 3 Days**, **Last Week**, **Last 2 Weeks**, **Last Month**.

Related Information

- 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.

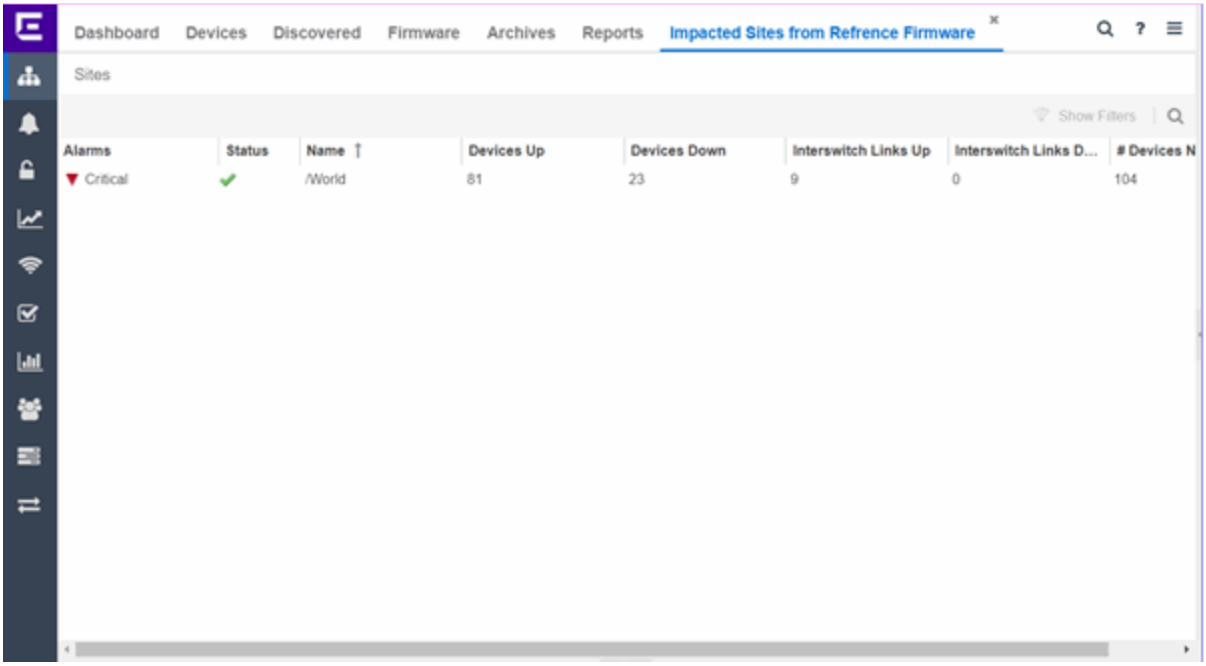
Asset Tag
A unique asset number assigned to the module or component for inventory tracking purposes.

Related Information

- 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.

Related Information

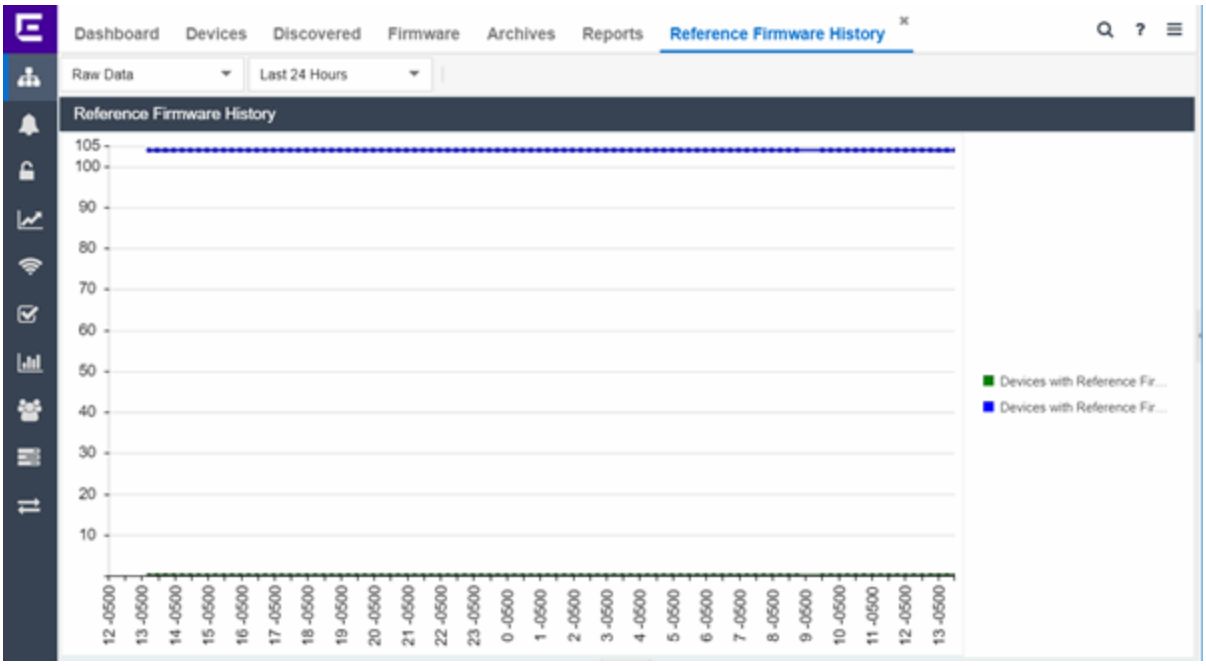
- Impact Analysis Dashboard Overview

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**.



Related Information

- 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
  - CLI Commands
  - Port Tree
  - Interfaces
  - User Sessions
- 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/ TCP Echo)
  - 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
    - Register/ Export Serial Numbers
- Archives
    - Backup Configuration
    - Restore Configuration
    - Compare Last Configurations
    - Inventory Settings
- Tasks
- 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.

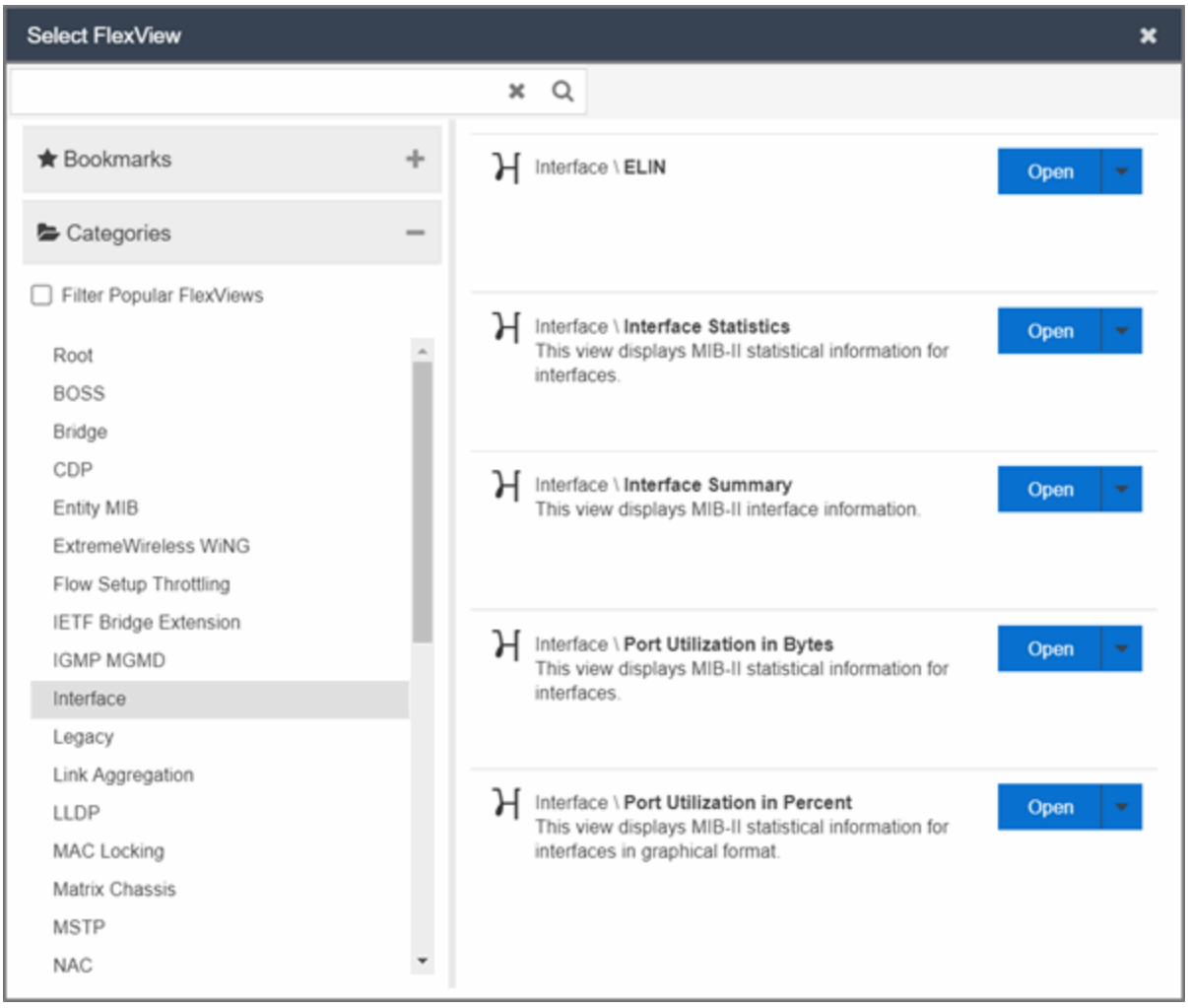
FlexViews

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

CLI Commands

To run commands against multiple devices, use the More Views > CLI Commands option:

1. Select the **Menu** icon (☰) or right-click in the Devices list.
2. Select **More Views** > **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.

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
    - 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.

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**.

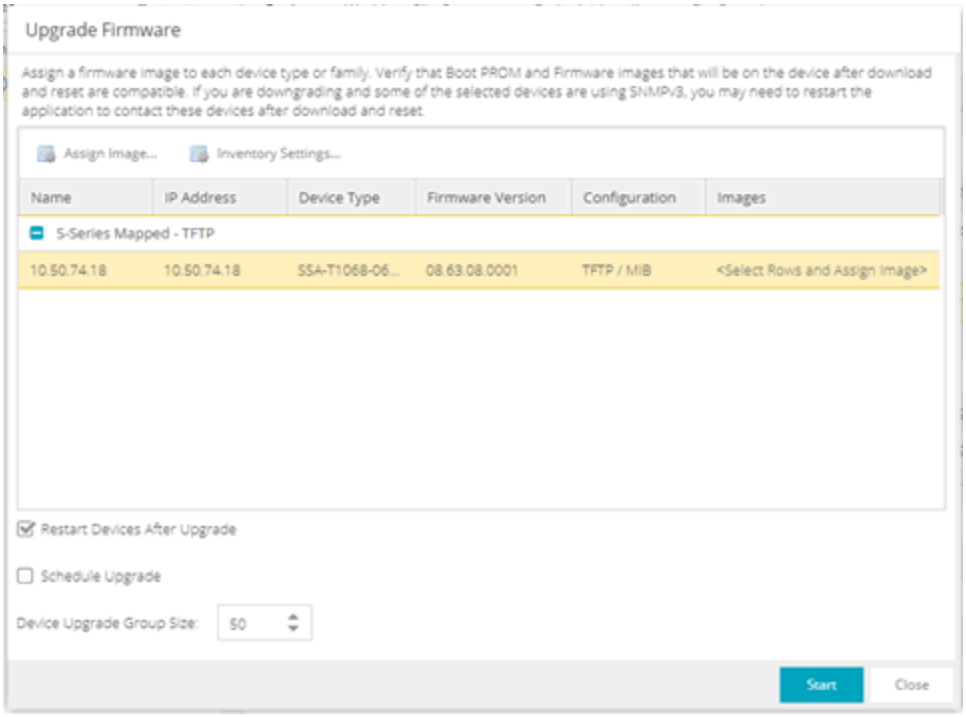
   The alarms on the selected devices clear.

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 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 Profile**.

   The Set Device 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.

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 / TCP Echo)

Select Ping Device (ICMP / TCP Echo) 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 / TCP Echo).**

NOTES: If ExtremeCloud IQ - Site Engine is installed to run as root, an ICMP Request is sent.

If ExtremeCloud IQ - Site Engine is installed to run as non-root user, a TCP Echo Request is sent.

After ExtremeCloud IQ - Site Engine sends either request type, it 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 ExtremeControl engine, ExtremeAnalytics engine, or ExtremeWireless Controller, read through the following notes:

- **ExtremeControl Engine** —When collecting statistics on an ExtremeControl 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 ExtremeControl 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.

Register/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** > **Register/ Export Serial Numbers**.

   The **Register/Export Serial Numbers** window opens.

4. Select whether you want to register or export to a file.
   - **Register**—Collects all the serial numbers for the selected devices and uploads them to Support at Extreme Networks. This feature requires an Extreme Networks account, which you can create through Support at ExtremeNetworks.com. Unless you have entered your account credentials in the ExtremeNetworks.com Update options panel (Console > Tools > Options > Suite Options), you are prompted for them when you register.

     Select the **Refresh the Devices before registering** checkbox if you want to refresh the devices before the serial numbers are collected to ensure the most current information. If you are registering a large number of devices, the refresh could take a long time. Because of this, the refresh operation runs as a background task on the server and you can view the progress of the operation in the Inventory event log (**Alarms and Events** tab).
   - **Export to File**—Collects all the serial numbers for the selected devices and downloads them to the browser in comma separated value (CSV) format. Use this feature to view the serial numbers before registering.

NOTES: Devices without serial numbers (for example, ExtremeWireless controllers) are not included in **Register** feature or the exported into the CSV formatted file.

Serial Numbers for SNMP Managed devices are retrieved from:

- entityMIB objects: entPhysicalSerialNum, entPhysicalClass
- ExtremeXOS-specific: extremeSystemID from extremeSystemCommon

Serial numbers are part of the poll messages exchanged with devices being managed via ZTP+.

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.

Notes:	For VOSS 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.

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.

Notes:	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.
- **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.
- **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 21.11.10, 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.
- **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.
- **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.
- **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** tab 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 

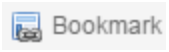
The paging toolbar provides four buttons that let you easily page through the table: first, previous, next, and last page.

Refresh

Use the refresh button to update the data in the table.

Reset 

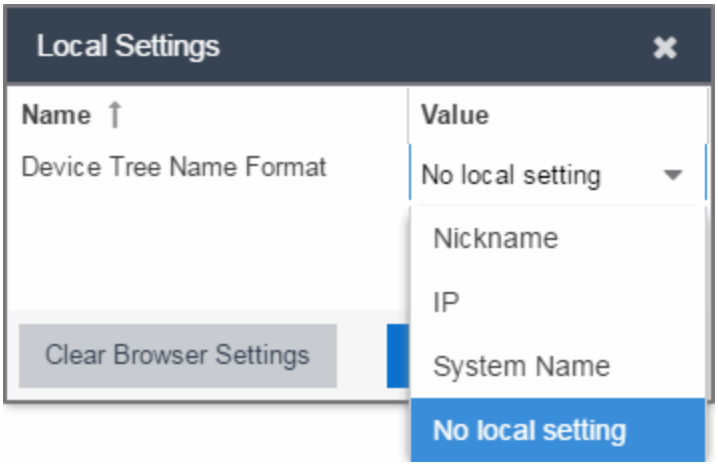
The reset button clears the search field and search results, clears all filters, and refreshes the table.



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.

Related Information

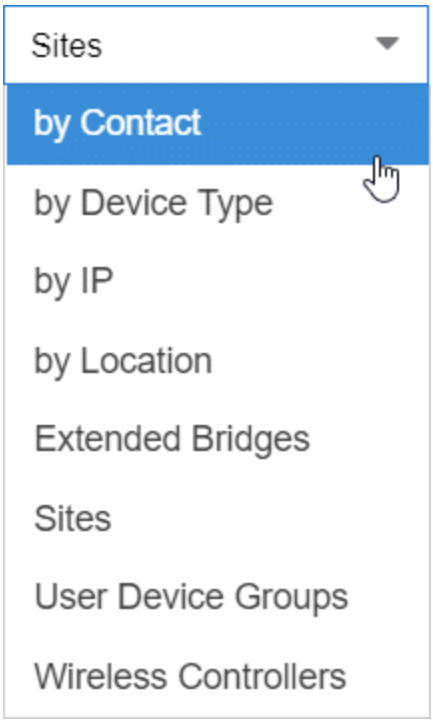
For information on related topics:

- Network Tab
- Sites
- How to Upgrade Firmware
- Create and Edit Maps
- Tasks
- Compare Device Configurations in ExtremeCloud IQ - Site Engine

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.

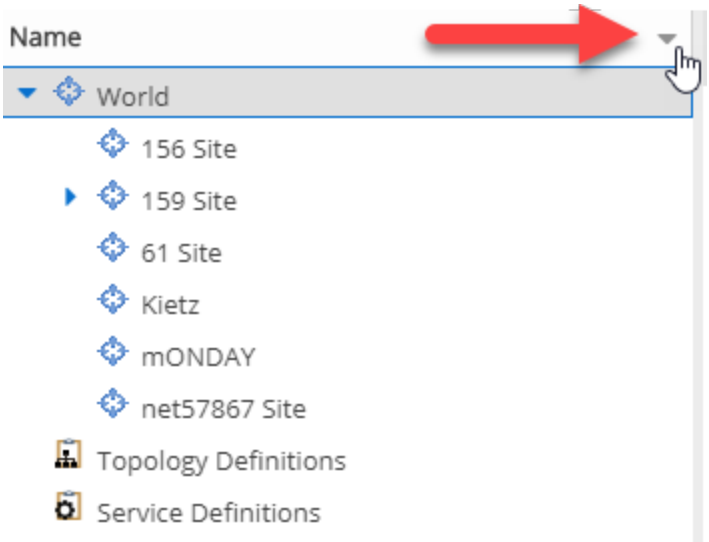
Wireless Controllers

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.

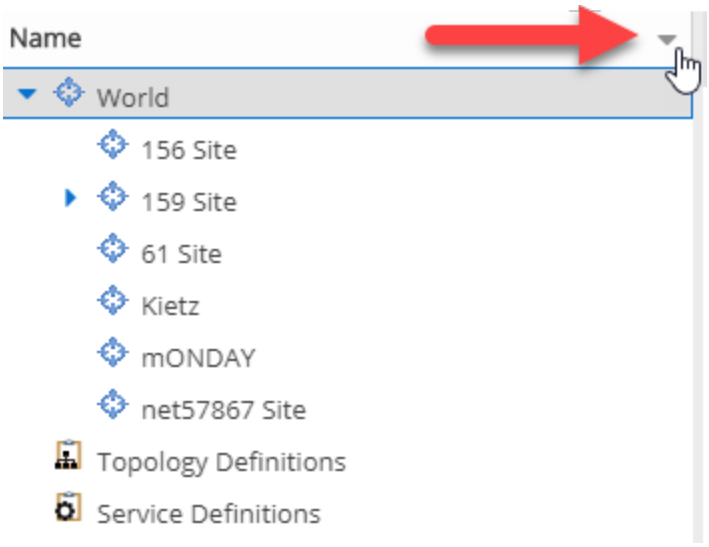
After adding or renaming a item, it may not move to the correct position in the Tree View. Refresh the window to update the items displayed.

Select a device, device group, map, or site in the left-panel and use the right-panel to perform a variety of device operations.

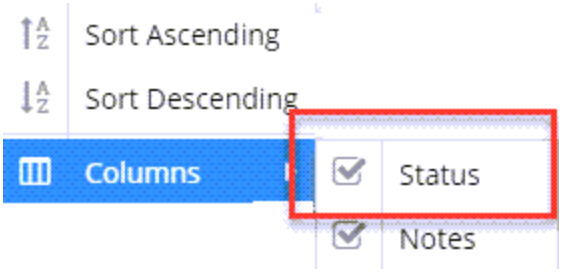
Status

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.



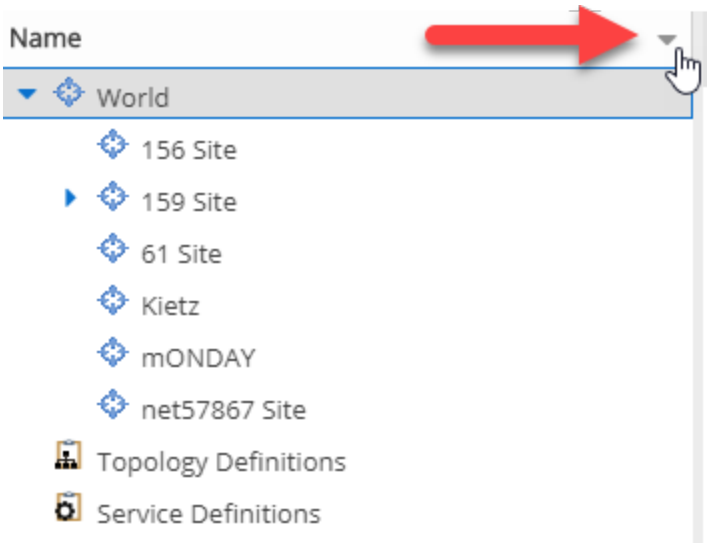
Select the **Columns** > **Status** checkbox from the menu.



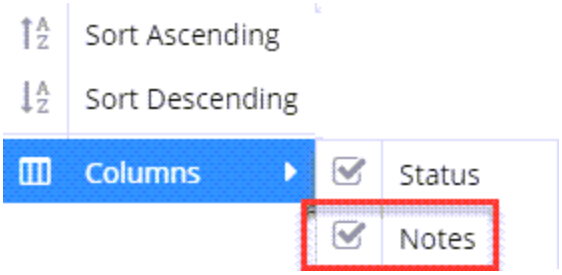
Notes

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.



Related Information

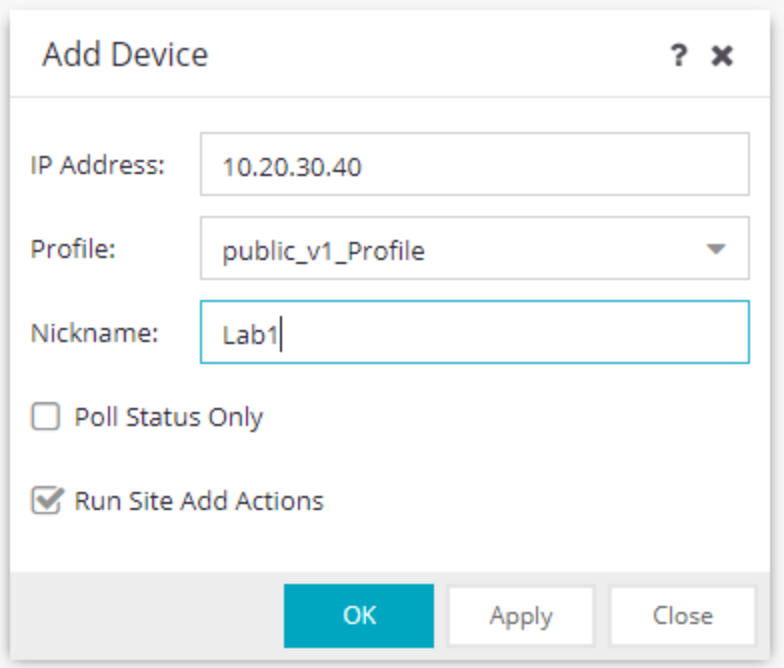
For information on related topics:

- Devices
- Site
- Maps
- How to Create and Edit Maps
- Advanced Map Features

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 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. The **Profile** determines the method by which the device is polled (SNMP or Ping).

Run Site Add Actions

Run Site 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 ad hoc. See Run Site's Add Actions in More Views.

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.

Related Information

For information on related windows:

- Discovered

Configure Device

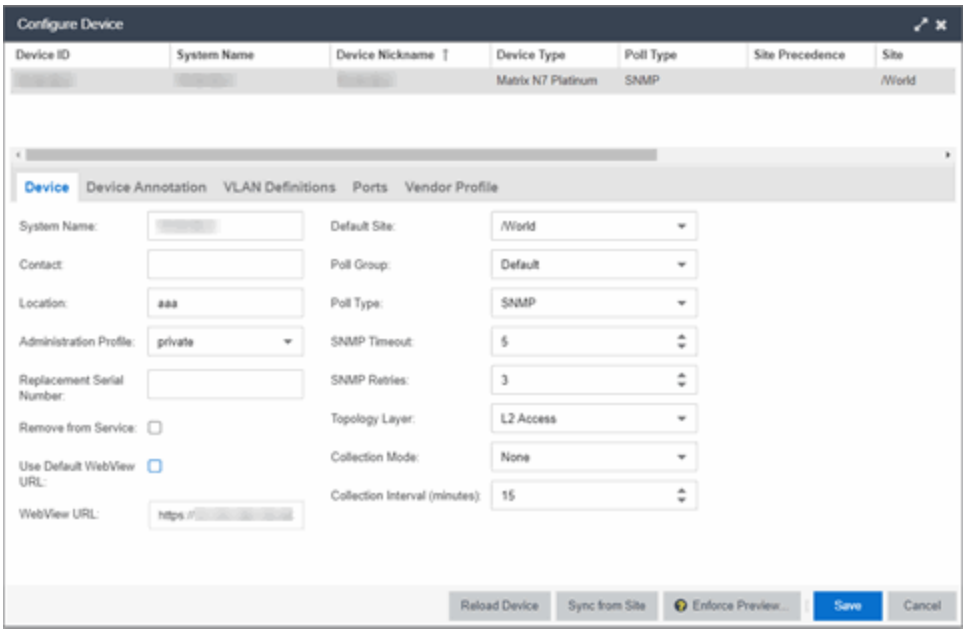
Use this window to configure information for an existing device. From this window you can edit basic information about the device, the device annotation, configure actions for the device, add or remove ports for the device, and configure VLANs for the device.

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
- Topology
- 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://%dIP”. The “%dIP” macro is replaced with the device's actual IP when Launch WebView is attempted.

If the "%dIP” 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 "%dIP” macro is mandatory, so that "%dIP" 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 devices, the default WebView URL ("http://%dIP%" ") 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://%dIP%: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 (SNMPv1or 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.

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 1and 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 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 value entered in this field overrides the default entered in the SNMP Advanced view in the **Administration** > **Options** tab.

Topology Layer

The layer and networking attributes for the device.

Collection Mode

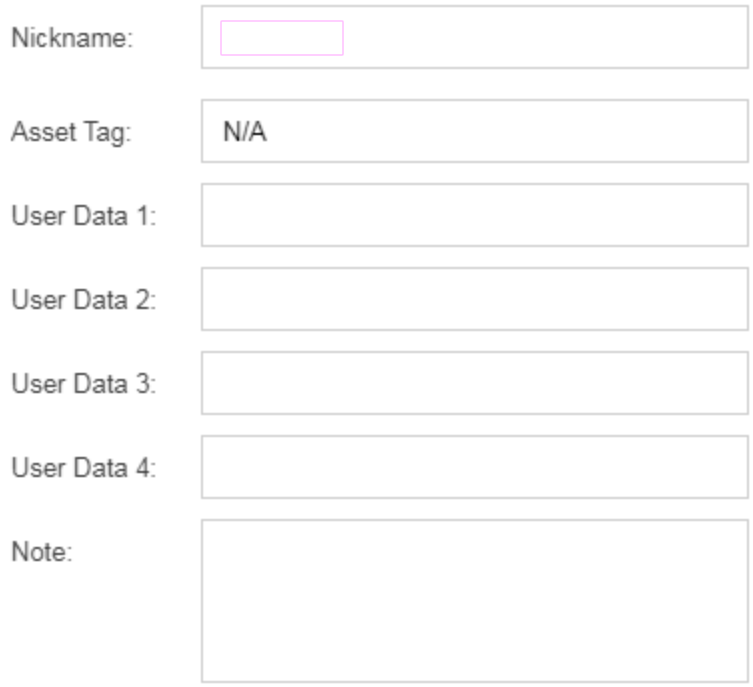
Select **None**, **Threshold Alarms**, or **Historical** from the check box Mode drop-down menu to indicate the mode to collect device statistics.

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

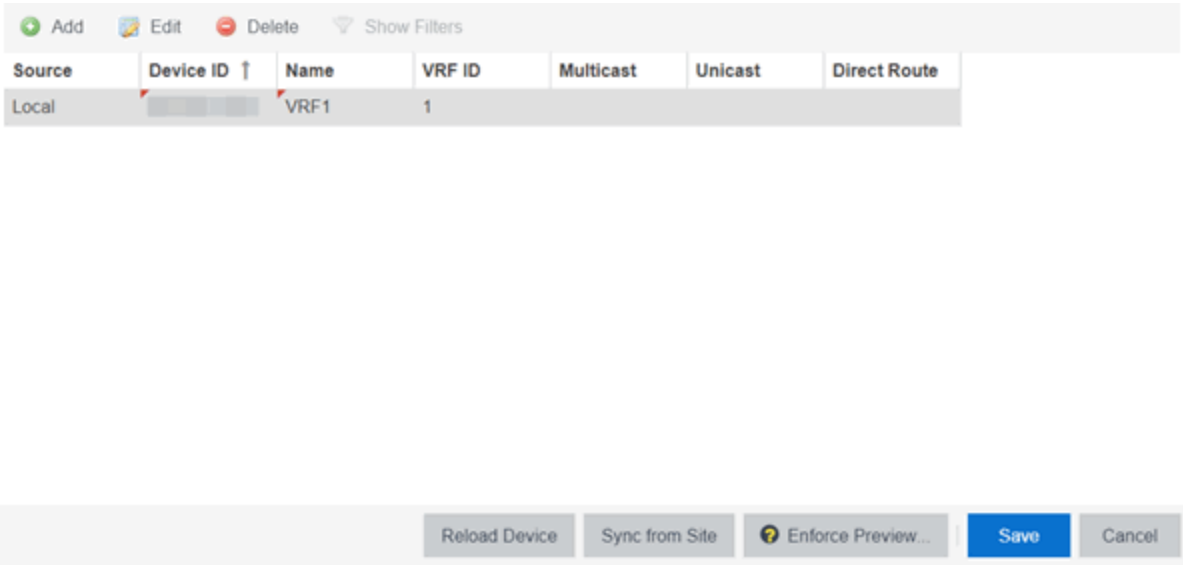
The user-defined information displayed in the devices table in the **User Data** columns. Additionally, enter a backslash "/" between user data to create a device group in a tiered tree structure. For example, to move the device into a device group called "Dorm 1" within a device group called "Campus", 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 1and 4094 that identifies a particular VLAN. VID 1is reserved for the Default VLAN.

VRF ID

Displays the ID number of the VRF associated with the VLAN.

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 1or 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 VOSS devices.

VOSS 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 VOSS 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.

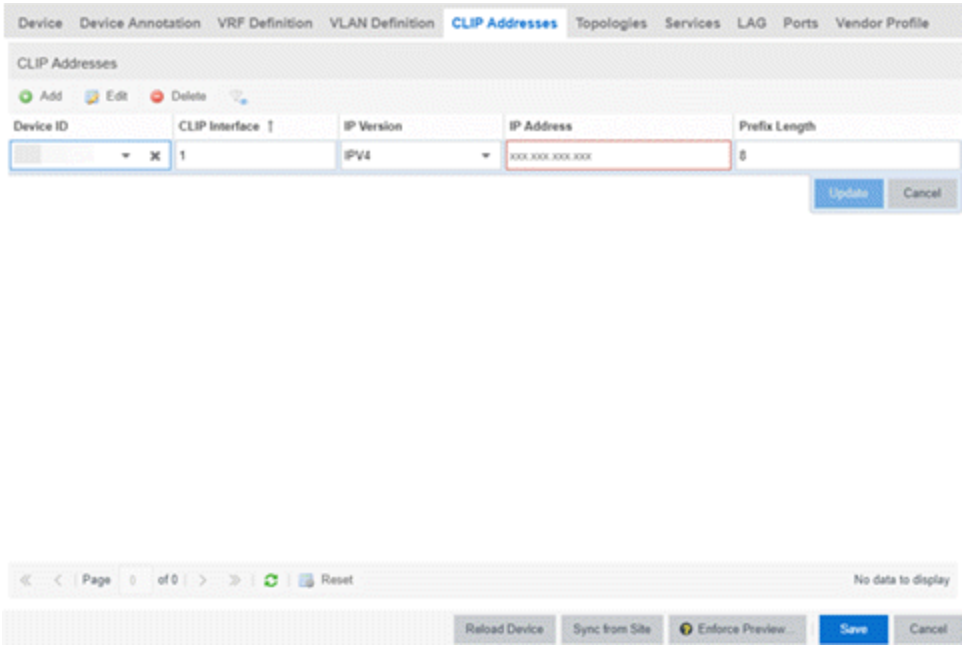
ARP Inspection

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.



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

Select the IP Address version from the drop-down menu: IPV4 or IPV6

IP Address

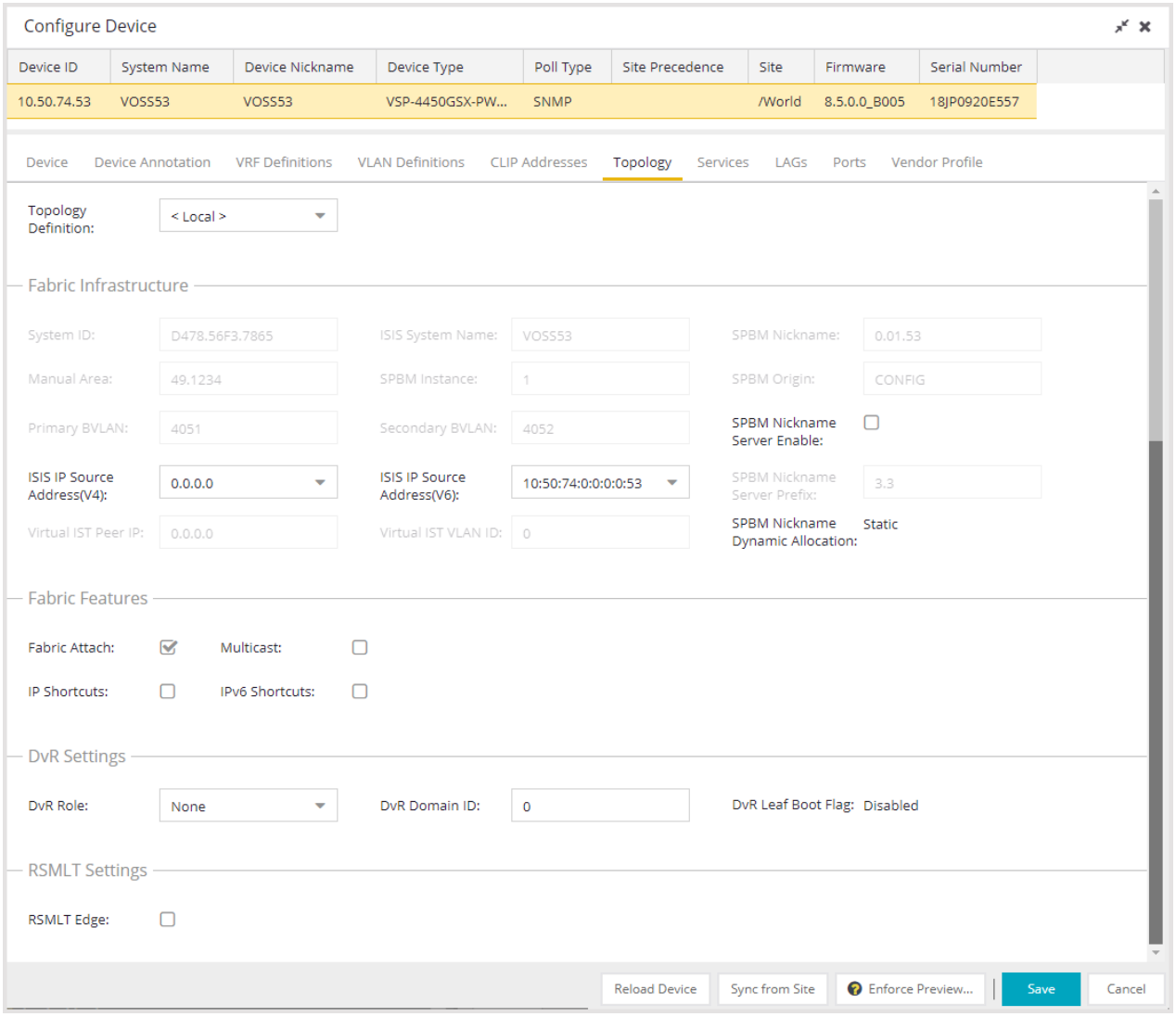
The device's IP Address.

Prefix Length

Enter 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.

Topology

The **Topology** 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 the Nickname Server on a VOSS 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.

SPBM Nickname Server Prefix

This is the 1-byte "x.y" portion of the larger "123.45" 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.

DvR Settings

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.
- Global Backbone - Indicates the device is a standard Fabric Connect device 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.

DvR Leaf Boot Flag

Indicates that the Leaf Boot Flag has been configured for the device (a system workflow is used to set the DvR Leaf Boot Flag to enabled or disabled). If the boot flag is set to Enabled, the DvR Role can be None or Leaf. If the boot flag is set to Disabled, the DvR Role can be None, Controller or Global Backbone.

Fabric Features

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:

VOSS, 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

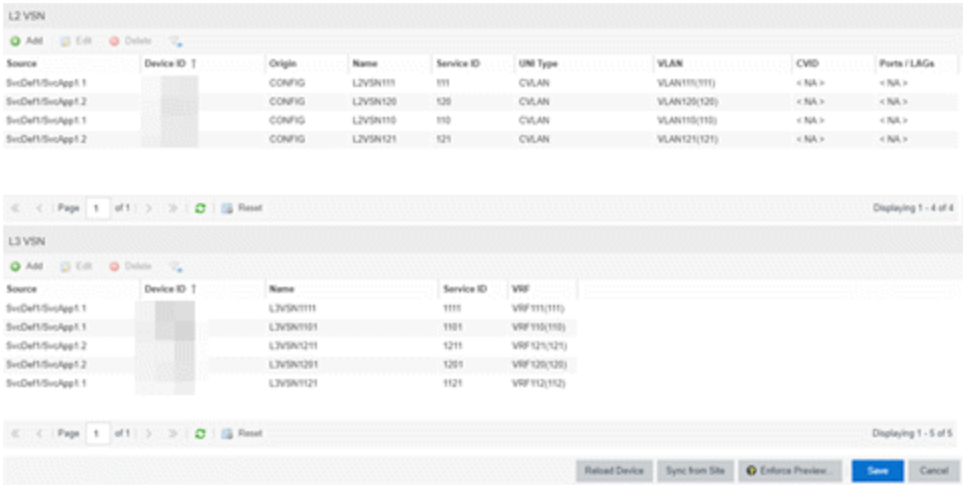
Select the check box to enable Multicast for the device.

IPv6 Shortcuts

Select the check box to enable IPv6 Shortcuts for the device.

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 assigned to the fabric service.

L3 VSN

Source
Indicates the service definition from which the service is inherited.

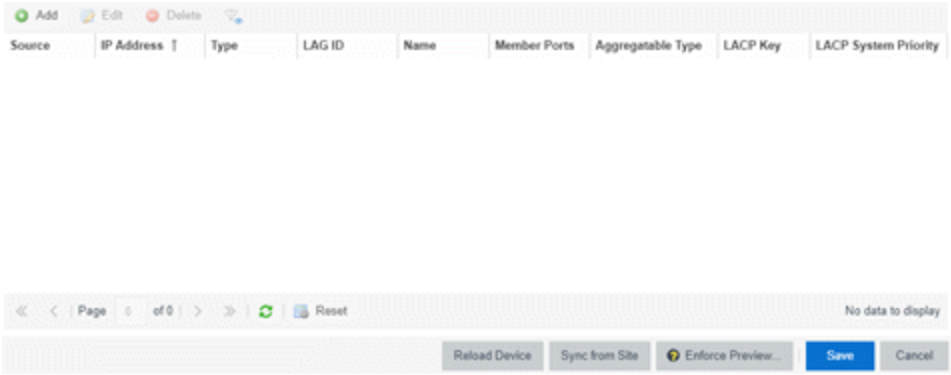
Name
The name of the Layer 3 service.

Service ID
The ID number assigned to the service.

VRF
Select the virtual routing and forwarding definition included as part of the service.

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:

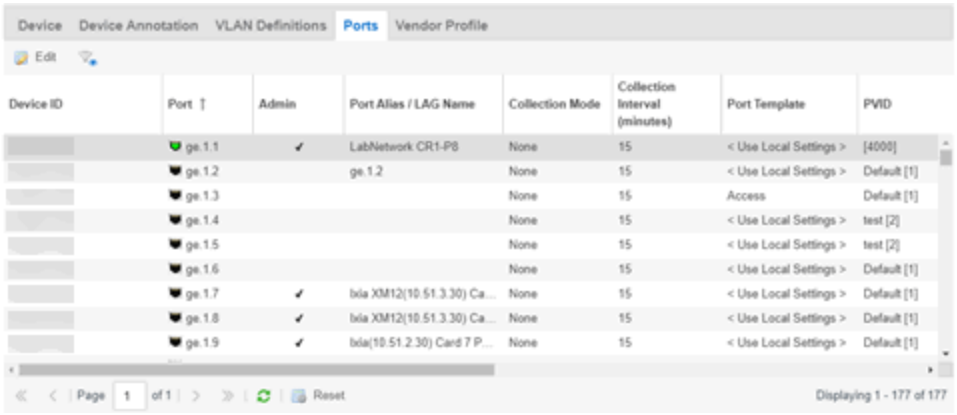
- Static —the LAG is static.
- LACP —the LAG is dynamic via LACP.

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 1and 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 devices and provision them as FA Proxy devices. Select "Fabric Attach" or "" from the drop-down list to enable the port on a VOSS device (acting as FA Server) to connect to an ExtremeXOS device (acting as FA Proxy).

- **Fabric Attach** - Enable Fabric Attach server functionality on the port of a VOSS device acting as a Fabric Attach server) to connect to an ExtremeXOS device (acting as a Fabric Attach proxy).
- **Fabric Attach and Switched UNI** - Enable Fabric Attach server functionality on the port of a VOSS device acting as a Fabric Attach server) to connect to an ExtremeXOS 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 VOSS 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. Select the check box to enable ZTP+ devices being discovered to broadcast MVRP (Multiple VLAN Registration Protocol) information. Select the appropriate logging level from the drop-down list.

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.

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.

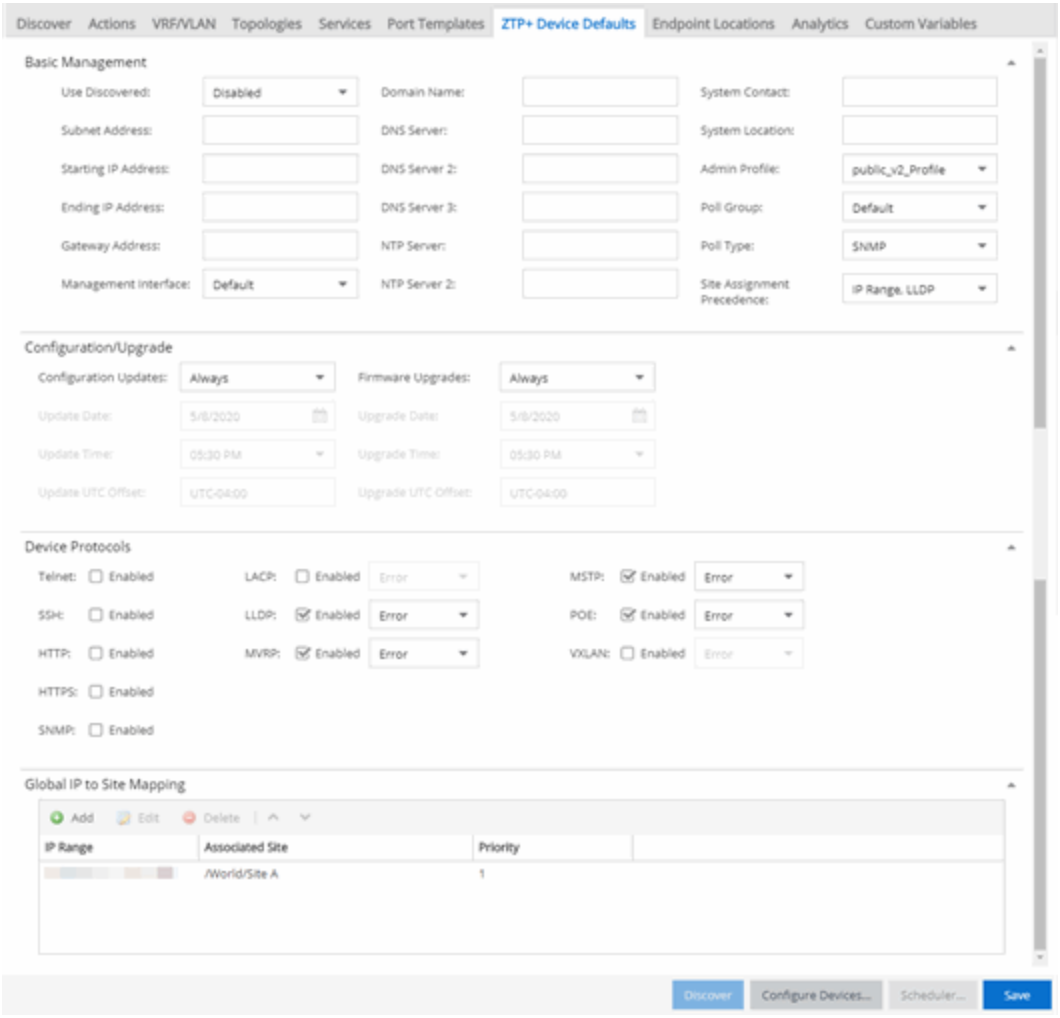
PoE Priority
Indicates the priority of PoE for the port; **LOW**, **HIGH**, or **CRITICAL**.

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 (a VLAN or **Out-Of-Band** management) the device uses for Management and assigns the device IP to that interface.

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

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. Select the appropriate logging level from the drop-down list.

LLDP

Select the check box to enable LLDP (Link Layer Discovery Protocol) access on the ZTP+ device. Select the appropriate logging level from the drop-down list.

MSTP

Select the check box to enable MSTP (Multiple Spanning Tree Protocol) access on the ZTP+ device. Select the appropriate logging level from the drop-down list.

MVRP

Select the check box to enable MVRP (Multiple VLAN Registration Protocol) access on the ZTP+ device. Select the appropriate logging level from the drop-down list.

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.

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.

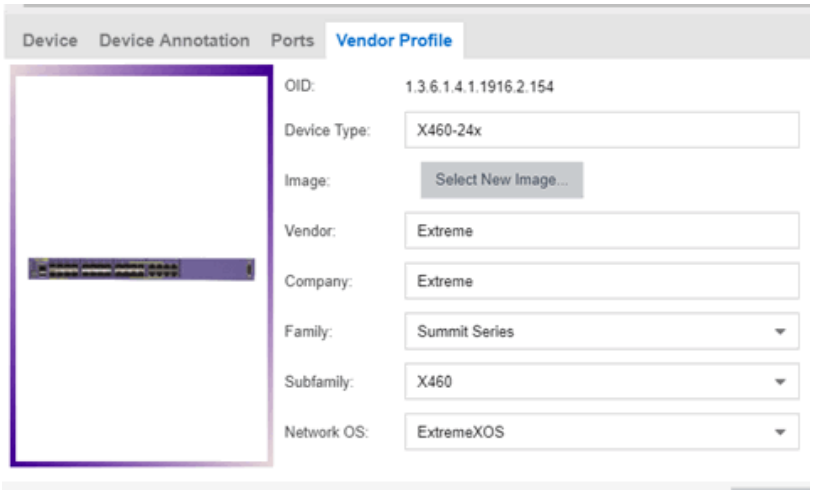
Test

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

Reload Device
Select to read configuration information from the device to populate ExtremeCloud IQ - Site Engine. **Reload Device** reads the configuration (e.g. VLAN Definition, Ports, Port VLANs) from the device and reloads it in ExtremeCloud IQ - Site Engine.

NOTE: Selecting **Reload 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, topology, 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.

Related Information

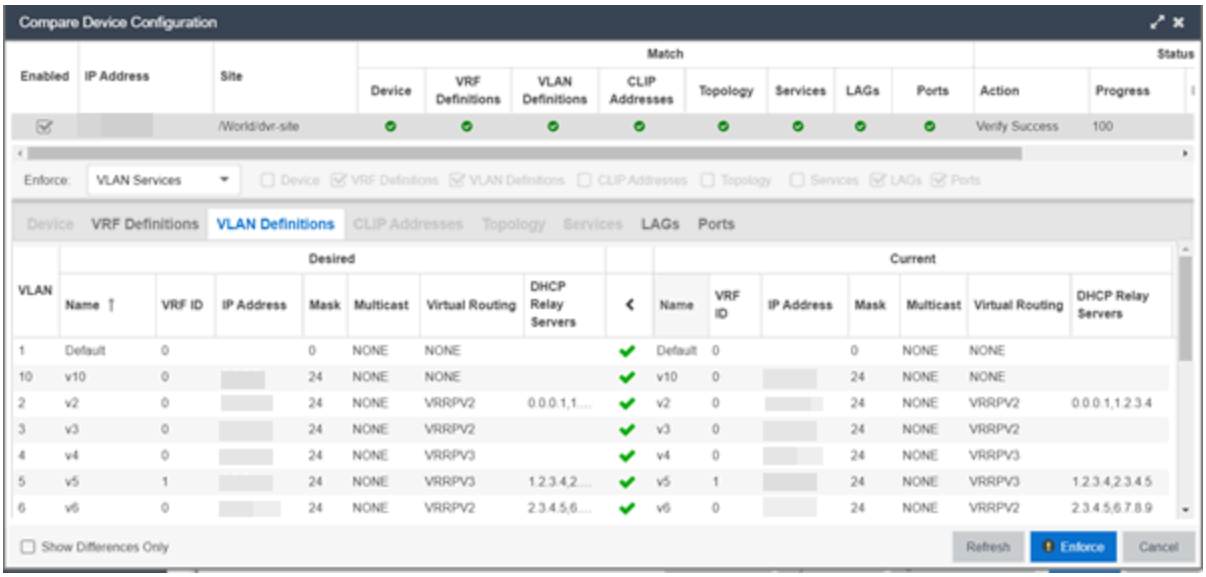
For information on related windows:

- Edit Policy Mapping Configuration Window

Compare Device Configuration

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

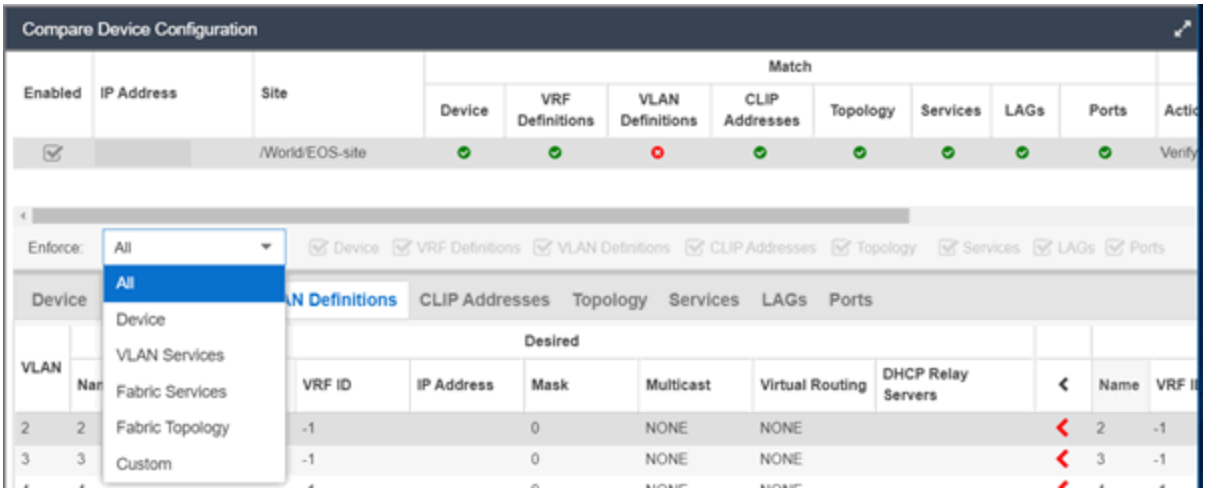
Devices on which the current configuration matches the desired configuration display a check icon (), while devices on which differences are detected display a red x ().

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.

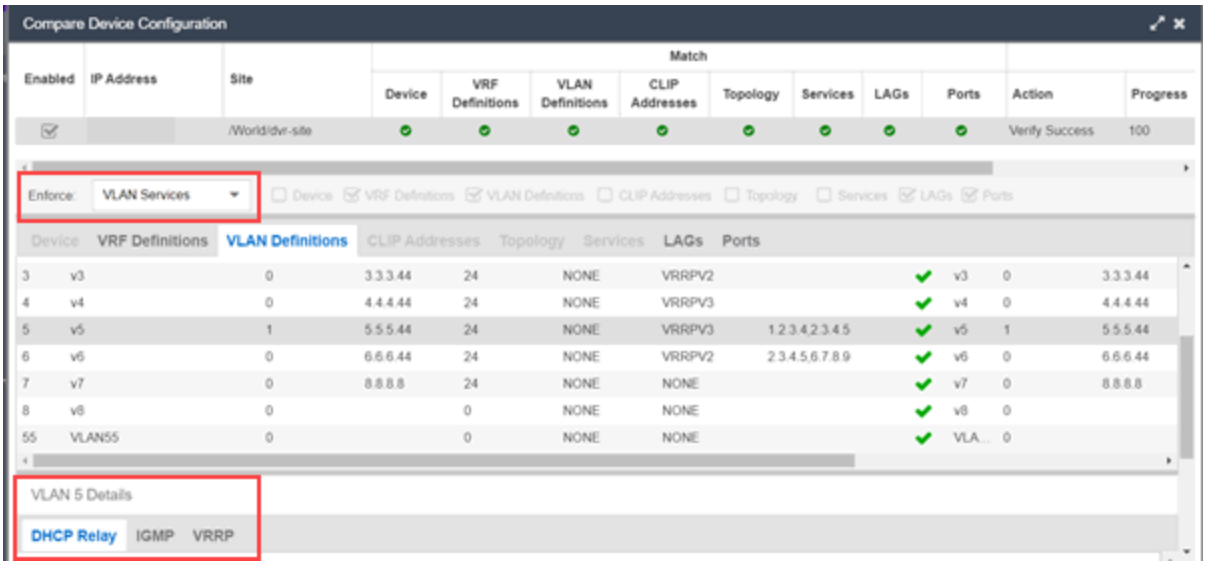
Device

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 Topology 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
- Topology Services

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
- Topology
- 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.

Mask
Displays the IP/ subnet mask.

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 1or 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 VOSS devices.

VOSS 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 VOSS 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

Topology

The **Topology** 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.

System ID

The system-defined fabric service identifier assigned to the device. The default is the MAC address for the device.

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.

Primary BVLAN

The Primary Backbone VLAN. This information is configured on the **Sites > Topology Definition** tab.

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.

System Name

The system name of the device.

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.

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.

SPBM Nickname
A value that other fabric devices use to identify the device. The SPBM nickname must be unique within the 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
Displays the identifying number for the DvR domain.

Fabric Attach
The check box is selected if Fabric Attach functionality is supported.

IP Shortcuts
The check box is selected if IPv4 Shortcuts are enabled for the device.

Multicast
The check box is selected if Multicast is enabled for the device.

IPv6 Shortcuts
The check box is selected if IPv6 Shortcuts are enabled for the device.

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

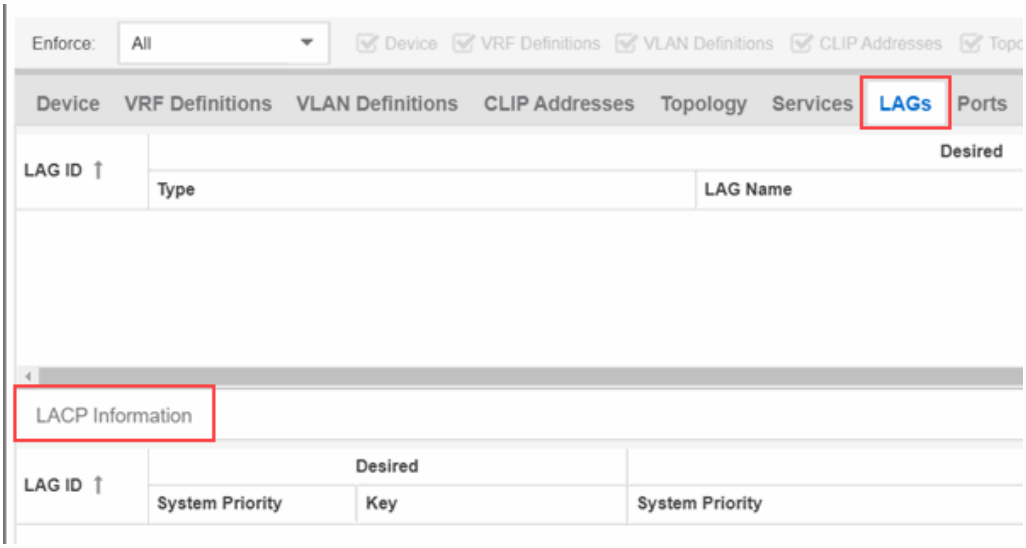
Displays the ports that are included in the LAG.

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 1and 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 1through 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 devices and provision them as FA Proxy devices. Select "Fabric Attach" or "" from the drop-down list to enable the port on a VOSS device (acting as FA Server) to connect to an ExtremeXOS device (acting as FA Proxy).

- **Fabric Attach** - Enable Fabric Attach server functionality on the port of a VOSS device acting as a Fabric Attach server) to connect to an ExtremeXOS device (acting as a Fabric Attach proxy).
- **Fabric Attach and Switched UNI** - Enable Fabric Attach server functionality on the port of a VOSS device acting as a Fabric Attach server) to connect to an ExtremeXOS 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 VOSS 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

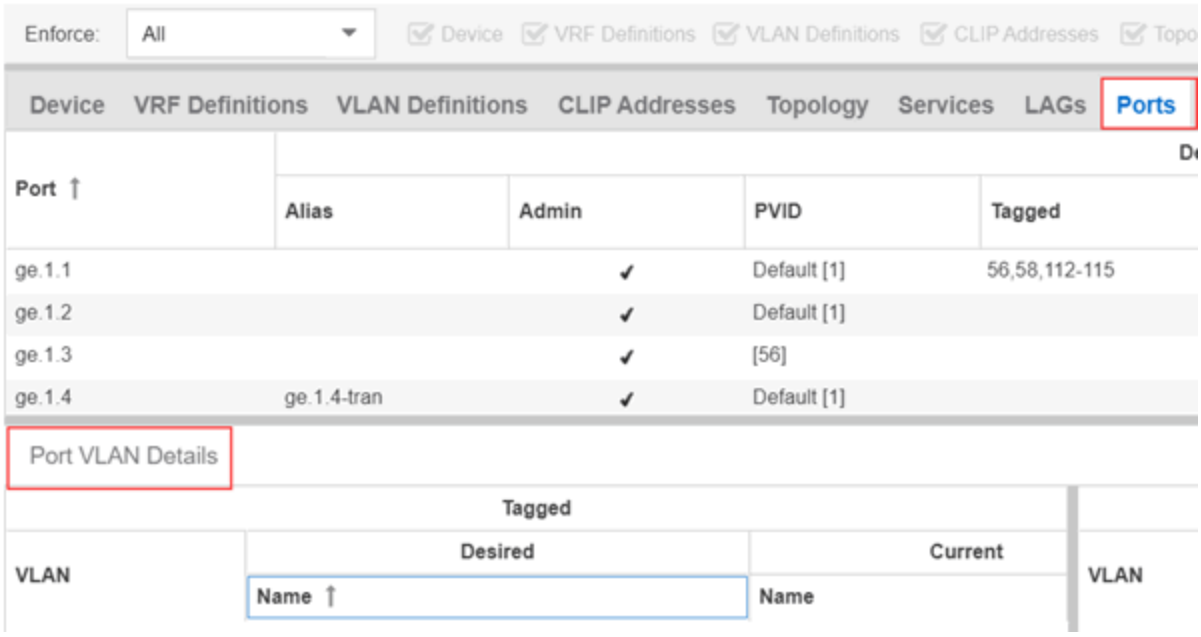
Indicates whether SLPP Guard is enabled on the port. Use SLPP Guard to provide additional loop protection to protect wiring closets from erroneous connections. SLPP Guard requires **SLPP** to be enabled. SLPP detects loops in an SMLT network. Because SMLT networks disable Spanning Tree (STP), Rapid Spanning 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 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.

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.

Related Information

For information on related topics:

- VLAN Concepts
- Configure Device
- Site Tab

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**.

Related Information

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 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
```

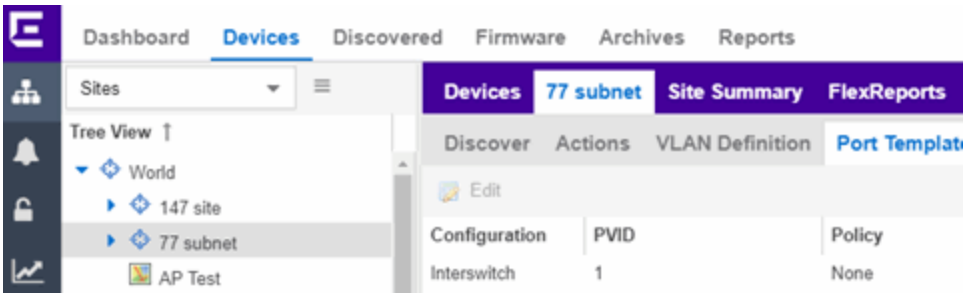
The **Sites tab** is divided into multiple sections, which you can expand to display more information.

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
- Topologies
- Services
- LAG Topologies
- Port Templates
- ZTP+ Device Defaults

- Endpoint Locations
- Analytics
- Custom Variables

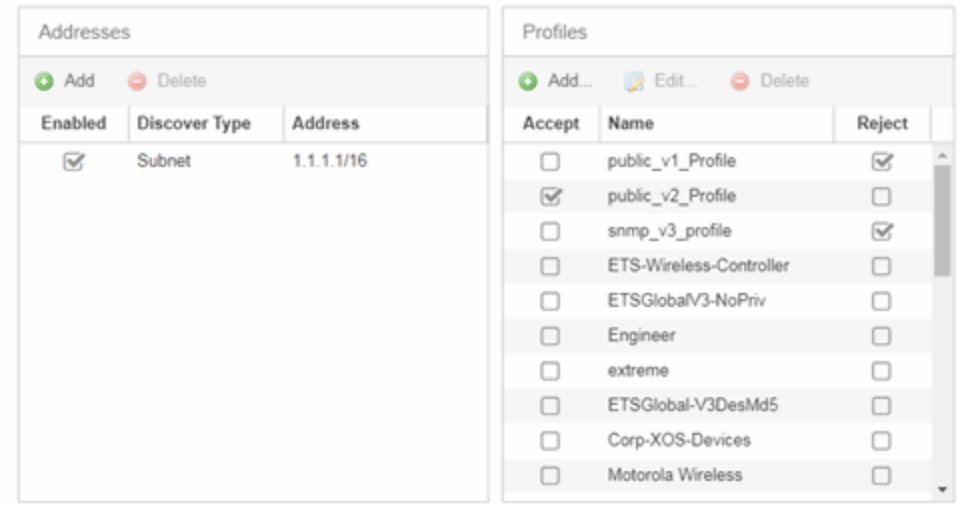
Additionally, the bottom of the tab contains buttons to save your configurations in ExtremeCloud IQ - Site Engine and on the devices included in the site.

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.

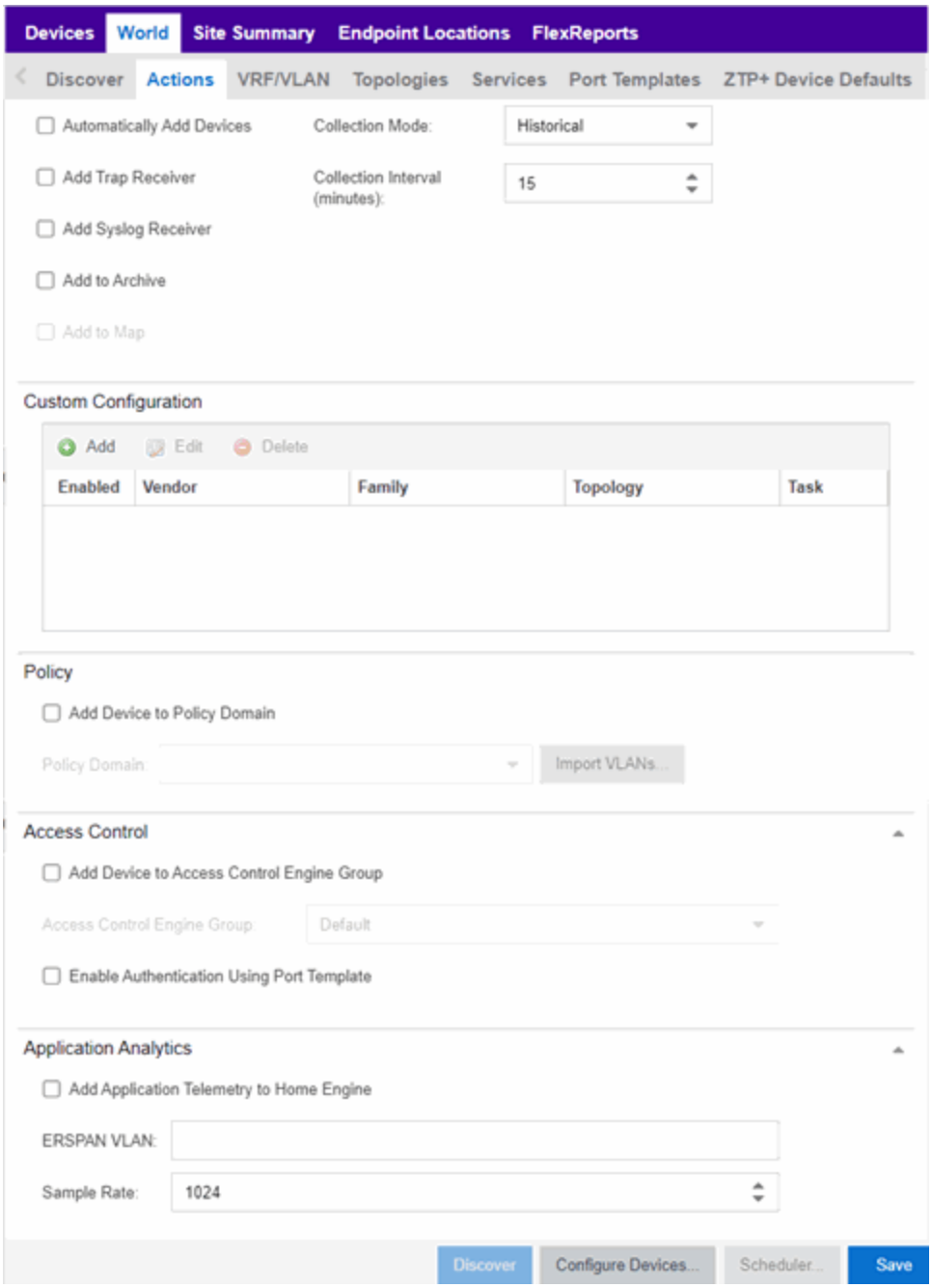
Click the **Discover** button at the bottom of the tab to begin the device discover. The results of the Discover process are displayed in the left-panel tree when added to the ExtremeCloud IQ - Site Engine database.

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.

ExtremeControl

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 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 Application Telemetry to Home Engine

Select this checkbox to add application telemetry to the ExtremeAnalytics engine configured as the site's home engine.

ERSPAN VLAN

Enter the Encapsulated Remote Switch Port Analyzer (ERSPAN) VLAN to add to devices added to the site.

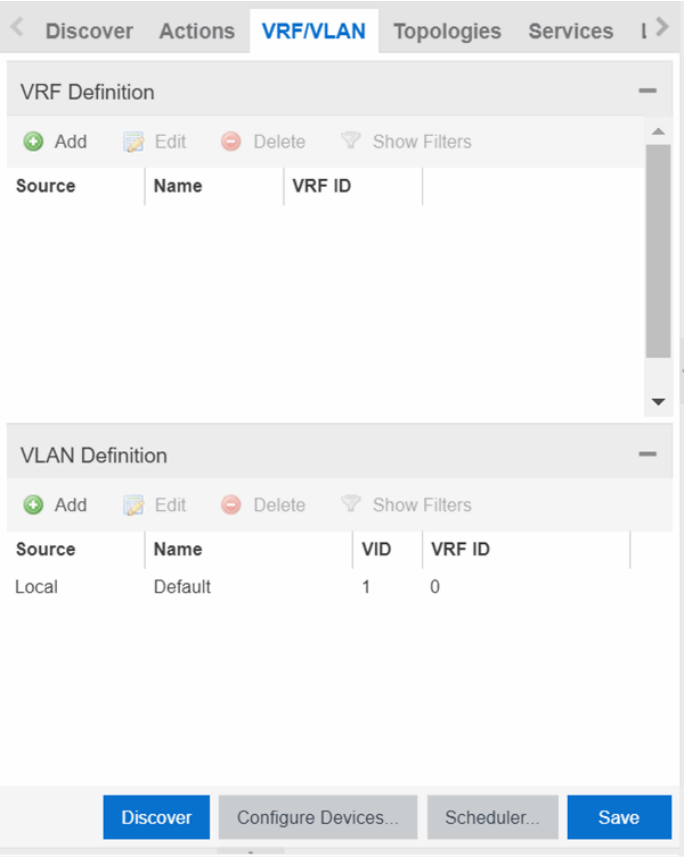
Sample Rate

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.

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 1and 4094 that identifies a particular VLAN. VID 1is 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 1or 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 VOSS 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

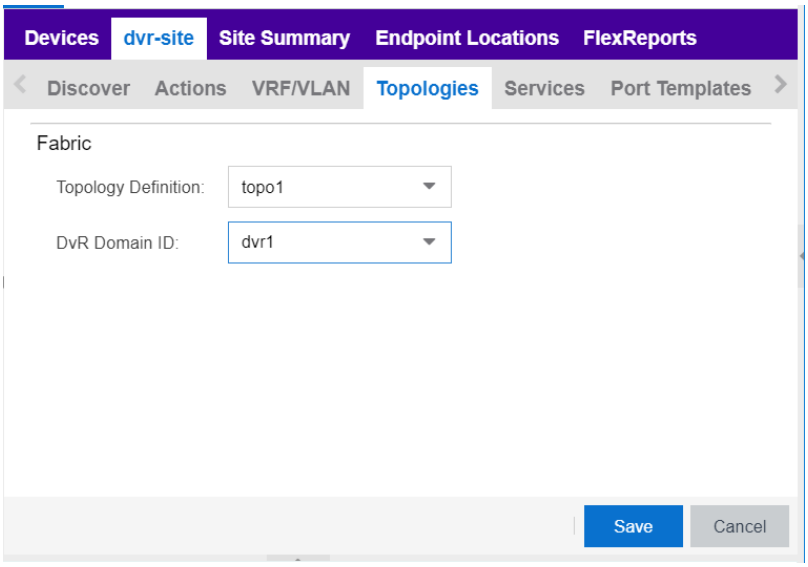
Indicates the site from which the DHCP Relay Server is inherited. Currently, the VLAN definition Source can only be **Local**, indicating the DHCP Relay Server is configured in the current site.

Server IP

The IP address of the DHCP server.

Topologies

The **Topologies** 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

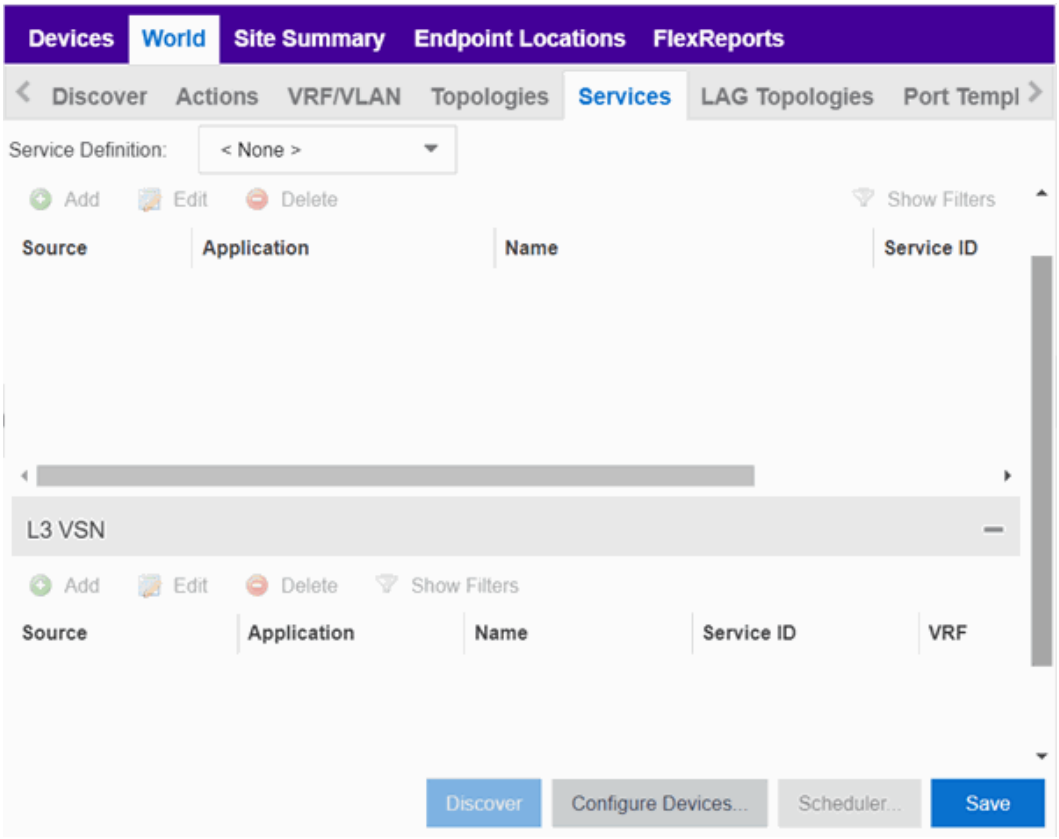
Select the DvR Domain ID that applies to the site. The DvR Domain IDs available in the drop-down list are configured in the **Topology Definition** tab.

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

Application
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.

VLAN
The VLAN assigned to the fabric service.

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.

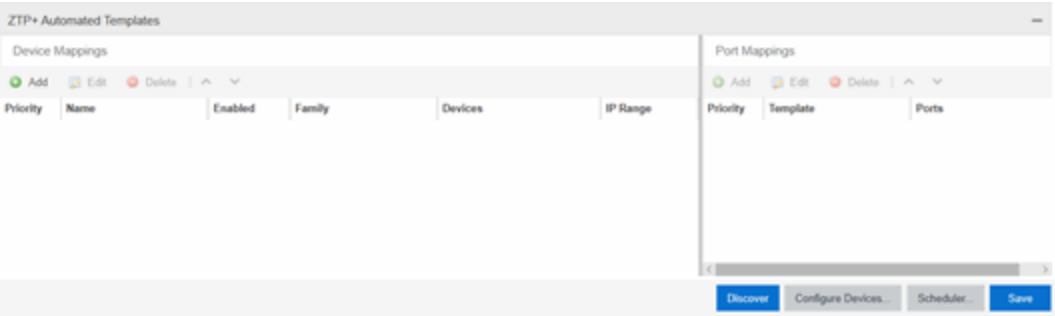
L2 ISID
The service instance identifier.

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

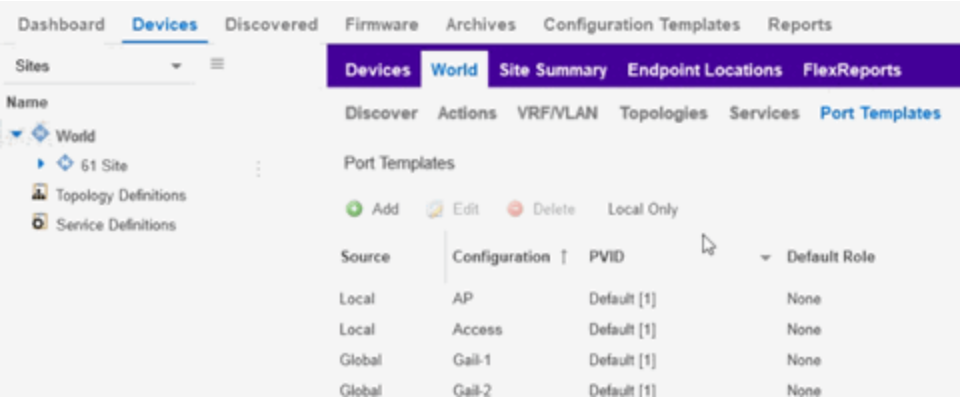
The **Port Templates** tab has two panels. The top panel displays information about user-defined port templates. For more information, see Port Templates Panel.

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.

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.

ExtremeCloud IQ - Site Engine can extend FA functionality to ExtremeXOS devices

and provision them as FA Proxy devices. Select "Fabric Attach" or "" from the drop-down list to enable the port on a VOSS device (acting as FA Server) to connect to an ExtremeXOS device (acting as FA Proxy).

- **Fabric Attach** - Enable Fabric Attach server functionality on the port of a VOSS device acting as a Fabric Attach server) to connect to an ExtremeXOS device (acting as a Fabric Attach proxy).
- **Fabric Attach and Switched UNI** - Enable Fabric Attach server functionality on the port of a VOSS device acting as a Fabric Attach server) to connect to an ExtremeXOS 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 VOSS 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. Select the checkbox to enable ZTP+ devices being discovered to broadcast MVRP information. Select the appropriate logging level from the drop-down list.

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.

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 Panel

The **ZTP+ Automated Templates** panel 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.

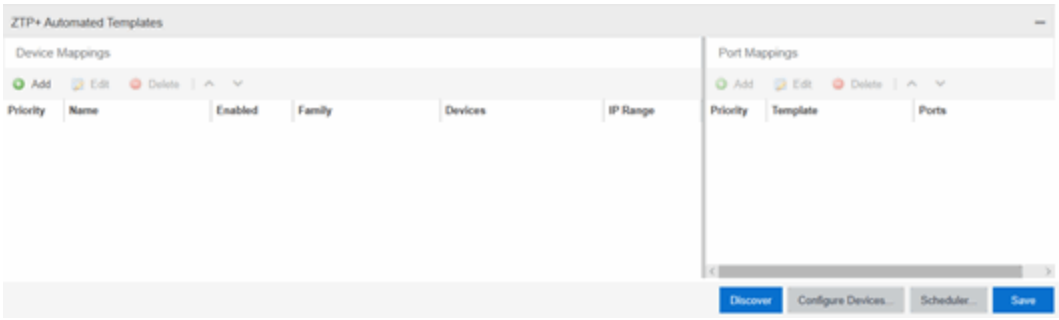
NOTE: ExtremeCloud IQ - Site Engine supports automated port templates for ZTP+ devices only.

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:

- 12.3.4 (v4)
- 1111:2222::3333:4444 (v6)
- 12.3.4/24 (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"
  - EXOS: "1" or "1,3,5,7"
  - EXOS 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"
  - EXOS: "5-7" or "5-7, 9-12, 15-19"

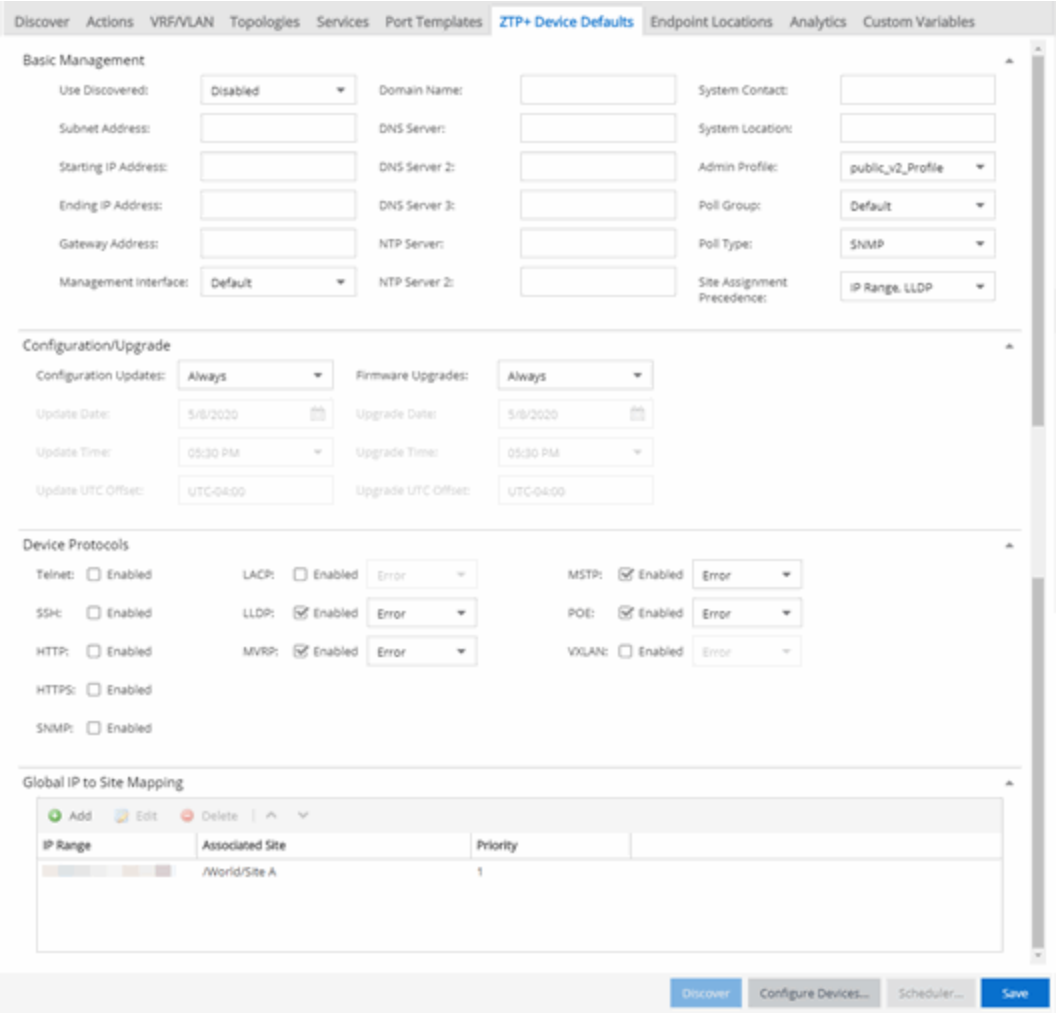
    - EXOS Stack: "1:5 - 1:7" or "1:5-1:7, 2:9-2:12, 3:15-3:19"
    - SLX: "Ethernet 0/1-Ethernet 0/4" or "Ethernet 0/1-Ethernet 0/5, Ethernet 0/8-Ethernet 0/15"
  - Wildcarding:
    - "*" is always allowed, matches anything, useful as default rule at the end of a set of bindings
    - In a single port scenario, 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/*"
      - EXOS: "*"
      - EXOS 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**.

  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 (SNMPv1or 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+**, 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**.

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 set:

- **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 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

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. Select the appropriate logging level from the drop-down list.

LLDP
Select the checkbox to enable LLDP (Link Layer Discovery Protocol) access on the ZTP+ device. Select the appropriate logging level from the drop-down list.

MSTP

Select the checkbox to enable MSTP (Multiple Spanning Tree Protocol) access on the ZTP+ device. Select the appropriate logging level from the drop-down list.

MVRP

Select the checkbox to enable MVRP (Multiple VLAN Registration Protocol) access on the ZTP+ device. Select the appropriate logging level from the drop-down list.

POE

Select the checkbox to indicate the ZTP+ devices being discovered for the site are electrically powered via the 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.

Global IP To Site Mapping

IP Range

Select **Add** or **Edit** to enter a single IP address or an IP range.

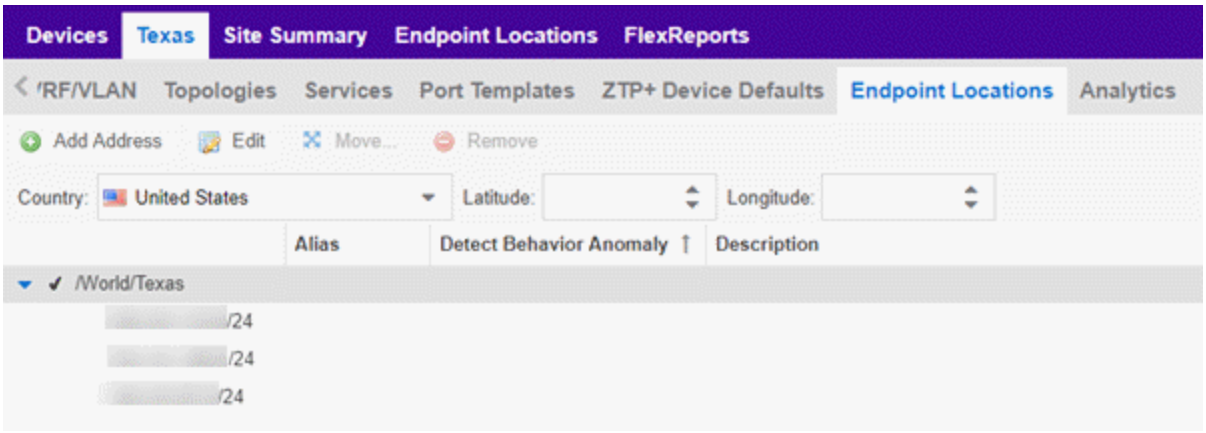
Associated Site

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.

Detect Behavioral Anomaly
Select the checkbox to enable ExtremeCloud IQ - Site Engine functionality that alerts you in the event unexpected behavior is detected for the site or its specified subnet.

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

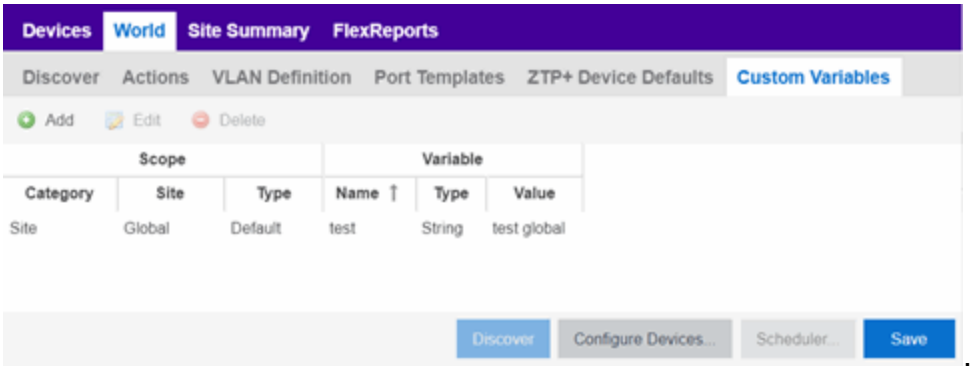
Displays the ExtremeAnalytics engine located with the devices associated with the site.

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.

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.

Related Information

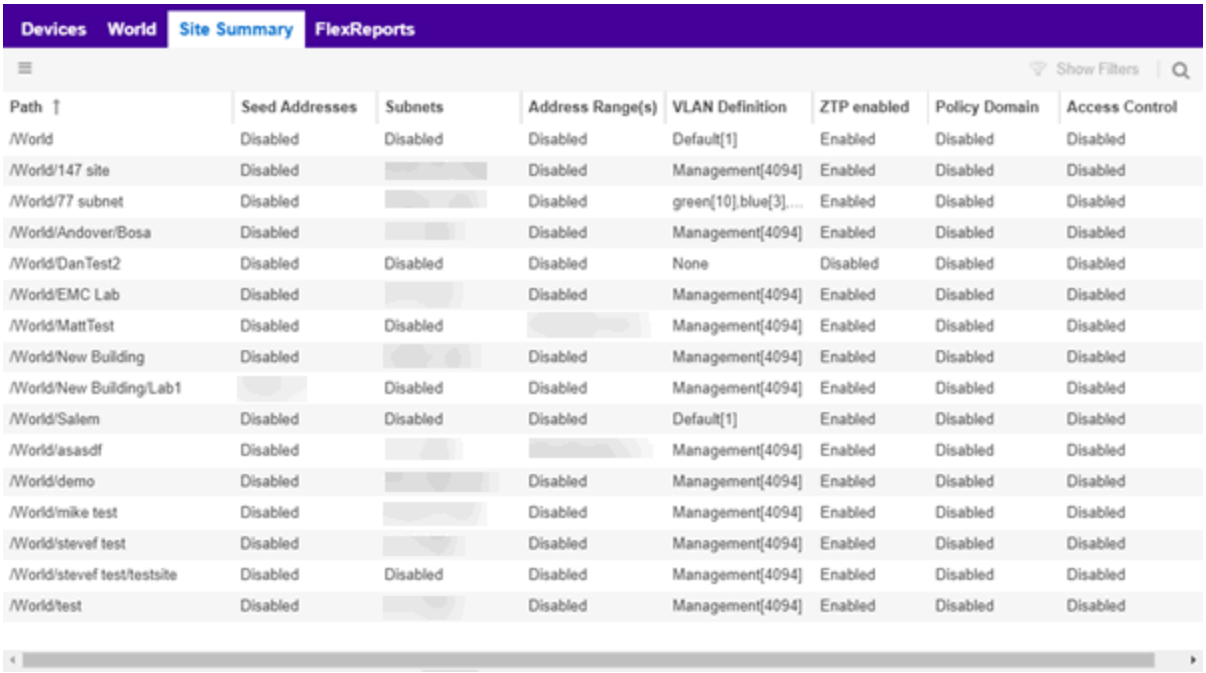
For information on related topics:

- 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 ExtremeControl'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.

Enable Behavioral Anomaly Detection
Indicates whether ExtremeCloud IQ - Site Engine alerts you in the event unexpected applications are accessed on your network.

Related Information

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.

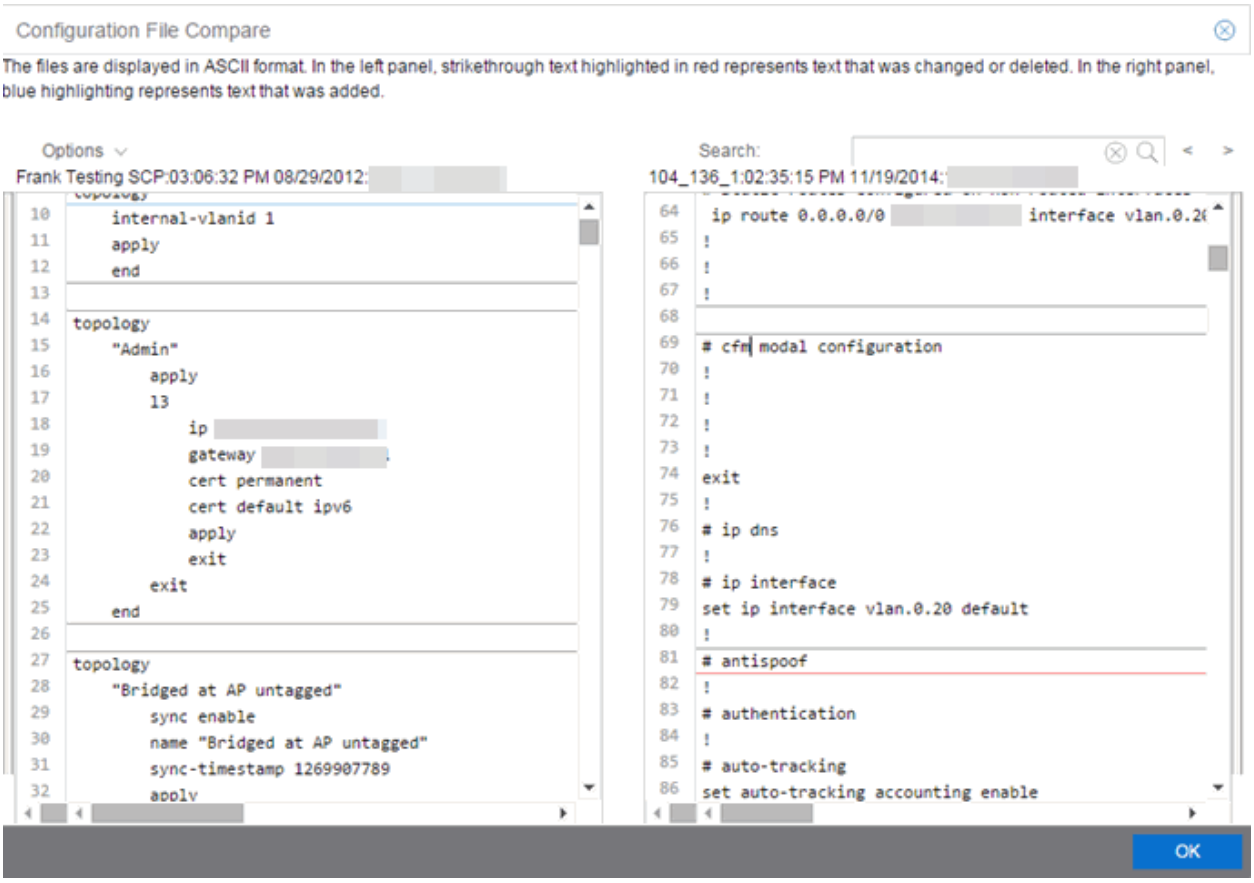
Select the Device > Device Archives report. Select the **Archive Details** tab in the right panel and then select the **Archives by Device** sub-tab.

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.

Related Information

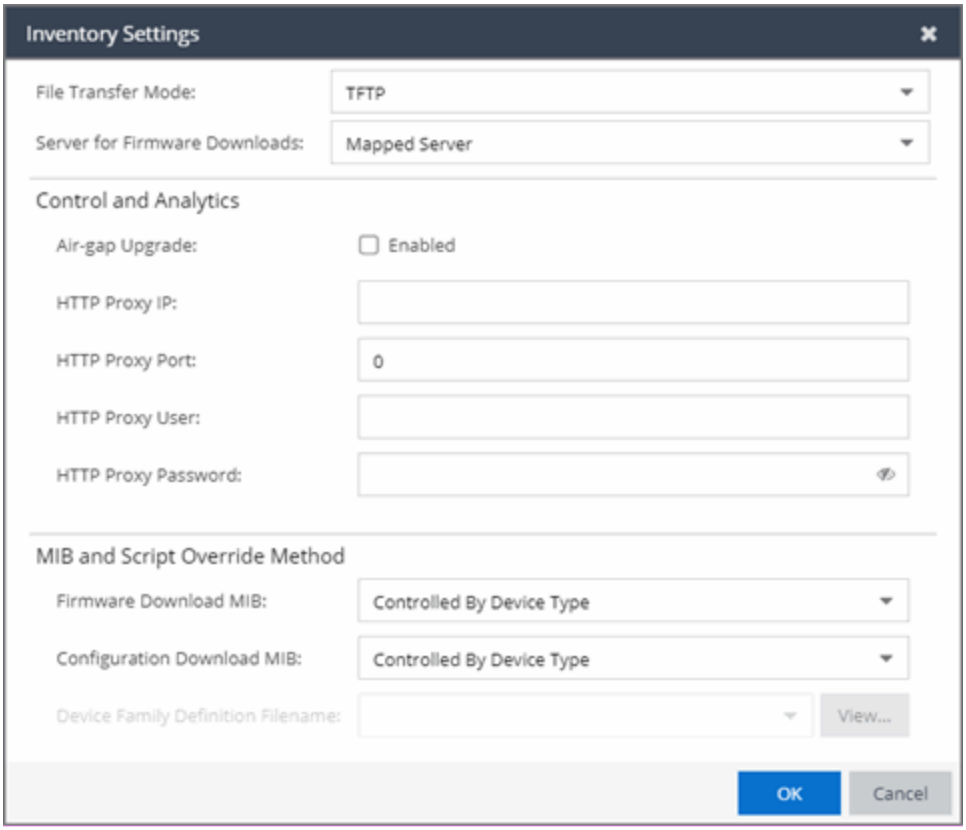
For information on related topics:

- Network
- Reports

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.

Related Information

For information on related windows:

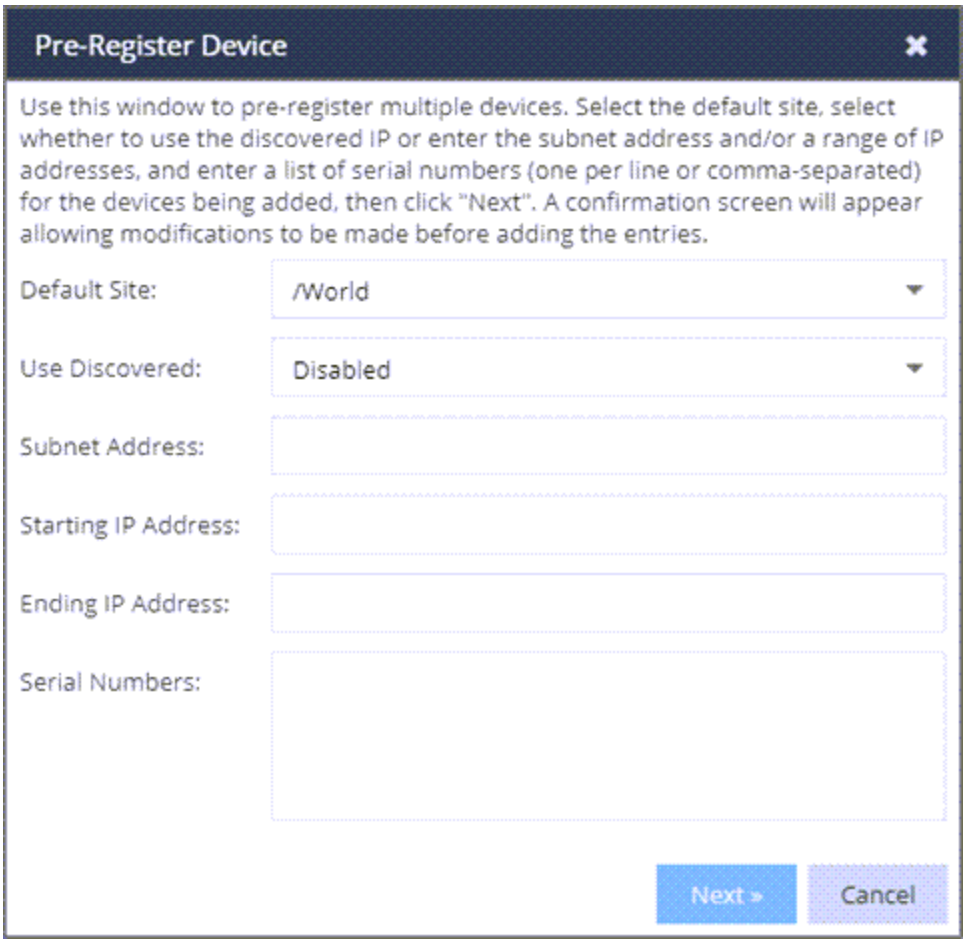
- Devices

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

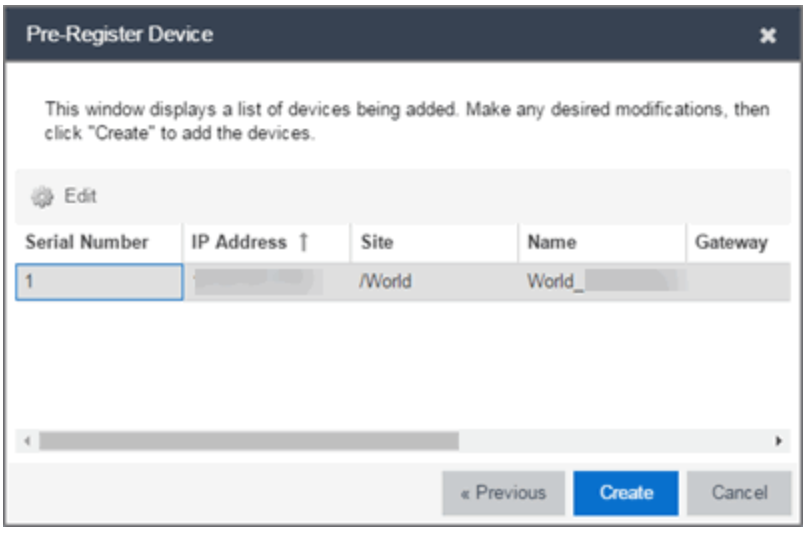
Select the **Next** button to open a confirmation window allowing you to verify the device information entered. Although it is recommended you enter device information in the site's **ZTP+ Device Defaults** window, you can also use this window to enter the Gateway, Domain Name, and DNS Server information 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.

Related Information

For information on related windows:

- Discovered

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 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
```

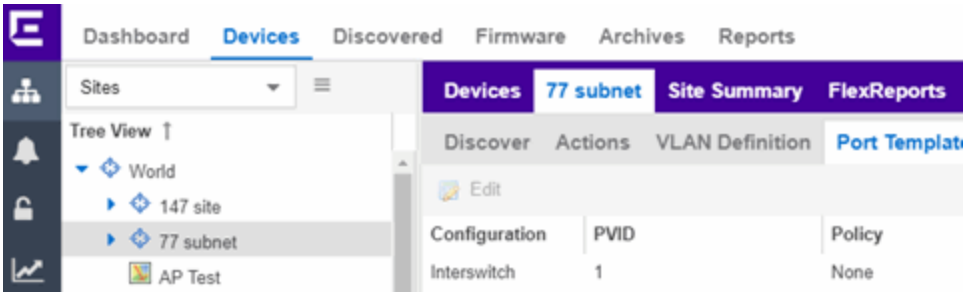
The **Sites tab** is divided into multiple sections, which you can expand to display more information.

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
- Topologies
- Services
- LAG Topologies
- Port Templates
- ZTP+ Device Defaults
- Endpoint Locations

- Analytics
- Custom Variables

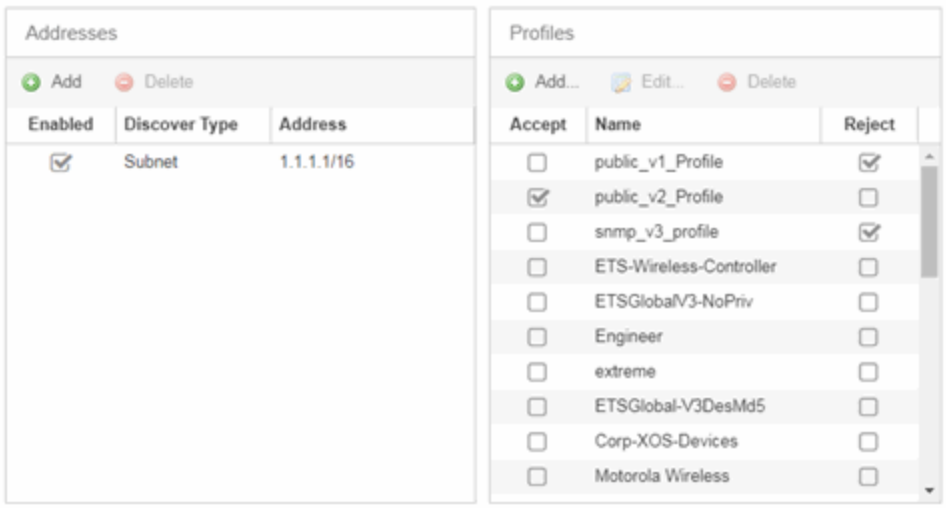
Additionally, the bottom of the tab contains buttons to save your configurations in ExtremeCloud IQ - Site Engine and on the devices included in the site.

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.

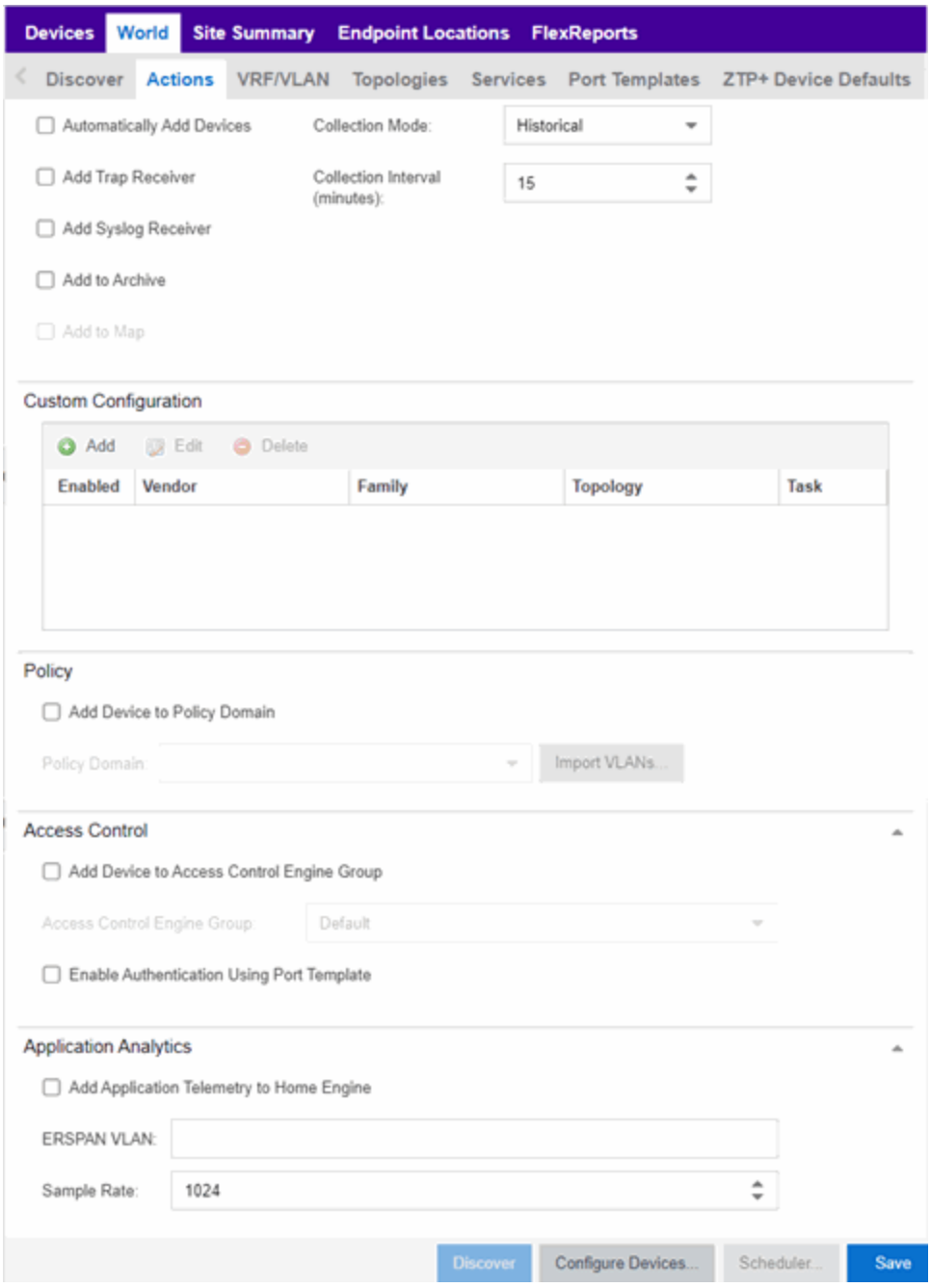
Click the **Discover** button at the bottom of the tab to begin the device discover. The results of the Discover process are displayed in the left-panel tree when added to the ExtremeCloud IQ - Site Engine database.

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.

ExtremeControl

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 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 Application Telemetry to Home Engine

Select this checkbox to add application telemetry to the ExtremeAnalytics engine configured as the site's home engine.

ERSPAN VLAN

Enter the Encapsulated Remote Switch Port Analyzer (ERSPAN) VLAN to add to devices added to the site.

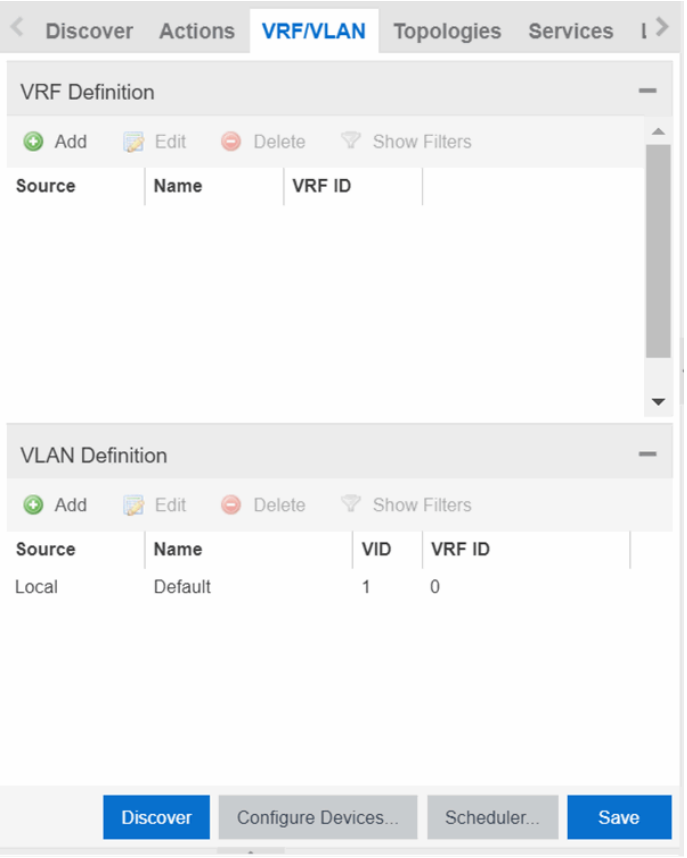
Sample Rate

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.

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 1and 4094 that identifies a particular VLAN. VID 1is 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 1or 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 VOSS 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

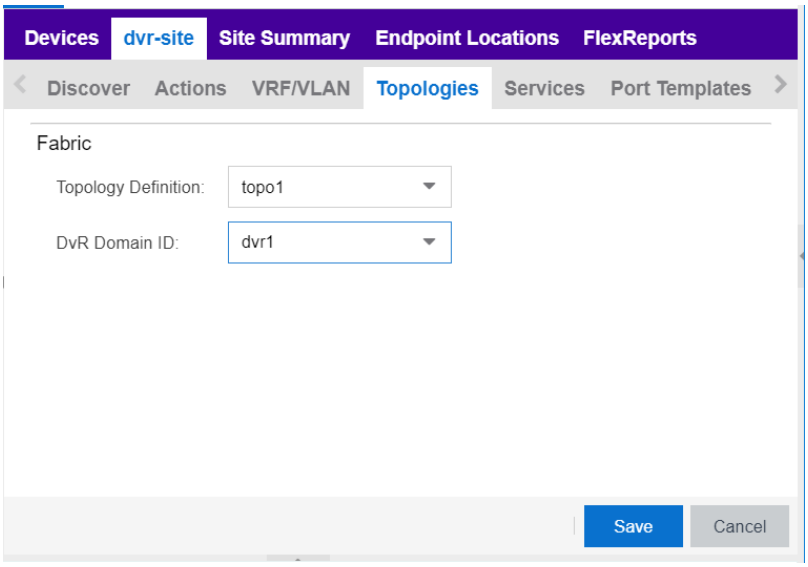
Indicates the site from which the DHCP Relay Server is inherited. Currently, the VLAN definition Source can only be **Local**, indicating the DHCP Relay Server is configured in the current site.

Server IP

The IP address of the DHCP server.

Topologies

The **Topologies** 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

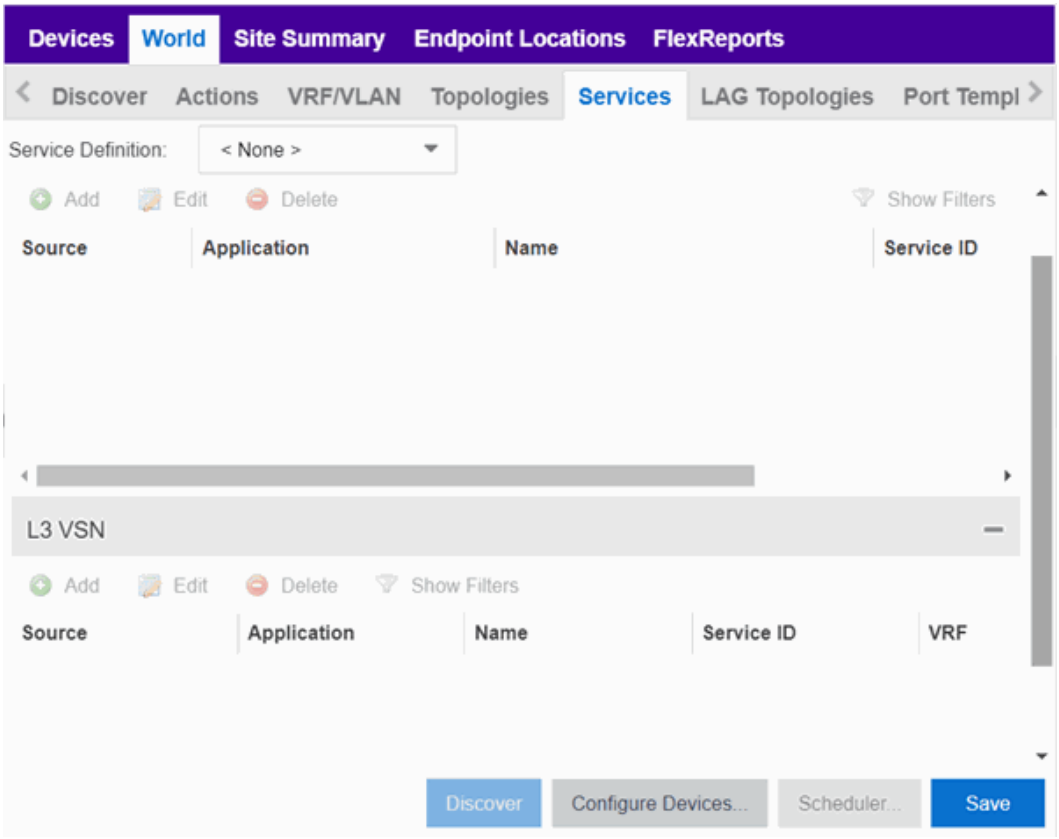
Select the DvR Domain ID that applies to the site. The DvR Domain IDs available in the drop-down list are configured in the **Topology Definition** tab.

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

Application
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.

VLAN
The VLAN assigned to the fabric service.

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.

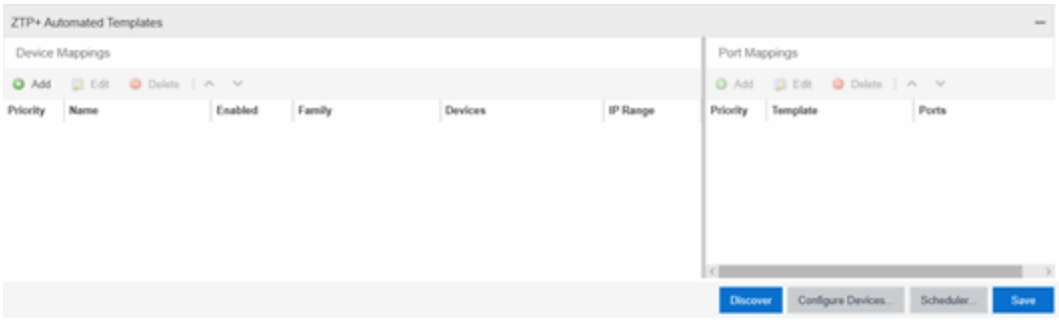
L2 ISID
The service instance identifier.

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

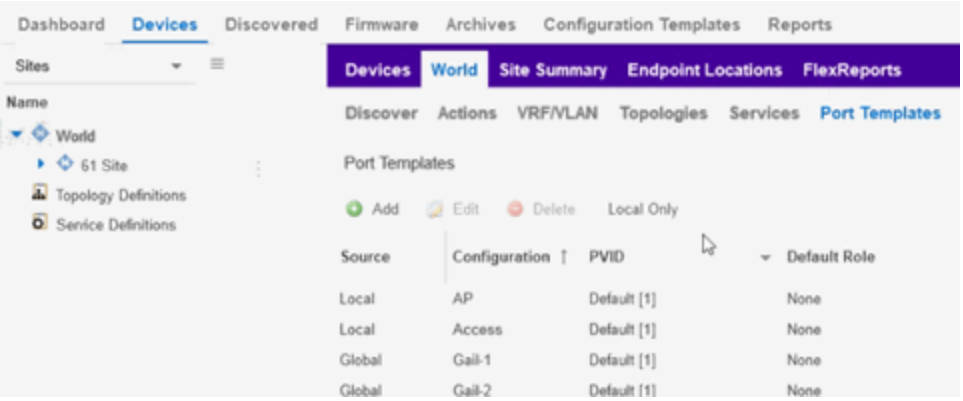
The **Port Templates** tab has two panels. The top panel displays information about user-defined port templates. For more information, see Port Templates Panel.

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.

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.

ExtremeCloud IQ - Site Engine can extend FA functionality to ExtremeXOS devices

and provision them as FA Proxy devices. Select "Fabric Attach" or "" from the drop-down list to enable the port on a VOSS device (acting as FA Server) to connect to an ExtremeXOS device (acting as FA Proxy).

- **Fabric Attach** - Enable Fabric Attach server functionality on the port of a VOSS device acting as a Fabric Attach server) to connect to an ExtremeXOS device (acting as a Fabric Attach proxy).
- **Fabric Attach and Switched UNI** - Enable Fabric Attach server functionality on the port of a VOSS device acting as a Fabric Attach server) to connect to an ExtremeXOS 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 VOSS 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. Select the checkbox to enable ZTP+ devices being discovered to broadcast MVRP information. Select the appropriate logging level from the drop-down list.

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.

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 Panel

The **ZTP+ Automated Templates** panel 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.

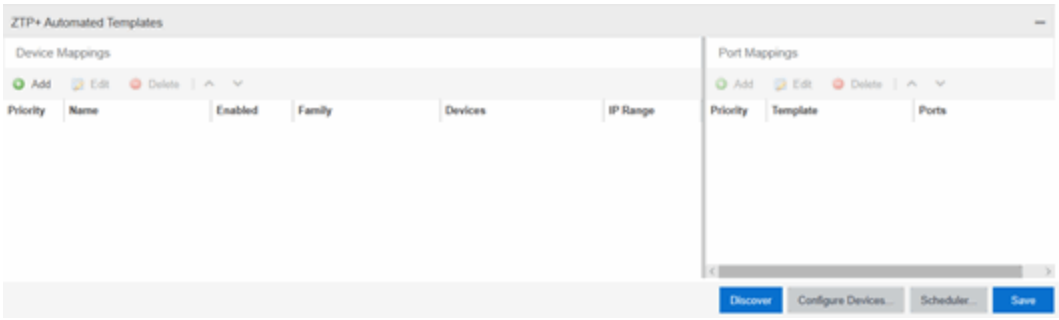
NOTE: ExtremeCloud IQ - Site Engine supports automated port templates for ZTP+ devices only.

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:

- 12.3.4 (v4)
- 1111:2222::3333:4444 (v6)
- 12.3.4/24 (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"
  - EXOS: "1" or "1,3,5,7"
  - EXOS 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"
  - EXOS: "5-7" or "5-7, 9-12, 15-19"

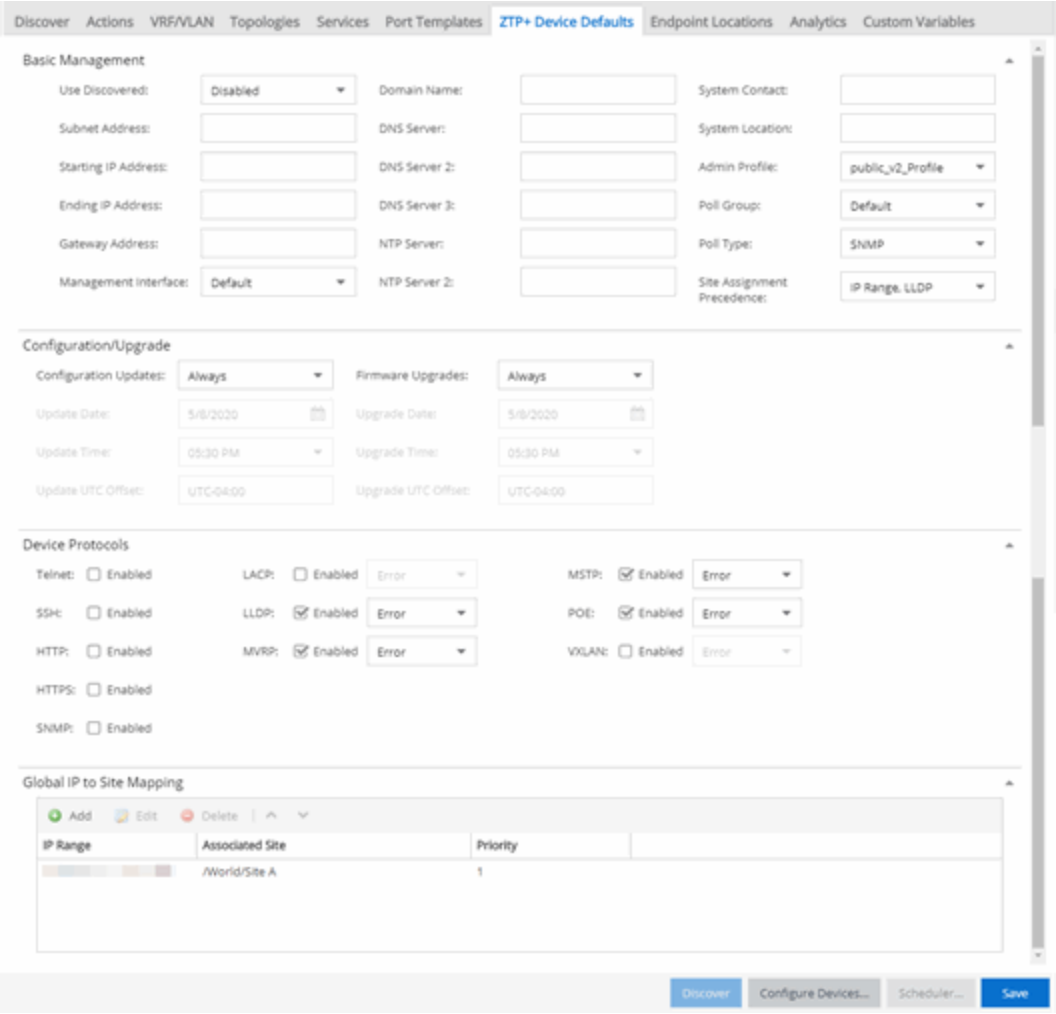
    - EXOS Stack: "1:5 - 1:7" or "1:5-1:7, 2:9-2:12, 3:15-3:19"
    - SLX: "Ethernet 0/1-Ethernet 0/4" or "Ethernet 0/1-Ethernet 0/5, Ethernet 0/8-Ethernet 0/15"
  - Wildcarding:
    - "*" is always allowed, matches anything, useful as default rule at the end of a set of bindings
    - In a single port scenario, 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/*"
      - EXOS: "*"
      - EXOS 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**.

  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 (SNMPv1or 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+**, 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**.

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 set:

- **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 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

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. Select the appropriate logging level from the drop-down list.

LLDP

Select the checkbox to enable LLDP (Link Layer Discovery Protocol) access on the ZTP+ device. Select the appropriate logging level from the drop-down list.

MSTP

Select the checkbox to enable MSTP (Multiple Spanning Tree Protocol) access on the ZTP+ device. Select the appropriate logging level from the drop-down list.

MVRP

Select the checkbox to enable MVRP (Multiple VLAN Registration Protocol) access on the ZTP+ device. Select the appropriate logging level from the drop-down list.

POE

Select the checkbox to indicate the ZTP+ devices being discovered for the site are electrically powered via the 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.

Global IP To Site Mapping

IP Range

Select **Add** or **Edit** to enter a single IP address or an IP range.

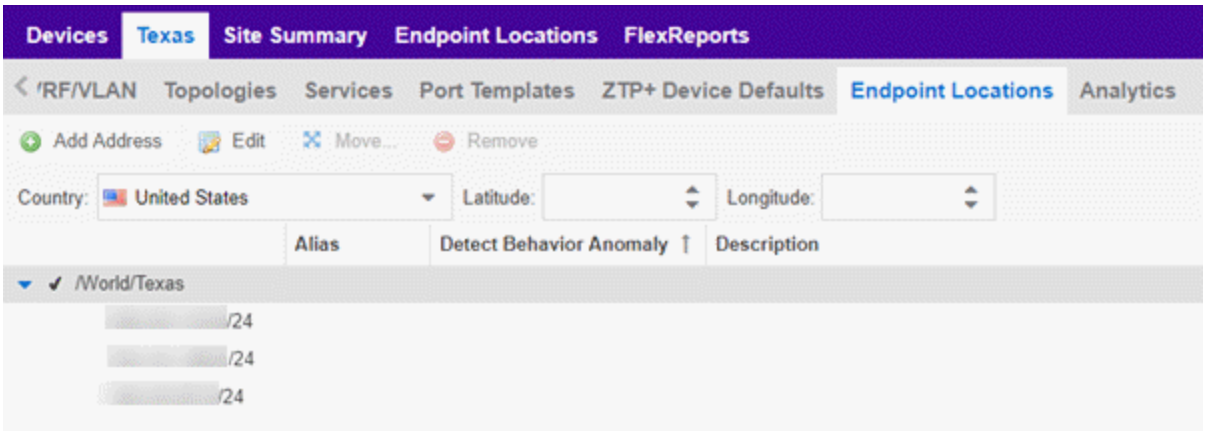
Associated Site

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.

Detect Behavioral Anomaly
Select the checkbox to enable ExtremeCloud IQ - Site Engine functionality that alerts you in the event unexpected behavior is detected for the site or its specified subnet.

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

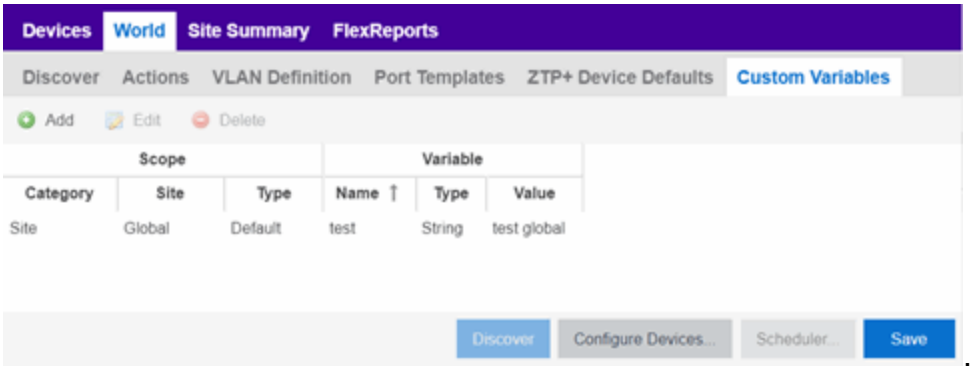
Displays the ExtremeAnalytics engine located with the devices associated with the site.

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.

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.

Related Information

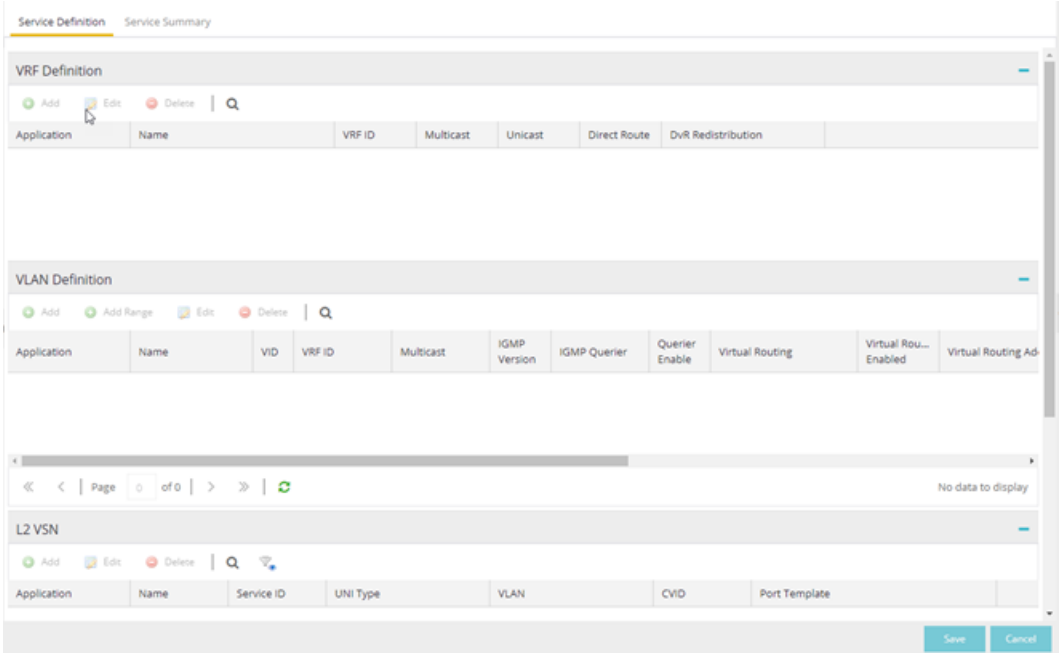
For information on related topics:

- 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.

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 1or 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 VOSS 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.

Flex UNI
Indicates that the fabric service is using the User-Network-Interface (UNI).

The following interface types are available:

- Switched —A VLAN-ID and a given port (VID, port) maps to a Layer 2 VSN I-SID. With this UNI type, VLAN-IDs can be reused on other ports and therefore mapped to different ISIDs.
- Transparent —A physical port maps to a Layer 2 VSN I-SID (all traffic through that port, 802.1Q tagged or untagged, ingress and egress is mapped 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.

VLAN

The VLAN assigned to the fabric service.

CVIDs

Specifies the customer VLAN ID of the associated switched UNI port.

Port Template

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** —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 that 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.

DVR Enable
Select to enable distributed virtual routing.

> **IMPORTANT:** A device on which you enable DVR Leaf mode does not support all ExtremeCloud IQ - Site Engine features. DVR Leaf mode is a constrained operating mode for the device and previous configurations defined on a device may no longer function properly.

DVR Gateway
Enter the gateway address of the DVR device.

Multicast Snooping
Select to configure the service to listen to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers.

Multicast Routing
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
The version of IGMP the service is using: Version 1, 2, or 3.

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.

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.

Related Information

For information on related topics:

- Service Summary
- Fabric
- Sites

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.

Related Information

For information on related topics:

- Services
- Fabric
- Sites
- Devices

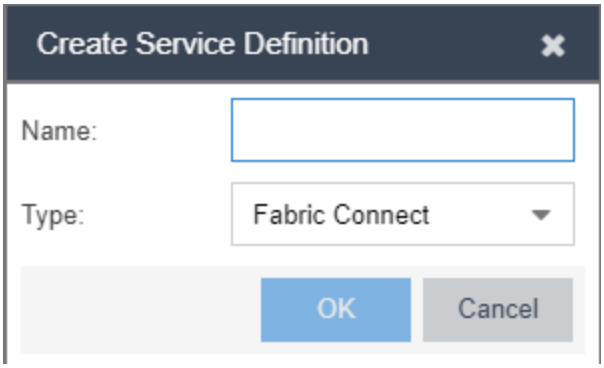
How to Create a Fabric Service Definition

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.

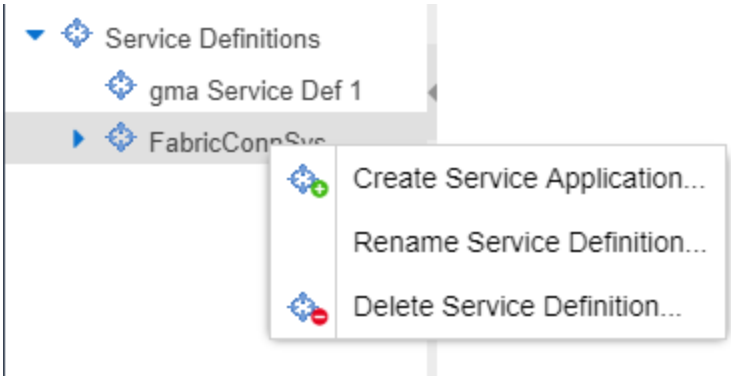
After the service definition is created and configured, you can apply it to a site within your network. When fabric services have been assigned to a site, they cannot be deleted.

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.

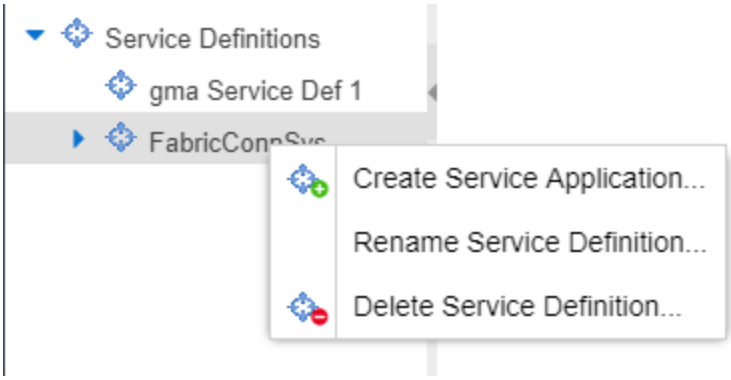


To rename a service definition:

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.

Related Information

For information on related topics:

- Services
- Fabric
- Sites
- Devices

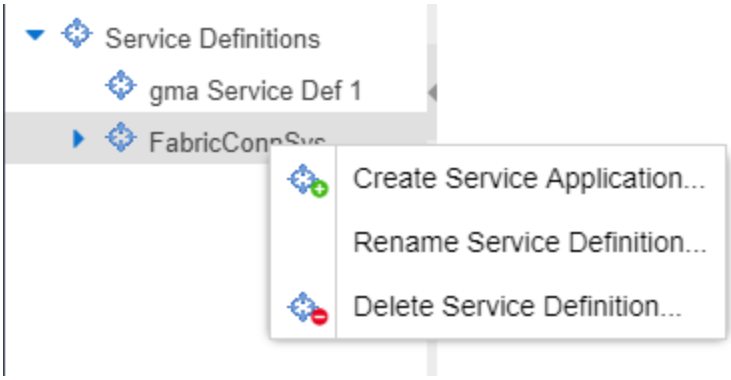
How to Create a Service Application

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.

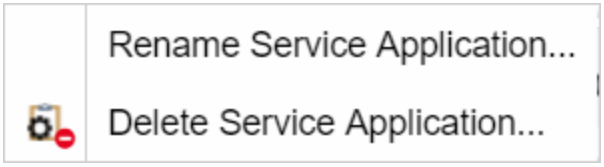
NOTE: A Service Application must have the same fabric type as its associated Service Definition. For example, if a Service Definition is created with Fabric Connect type, it can only have Service Applications of Fabric Connect type. Currently, Fabric Connect is the only fabric type available.

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:

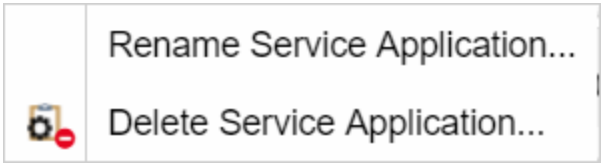
1. Open the **Devices** tab.
2. Select **Sites** from the left-panel tree drop-down list.
3. Expand **Service Definitions** in the left-panel.
4. Right-click the service application you are renaming.



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.

Related Information

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.

Related Information

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.

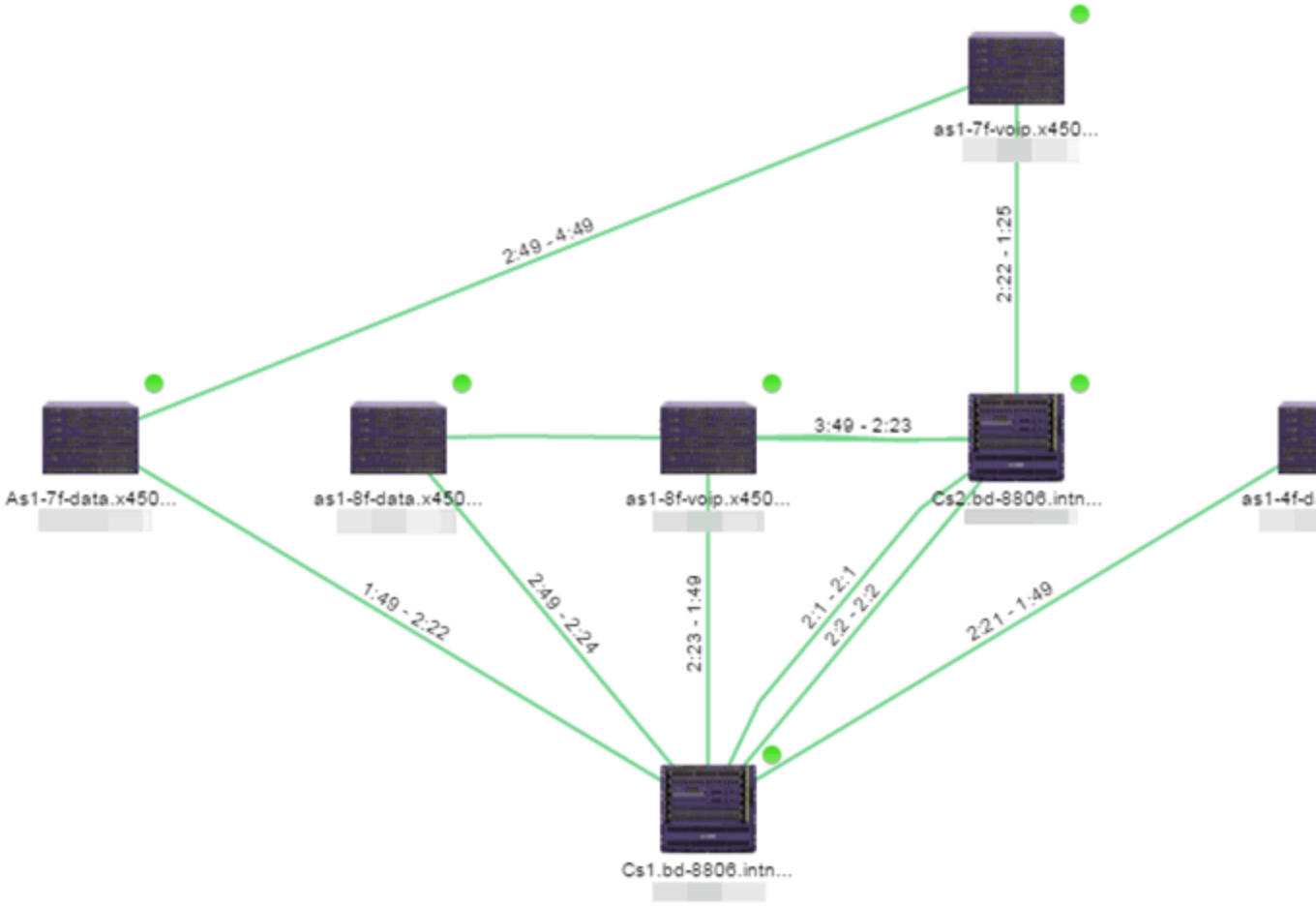
You can include port extenders in a map. If you choose not to add port extenders to a map, the ports on the port extender are shown as part of the controlling bridge.

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.



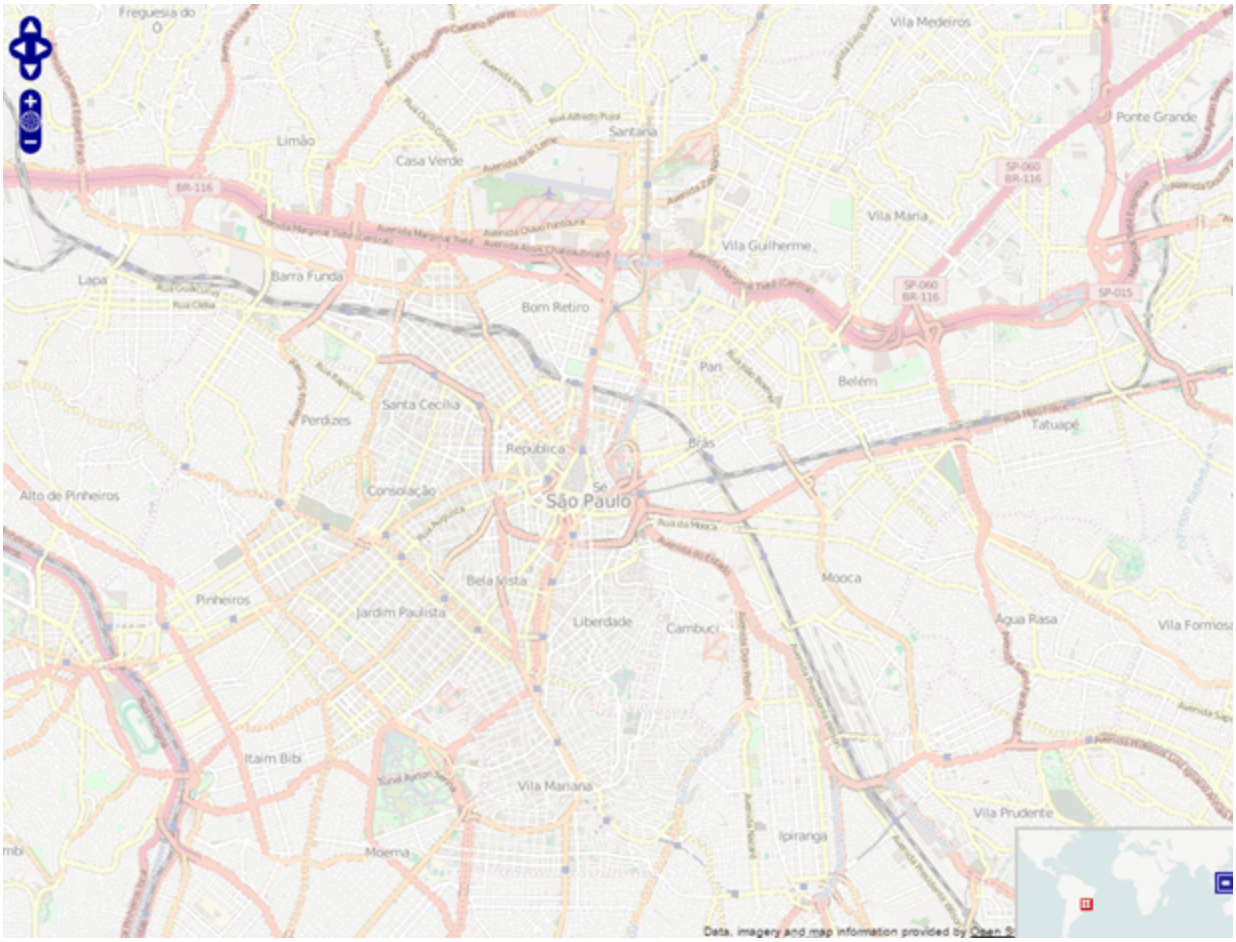
For additional information about devices and links in a Topology map, see the Viewing Alarm and Device Status and Link Information sections.

- 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.

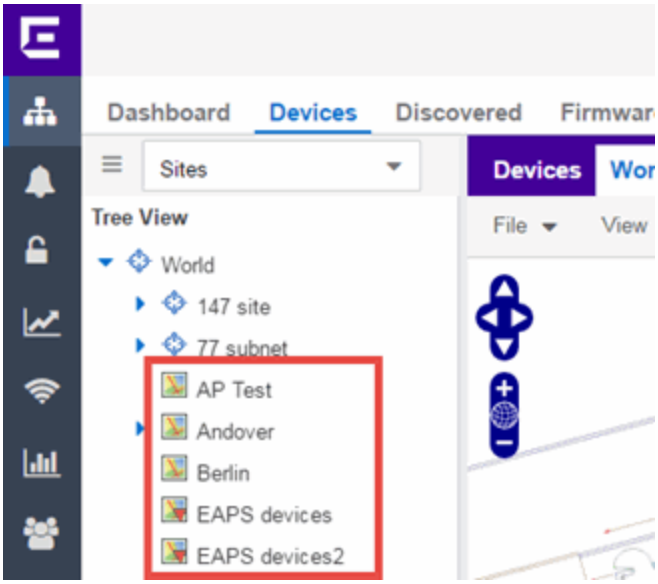
To view or search Maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read Access or Maps Read/Write Access capability.

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.

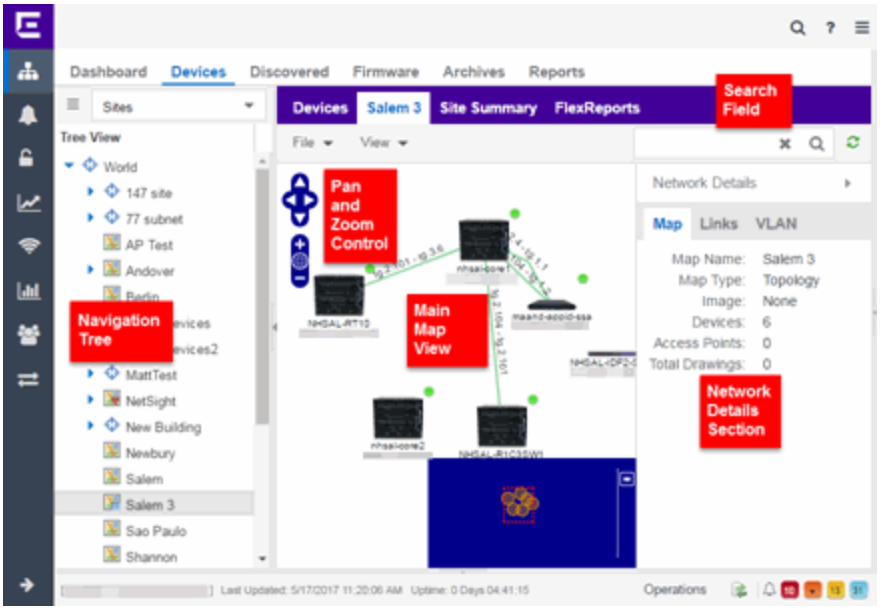
Import Map

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:

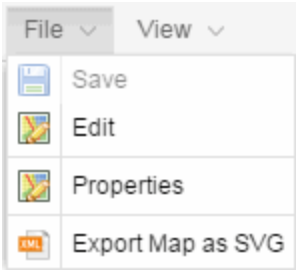
- File, View, and Tool Menus
- Pan and Zoom Control
- Search Field



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.

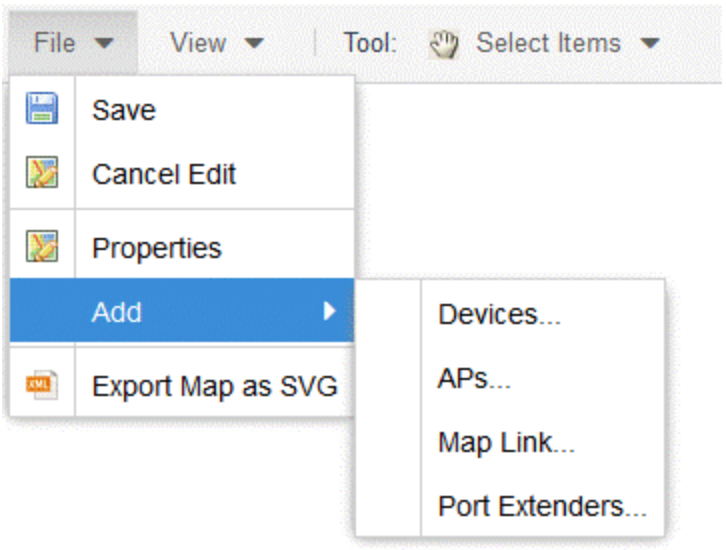
When exporting a map in SVG format, the exported SVG file may open in a new tab or window, depending on how your browser is configured. The SVG file displays your exact view when you select **Export Map as SVG**. For example, if your map is zoomed in to only show two devices and the VLANs associated 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.

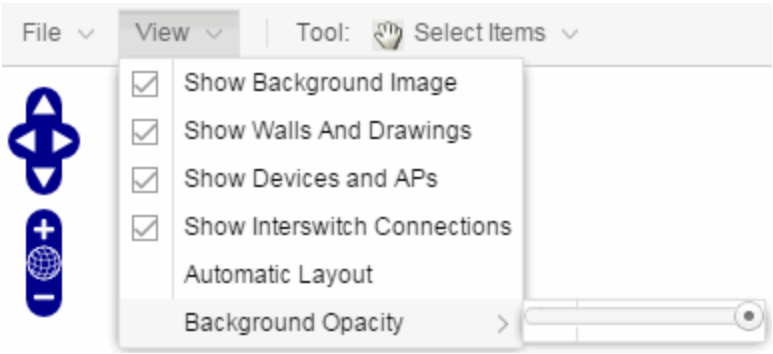
The **Add** submenu is available, from which you can add Devices, APs, Map Links, and Port Extenders to the map. Edit mode also allows you to manipulate the existing Devices, APs, Map Links, and Port Extenders currently displayed on the map. Select **Cancel Edit**

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.

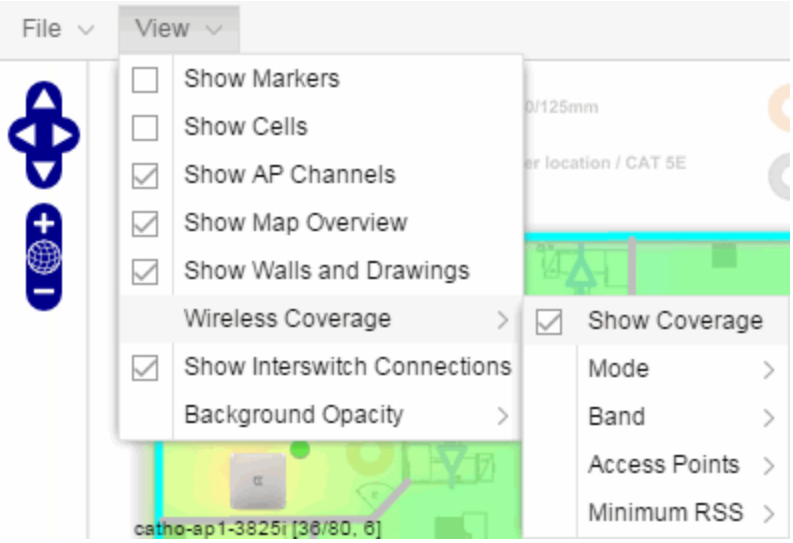


View Menu

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. 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: 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.

Drawing Tool	Definition
	**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

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.

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

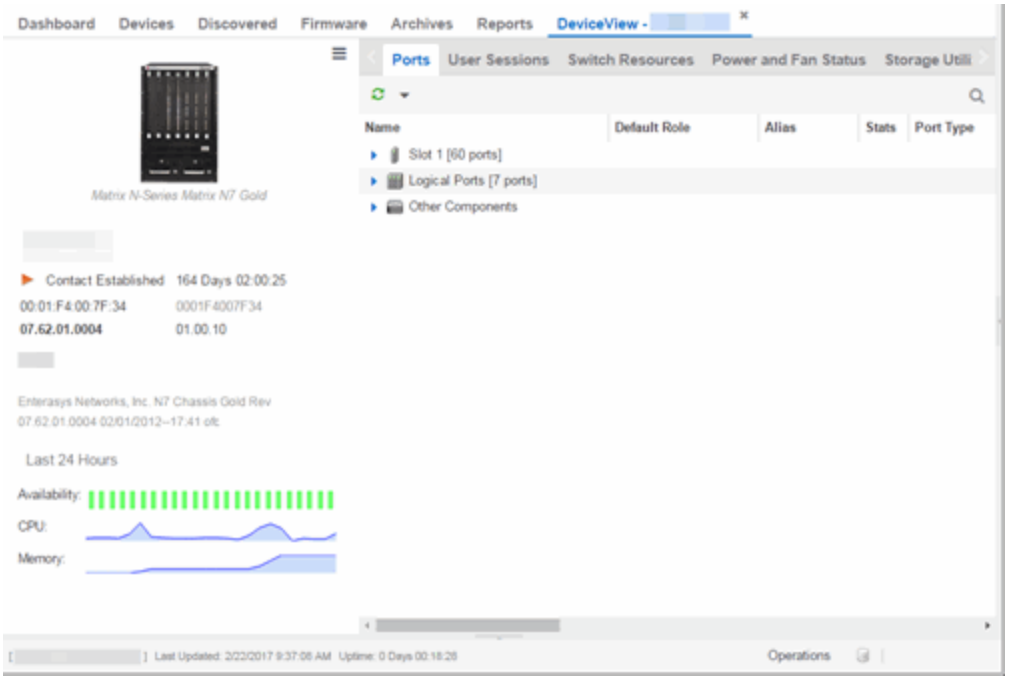
There are two ways to access additional device information from a map.

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

Each connection type is represented by a different line style:

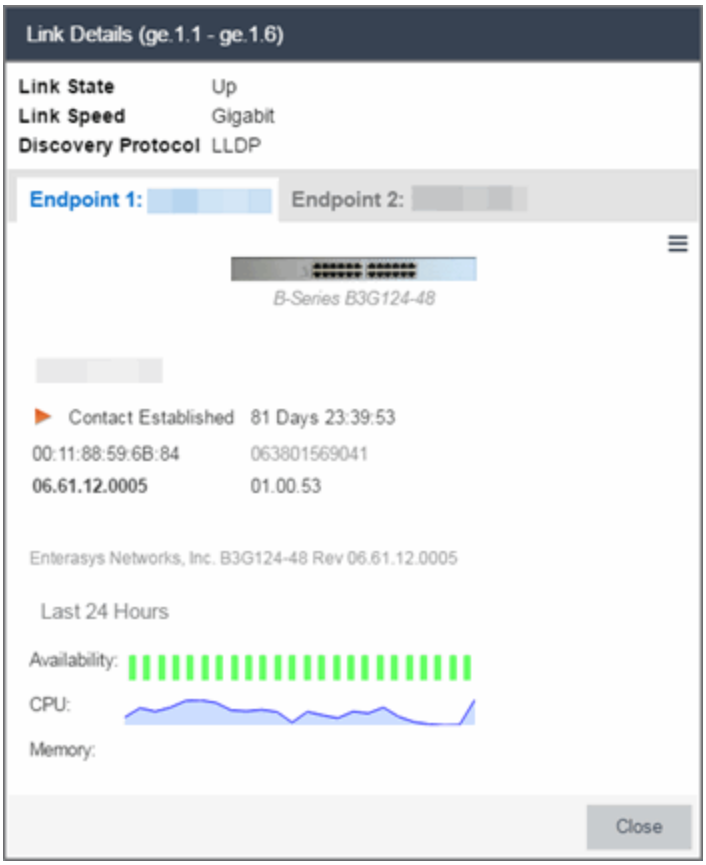
- Basic links appear as thin green lines with no outlining.

- 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.

- 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.

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

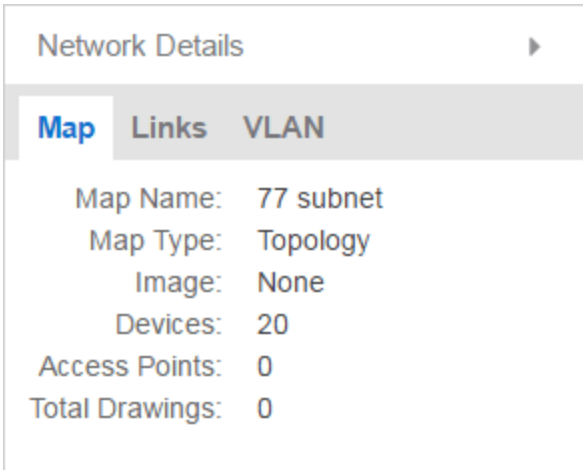
The Network Details section is available in topology and geographic maps. It contains up to five tabs, depending on the devices included in the map:

- 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.

Map tab

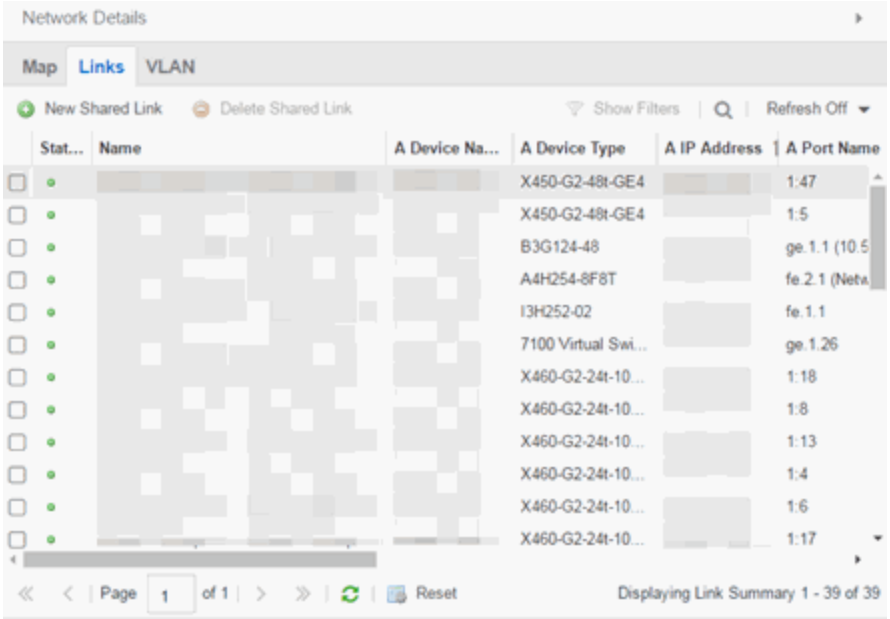
The **Map** tab displays basic information about the map, including the name of the map, the map type, and the background image, as well as the number of devices, APs, and

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.



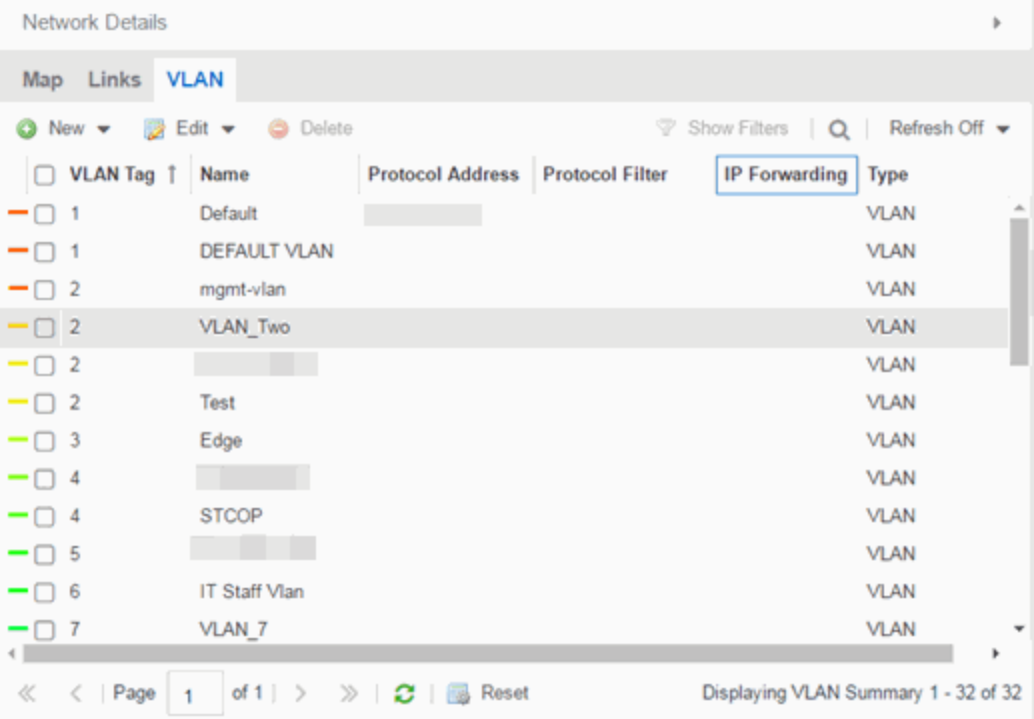
The top of the **Links** tab contains a search field, which allows you to find a particular Link by entering specific criteria. Additionally, you can manually browse links using the scroll bar and page navigation at the bottom of the section.

Double-clicking a link opens the Link Details window.

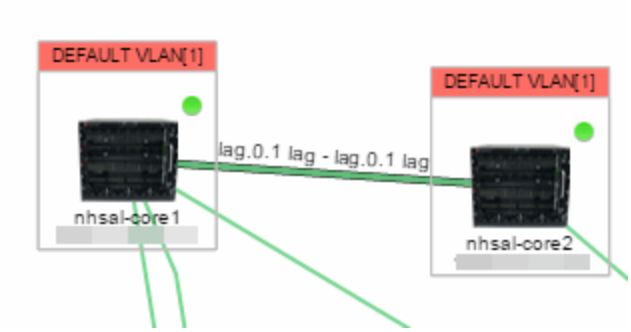
The top of the window displays information about the link, while information about the devices it connects are contained on two tabs, Endpoint 1 and Endpoint 2.

VLAN tab

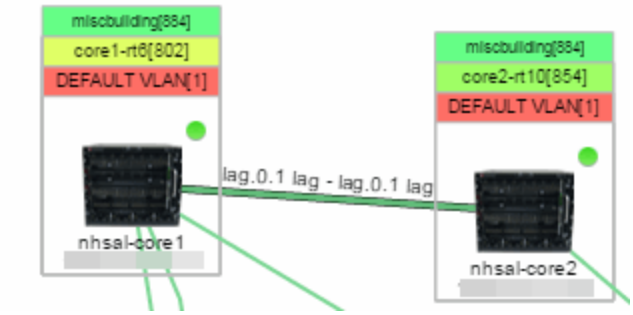
The **VLAN** tab displays VLANs configured as part of devices included in the map. Columns in the **VLAN** tab provide additional information, including the VLAN tag, the name of the VLAN, any protocol filters applied for devices on which the VLAN is configured, and whether or not IP forwarding is enabled 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.

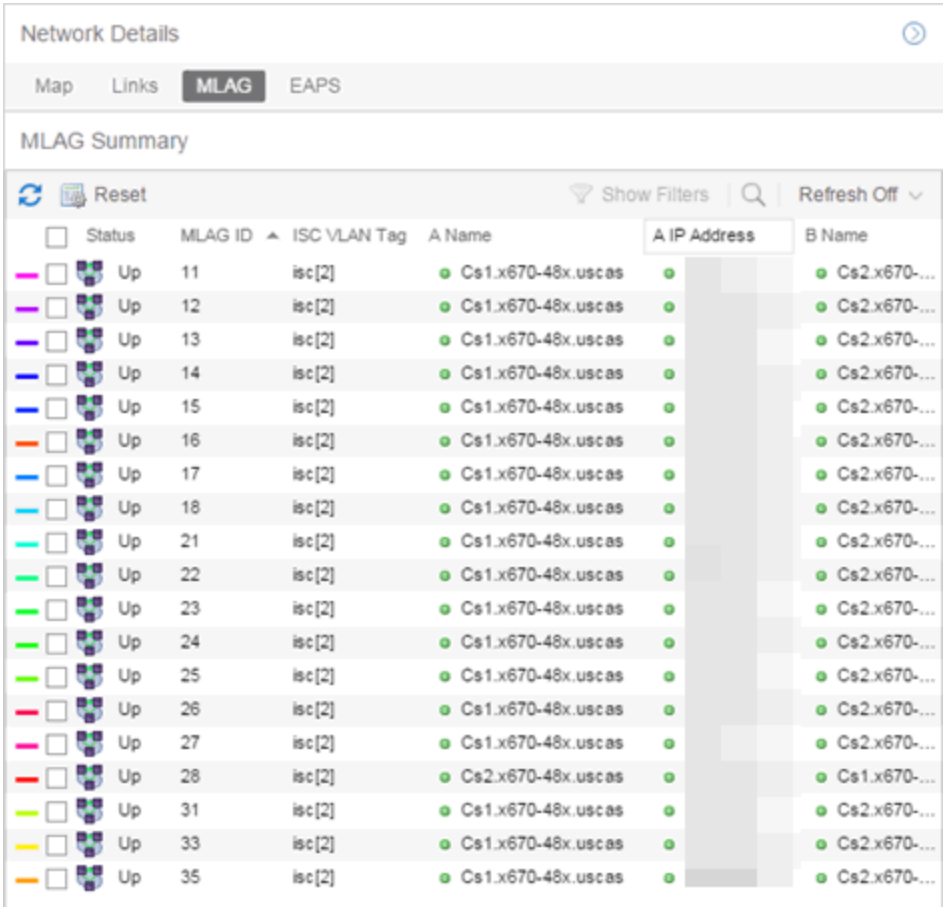


Additionally, from the **VLAN** tab, you can create a new VLAN and create a VLAN protected by an EAPS domain via the New drop-down list or edit the ports, name, and devices associated with an existing VLAN via the **Edit** drop-down list. For more information, see How to Create and Edit VLANs.

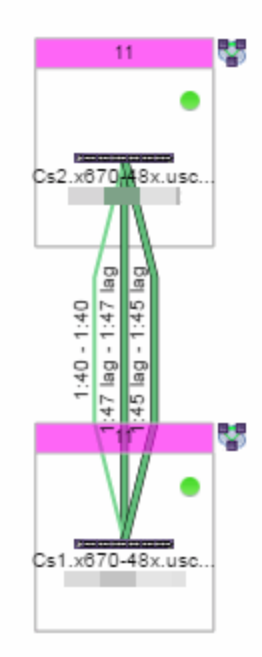
MLAG tab

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.

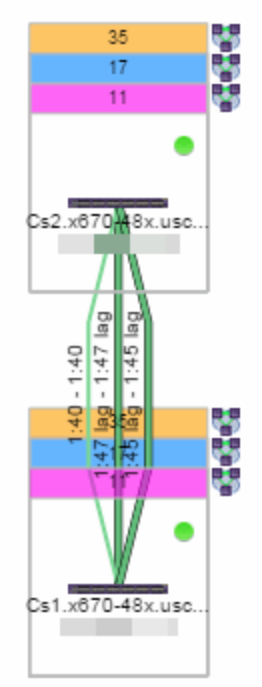
NOTE: One-armed MLAGs, which may be utilized in a VPEX Ring topology, will normally display an MLAG port on only one of the devices.



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.

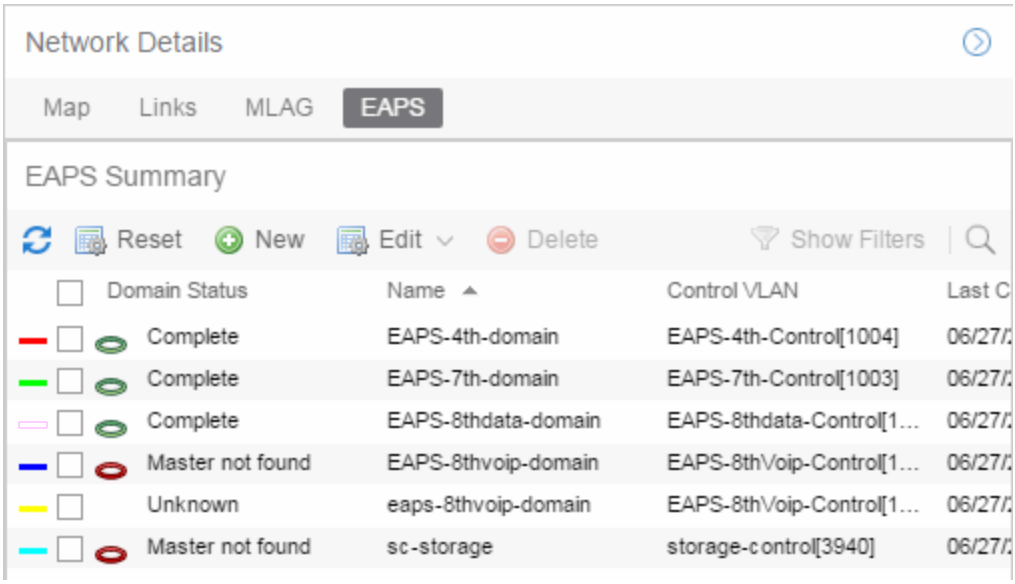


Selecting multiple MLAGs assigned to the same device adds a new title bar to the box containing the VLAN name and associated color.

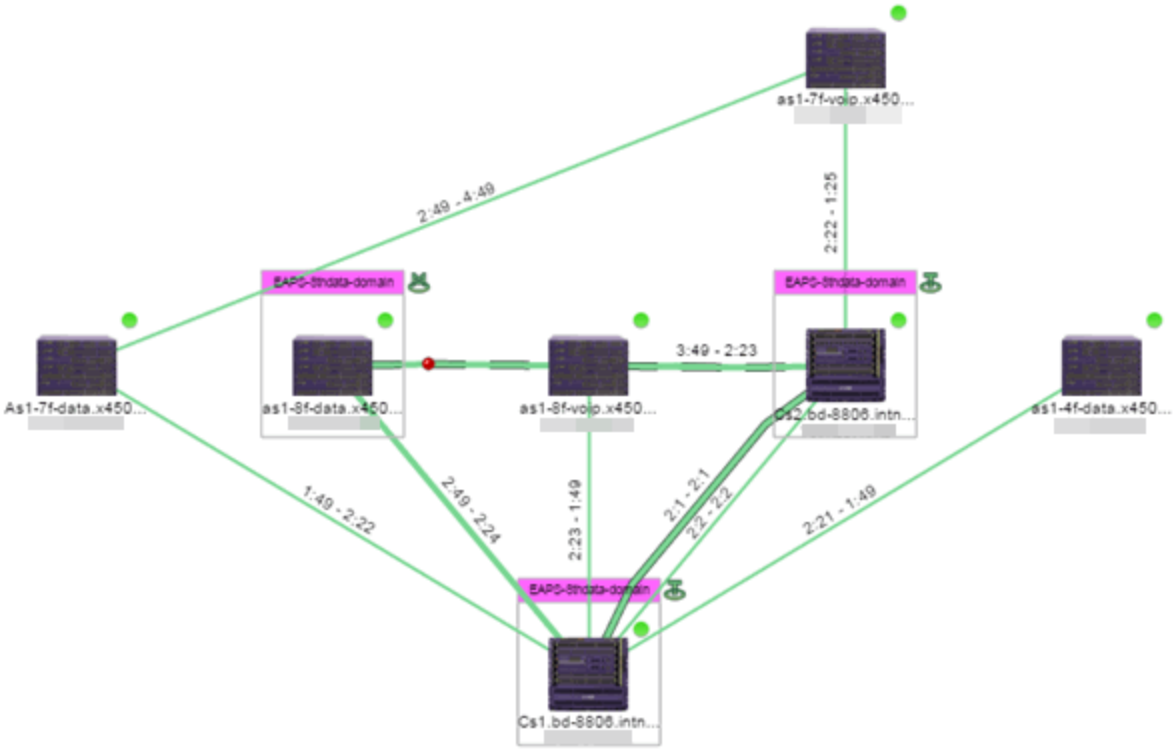


EAPS tab

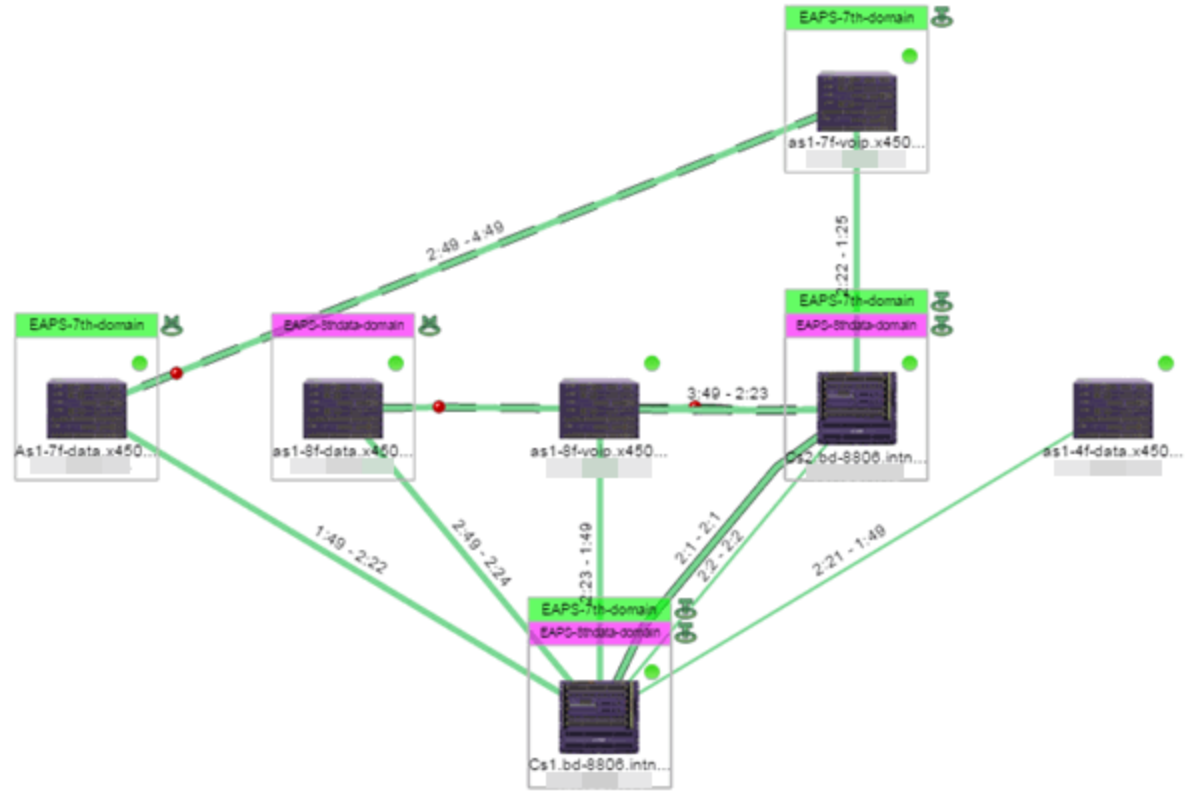
The **EAPS** tab displays a list of the EAPS domains, including their status, name, the control VLAN name, and the IP addresses of the devices utilizing the EAPS domain.



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.



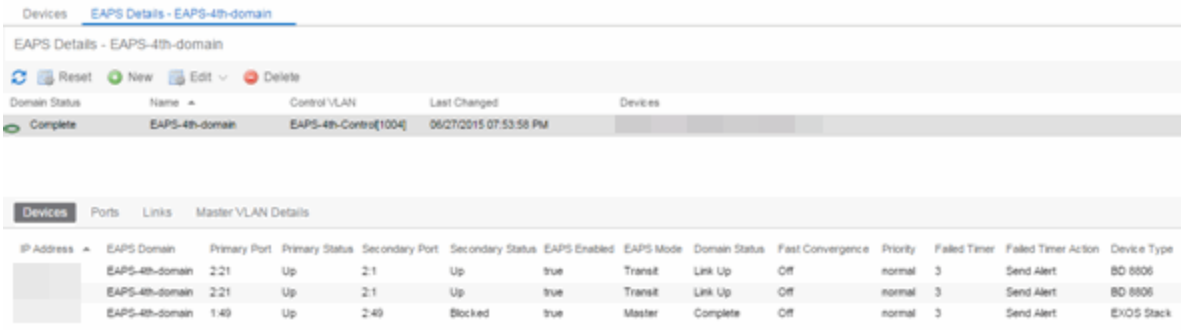
An icon next to the title bar indicates if the node is a master node, indicated by an "M" icon , or if the node is a transit node, indicated by a "T" icon .

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

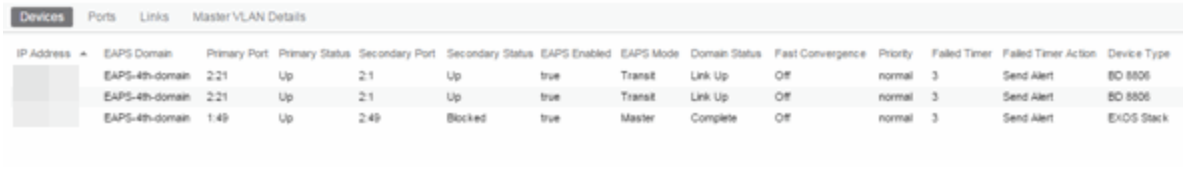
When selecting an EAPS domain, link information is also displayed. A single green line means a link that is not shared, while a dashed line between devices means the link is shared. A red dot icon on a shared link indicates the secondary link is blocked.

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.



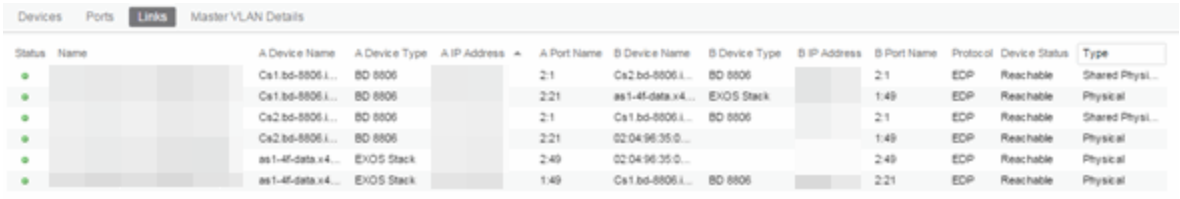
The top of the EAPS Details view displays a summary of the EAPS domain, identical to the information displayed in the **EAPS** tab. At the bottom of the window are three sub-tabs, which display additional information:

- **Devices**—Displays information about the devices using the EAPS domain.

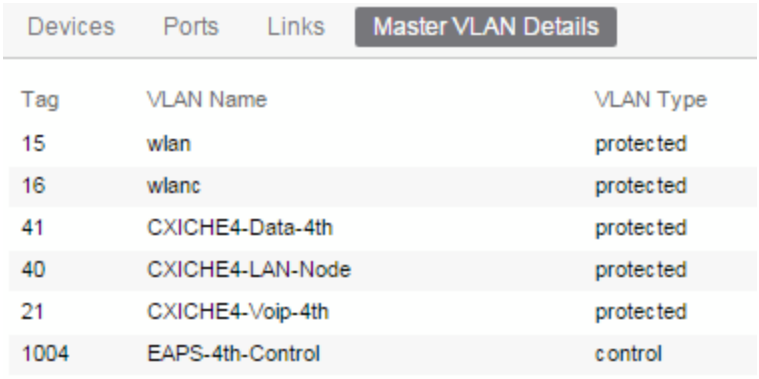


- **Ports**—Displays information about the shared ports associated with the EAPS domain.

- **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.

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.

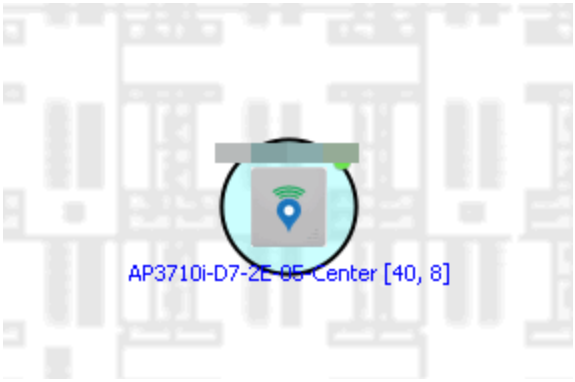
Finding a Wireless Client

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 1meter

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

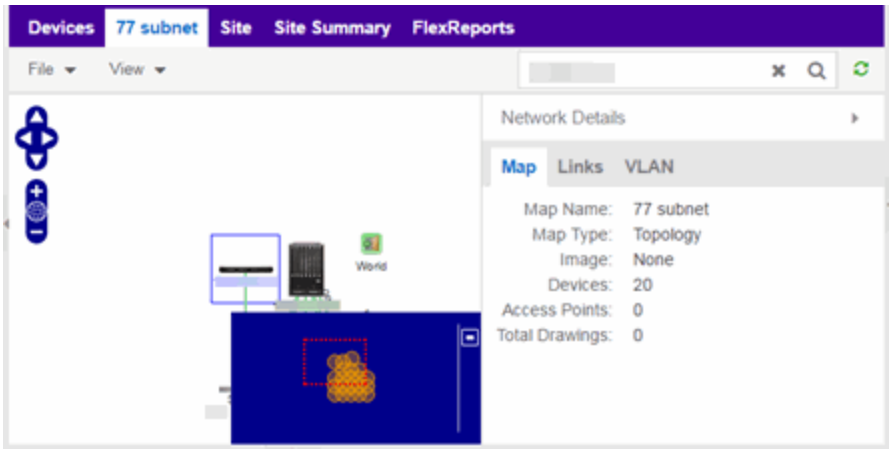
You can locate an AP from the Wireless > APs Summary report on the **Reports** tab. Select an AP in the table, right-click and select **Search Maps**. If a map contains the AP, the map opens with the AP centered on the map.

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 ExtremeControl 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 ExtremeControl authenticated wired client from the **Control > ExtremeControl** 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.

Related Information

For information on related topics:

- How to Create and Edit Maps
- Advanced Map Features
- Sites

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.

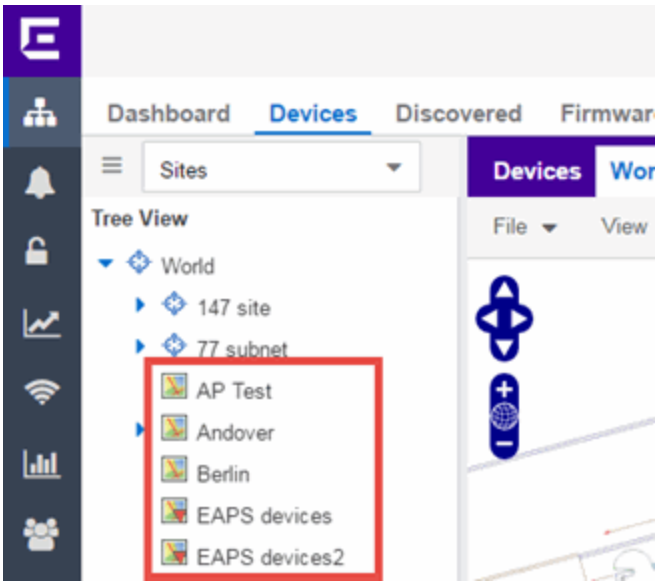
To view or search maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read Access or Maps Read/Write Access capability.

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

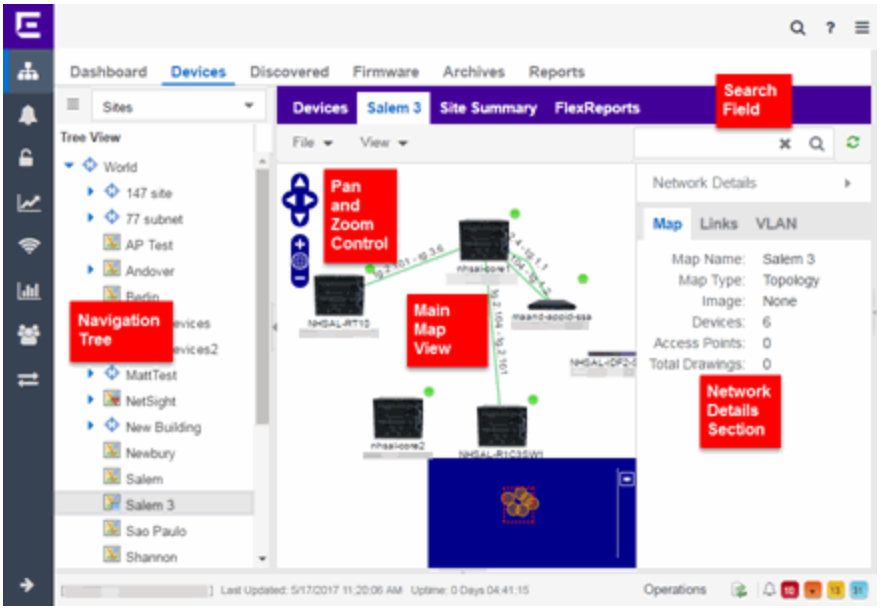
You can also import a saved map by right-clicking a map in the navigation tree and selecting **Maps** > **Import Map**. This opens the Import Map window.

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:

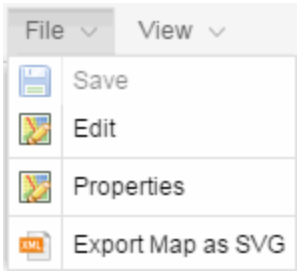
- File, View, and Tool Menus
- Pan and Zoom Control
- Search Field



File, View, and Tool Menus

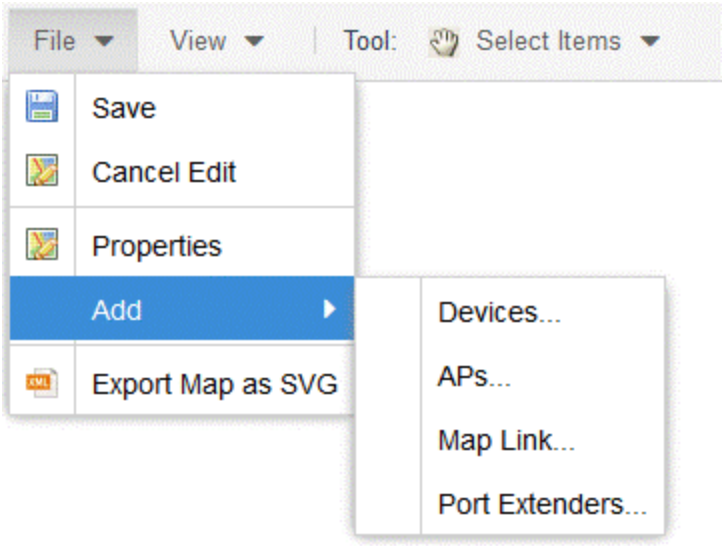
File Menu

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**.

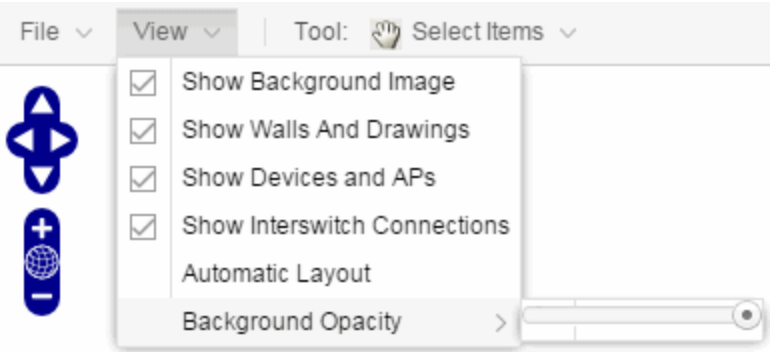
Only floorplan maps can be exported as a ZIP file. Floorplan maps you export as a ZIP file are typically used to import a floorplan into another instance of ExtremeCloud IQ - Site Engine.

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

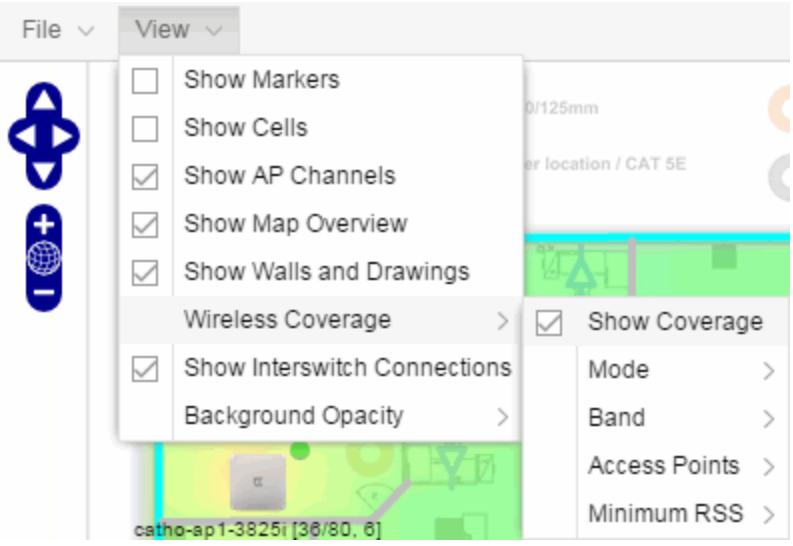
map. Edit mode also allows you to manipulate the existing devices, APs, and map links currently displayed on the map. Select **Cancel Edit** to exit Edit mode. If you made any changes to the map, a dialog box appears from which you can choose to save the changes or exit Edit mode without saving your 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.
	**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

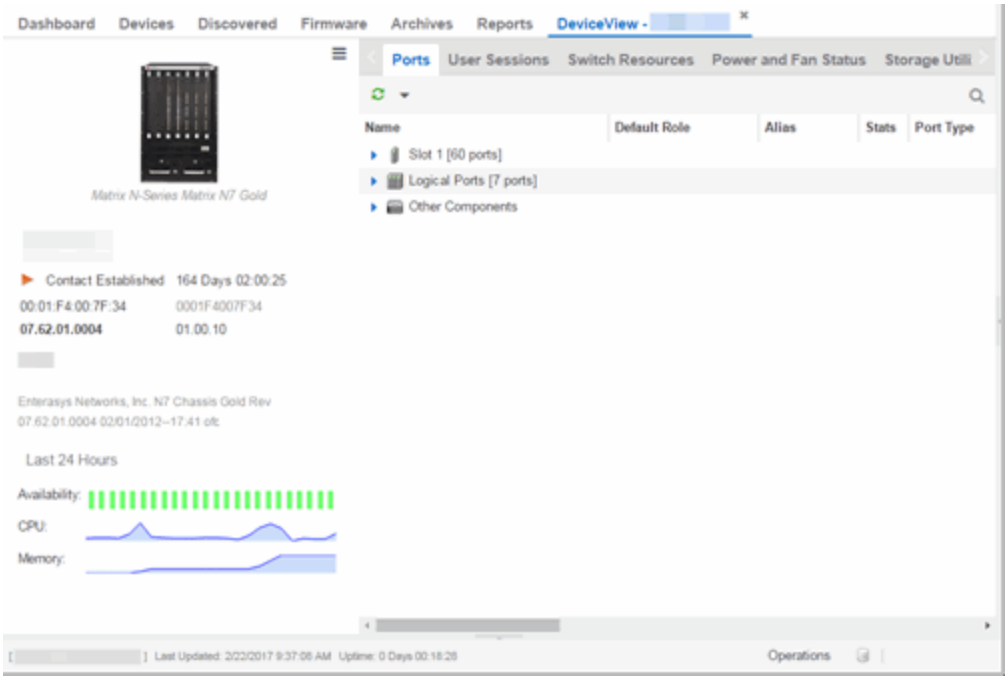
There are two ways to access additional device information from a map.

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:

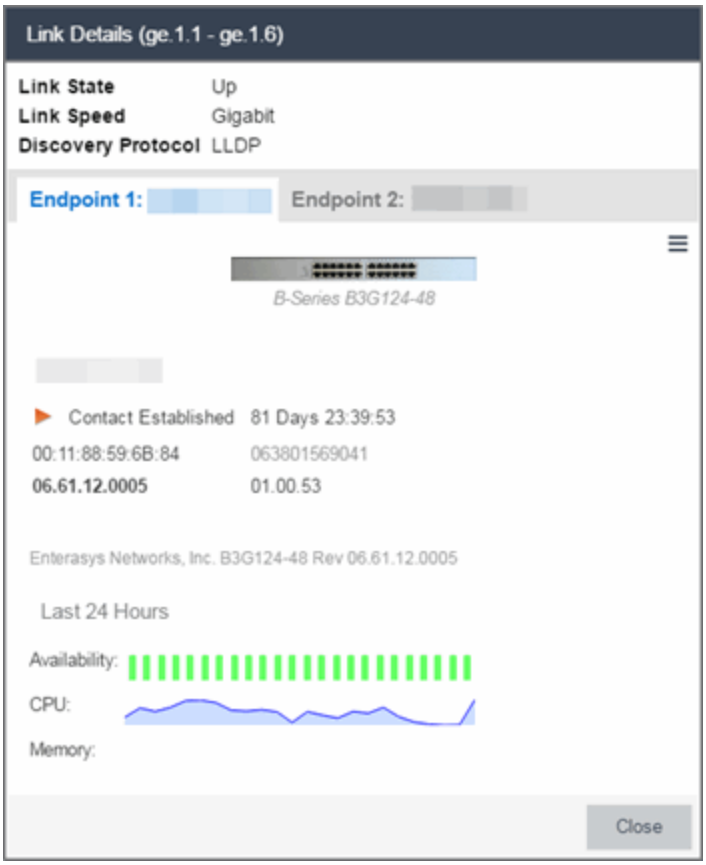
- Basic links appear as thin green lines with no outlining.

- 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

---

Related Information

- 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**.

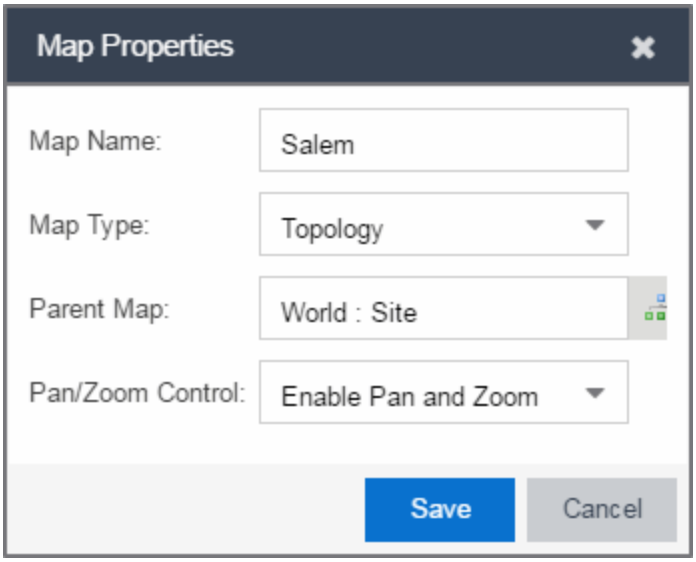
NOTE: You cannot create a new map if you are currently editing another map.

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.

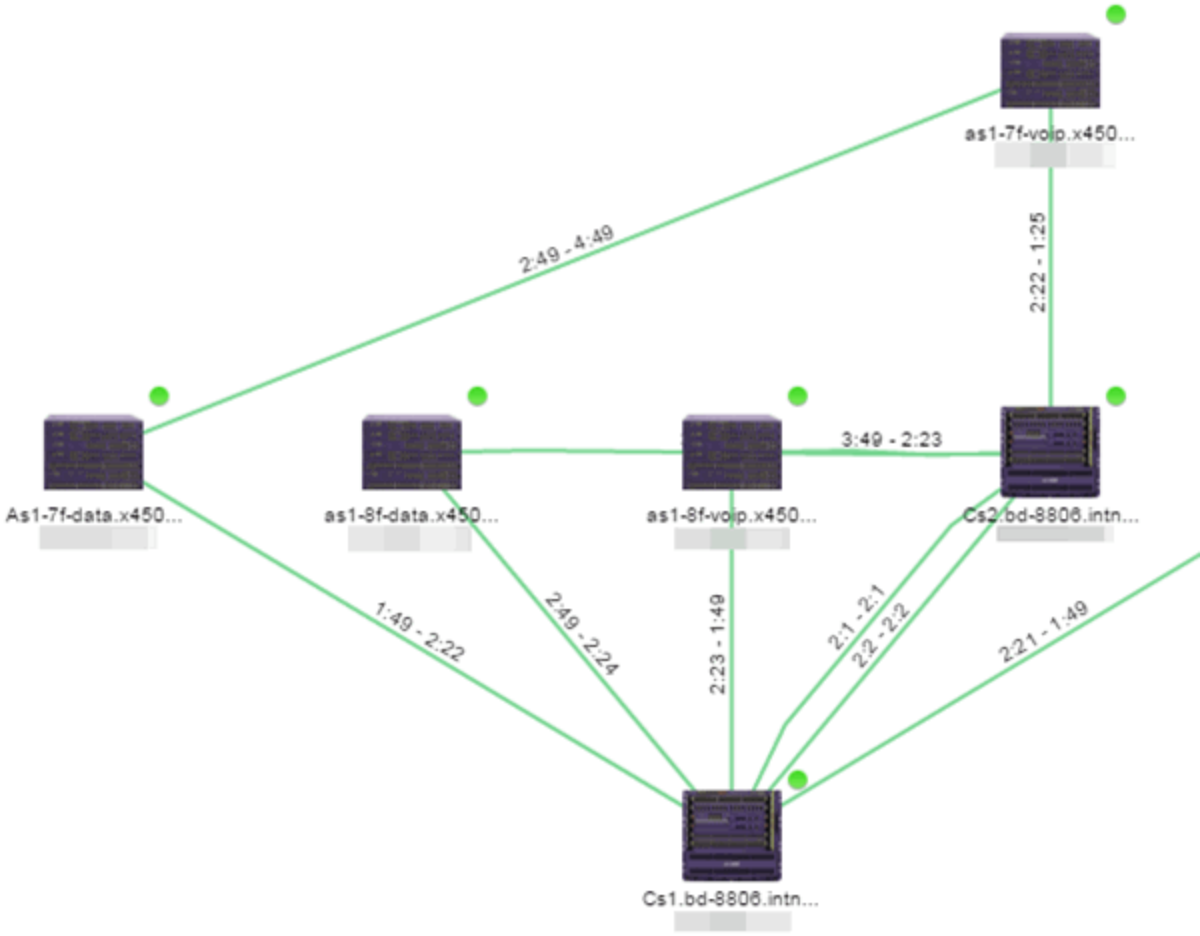
6. Select **File** > **Properties** to open the Map Properties window from which you can edit the map criteria.



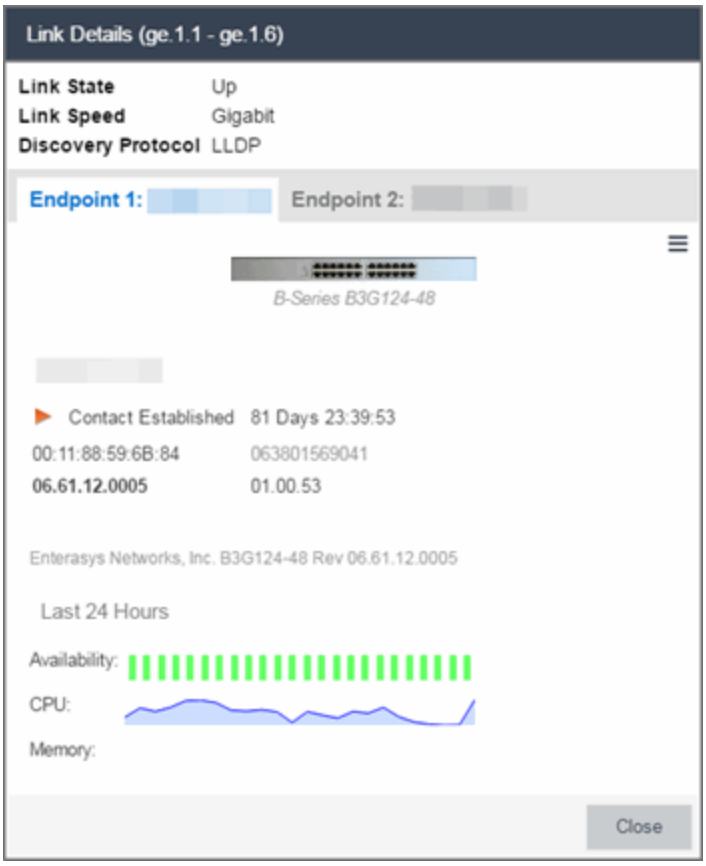
   a. In the **Map Name** field, change the name for the map, if necessary.

   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 the .png, .PNG, and .PNG format. 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.

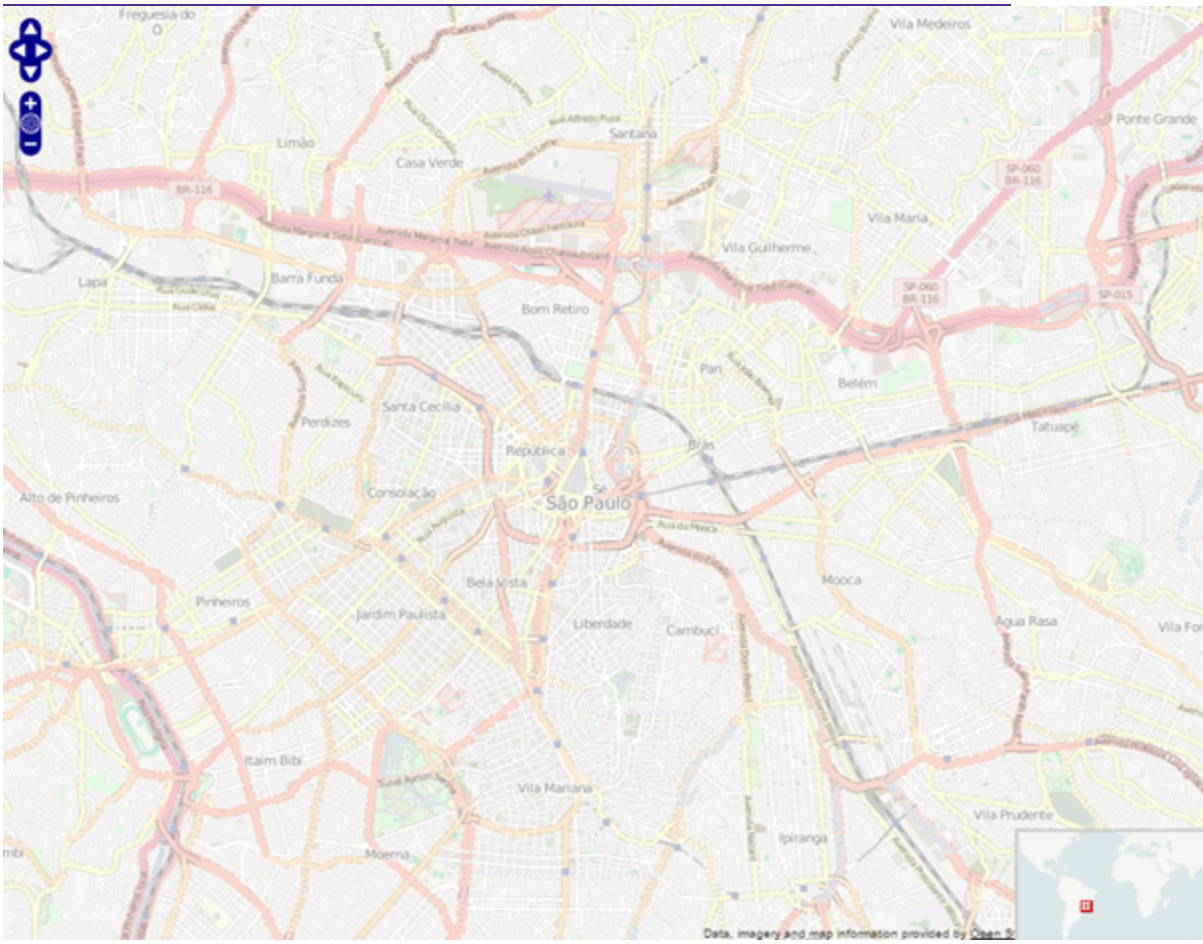
NOTE: If you upload a map image and an image with the same name already exists, the existing image is replaced.

The Map feature supports images in the .png, .PNG, and .PNG format. 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.

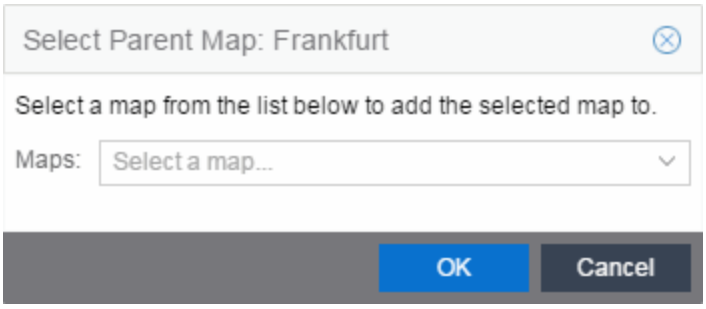
- Geographic —Displays a global or regional map where network locations are shown geographically.

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**.

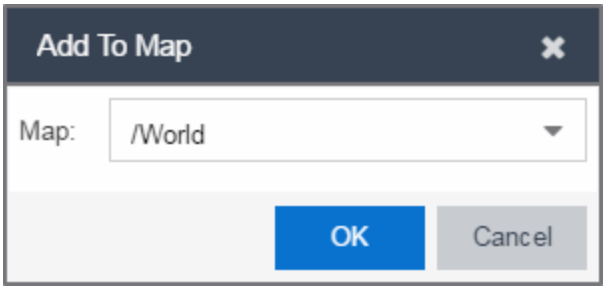
Adding Devices/APs from ExtremeCloud IQ - Site Engine Devices and Wireless

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.

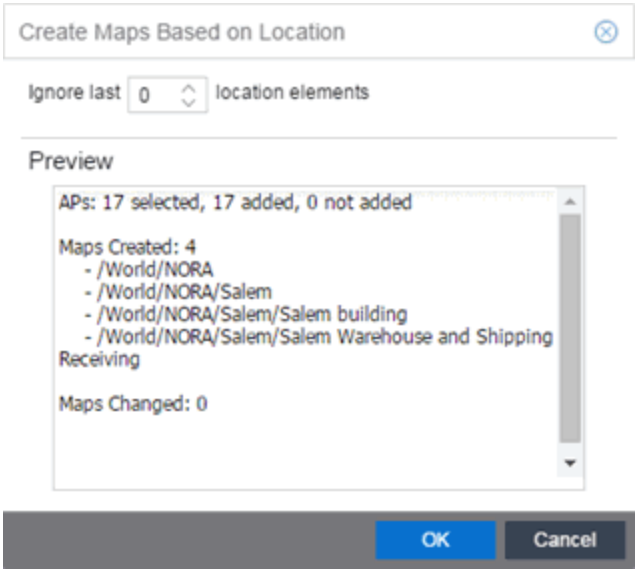
Add to New Maps Based on Location

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.

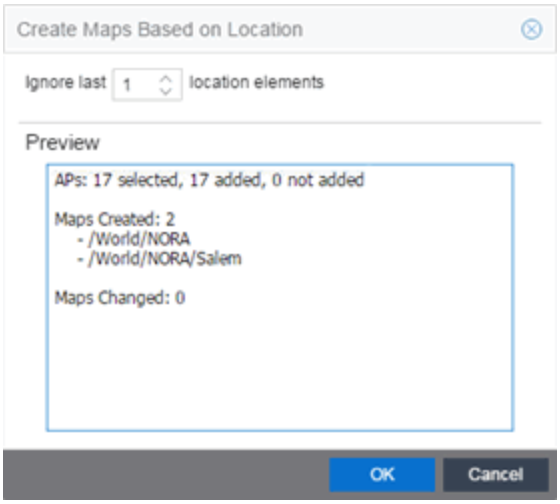
1. On the **Network** > **Devices** tab, right-click on one or more devices and select **Maps** > **Create Maps for Locations**.
   On the **Wireless** tab, select the Access Points report, right-click on one or more APs, and select **Maps** > **Create Maps for Locations**.
2. The Create Maps Based on 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

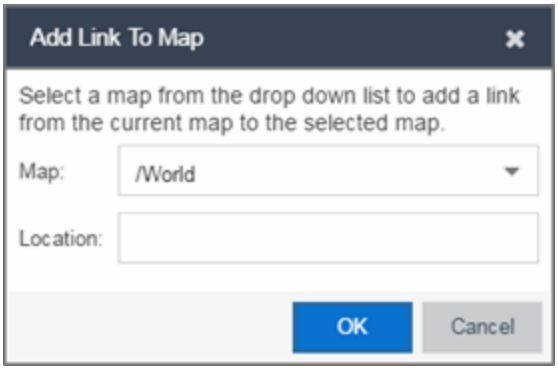
You can use map links to jump from one map to another. Map links display the name of the map and an aggregated alarm/device status for the linked map. Double-click on the link to go to the linked map.

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.

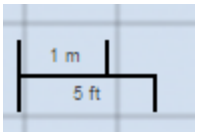
5. Enter information in **Location** about the location to which the link connects and select **OK**.
6. The map link is added to the map and can be repositioned, if desired.
7. Select the **Save** button to save the map and close the properties panel.

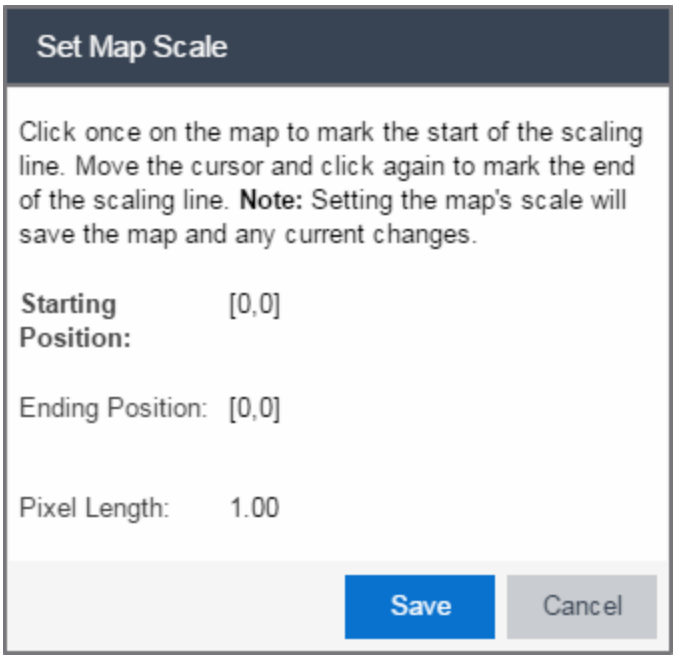
Setting the Map Scale

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.

Related Information

- 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.

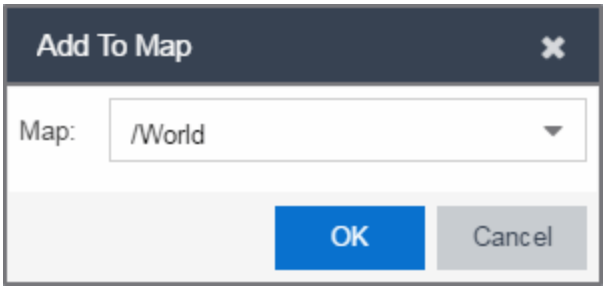
In order to edit maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

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.

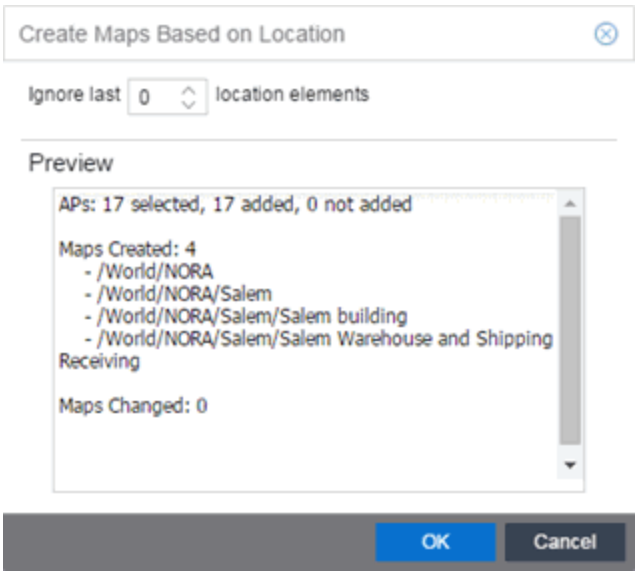
Add to New Maps Based on Location

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.

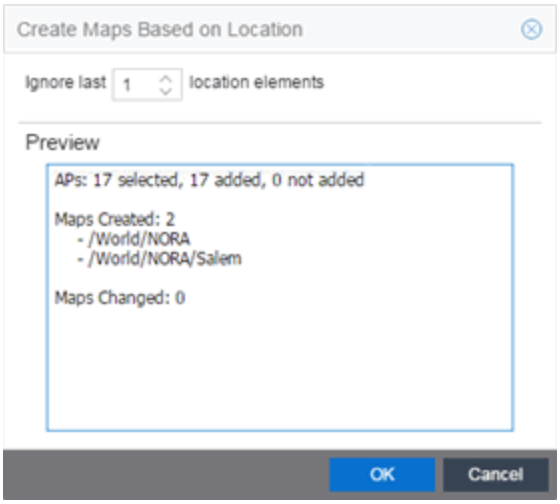
1 On the **Network** > **Devices** tab, right-click on one or more devices and select **Maps** > **Create Maps for Locations**.
On the **Wireless** tab, select the Access Points report, right-click on one or more APs, and select **Maps** > **Create Maps for Locations**.

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.

Related Information

- 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:

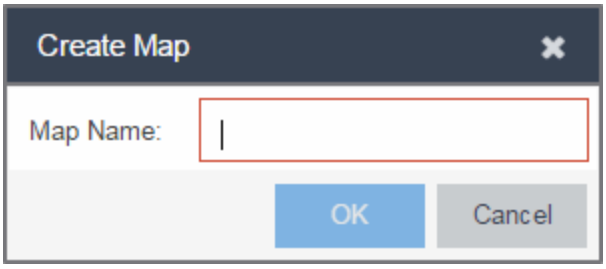
1. In the left-panel Groups/ Maps navigation tree, right-click on the World Site (or any other map in the tree) and select **Maps** > **Create Map**.

   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.

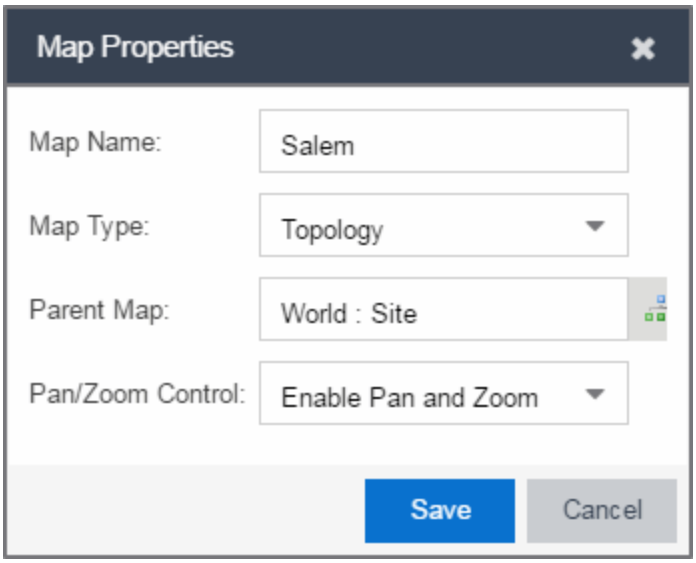
2. Enter a name for the map and select **OK**.



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.

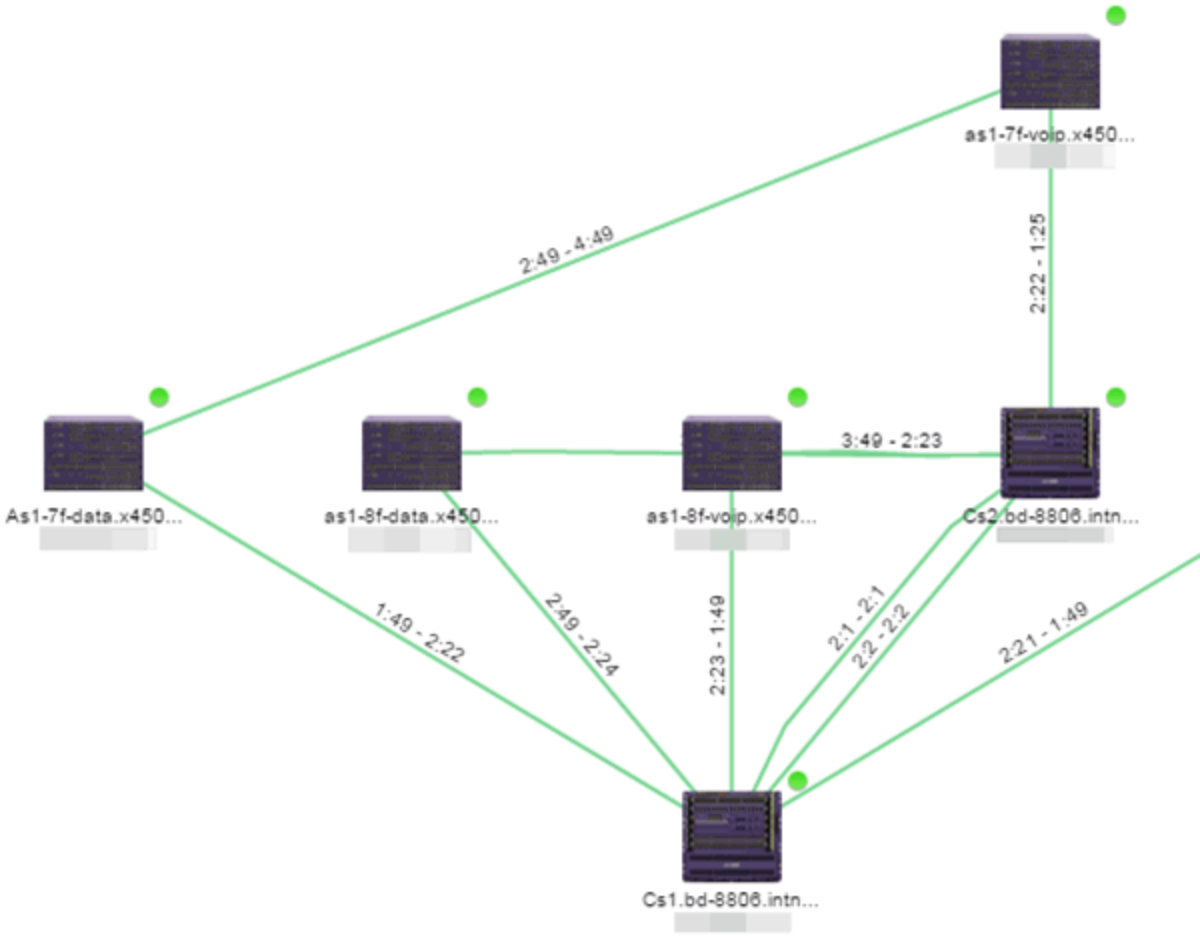


   a. In the **Map Name** field, change the name for the map, if necessary.

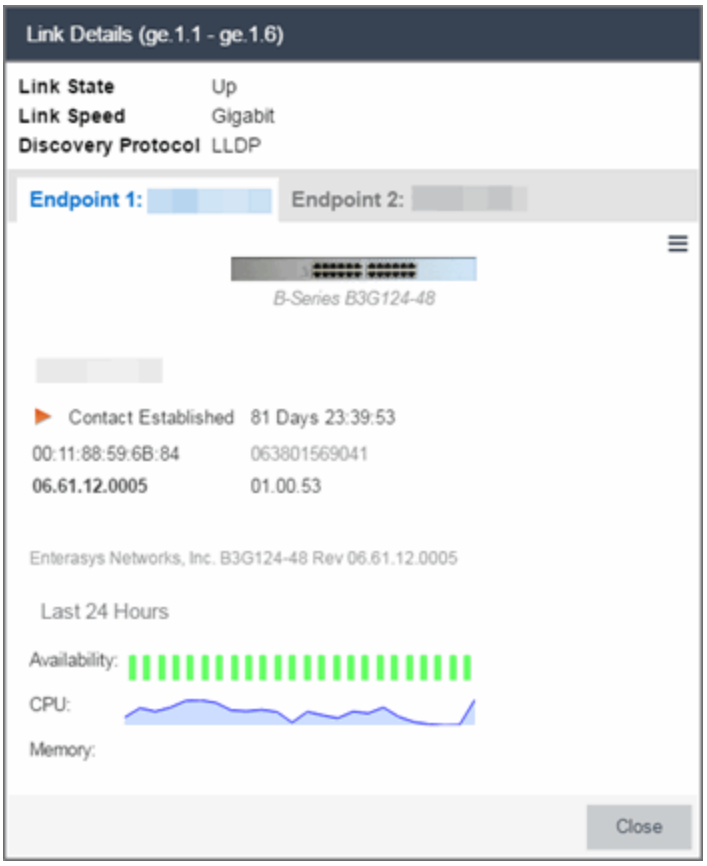
   b. In the **Map Type** drop-down list, select the type of map you are creating:

      - 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, .PNG, and .PNG 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.

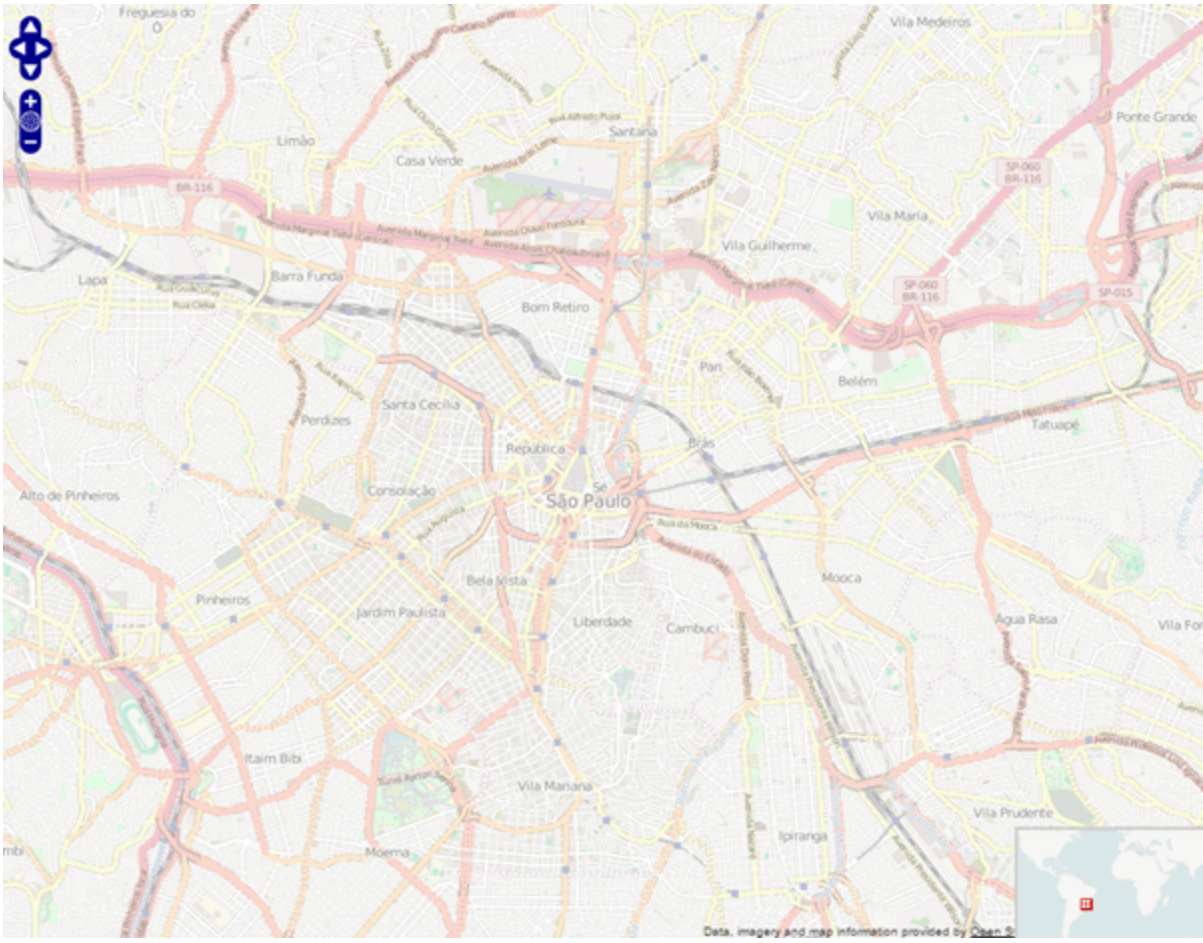
- Open space —The wireless APs are located in an environment with no walls or cubicles.
- Office cubicles —The wireless APs are located in an environment with cubicle offices present.
- Drywall —The wireless APs are located in an environment where the office wall composition is drywall.
- Brick walls —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.

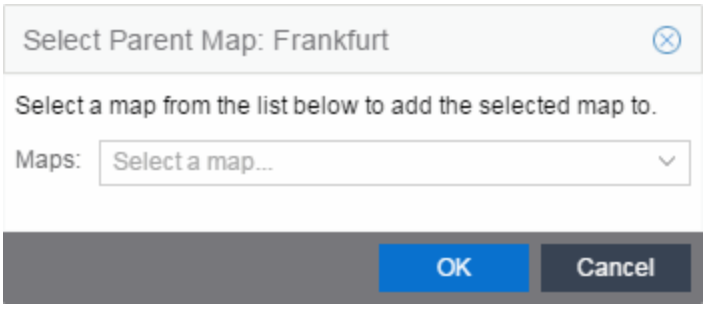
NOTE: If you upload a map image and an image with the same name already exists, the existing image is replaced.

- 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.

Related Information

- 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:

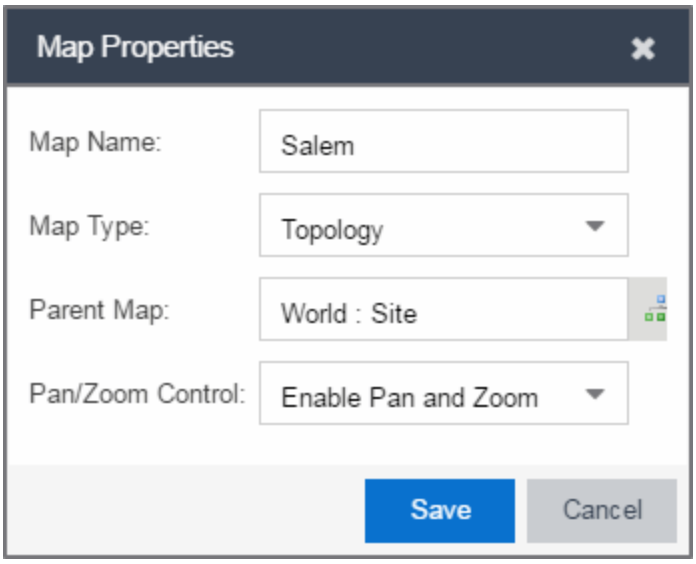
1. Launch ExtremeCloud IQ - Site Engine.
2. Select the **Network** > **Devices** tab.
3. Select **Sites** from the left-panel drop-down list. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.
4. Expand a site 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**.

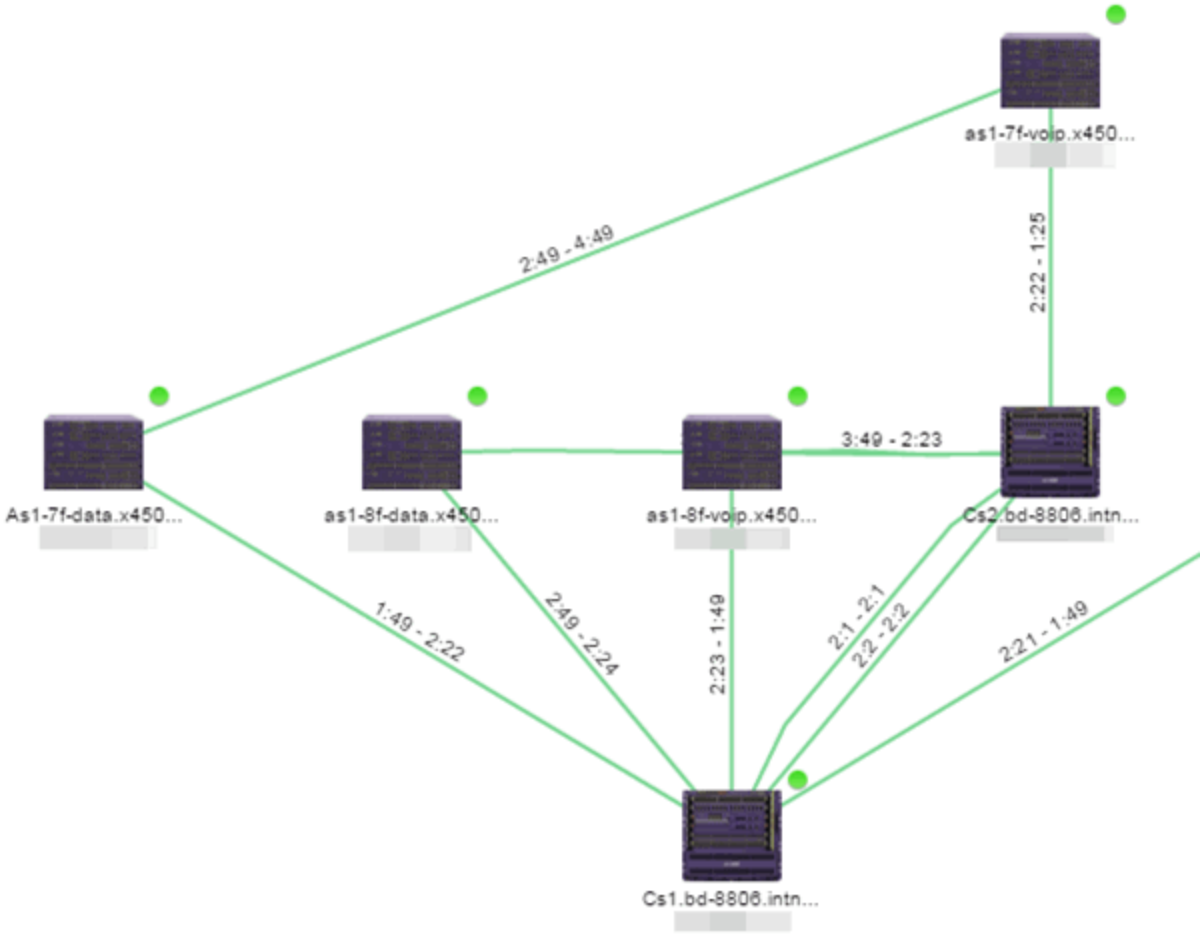
2. Select **File** > **Properties** to open the Map Properties window from which you can edit the map criteria.



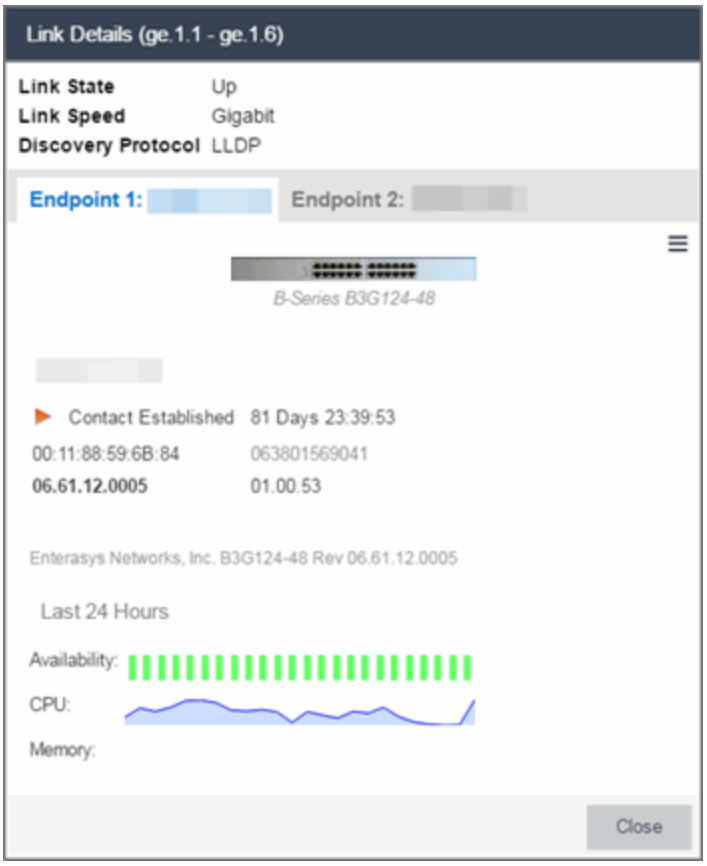
   a. In the **Map Name** field, change the name for the map, if necessary.

   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 the .png, .PNG, and .PNG format. 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.

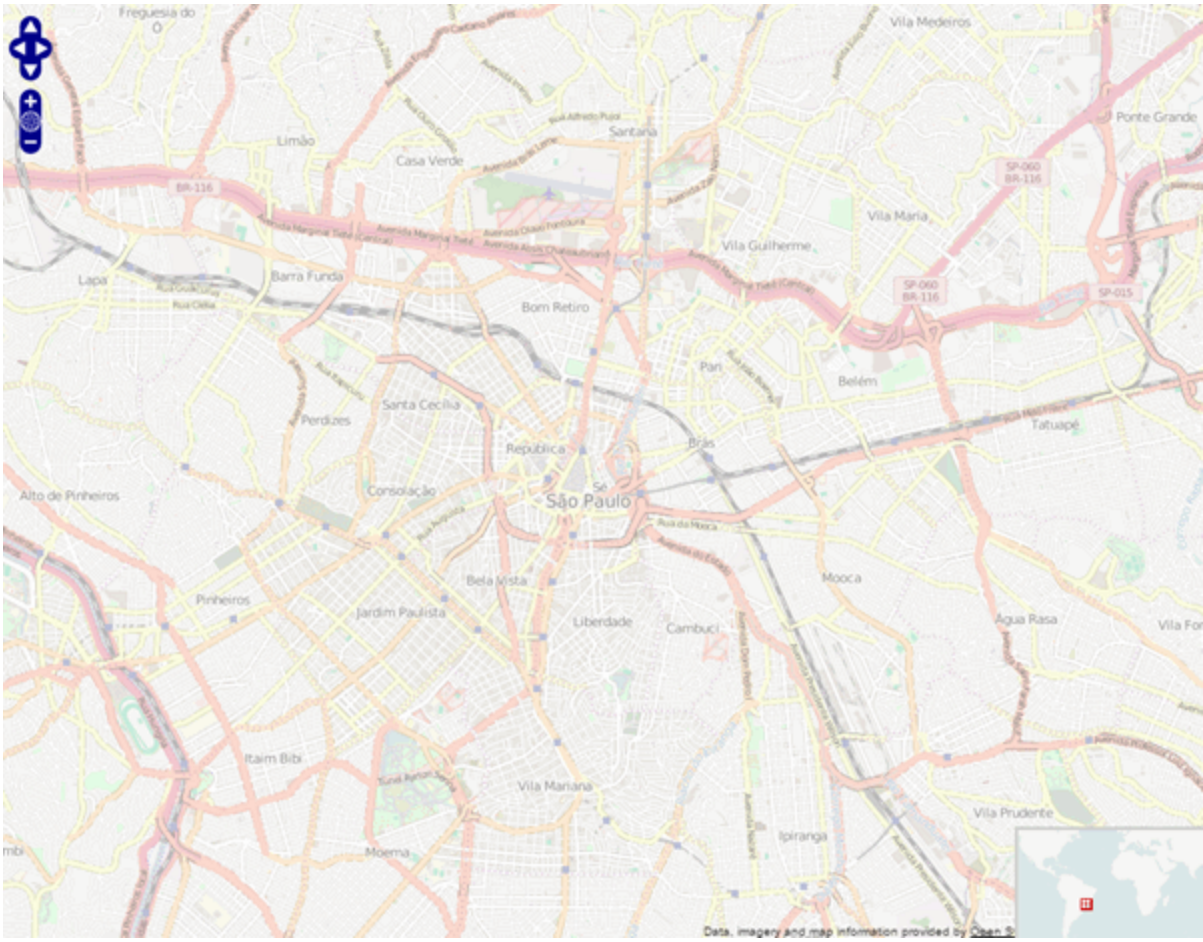
- Open space —The wireless APs are located in an environment with no walls or cubicles.
- Office cubicles —The wireless APs are located in an environment with cubicle offices present.
- Drywall —The wireless APs are located in an environment where the office wall composition is drywall.
- Brick walls —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.

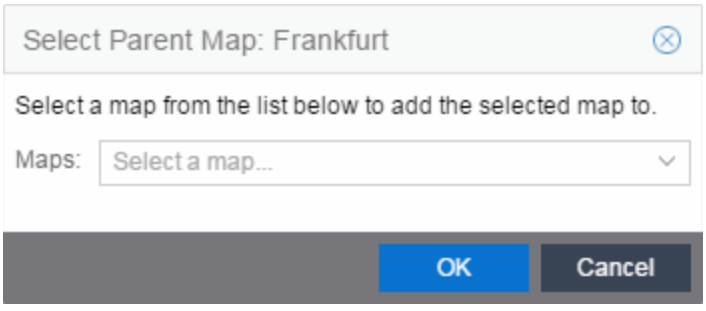
NOTE: If you upload a map image and an image with the same name already exists, the existing image is replaced.

- 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.

Related Information

- 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**—The map import function gives you the ability to import Ekahau maps into floor plan maps. This function also lets you export floor plan maps to a ZIP file.
- **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 8.31or 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.

Related Information

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:

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 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 floorplan and wall information used to provide accuracy in the signal strength computation.
- **Import and Export Maps**—The map import function gives you the ability to import Ekahau maps into floorplan maps. This function also lets you export floorplan maps to a ZIP file.
- **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 8.31or 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.

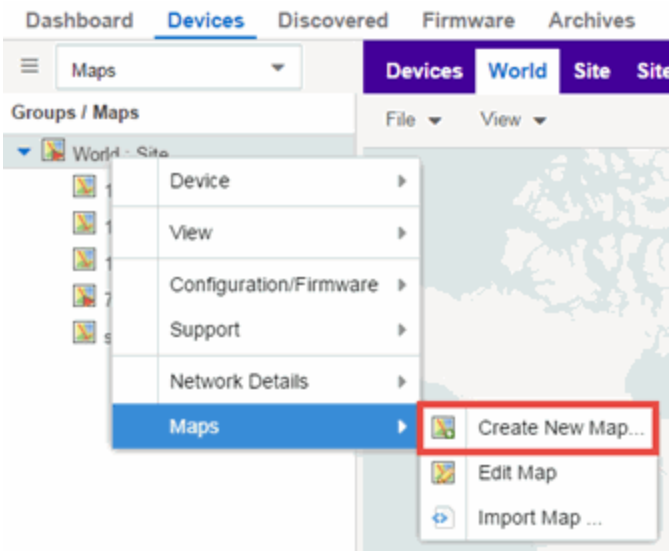
The wall information from the floorplan is used to help determine the degradation of signal strength that occurs as a wireless radio signal passes through the walls, and helps define the probable distance of a client from a given access point. ExtremeCloud IQ - Site Engine uses the wall information to 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 the .png, .PNG, and .PNG 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.

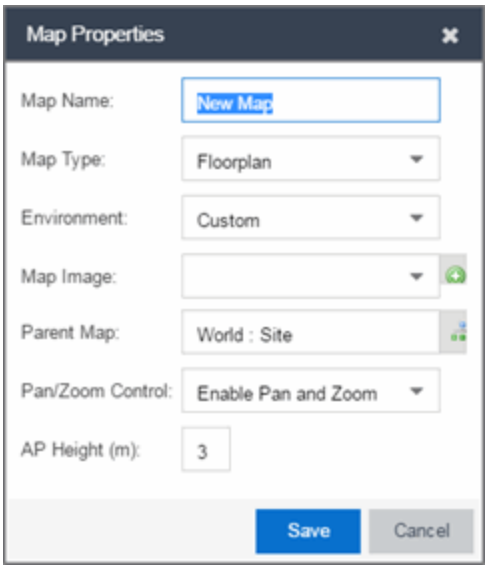
The following steps provide a workflow for creating a floorplan showing the exterior and interior walls of a building. By drawing the walls over an existing floorplan image, you can add information that provide greater accuracy in wireless calculations.

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 the .png, .PNG, and .PNG formats. The maximum image size is 890 x 670 pixels. Images that are larger than this are automatically scaled down to the maximum size allowed.

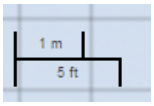
h. Set the **AP Height** property. This value is the distance from the floor to the AP position on the wall or ceiling in meters. This is a single value used for all access points. Setting a reasonable value helps with the accuracy of the location feature. The default for this value is three meters, which is at the top of a wall with a nine foot ceiling.

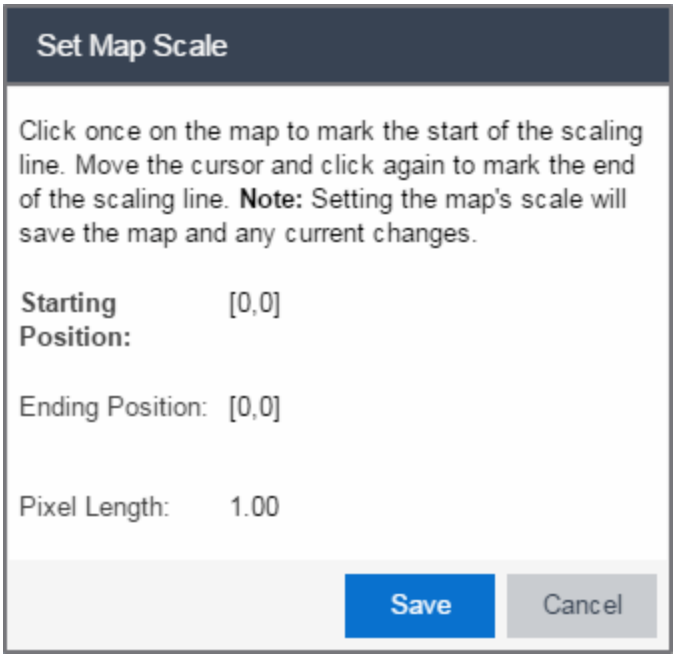
i. Select **Save** to save the map and display the image.

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.

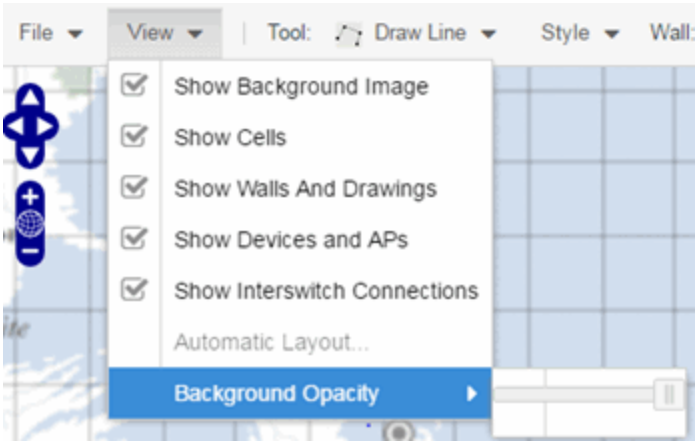
d. Use these same steps to draw the remaining walls on your floorplan. Be sure to deselect the **Exterior** checkbox for the other walls.

   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.

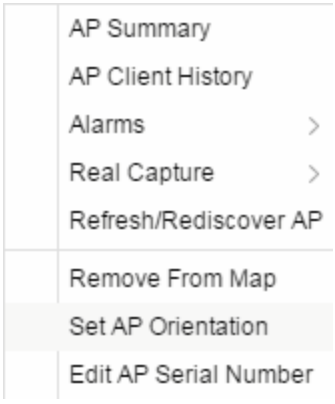


4. **Add your APs to the map.** In Edit mode, a panel that lists equipment available to add to the map is visible beneath the properties panel. The display is filtered on either the currently discovered devices or the APs known to wireless controllers on your network, depending on your selection (APs or Devices) in the panel title bar. You can

use the search field to locate a specific device or AP.

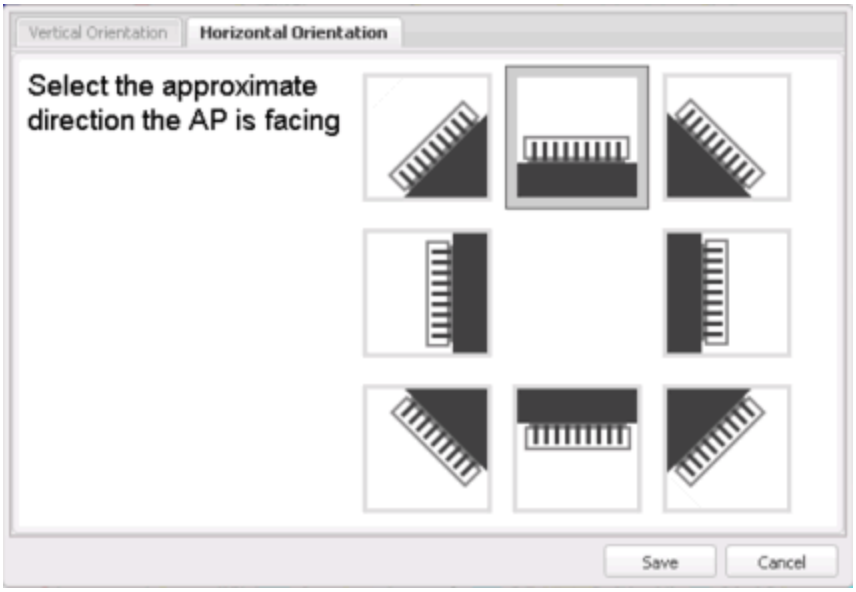
Drag the desired devices and APs onto the map area and position them to produce your network map. Be sure the APs are in the correct location, so your location and coverage maps are accurate. The center of the image is roughly the position of the AP. Be sure to place an AP on the correct side of a wall.

5. Set AP orientation.
    a. Right-click on an AP in the map and select **Set AP Orientation**.

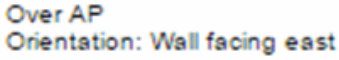


b. Select the **Vertical Orientation** tab to set whether the AP is on the ceiling or wall.

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.

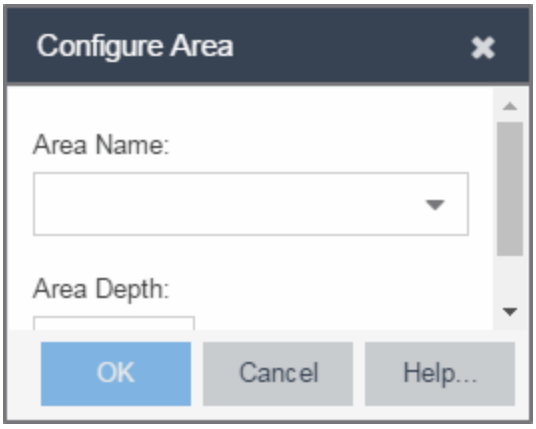
Drawing Tool	Definition
	**Draw Polygon** Position your cursor where you want to start drawing the polygon shape. Select and draw the first line of the polygon. Select each corner of the polygon. Double-click to release the polygon line. When you are finished drawing, right-click to release the draw 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.)
	**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.

Style Option	Description
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

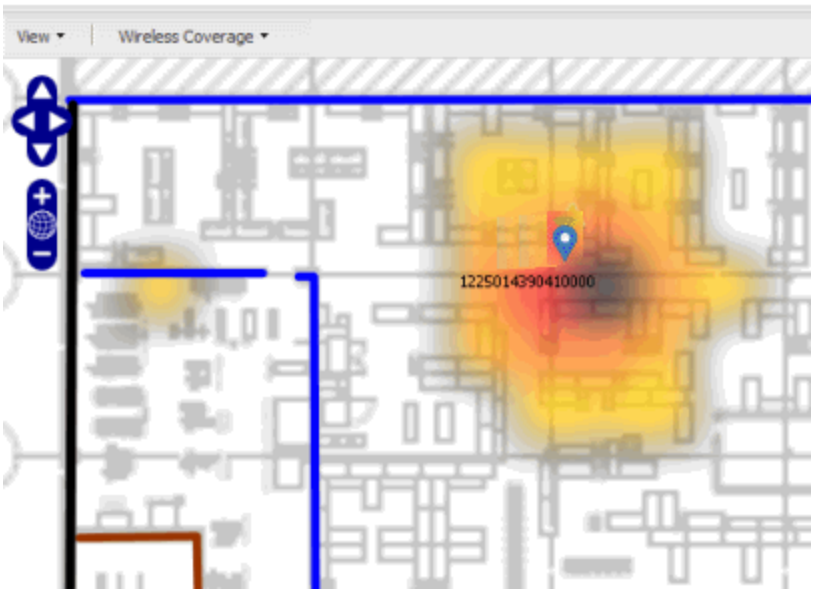
The wireless location feature requires you enable the location engine on the wireless controller. After you add APs to your custom floorplan and save the map, a copy of the floorplan is sent to each controller. The location engine incorporates information defined in the floorplan data and signal information 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.

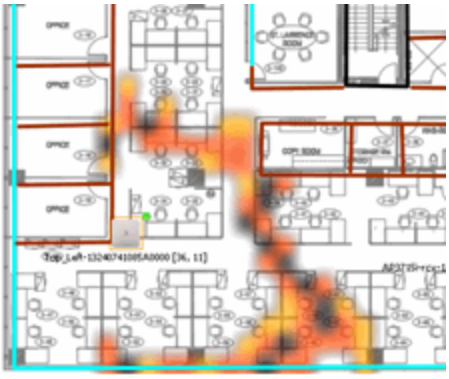
Mouse over the client icon to see a tooltip with client information.

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.

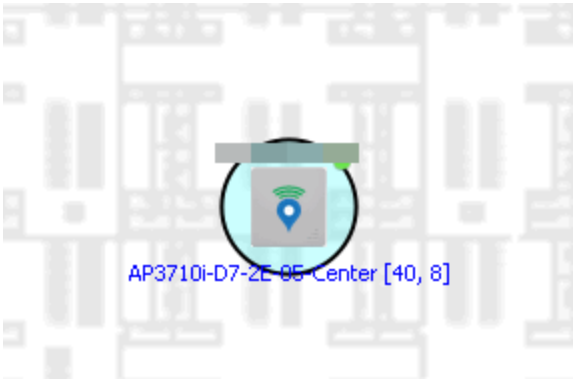


If the location result is based on only one AP, the map displays probabilities for the location but with a few differences:

- 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 802.11channel over the last 30 seconds. Noise floor is measured during the quiet time, between the valid transmission or reception of 802.11frames.
- **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 Ekahau maps into ExtremeCloud IQ - Site Engine floorplan maps.

The map export function exports floorplan maps to a ZIP file.

Importing Maps

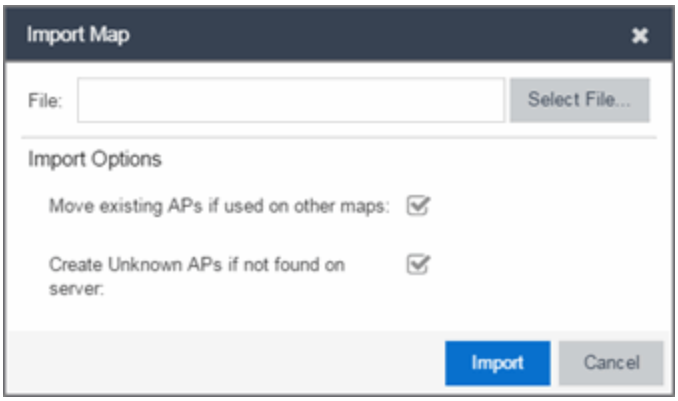
The map import function gives you the ability to import Ekahau maps into ExtremeCloud IQ - Site Engine floorplan maps and gives you the ability to import floorplan maps are previously exported from ExtremeCloud IQ - Site Engine maps.

When Ekahau maps are exported, all the maps in the system are combined into a single ZIP file. When the Ekahau ZIP file is imported into ExtremeCloud IQ - Site Engine, each Ekahau map is re-created into an individual map again.

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:

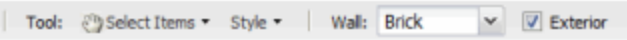
1. Launch ExtremeCloud IQ - Site Engine and select the **Network** > **Devices** tab.
2. In the left-panel, select Maps from the drop-down list.
3. In the Groups/ Maps navigation tree, right-click on the World map and select **Maps** > **Import Map**.
4. The Import Map window opens. Use the **Select 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. All the walls in an Ekahau map are imported as internal walls. You need to 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.



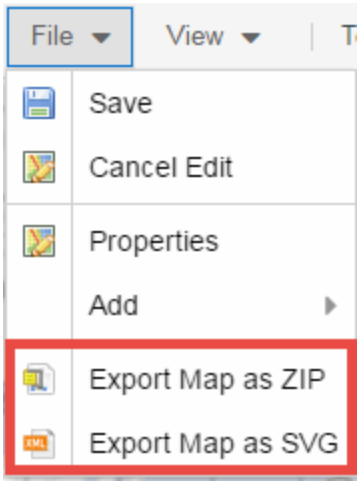
    c. Select **Save** to save the map.

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.

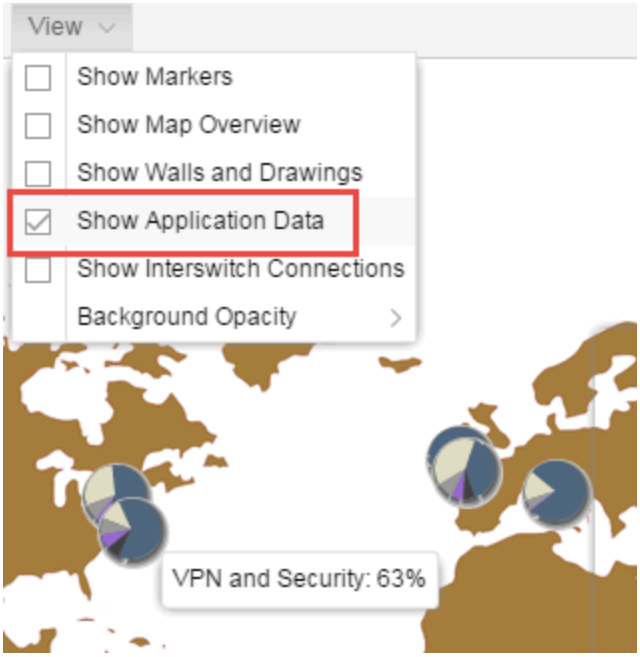
NOTE: The Export Map as ZIP option is only available for Floorplan map types.

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.

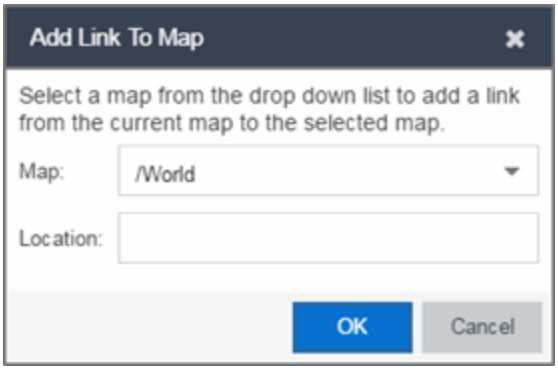
When the **Show Application Data** checkbox in the **View** menu is selected, a pie chart is generated for every map link on the current map. The application data in the pie chart is based on the **Site** field specified for the link and corresponds to a site defined in the Site tab.

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.

Related Information

- 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, .PNG, and .PNG 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.

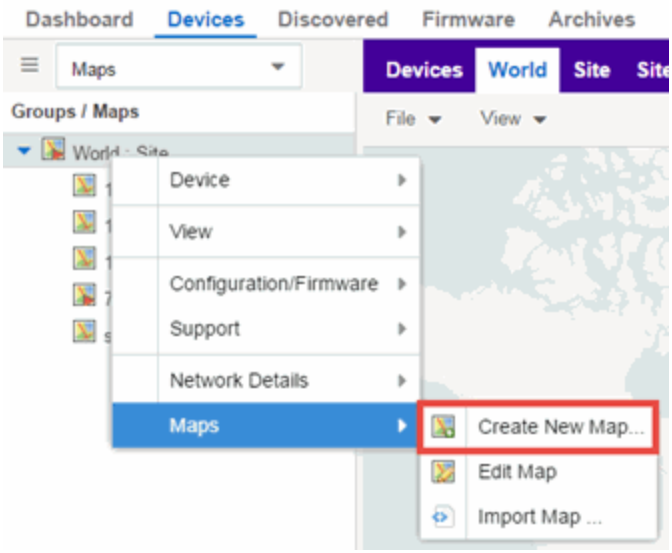
When editing a floorplan, use the View menu to select whether to view or hide the background image, map cells, floorplan walls and drawings, devices and APs, and interswitch connections. You can also set the background image opacity.

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.

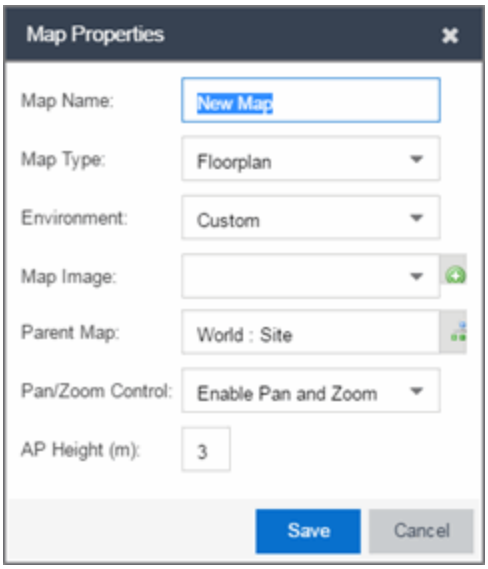
   b. In the left-panel Groups/ Maps navigation tree, right-click on the World map (or any other map that you want as the parent of the new map) and select **Maps** > **Create New Map**.



   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 the .png, .PNG, and .PNG formats. The maximum image size is 890 x 670 pixels. Images that are larger than this are automatically scaled down to the maximum size allowed.

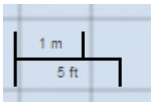
h. Set the **AP Height** property. This value is the distance from the floor to the AP position on the wall or ceiling in meters. This is a single value used for all access points. Setting a reasonable value helps with the accuracy of the location feature. The default for this value is three meters, which is at the top of a wall with a nine foot ceiling.

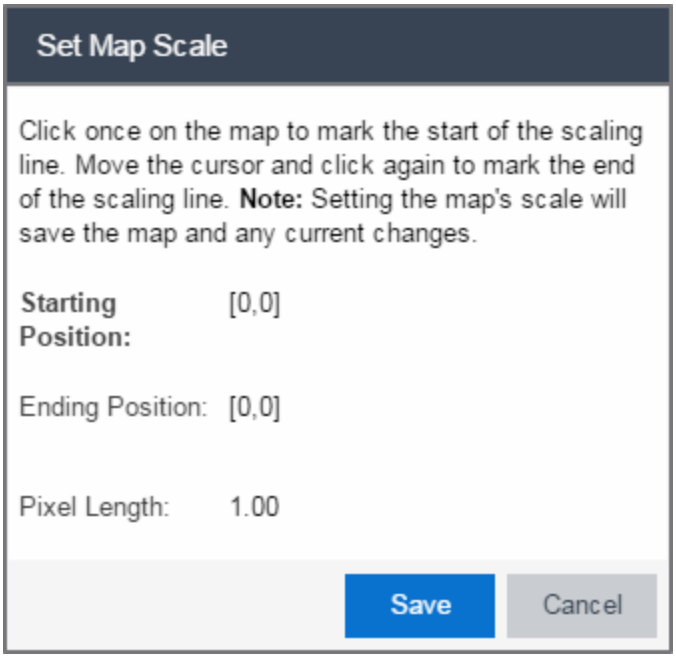
i. Select **Save** to save the map and display the image.

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.

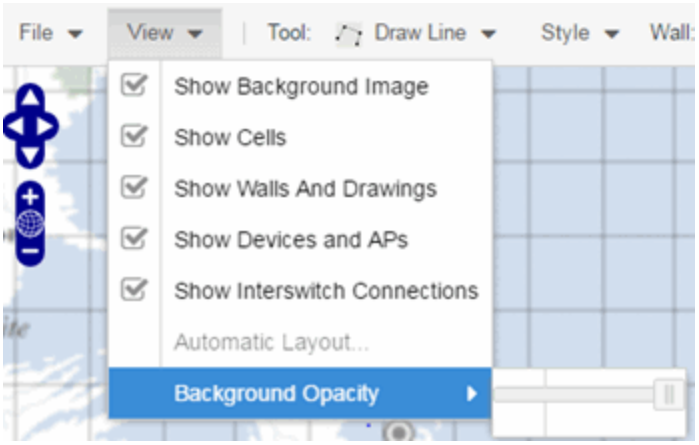
d. Use these same steps to draw the remaining walls on your floorplan. Be sure to deselect the **Exterior** checkbox for the other walls.

   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.

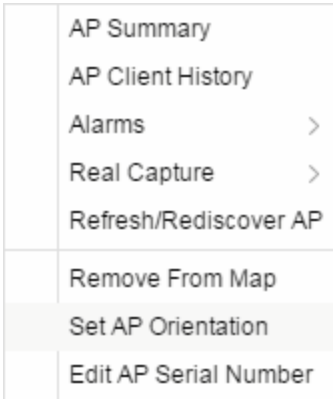


4. **Add your APs to the map.** In Edit mode, a panel that lists equipment available to add to the map is visible beneath the properties panel. The display is filtered on either the currently discovered devices or the APs known to wireless controllers on your network, depending on your selection (APs or Devices) in the panel title bar. You can

use the search field to locate a specific device or AP.

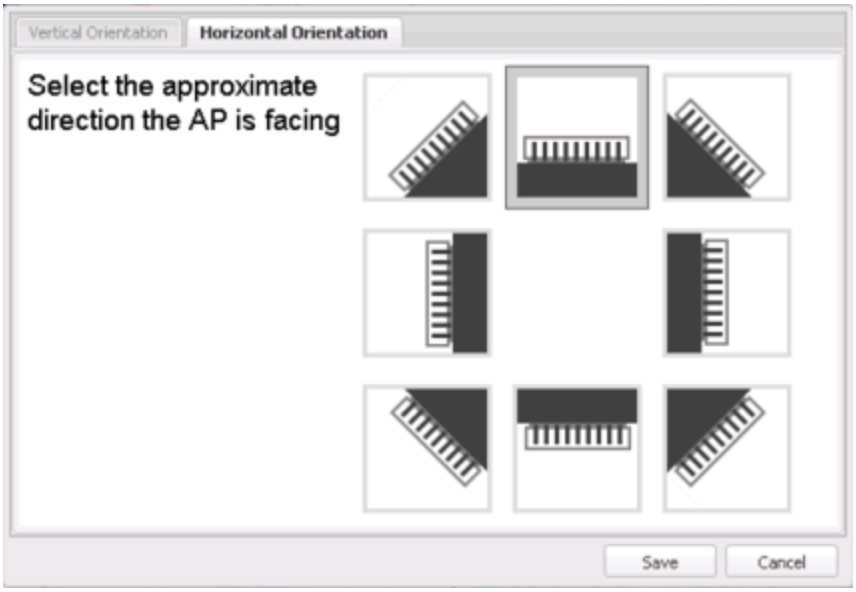
Drag the desired devices and APs onto the map area and position them to produce your network map. Be sure the APs are in the correct location, so your location and coverage maps are accurate. The center of the image is roughly the position of the AP. Be sure to place an AP on the correct side of a wall.

5. Set AP orientation.
    a. Right-click on an AP in the map and select **Set AP Orientation**.

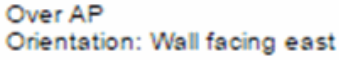


b. Select the **Vertical Orientation** tab to set whether the AP is on the ceiling or wall.

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.

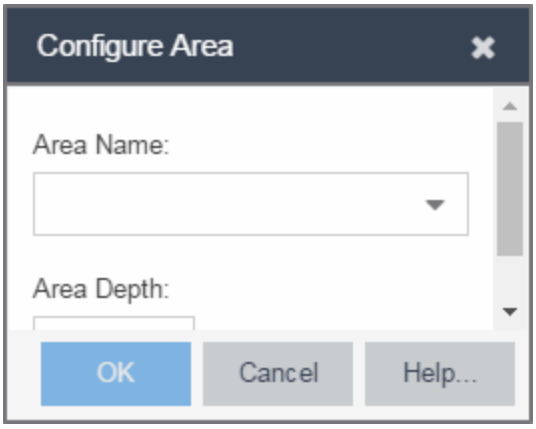
Drawing Tool	Definition
	**Draw Polygon** Position your cursor where you want to start drawing the polygon shape. Select and draw the first line of the polygon. Select each corner of the polygon. Double-click to release the polygon line. When you are finished drawing, right-click to release the draw 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.)
	**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.

Style Option	Description
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.

Related Information

- 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.

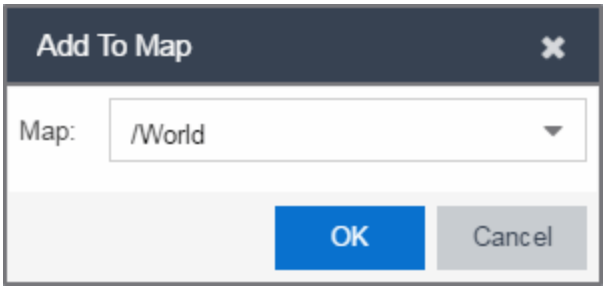
In order to edit maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

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.

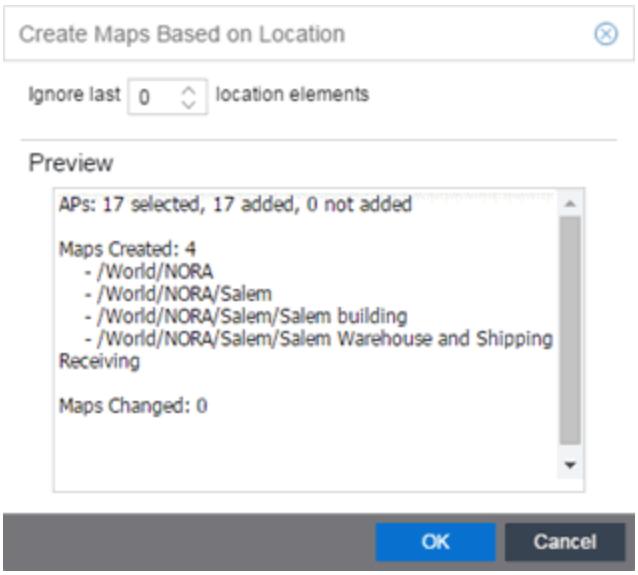
Add to New Maps Based on Location

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.

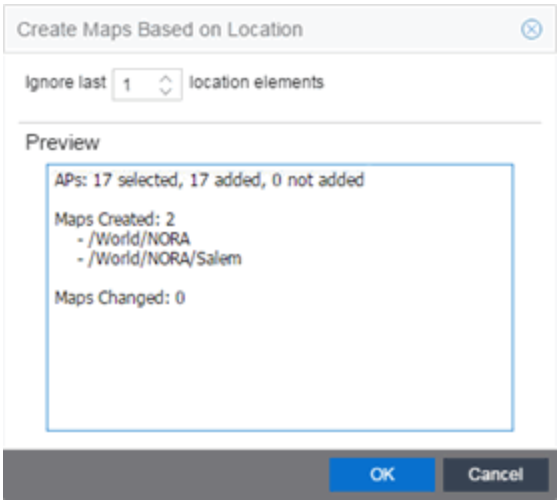
1 On the **Network** > **Devices** tab, right-click on one or more devices and select **Maps** > **Create Maps for Locations**.
On the **Wireless** tab, select the Access Points report, right-click on one or more APs, and select **Maps** > **Create Maps for Locations**.

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.

Related Information

- ExtremeCloud IQ - Site Engine Maps
- Advanced Map Features

How to Display Map Application Data

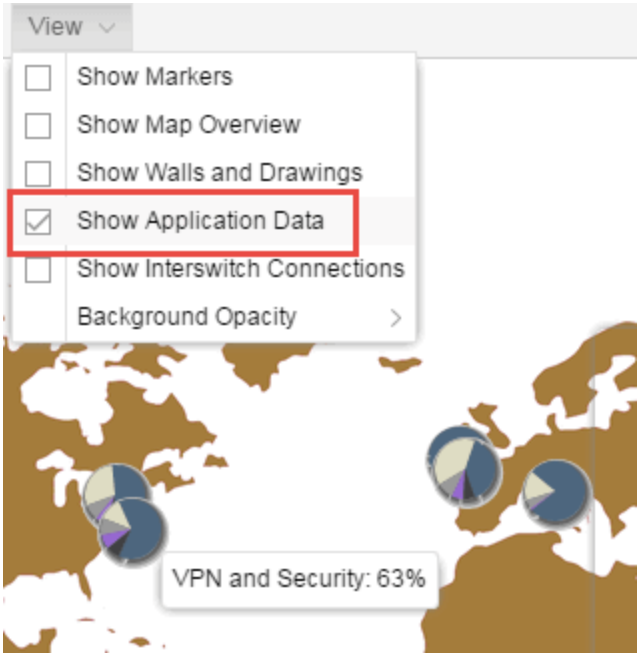
The **Network** > **Devices** tab contains Map features that let you create geographic and topological maps of the devices and floor plans of wireless access points (APs) on your network. The advanced Map features allows you to display application data in maps by creating map links tied to sites. Application 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.

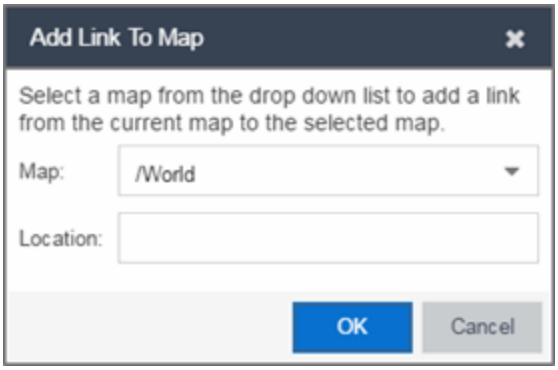
The pie chart displays the top five application groups (by bytes transferred) for the site specified for the map link.

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.

Related Information

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.

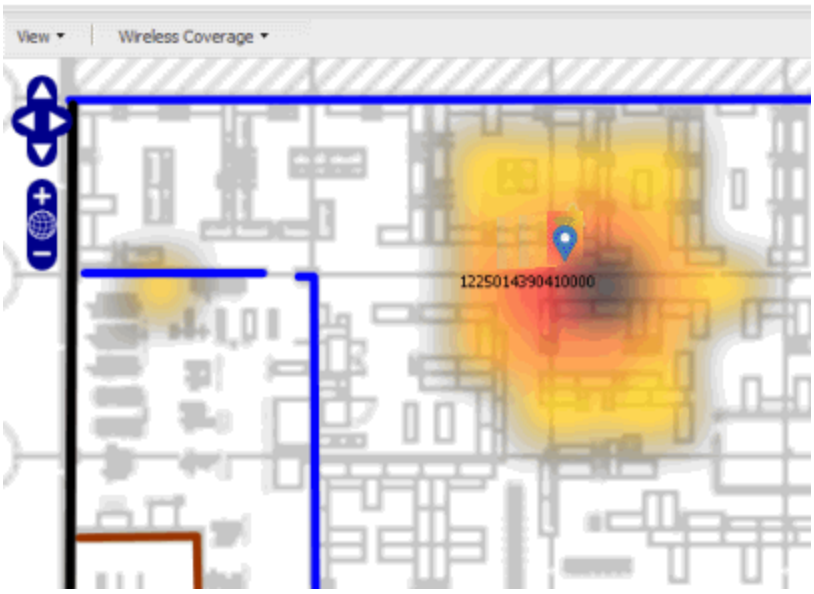
The location engine incorporates information defined in the floorplan data and signal information from a client's contact with APs in order to calculate a client's precise location in the covered area. Client information from within a short time frame must be reported by at least three APs in order to 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.)

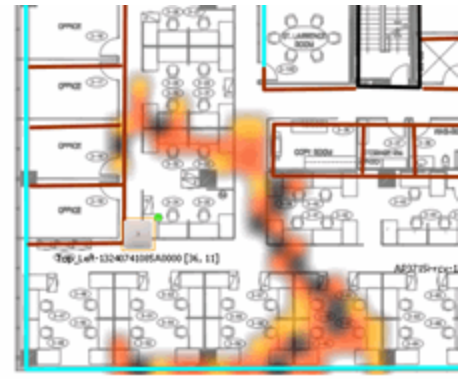
   The map containing the AP is displayed with an icon for the client. A colored distribution of location confidence is shown on the map with black being highest confidence, red medium confidence, and yellow lowest confidence.
5. On the View tab, use the **Min. Location Confidence** slider to filter out 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.

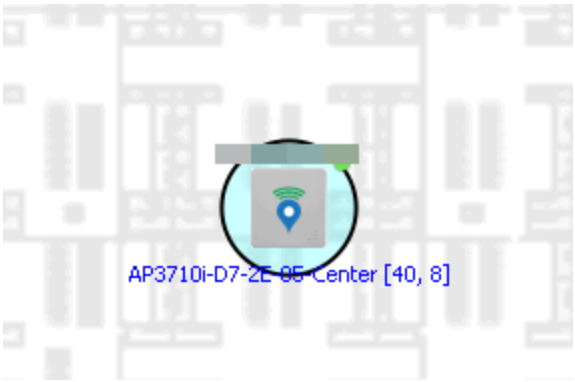


If the location result is based on only one AP, the map displays probabilities for the location but with a few differences:

- 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.

Related Information

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 802.11channel over the last 30 seconds. Noise floor is measured during the quiet time, between the valid transmission or reception of 802.11frames.
- **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.

Related Information

For information on related topics:

- ExtremeCloud IQ - Site Engine Maps
- Advanced Map Features

How to Export Maps

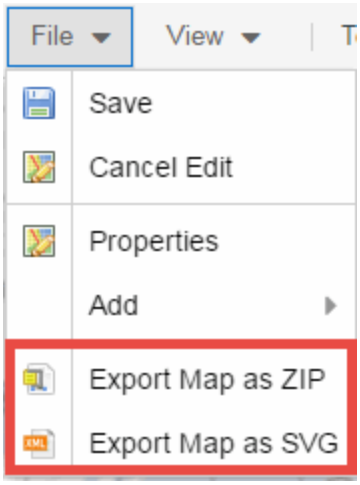
The ExtremeCloud IQ - Site Engine Maps lets you import saved maps of devices and wireless access points (APs) from your local drive or network, and configure the behavior of the imported maps.

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.

Related Information

- 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.

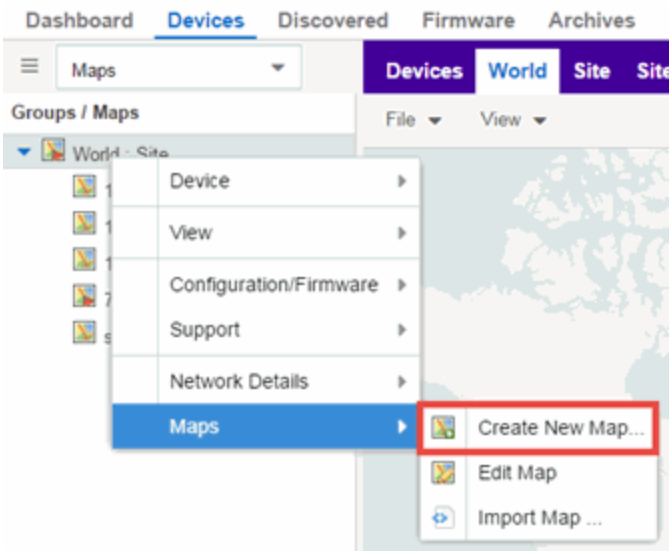
The wall information from the floorplan is used to help determine the degradation of signal strength that occurs as a wireless radio signal passes through the walls, and helps define the probable distance of a client from a given access point. ExtremeCloud IQ - Site Engine uses the wall information to 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, .PNG, and .PNG 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.

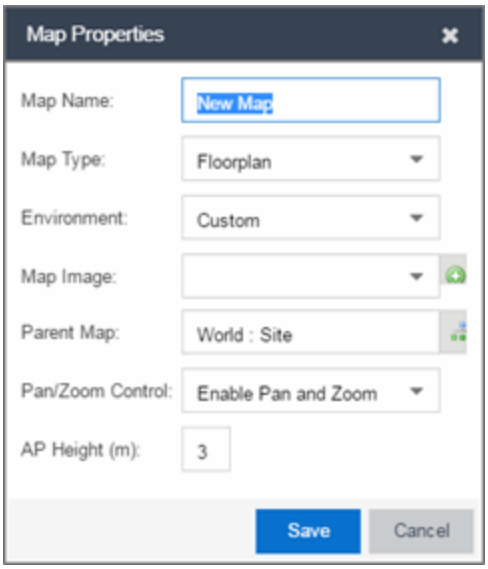
1. **Create and configure a new map.**
   a. Launch ExtremeCloud IQ - Site Engine and select the **Network** > **Devices** tab.
   b. In the left-panel Groups/ Maps navigation tree, right-click on the World map (or any other map that you want as the parent of the new map) and select **Maps** > **Create 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 the .png, .PNG, and .PNG formats. The maximum

image size is 890 x 670 pixels. Images that are larger than this are automatically scaled down to the maximum size allowed.

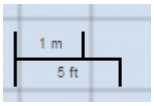
h. Set the **AP Height** property. This value is the distance from the floor to the AP position on the wall or ceiling in meters. This is a single value used for all access points. Setting a reasonable value helps with the accuracy of the location feature. The default for this value is three meters, which is at the top of a wall with a nine foot ceiling.

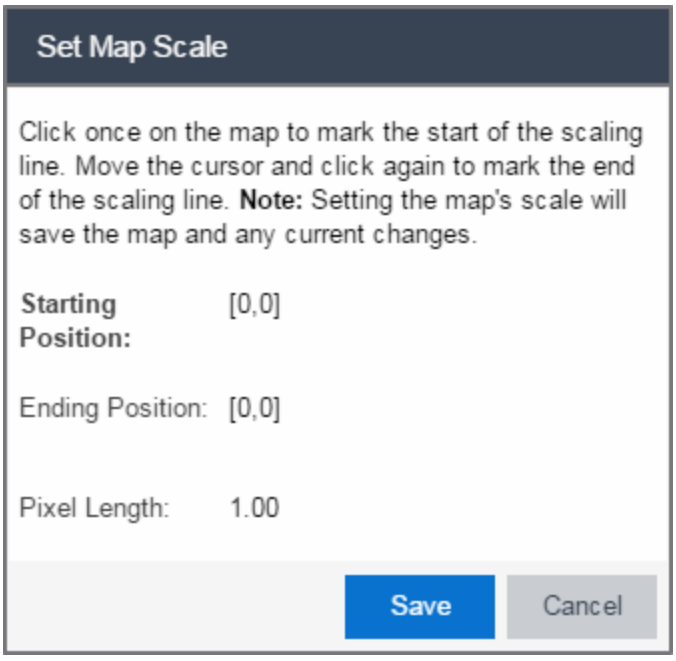
i. Select **Save** to save the map and display the image.

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.

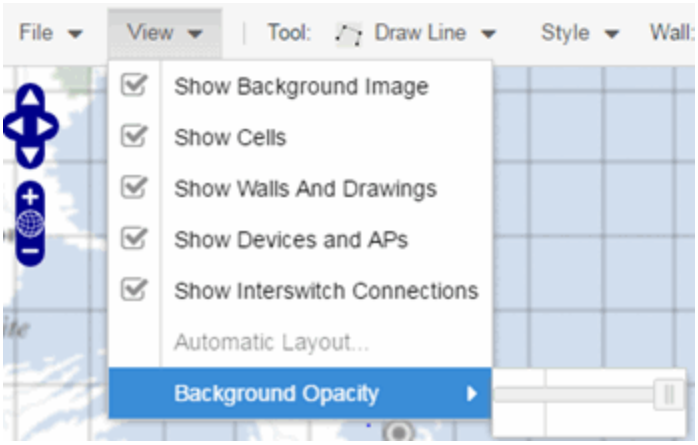
   You can trace over existing walls on the floorplan or add new walls, if necessary. Focus on high attenuation walls like concrete or large sections of glass. It is not necessary to incorporate walls and structures that do not fully divide the space,

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.

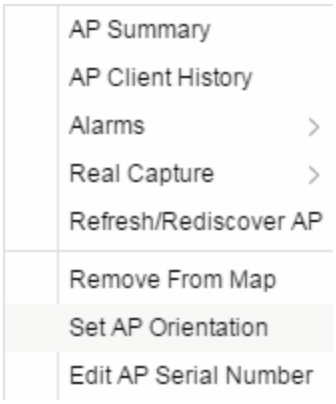
e. While editing, use the **View** menu to select whether to view or hide the background image, map cells, floorplan walls and drawings, devices and APs, and interswitch connections. You can also select an automatic layout and set the background image opacity.



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.

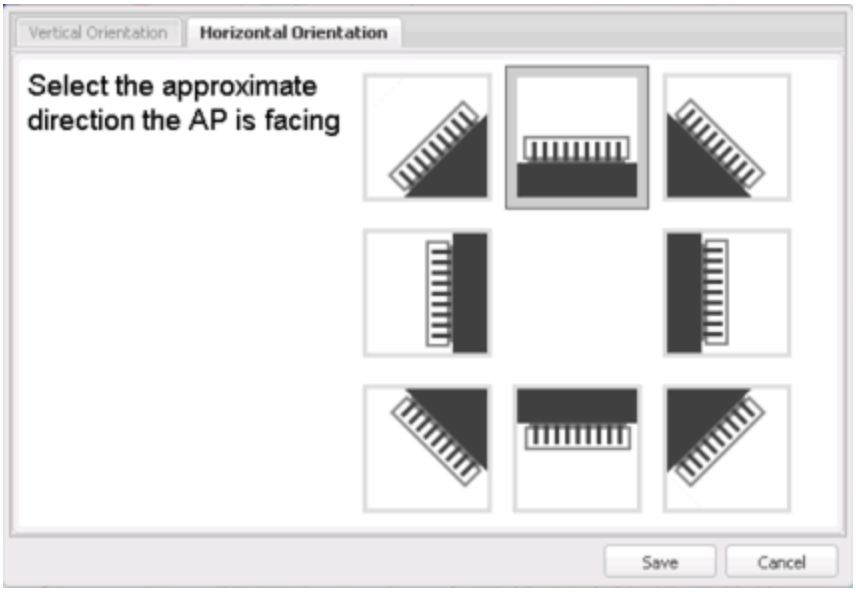
   Drag the desired devices and APs onto the map area and position them to produce your network map. Be sure the APs are in the correct location, so your location and coverage maps are accurate. The center of the image is roughly the position of the AP. Be sure to place an AP on the correct side of a wall.

5. Set AP orientation.
    a. Right-click on an AP in the map and select **Set AP Orientation**.

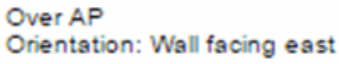


    b. Select the **Vertical Orientation** tab to set whether the AP is on the ceiling or wall.

    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.
	**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.

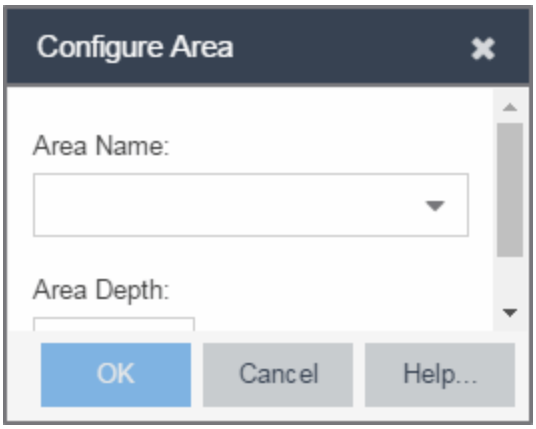
Drawing Tool	Definition
	**Draw Triangle** Position the cursor where you want the triangle. Select and drag to draw the triangle. When you are finished drawing, right-click to release the draw triangle tool.
	**Draw Line** Position your cursor where you want to start drawing the line. Select and draw 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.)
	**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.

Related Information

- ExtremeCloud IQ - Site Engine Maps
- Advanced Map Features

How to Export Maps

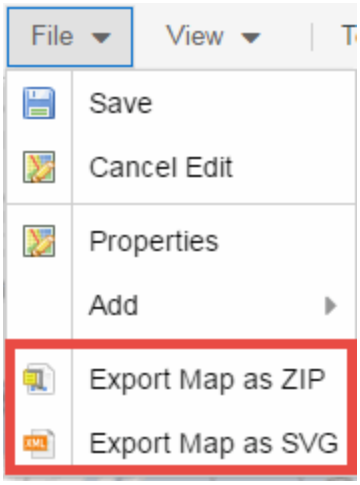
The ExtremeCloud IQ - Site Engine Maps lets you import saved maps of devices and wireless access points (APs) from your local drive or network, and configure the behavior of the imported maps.

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.

Related Information

- 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:

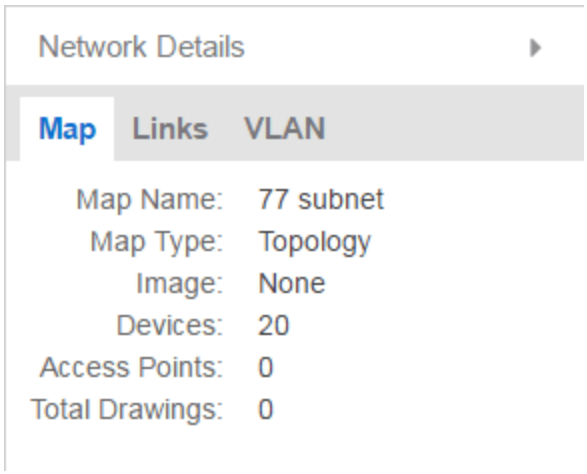
1. Launch ExtremeCloud IQ - Site Engine.
2. Select the **Network** > **Devices** tab.
3. Select **Sites** from the left-panel drop-down list. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.
4. Expand a site 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.



Related Information

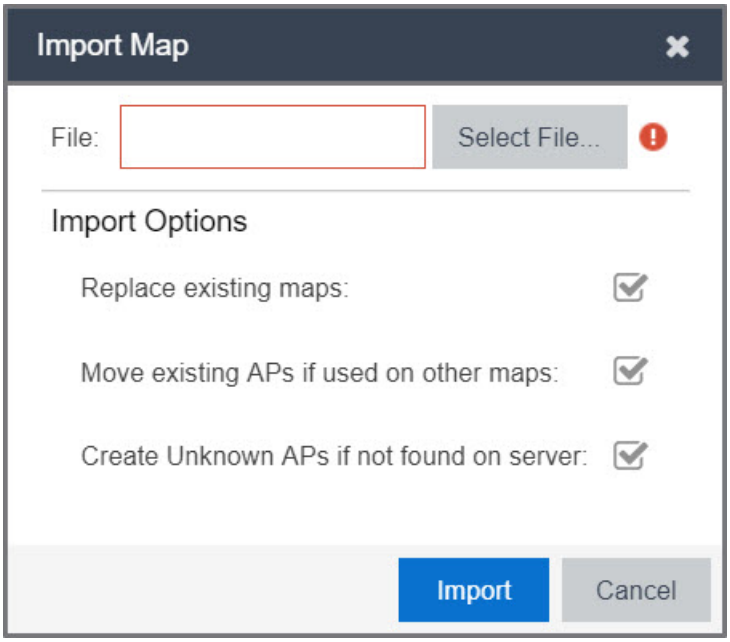
For information on related topics:

- 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.

Related Information

For information on related topics:

- Maps Overview
- Maps
- How to Create and Edit Maps

EAPS

The **EAPS** tab allows you to access information about any devices configured with Extreme's Ethernet Automatic Protection Switching feature.

Accessing Network Details

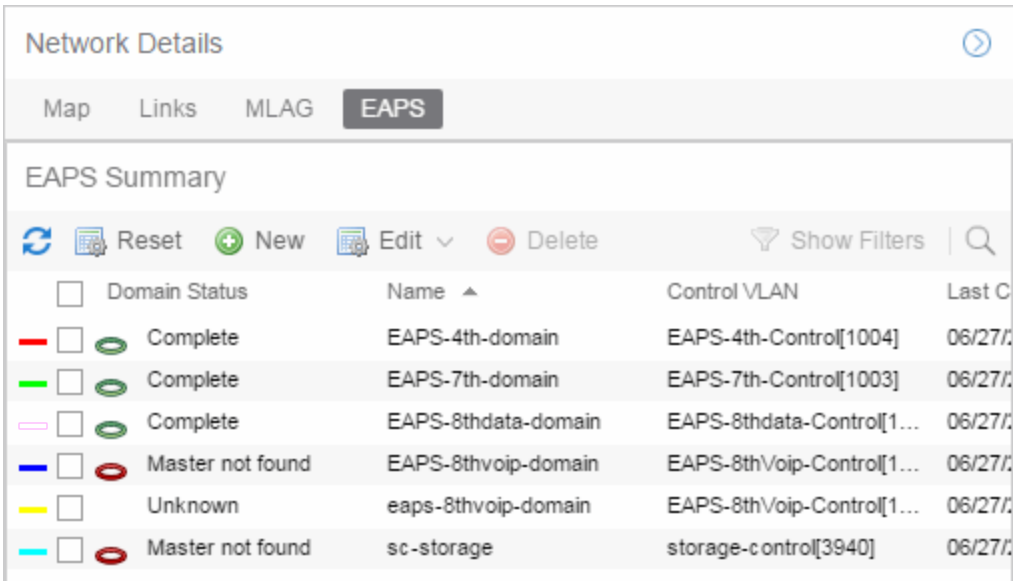
1. Right-click a map or map tree in the left-panel.
2. Select **Network Details** from the drop-down list.
3. Select **EAPS Summary.**

NOTE: For an alternate way to access the EAPS Summary tab:

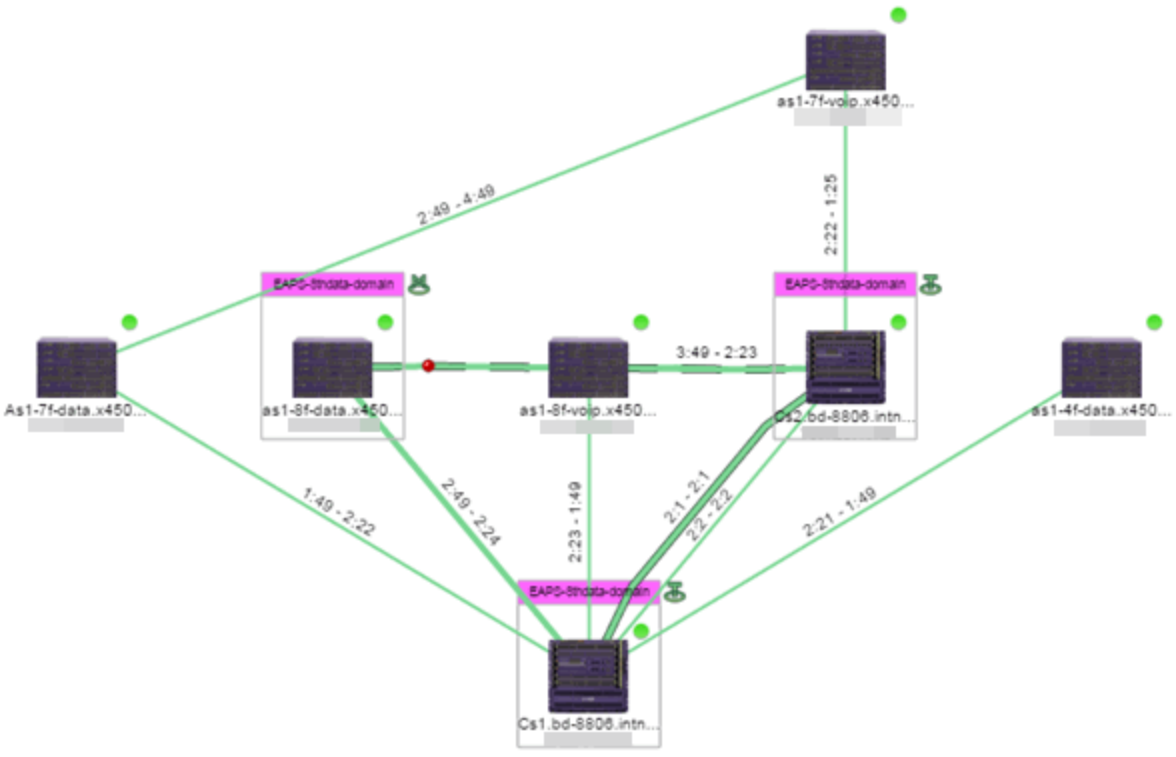
1. Select **Network > Devices**.
2. Select the second tab of the open **Devices** window, which is the **Map Tab** for the map you selected.
3. The **EAPS** tab will be included in the **Network Details** panel at the far right of the open **Devices** window.

EAPS Summary Tab

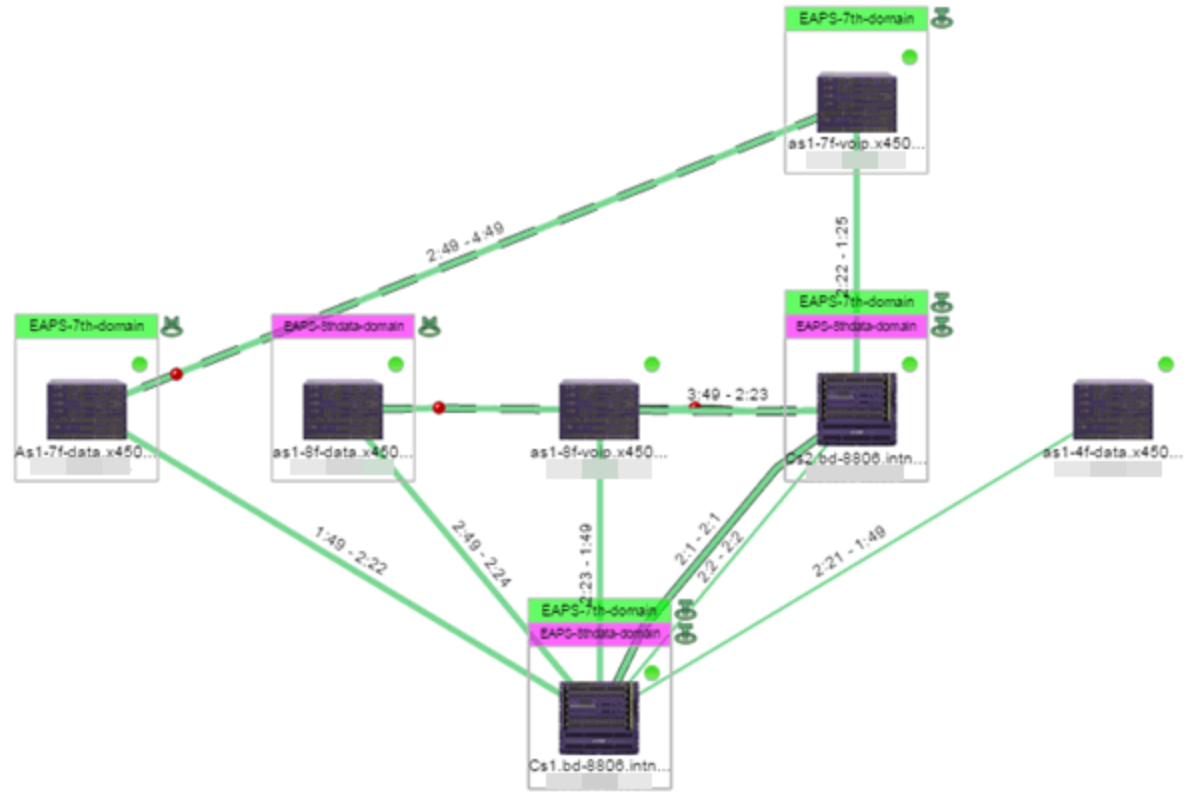
The **EAPS Summary tab** displays a list of the EAPS domains, including their status, name, the control VLAN name, and the IP addresses of the devices utilizing the EAPS domain.



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.

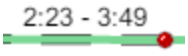


An icon next to the title bar indicates if the node is a master node, indicated by an "M" icon , or if the node is a transit node, indicated by a "T" icon .

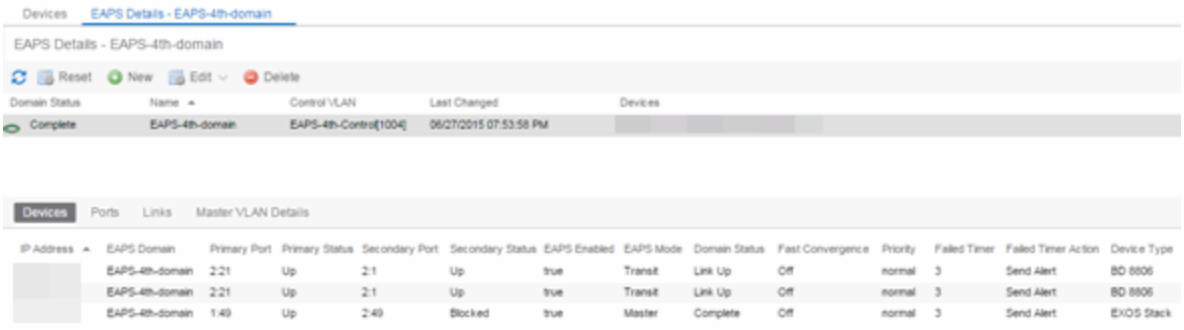
The color of the ring icon indicates the status of the domain:

- 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.

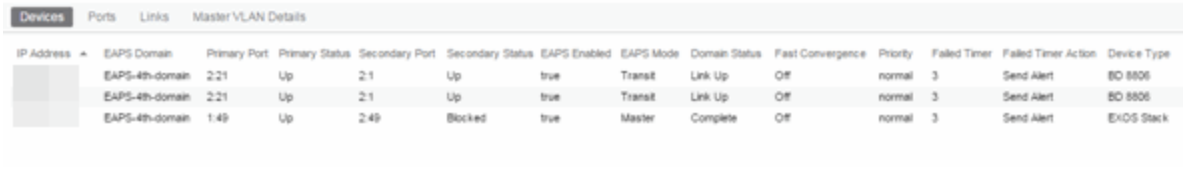


You can view additional details about the EAPS domain by right-clicking an EAPS domain on the **EAPS** tab and selecting **EAPS Details** to open the EAPS Detail view.



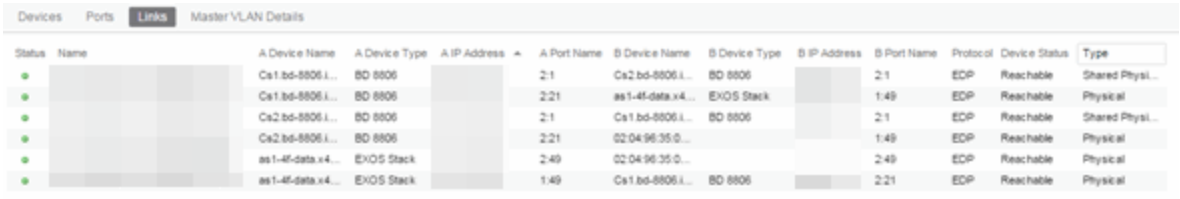
The top of the EAPS Details view displays a summary of the EAPS domain, identical to the information displayed in the **EAPS** tab. At the bottom of the window are three sub-tabs, which display additional information:

- **Devices**—Displays information about the devices using the EAPS domain.

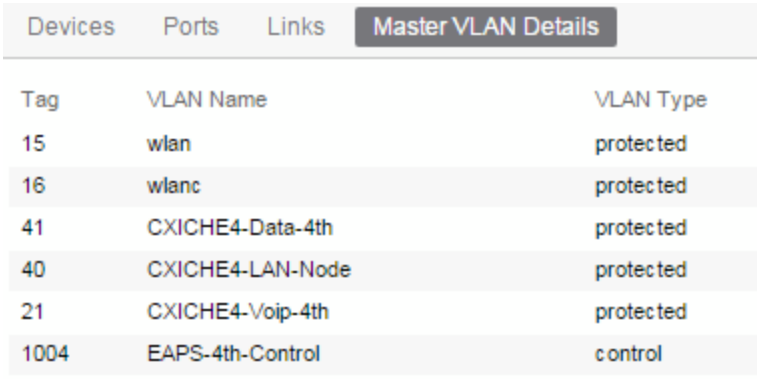


- **Ports**—Displays information about the shared ports associated with the EAPS domain.

- **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.

Related Information

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

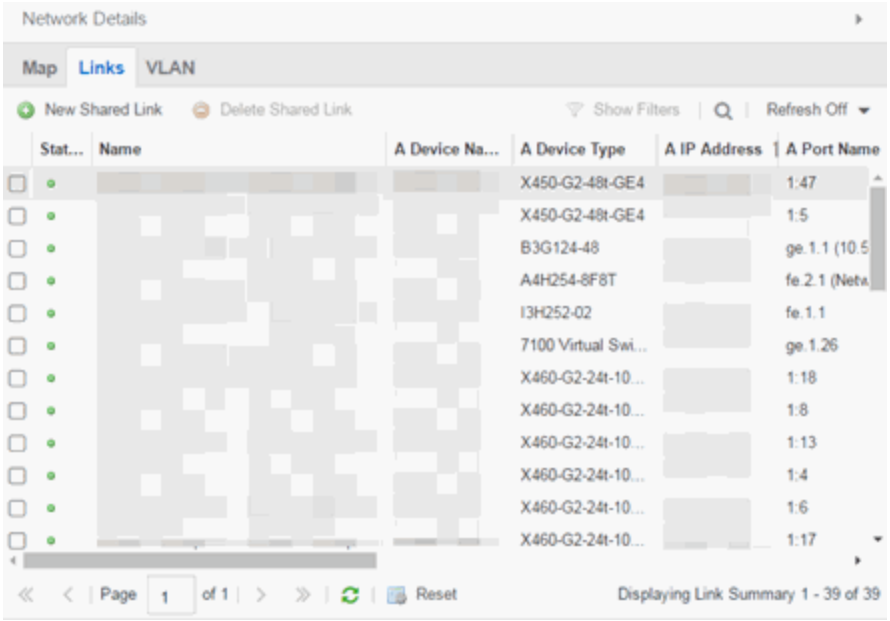
1. Right-click a map or map tree in the left-panel.
2. Select **Network Details** from the drop-down list.
3. Select **Links**.

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.

Related Information

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

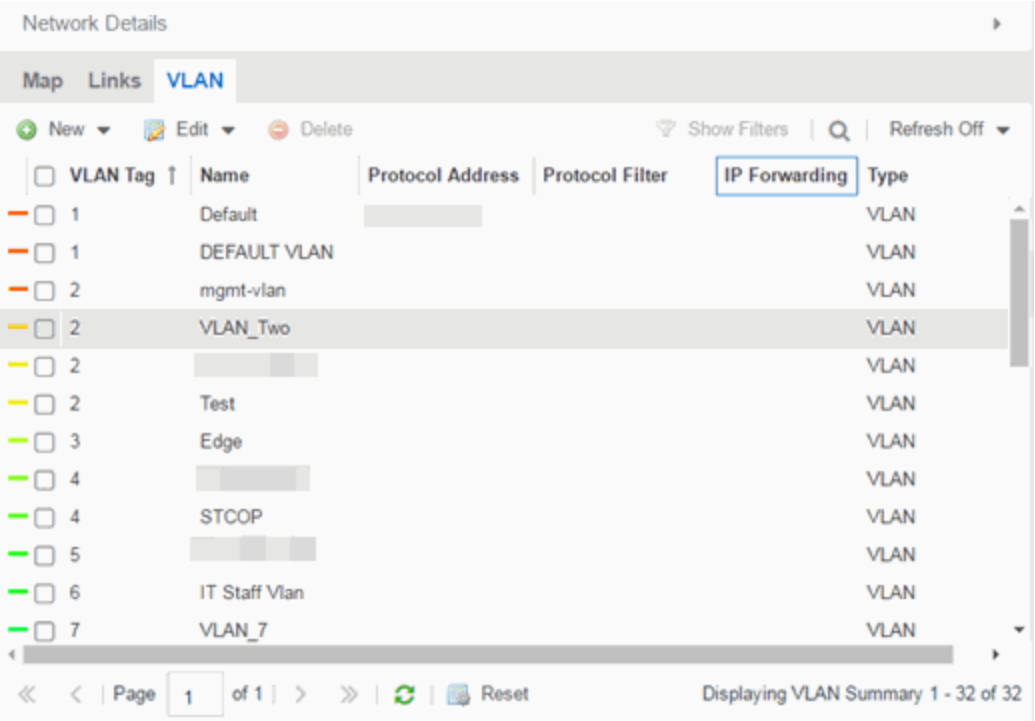
1. Right-click a map or map tree in the left-panel.
2. Select **Network Details** from the drop-down list.
3. Select **VLAN Summary**.

NOTE: For an alternate way to access the VLAN Summary tab:

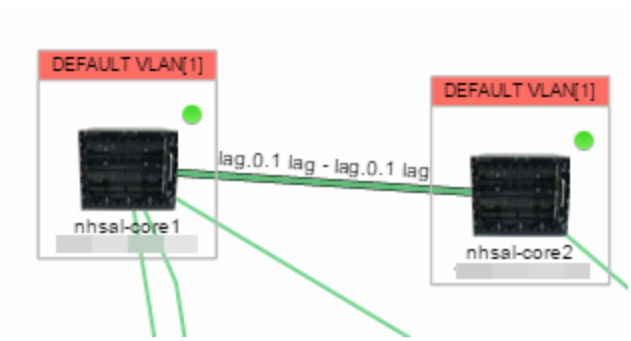
1. Select **Network > Devices**.
2. Select the second tab of the open **Devices** window, which is the **Map Tab** for the map you selected.
3. The **VLAN** tab will be included in the **Network Details** panel at the far right of the open **Devices** window.

VLAN Summary tab

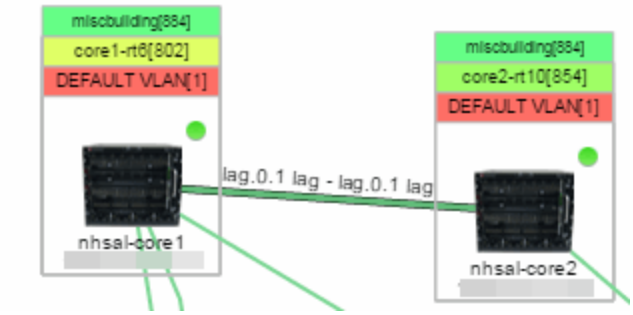
The **VLAN** Summary tab displays VLANs configured as part of devices included in the map. Columns in the **VLAN** tab provide additional information, including the VLAN tag, the name of the VLAN, any protocol filters applied for devices on which the VLAN is configured, and whether or not IP forwarding 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.

Related Information

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:

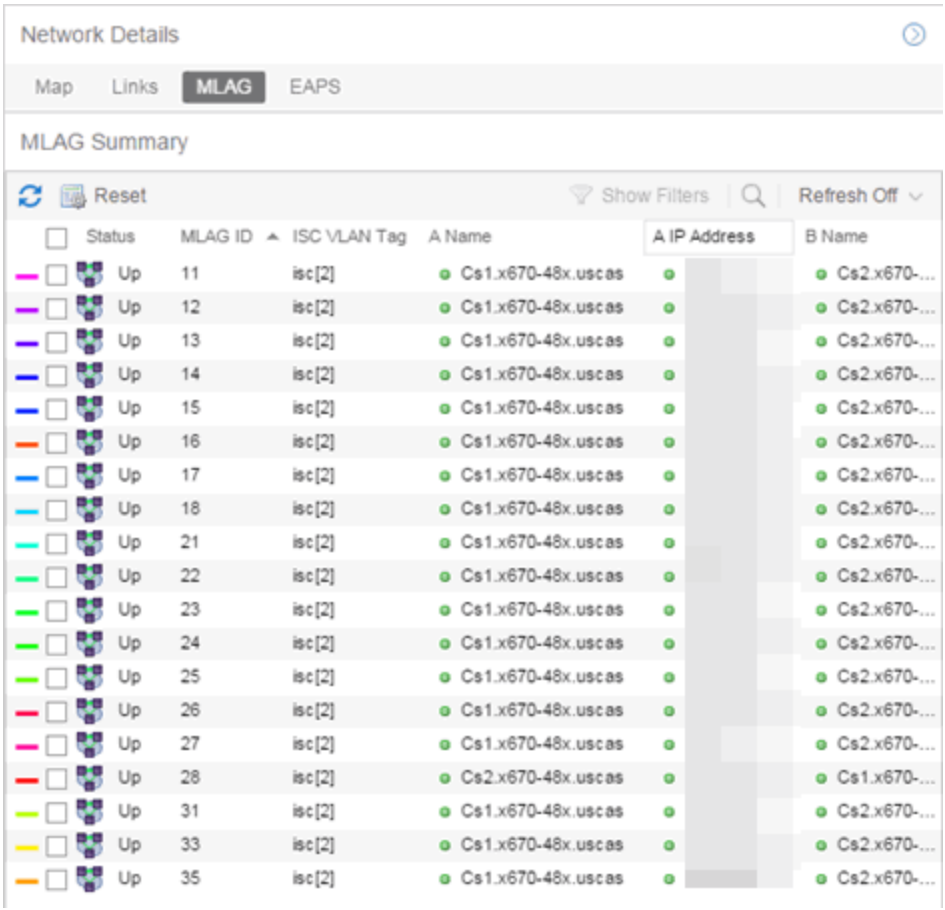
1. Select **Network > Devices**.
2. Select the second tab of the open **Devices** window, which is the **Map Tab** for the map you selected.
3. The **MLAG** tab will be included in the **Network Details** panel at the far right of the open **Devices** window.

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.

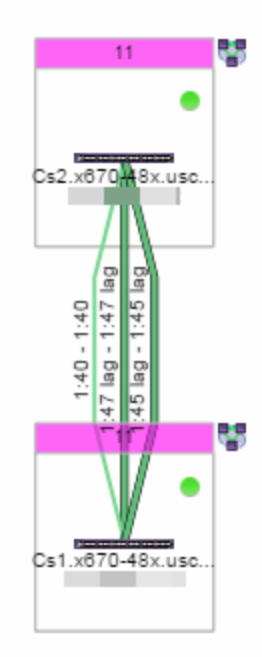
Ports

Lists the ports on those devices assigned as part of the MLAG.

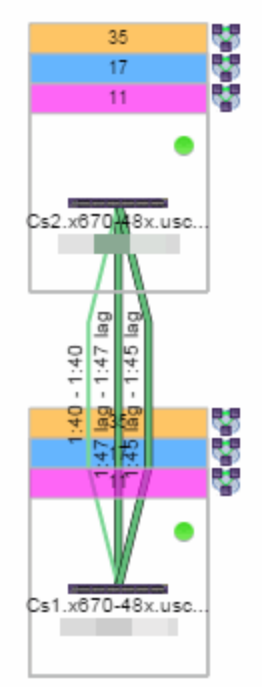
Connected IP

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.



Related Information

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

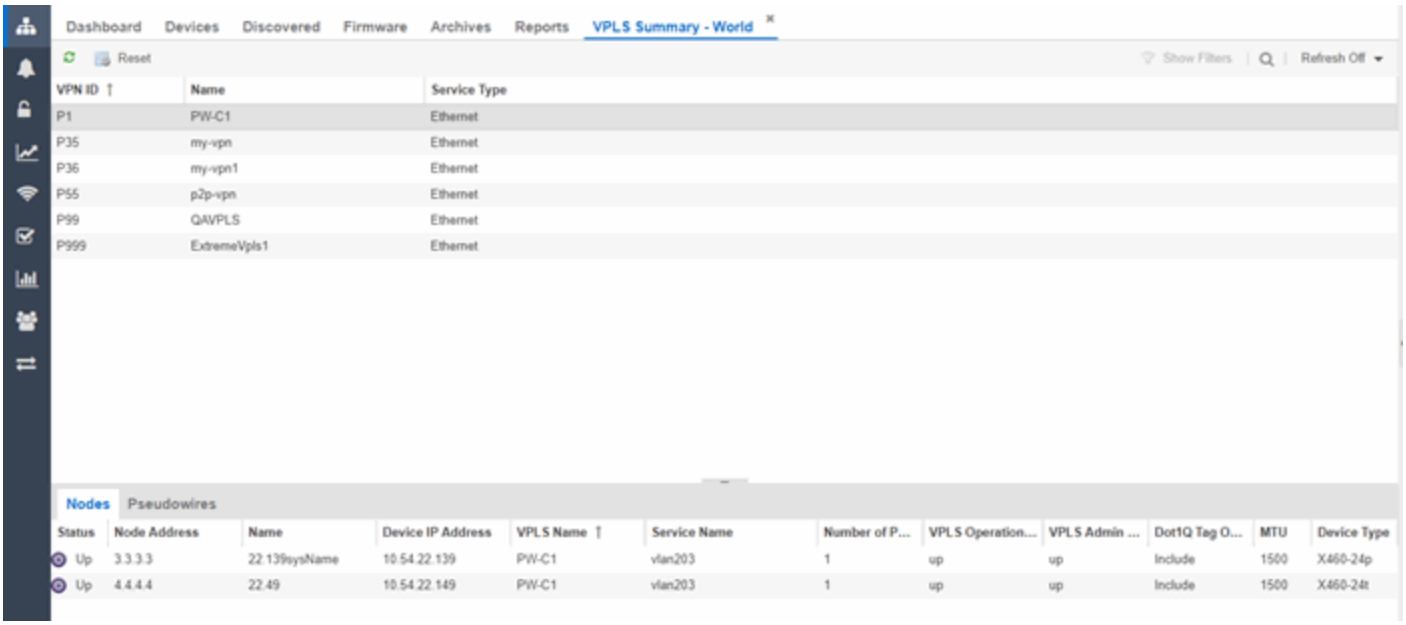
1. Right-click a map or map tree in the left-panel.
2. Select Network Details from the drop-down list.
3. Select **VPLS Summary**.

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.



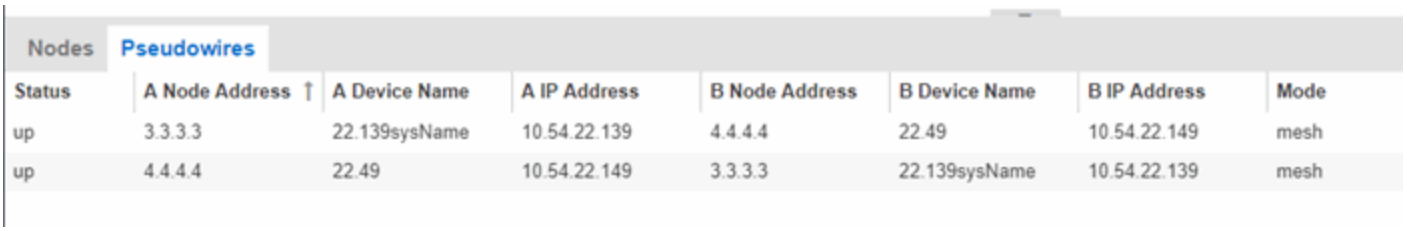
Nodes

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

Related Information

For information on related topics:

- ExtremeCloud IQ - Site Engine Maps
- Advanced Map Features

Map Types

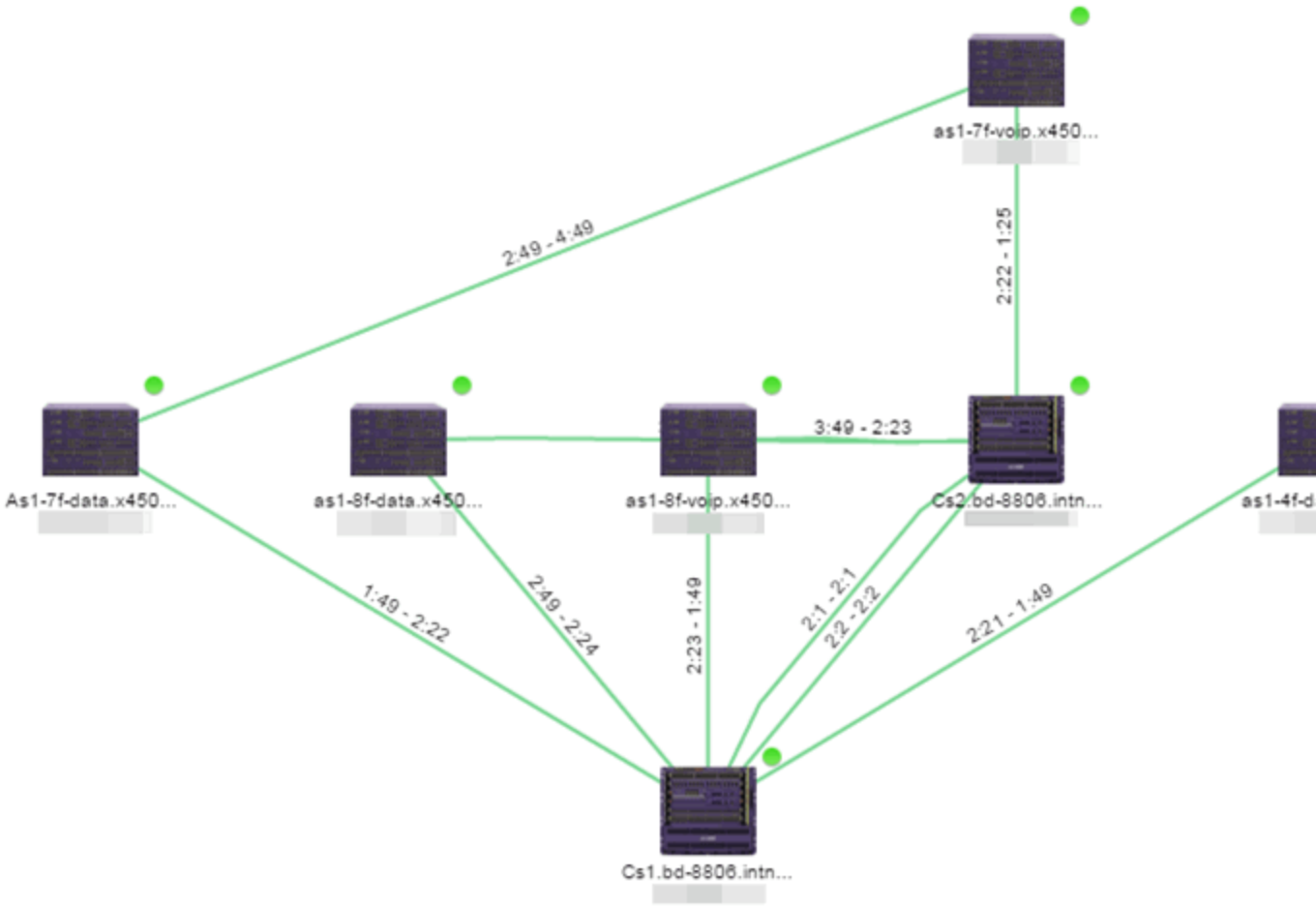
ExtremeCloud IQ - Site Engine allows you to create geographic and topology maps of devices and floorplans of wireless access points (APs) on your network.

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:

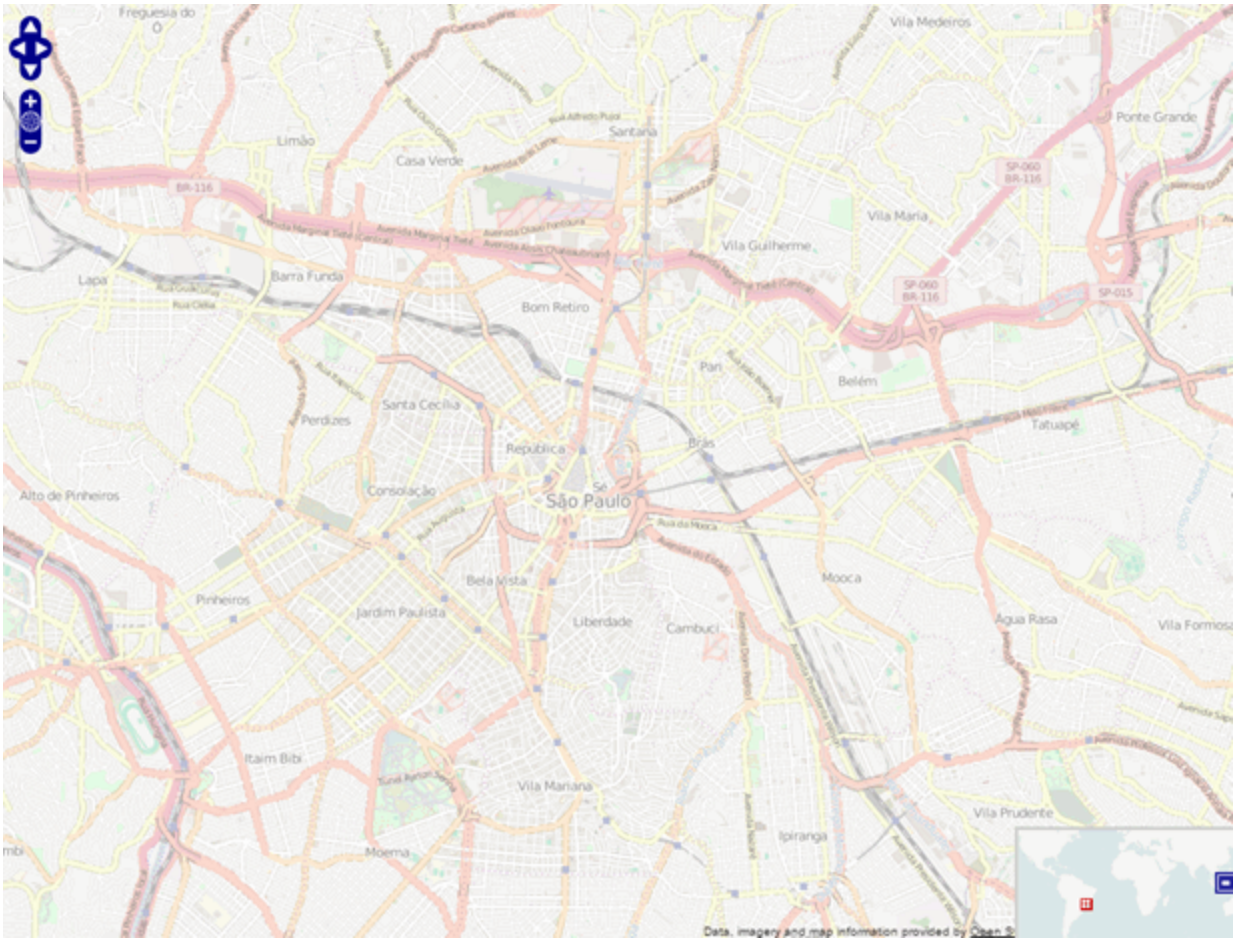
- Topology *(default)* —A topology map shows how devices are connected in a network, specifically, the state and speed of the network connections between devices as well as the state of the devices in the network. You can also create a topology map with a background image, giving you additional information 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.

Related Information

- 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.

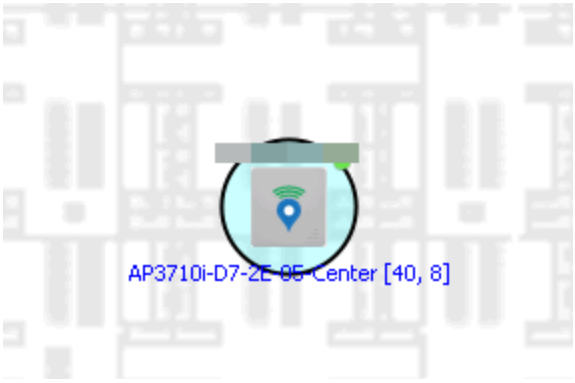
Finding a Wireless Client

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 1meter

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.

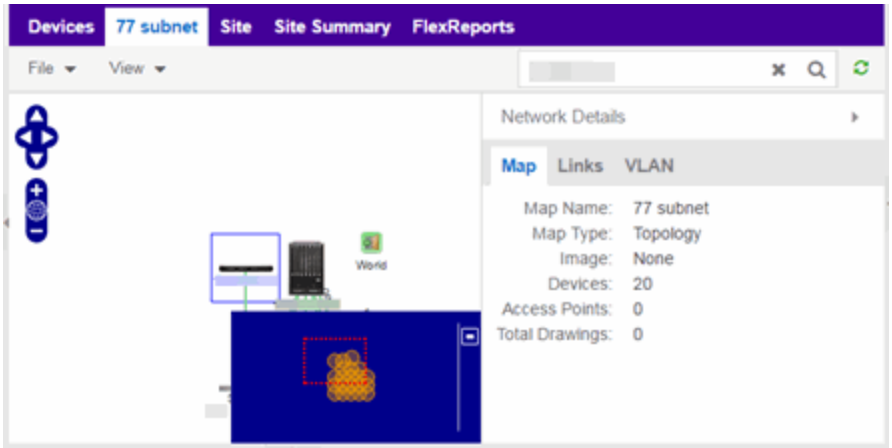
Finding a Device

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 ExtremeControl 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.

Related Information

For information on related topics:

- ExtremeCloud IQ - Site Engine Maps
- Advanced Map Features

How to Import Maps

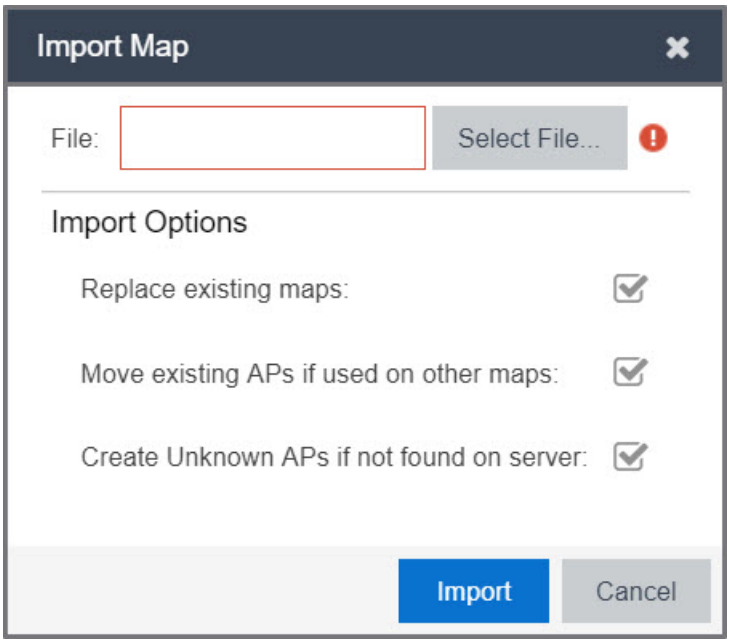
The ExtremeCloud IQ - Site Engine Maps lets you import saved maps of devices and wireless access points (APs) from your local drive or network, and configure the behavior of the imported maps.

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**.

Related Information

- 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

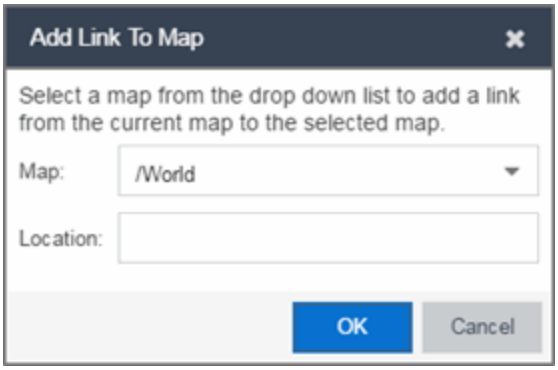
Map links display the name of the map and an aggregated alarm/device status for the linked map. Double-click on the link to go to the linked map.

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.

Related Information

- 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.

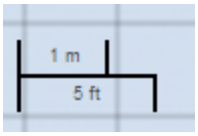
In order to edit maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

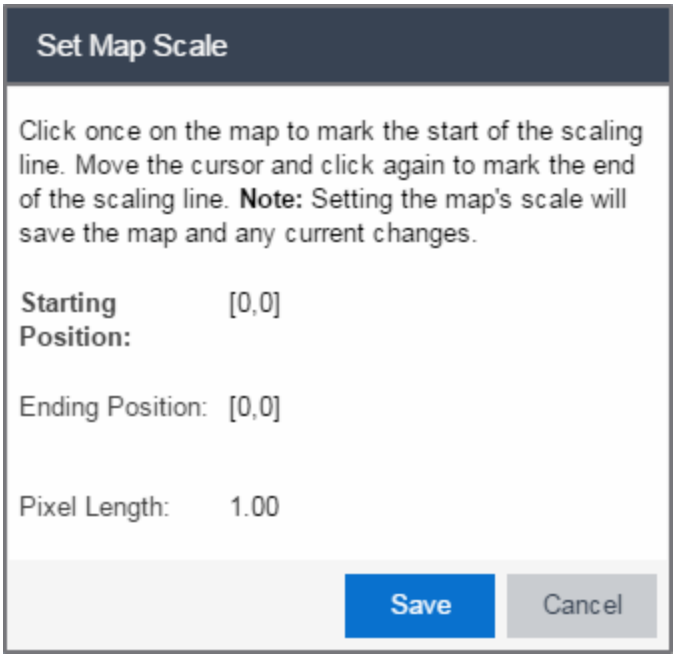
Setting the Map Scale

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.

Related Information

- ExtremeCloud IQ - Site Engine Maps
- Advanced Map Features

Next Generation Maps

Next Generation (NG) Maps add topology map support for fabrics: Fabric Connect, Fabric Attach, Fabric Extend, and VCS. NG Maps also improve the readability of maps by

displaying only the content that you are most interested in and providing additional tools to manipulate the maps..

NG Maps work the same way as Geographical and Floorplan maps 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.

After you create a map by right selecting any Site/Map and selecting **Maps** > **Create New Map**, a new entry for the map displays in the navigation pane. Then when you select the map, NG maps loads it in the right hand panel, under the tab with the name of the newly created map. NG Maps categorizes complex network data into different segments, called Layers. The Physical Layer is the default layer that the map opens with, however, you can change this default layer. More information about layers is explained in the Sidebar section.

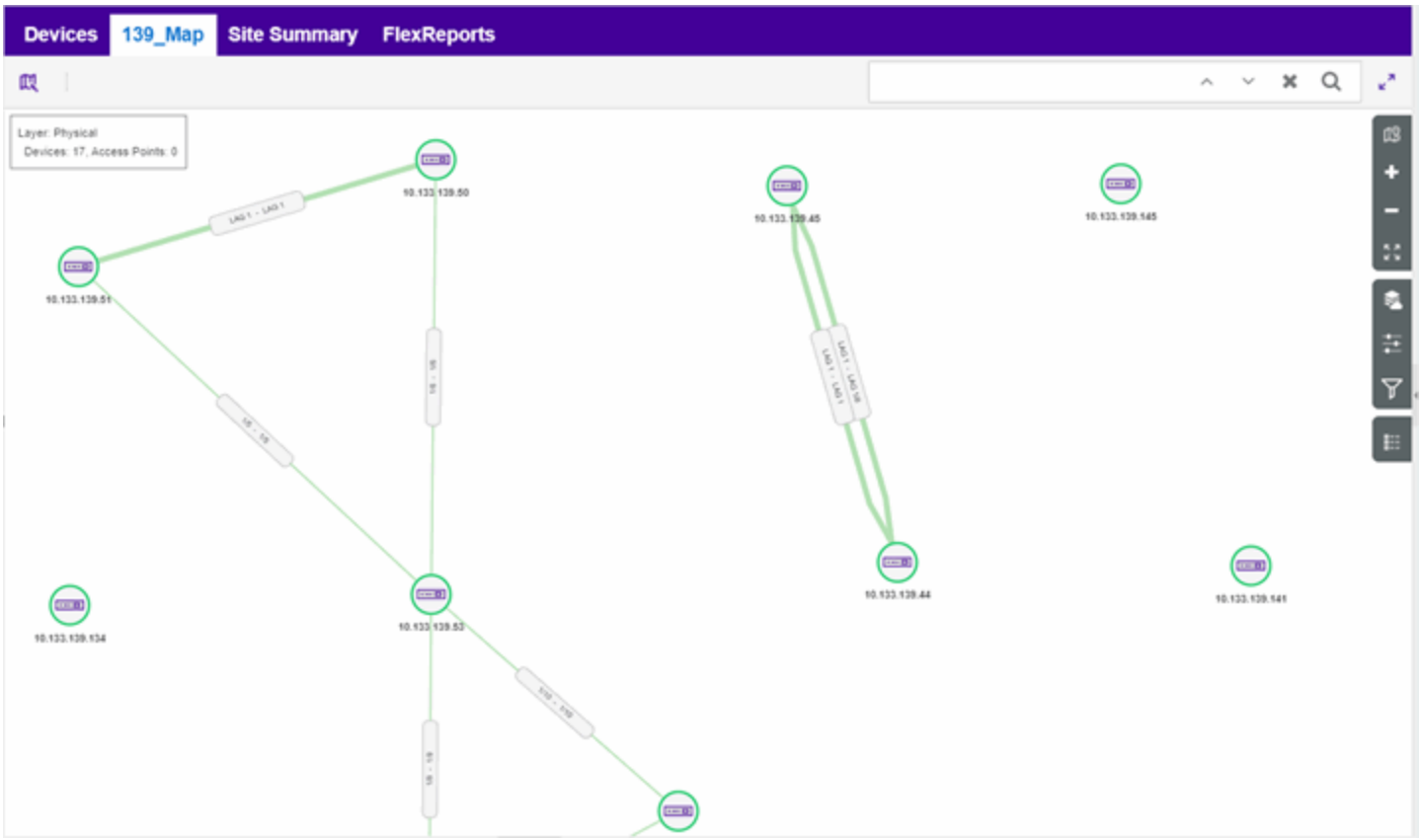
NG Maps has three main components:

- Map Area: This area displays the devices and their links.
- Toolbar: The toolbar provides options for configuring the map properties.
- Sidebar: The sidebar provides options for changing how the maps are presented.

The following sections describe the above components in detail.

Map Area

The Map Area displays the nodes, links, and LAGs. You can reorganize the orientation of elements in your map and view the status and details of any element within the map.



The Map Area also includes the following features:

- Node Information
- Link Information
- LAG Information
- Summary Information

Node Information

Nodes are the entities (switches, APs, and extenders) that ExtremeCloud IQ - Site Engine discovers and monitors. A node in the map can have multiple labels, which you can edit in the General Properties option in the sidebar on the right hand side.

- The icon represents the type of node it represents.
- The color around the node represents the node's alarm status.

- Node Actions:
  - Single select to select a node.
  - Double select to open the Device View.
  - Right select to open the context menu.
  - Hover over the node to show the tooltip containing basic device details. The tooltip details show more information about the node based on the Layer selected in the map showing the tooltip.

Link Information

Links show the connectivity between nodes with respect to the layer selected. The color of the link specifies the status of the connection and the link label shows the port names that participate in the connection.

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.

- 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.

- Link Actions:
  - Single select to select a link.
  - Double select to open the Details Window.
  - Right select to open the context menu, which includes the **Add Link** option.
  - Hover over the link to show the tooltip containing the link details.

LAG Information

LAG links have thicker lines than simple links. The color of the thick line connecting the nodes specifies the status of the connection.

The LAG tooltip looks similar to a simple link tooltip except it shows information about all the ports between the nodes where the LAG is configured. The bottom of the tooltip section shows the links for all the ports participating in the LAG and are connected.

Summary Information

In the top-left corner of the Map Area, ,there's a Summary of the current map. It displays the Layer selected, number of Devices, and the Access Points that are added to the map. The content in the Summary depends on the layer selected.

Toolbar

The Toolbar, which is directly above the Map Area, includes Edit, Save, Cancel, and Fullscreen buttons and a Search field.

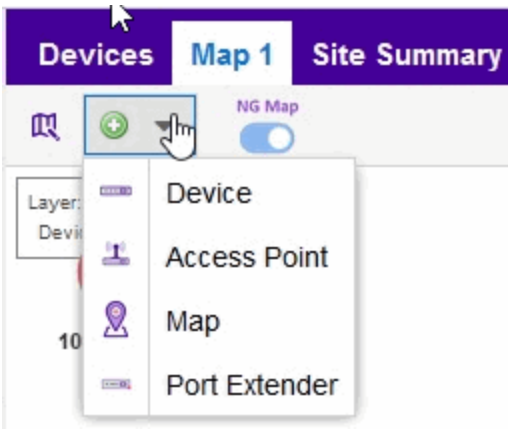
Non-Edit and Edit Modes

There are two map modes: **Non-Edit Mode** and **Edit Mode**.

Non-Edit Mode displays the nodes, links, and tooltips, but you cannot move them. In this mode, the toolbar includes the Edit and Fullscreen buttons in addition to the Search field.

Non-Edit Mode also includes an Add menu which you can use to add devices, access points, maps and port extenders. The Add menu is available only in the Physical Layer when edit mode is off.

Non-Edit Mode is the default mode and it does not show the Save and Cancel buttons.

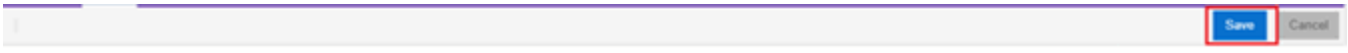


Edit Mode is available in all layers.

In Edit Mode, you can move nodes around, change background images, and add shapes and styles to the Geographic and Floorplan layers. This mode displays maps with a background grid that helps in moving the nodes to the desired position. After making your changes, you can choose to Save or Cancel the changes by selecting the appropriate button on the toolbar. When the save is complete, the Save and Edit buttons are disabled.

To enable Edit Mode, select the edit button on the toolbar.

Maps enter Edit Mode automatically if you make any changes in the Sidebar > General dialog that require saving. This feature brings up the Save and Cancel button so you can save these changes as well.

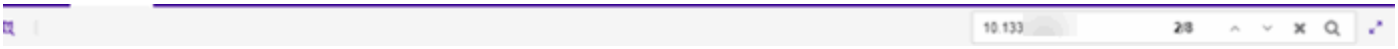


Search Field

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.

Based on matches to the search, the map area moves to include the selected nodes and highlights them with a fluorescent background. The number of nodes matching the searched criteria is shown next to the search field. You can move around the searched nodes by selecting the up and down arrows on the search box or by pressing the Up and Down arrow keys or **Enter** on your keyboard.

To clear the search highlighting, select the 'x' icon in the search field or press **Esc**.



3.1.3.7 Fullscreen

Fullscreen button () on the toolbar expands the map area by collapsing the expanded Tree View Pane.

Sidebar

The Sidebar is on the right side of the Map Area.

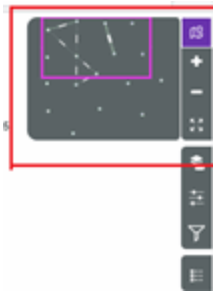
The Sidebar includes the following tools that enable you to change the content of the Map Area:

- Map Overview
- Zoom Controls
- Layer
- General Properties

- Feature Highlighting
- Legend

Map Overview

Map Overview provides a view of the whole map and enables you to move the Map Area display by dragging the red box inside the map overview.



Zoom Controls

The **Zoom** controls enable you to zoom in and out of the map by selecting the plus and minus icons. The **Zoom Reset** control returns the map zoom level to 100%.

Layer

NG Maps categorize complex network data into different segments, called Layers. Each of the following layers provides information and options based on the context of the layer.

- Physical Layer - Displays all the nodes in the network and their links.
- Fabric Virtual Cluster Switching (VCS) Layer - Displays multiple VCS networks with their fabric-related nodes and links.
- Fabric Connect Layer - Displays the fabric-enabled nodes and the IS-IS Links between them.

The information in the preceding sections (Map Area, Toolbar, and Sidebar) apply to the Physical Layer. The VCS Layer and Fabric Connect Layer have the same look and feel as the Physical Layer but with some minor changes and additional features. For more information, see VCS Layer and Fabric Connect Layer.

NG Maps continue to support the Geographical and Floorplan layers.

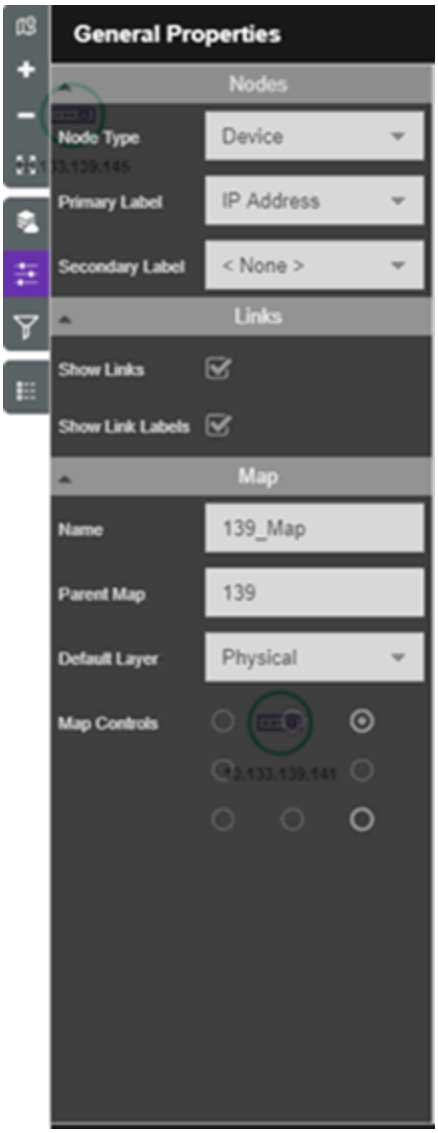
The **Layer** option enables you to change the Map Area to view a different layer. You can also change the layout to one of the predefined layouts and add a background image to the layer in view. At the bottom of the Layer dialog box, there are other options. You can delete a non-default layer, refresh the map, export the map as a screen shot or whole map, and a menu to add various types of nodes to the map.

To open the Layer dialog box, select the layer icon in the Sidebar.

General Properties

General Properties change the information displayed on the map. It consists of the following three groups of options:

- Nodes - This group enables you to select a node type, which is displayed in the current layer, and select its Primary and Secondary labels.
- Links - This group gives you the option to show or hide links and link labels in the map.
- Map -This group enables you to change the map properties. If you change the Map Name, Parent Map, or Default Layer, the map opens in Edit Mode automatically so that the **Save** and **Cancel** buttons are made available.

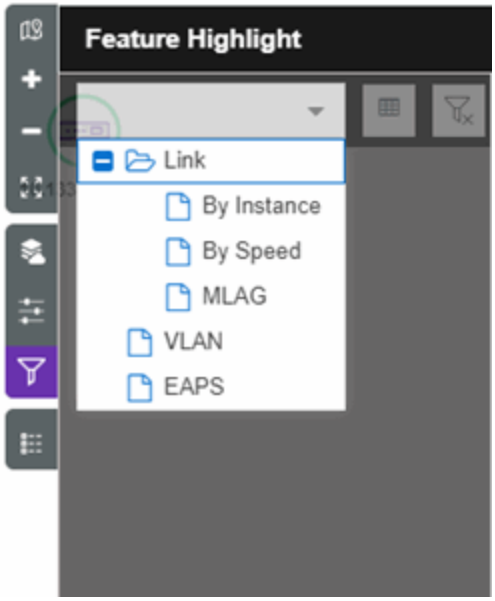


Feature Highlighting

Feature Highlighting enables you to select certain features to highlight on a map. The features listed in Feature Highlighting are layer dependent. For example, the Fabric Connect Layer only shows ISIS Links and Services in the drop-down menu. Apply a filter for the specific elements, nodes, or links that you want to see and then this feature highlights them on the map.

Feature highlighting is available for every layer and each layer has its own set of filters that you can apply to the maps. In the Feature Highlight dialog box, select a feature from the drop-down menu and then select the **grid icon** to select up to a maximum of ten options. You can check and uncheck entries in the option grid until satisfied and then select **Apply** to change the highlighting in the map.

To clear highlighting, select the clear highlight button next to the grid icon button.

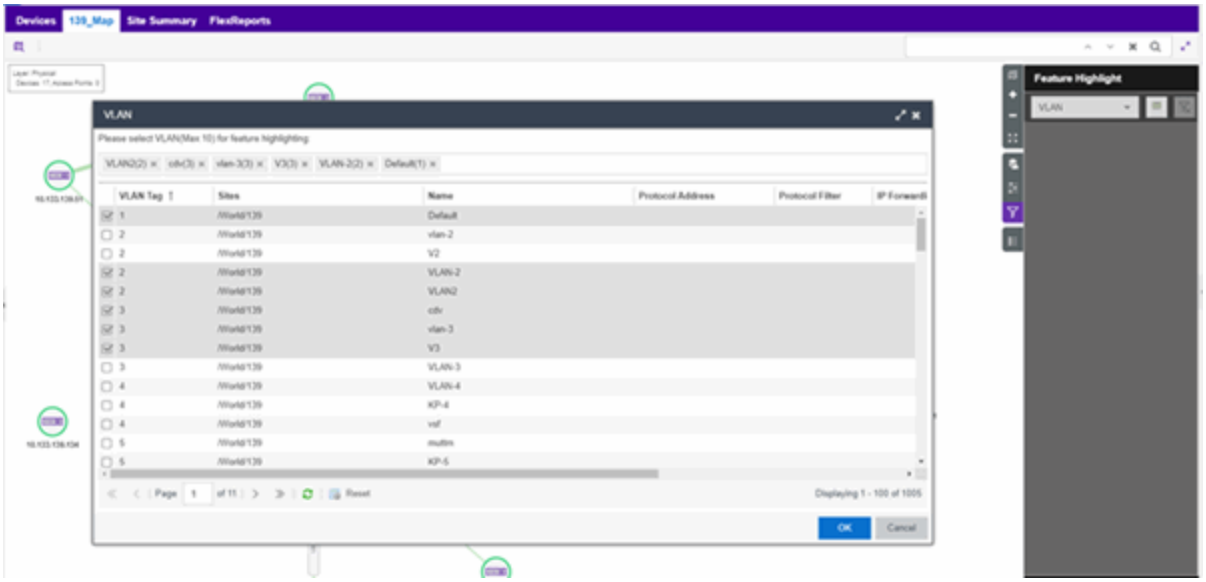


The following sections describe the features that you can highlight:

- VLAN Highlighting
- Links Highlighting
- MLAG Highlighting
- MLAG Highlighting
- VPEX Highlighting
- L2 / L3 Services Highlighting
- VCS and Fabric Connect Highlighting

VLAN Highlighting

In the **Feature Highlight** dialog box, select **VLAN** and then select the grid icon to display a list of the available VLANs in the devices on the map. You can select up to a maximum of ten VLANs.



After you select the VLANs and select OK, the selected VLANs are displayed in a Highlight Grid on the **Feature Highlight** dialog box. You can check and uncheck VLAN entries in this grid. Select **Apply** and the selected VLANs appear on the map in the shape of an arc over the node. The arcs are color-coded to match the VLANs in the Highlight Grid. If a node is part of multiple VLANs selected for highlighting, the arc will have multiple, colored segments.

Links Highlighting

Links Highlighting has the following options: **By Instance**, **By Speed**, and **MLAG**.

When you select **By Instance** or **MLAG**, and then select the grid icon, a Highlight Grid lists all the links or MLAG instances available in the devices that are added to the map. You can select up to a maximum of ten links or MLAGs. Select OK and the selected options are displayed in a Highlight Grid on the **Feature Highlight** dialog box. You can check and uncheck VLAN entries in this grid. Select **Apply** and the selected options appear on the map in the color-code that matches the Highlight Grid.

The grid icon is not available with the **By Speed** option because the Highlight Grid is pre-configured with all possible speeds available in the map. The links and LAGs are colored to match the speeds shown in the Highlight Grid.

MLAG Highlighting

In the **Feature Highlight** dialog box, select **MLAG** and then select the grid icon to display a list of the available MLAGs in the devices on the map. You can select up to a maximum of ten MLAGs.

After you select the MLAGs and select OK, the selected MLAGs are displayed in a Highlight Grid on the **Feature Highlight** dialog box. You can check and uncheck MLAG entries in this grid. Select **Apply** and the selected MLAGs appear on the map. The MLAGs are color-coded to match the MLAGs in the Highlight Grid. You can also select the segment to get more information about the MLAG instance on the nodes.

When you select a segment in the arc, the icon for each node changes to a colored M or T to represent either the Master or Transit Node.

EAPS Highlighting

EAPS Highlighting is similar to the VLAN filtering and highlighting where only the selected nodes are displayed on the map. One difference is that when you select a segment in the arc, the icon for each node changes to represent either the Master or Transit Node along with a tertiary label showing the EAPS Domain information and coloring the border of selected colored segment in all the nodes.

VPEX Highlighting

VPEX Highlighting is similar to the VLAN filtering and highlighting where only the selected nodes are displayed on the map. One difference is that when you select an arc segment, the icon for each node changes to represent the Peer Node (in case of Dual Home VPEX setup) along with coloring the border of selected colored segment in all the nodes.

L2 / L3 Services Highlighting

In the **Feature Highlight** dialog box, select **L2 / L3 Services** and then select the grid icon to display a list of the available Services in the devices on the map. You can select up to a maximum of ten Services.

After you select the Services and select OK, the selected Services are displayed in a Highlight Grid on the **Feature Highlight** dialog box. You can check and uncheck Service entries in this grid. Select **Apply** and the selected Services appear on the map. The Services are color-coded to match the Services in the Highlight Grid. Hover over the node with the Service for more information such as the ports participating in the service.

VCS and Fabric Connect Highlighting

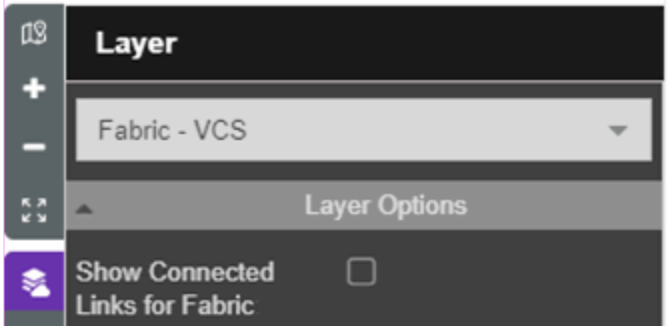
For information on VCS Highlighting and Fabric Connect Services Highlighting, see VCS Layer and Fabric Connect Layer.

Legend

The Legend lists the icons used in NG Maps and provides a description of each.

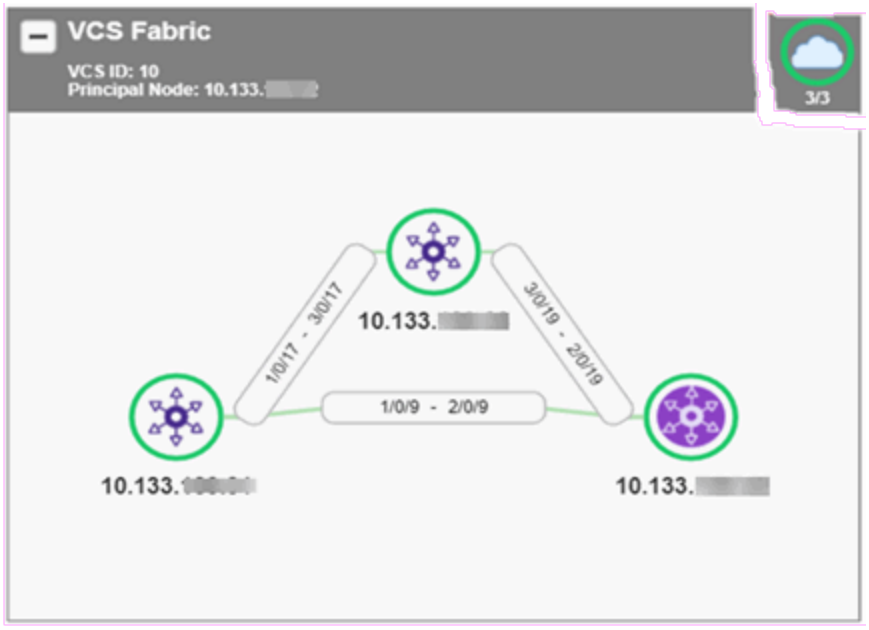
VCS Layer

The **VCS Layer** displays VCS Fabric-related nodes and links. To open the VCS Layer dialog box, select the layer icon in the Sidebar and select **Fabric - VCS**.



The VCS Layer has the same look and feel as the Physical Layer but with some minor changes and additional features like **Grouping**. You can also display external nodes connected to the VCS network nodes.

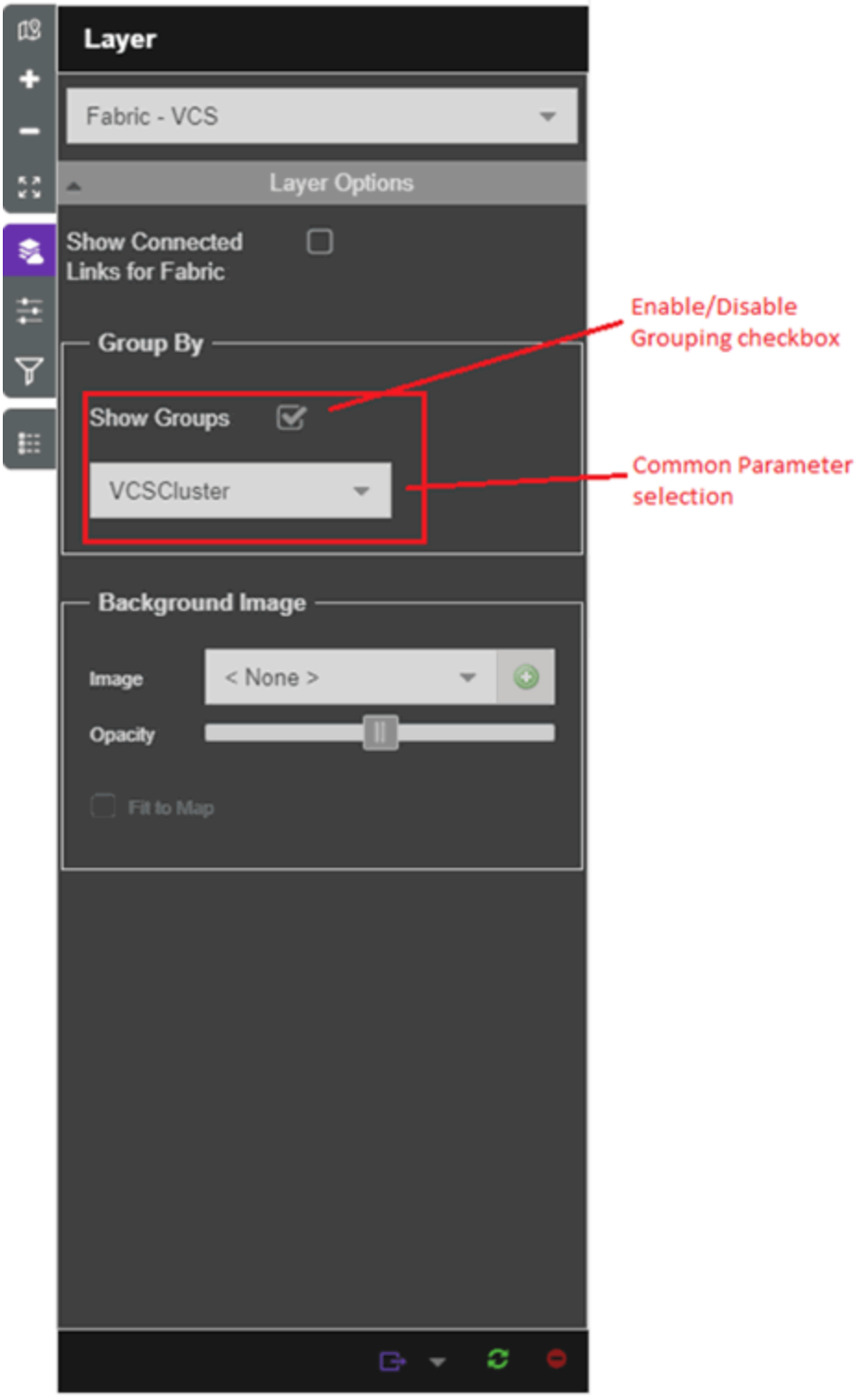
The Principal VCS Node is shaded dark purple to distinguish it from normal nodes.



VCS Grouping

The VCS Layer displays nodes grouped in a rectangular box based on a set of nodes that have a common parameter. The header of the group box displays the VCS ID and Principal Node information.

To enable and configure Grouping, check **Show Groups** and select an parameter from the drop-down menu.



The colored circle on the right side of the group header indicates the fabric status:

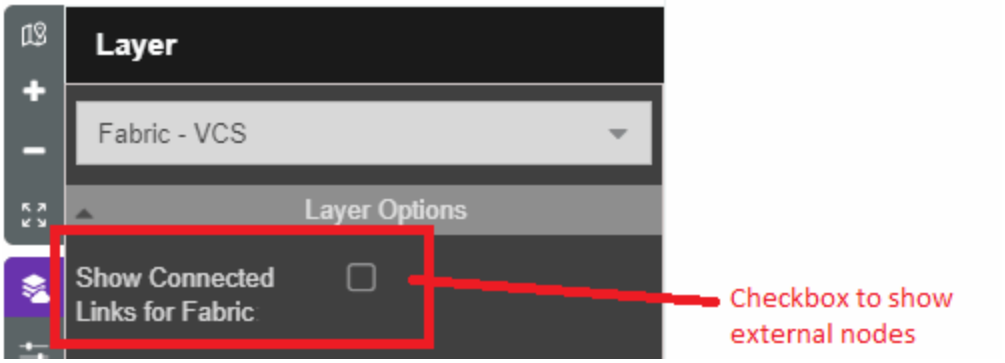
- **Green** indicates that all the nodes are up and running.
- **Red** indicates that all or some of the nodes are down.
- **Gray** indicates that some nodes that are part of the fabric are not in the map.

The following image shows two VCS groups that use the VCS ID as the common parameter. The group summaries in the headers describe some details pertaining to the VCS network.

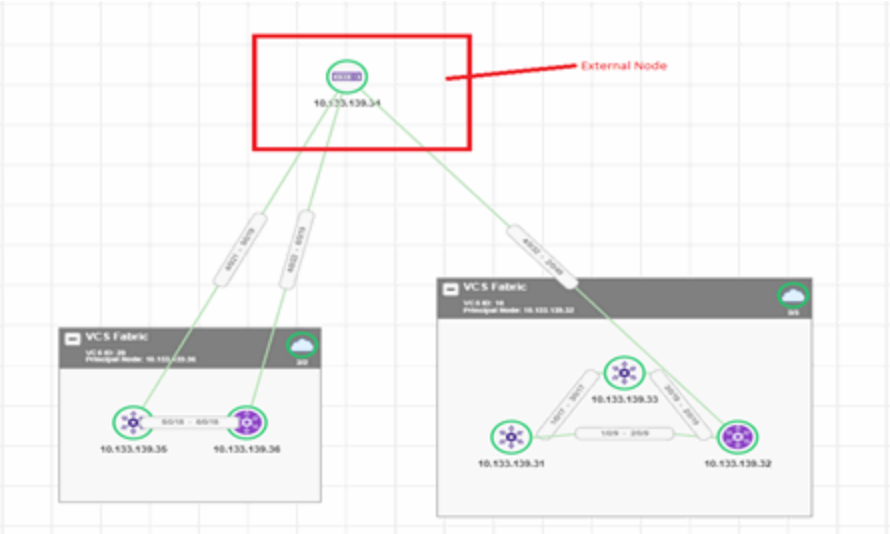
VCS External Nodes

The VCS Layer shows external nodes if any are connected to the VCS Network nodes. To enable this feature, check **Show Connected Links for Fabric**.

NOTE: External nodes are only shown if they are discovered and added to the NG Map.



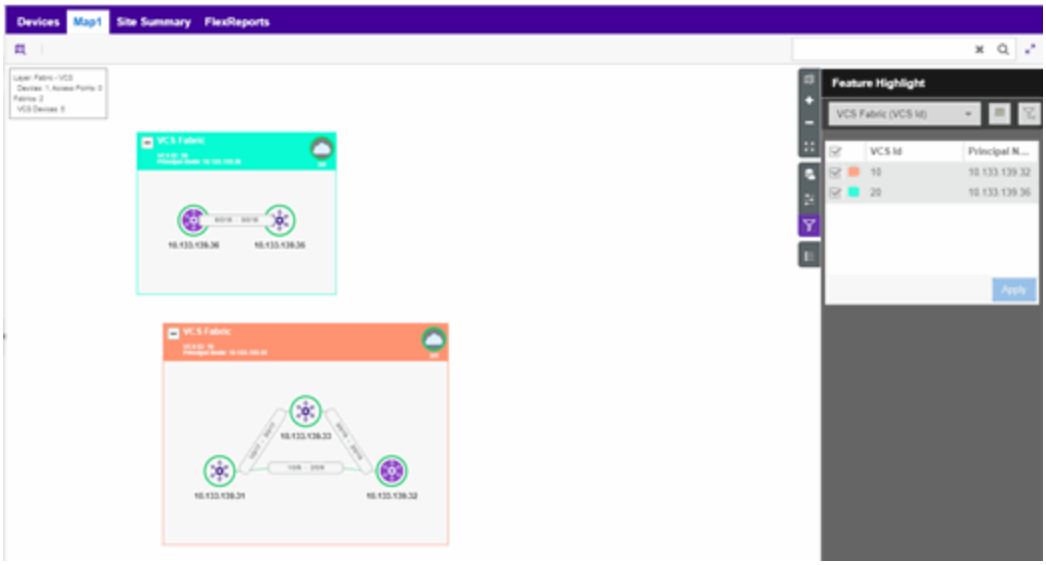
The following image shows an external node connected to 3 VCS network nodes which are a part of 2 VCS networks with VCS IDs 10 and 20 respectively along with Fabric Summary on top left



VCS Fabric Highlighting

In the **Feature Highlight** dialog box, select **VCS Fabric (VCS Id)** and then select the grid icon to display a list of the available VCS networks that you can select to highlight on the map. You can select up to a maximum of ten VCS IDs.

After you select the VCS IDs and select OK, the selected VCS networks appear in a Highlight Grid on the **Feature Highlight** dialog box. You can check and uncheck VCS ID entries in this grid. Select **Apply** and the selected VCS networks appear on the map in different colors for different VCS IDs. The color code matches the color of the VCS IDs in the Highlight Grid.



Fabric Connect Layer

This section is "Under Construction."

Fabric Connect Summary

IS-IS Topology

Services Highlighting

Related Information

For information on related topics:

- Geographic and Floorplan Maps
- How to Create and Edit Maps
- Sites

How to Access Interface Graphs

You can use ExtremeCloud IQ - Site Engine to access interface graphs directly out of NG Maps. This is a convenient way to access the same interface graphs that are available in

the Device View.

Accessing Interface Graphs from a Map

Use the following steps to access the interface graphs.

1. Launch ExtremeCloud IQ - Site Engine and select the **Network** tab.
2. Open the **Devices** tab.
3. In the left-panel, select **Sites**.
4. Select a map and open it.
5. Right-click on a link and select **Interface History** to display the interface graphs.

Related Information

- ExtremeCloud IQ - Site Engine Maps

Endpoint Locations

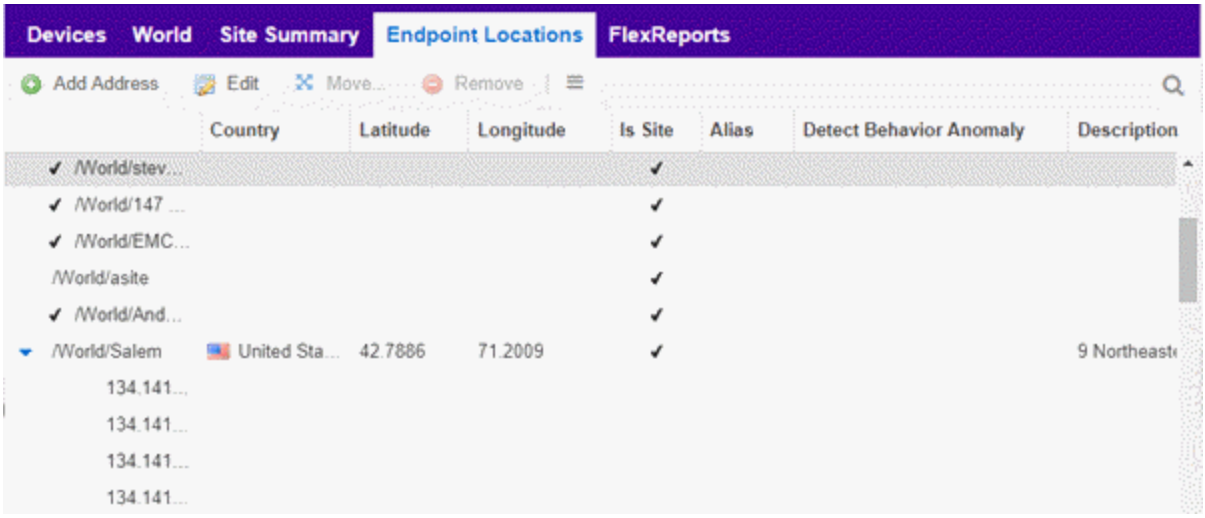
Use the **Endpoint Locations** tab to view and define the geographical locations of sites and subnet addresses in your network. When the geographical locations are defined, flows on the **Application Flows** tab display geographical information depending on the device on which the flow is observed.

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.

Detect Behavioral Anomaly
Select the checkbox to enable ExtremeCloud IQ - Site Engine functionality that alerts you in the event unexpected behavior is detected for the site or the specified subnet of the site.

Description
A description of the site or orphaned location.

Related Information

For information on related topics:

- Network Tab
- Sites Tab

Restart Devices

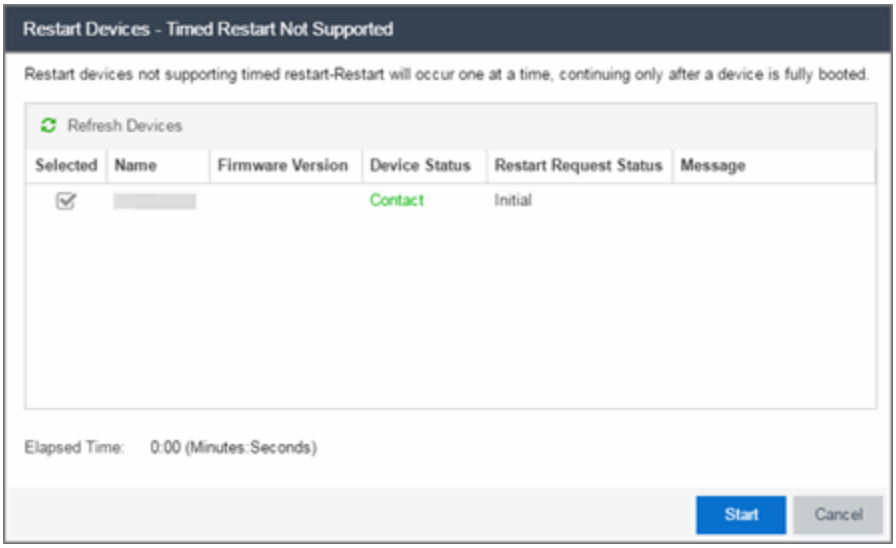
Use this window to restart a device. Devices can be restarted manually, or scheduled at a future date and time, if a timed restart is supported by the device. The window varies depending on the devices you select to restart:

- 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.

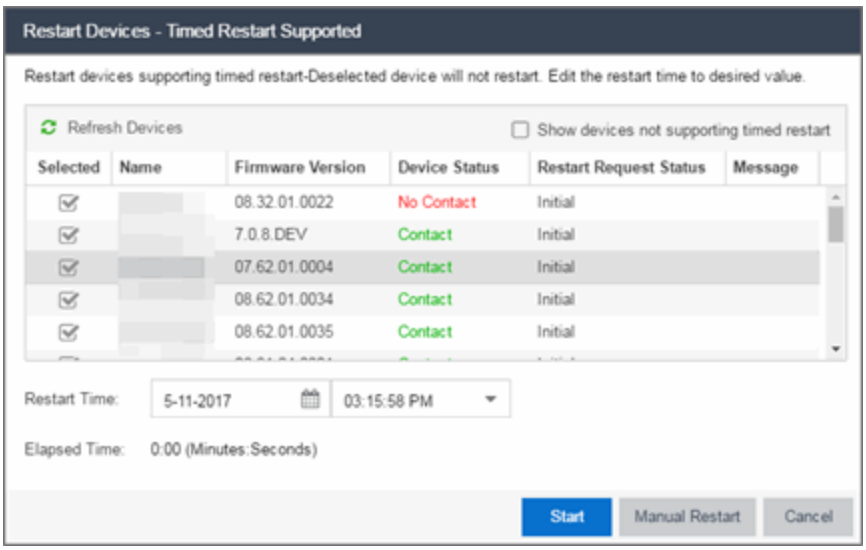
Elapsed Time
The time elapsed since the restart began.

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.

Related Information

For information on related topics:

- How to Restart a Device

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.

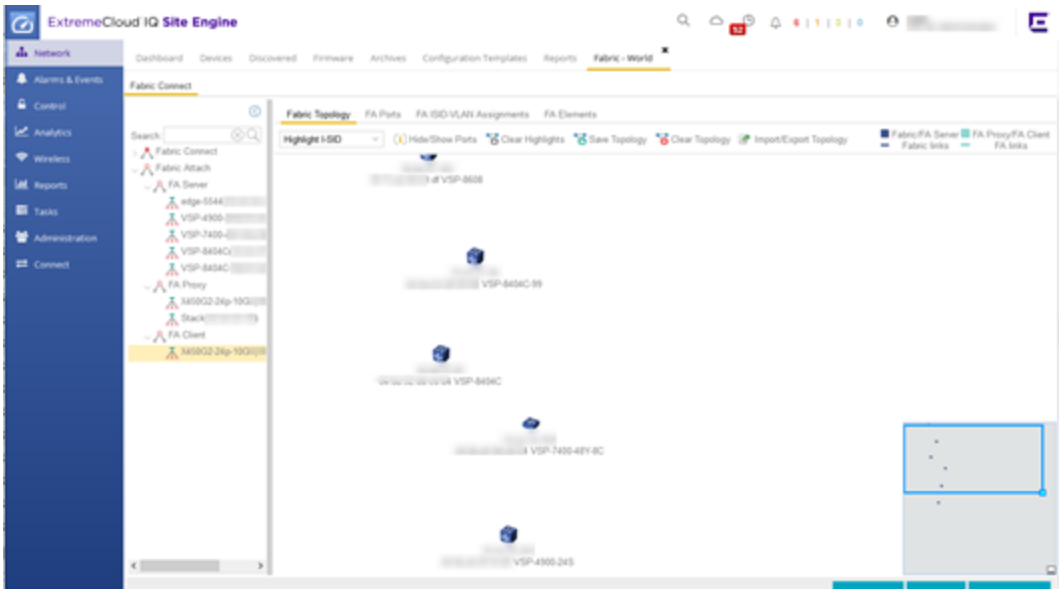
Accessing Fabric in ExtremeCloud IQ - Site Engine

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.

Related Information

For information on related topics:

- Services
- Service Summary
- Fabric Connect
- Fabric Assist

Fabric Manager Installation

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

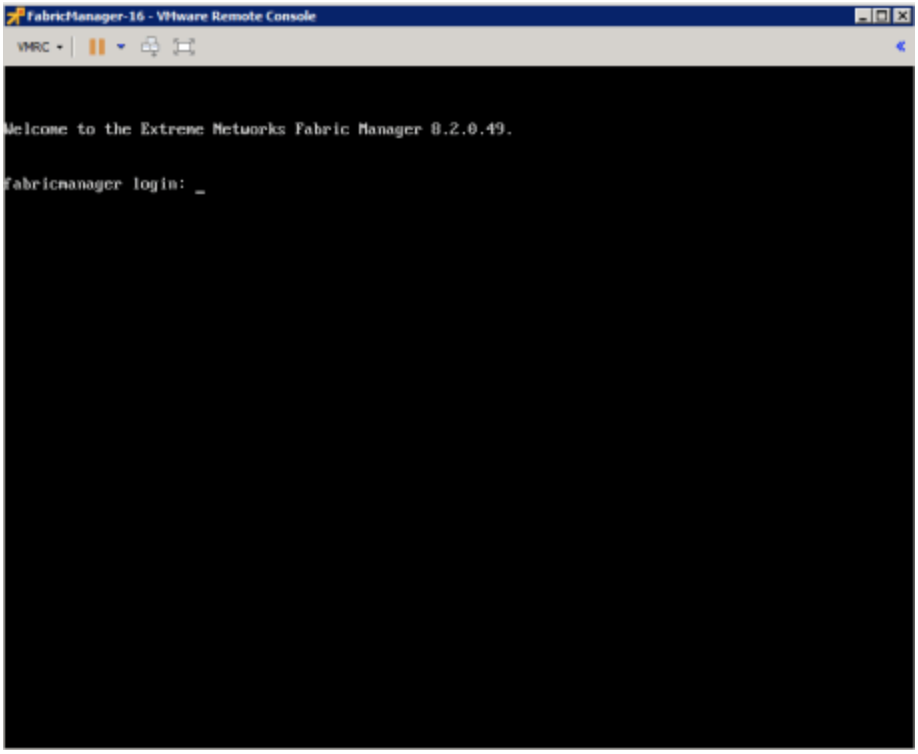
The DHCP mode is the default configuration mode during the Fabric Manager VM's initial startup. Use the static mode when providing a predefined set of networking configurations.

Fabric Manager Installation Static Mode

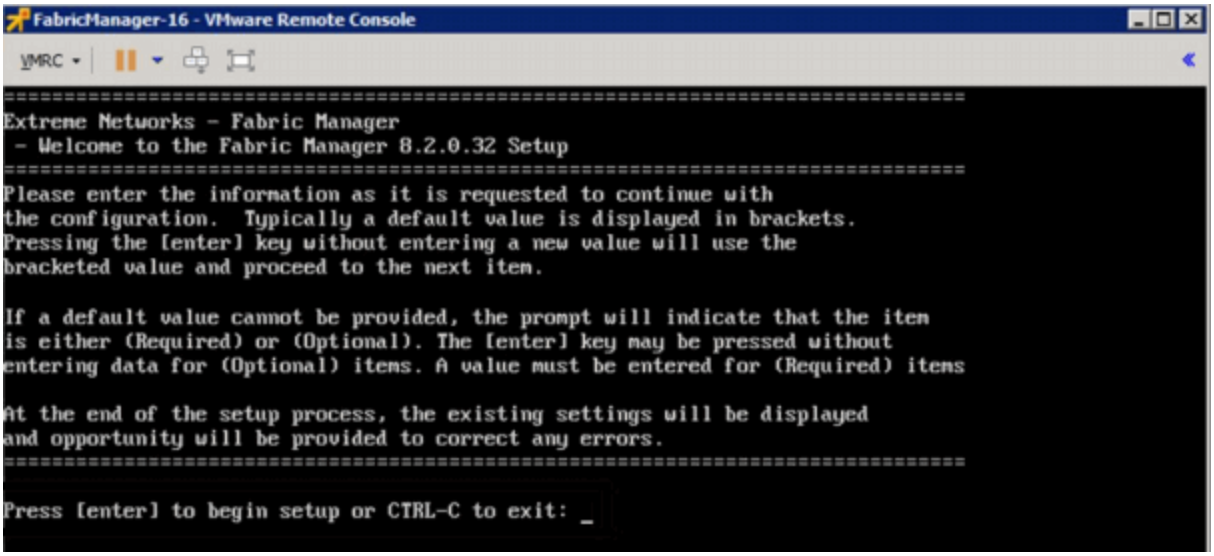
Fabric Manager begins installation in DHCP mode by default. Switch to static mode at any time during the initial installation by pressing the **ENTER** key.

Use the following instructions to install Fabric Manager in static mode:

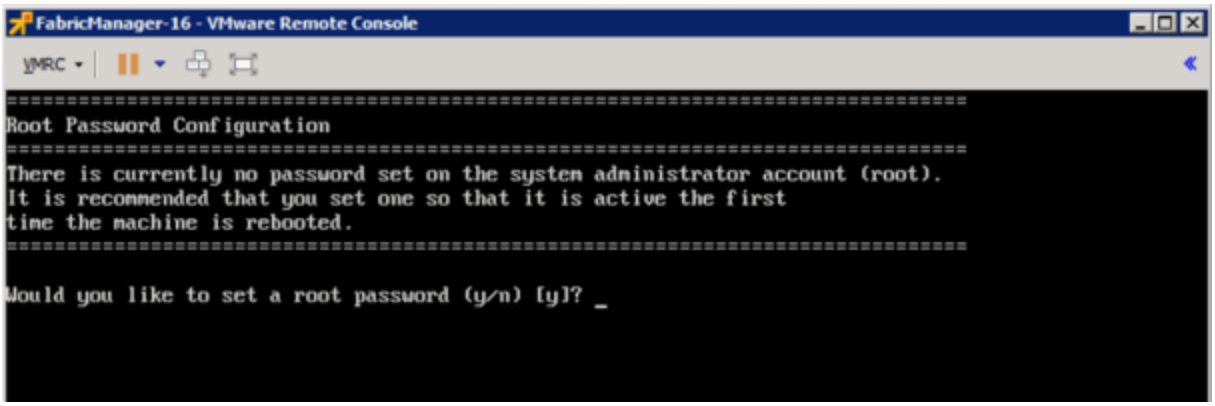
1 In the Console tab of the vSphere client, login as root with no password and press **Enter**.



2. Follow the installation process to complete installation of static mode:
    a. Begin the set-up.

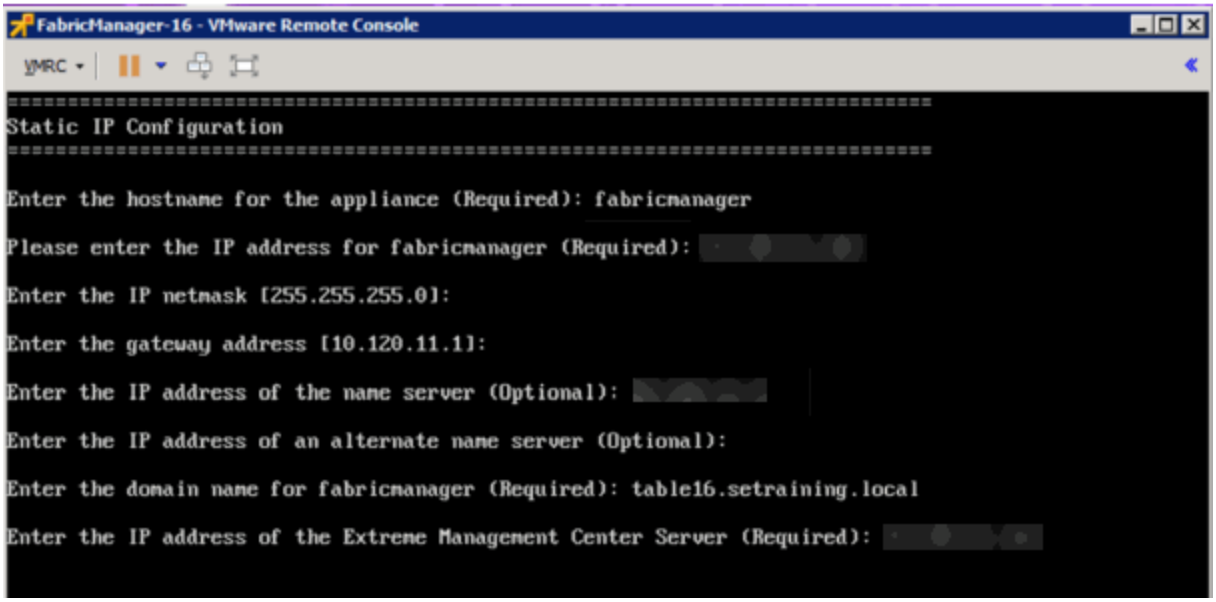


b. Set a root password by entering `y`.



c. Enter and re-type a UNIX password at the next prompt.

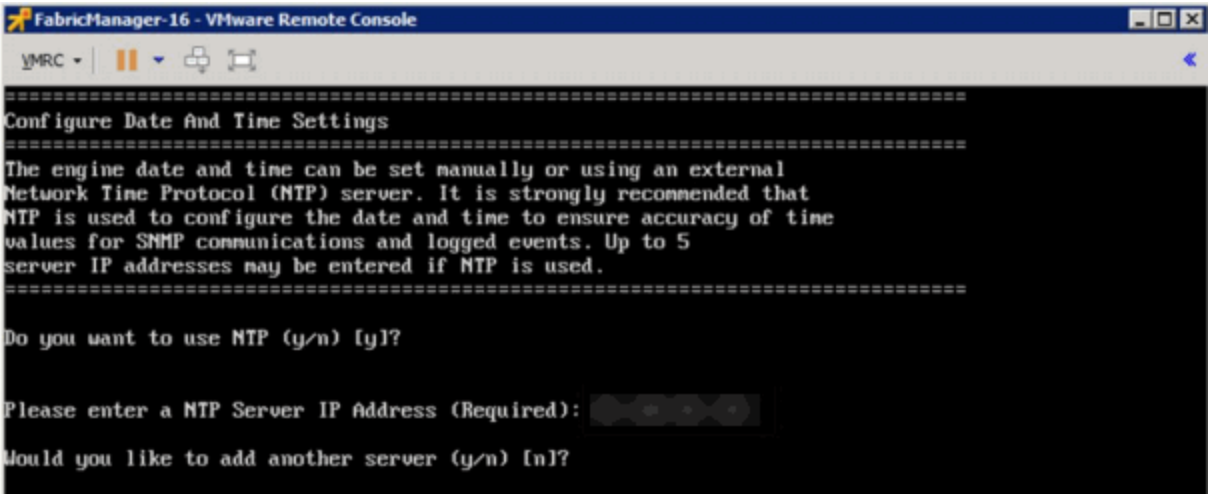
The Static Configuration screen opens.



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.

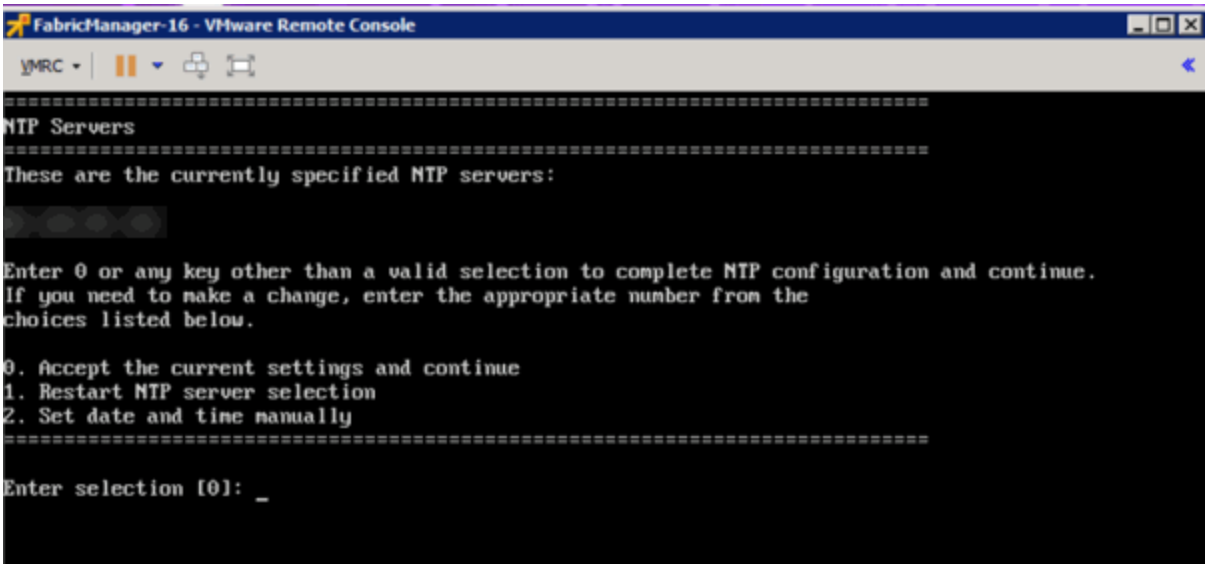
The Date and Time Configuration screen opens.



k. Enter `y` at the next prompt to use NTP (Network Time Protocol).

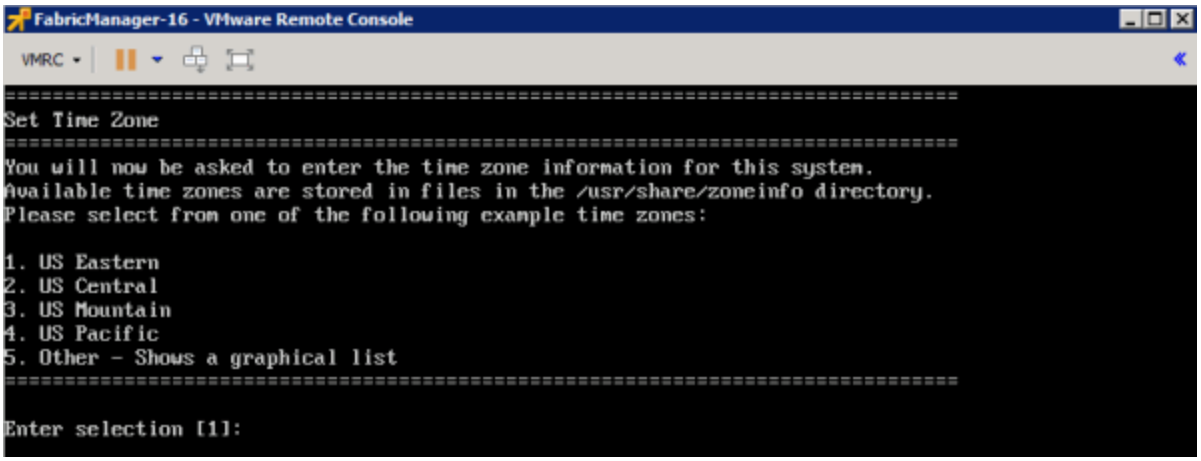
l. Enter the NTP Server IP Address.

m. Enter `n` at the next prompt to skip adding another NTP server. This is optional.



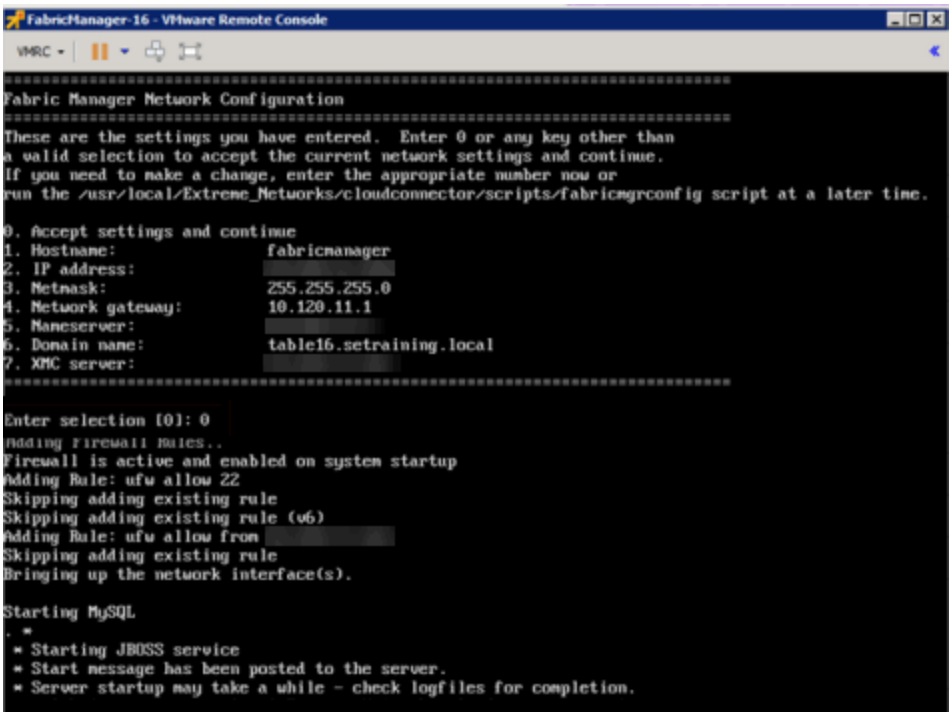
n. Enter the default `0` and accept the current settings and continue.

o. Select the correct Time Zone for your network.



p. Enter the number that corresponds to your time zone.

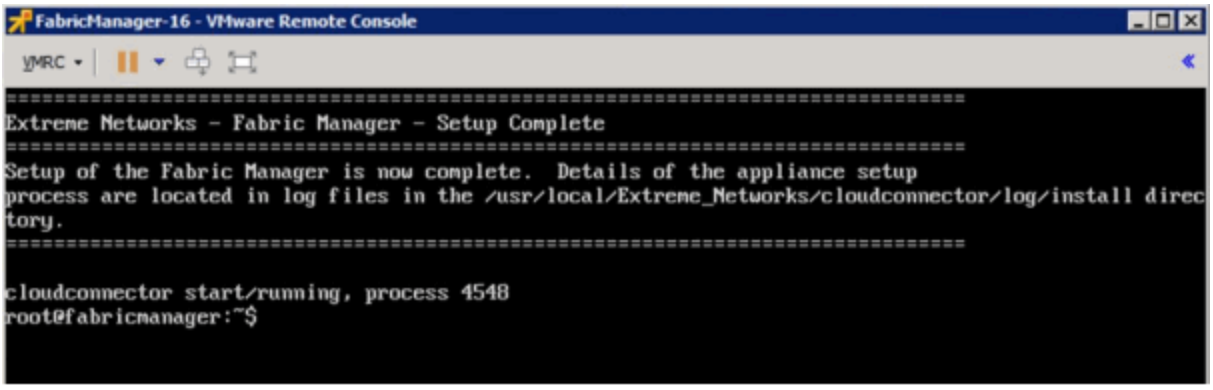
The Fabric Manager Network Configuration screen displays a summary of the configuration options you selected.



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.

Related Information

For information on related tabs:

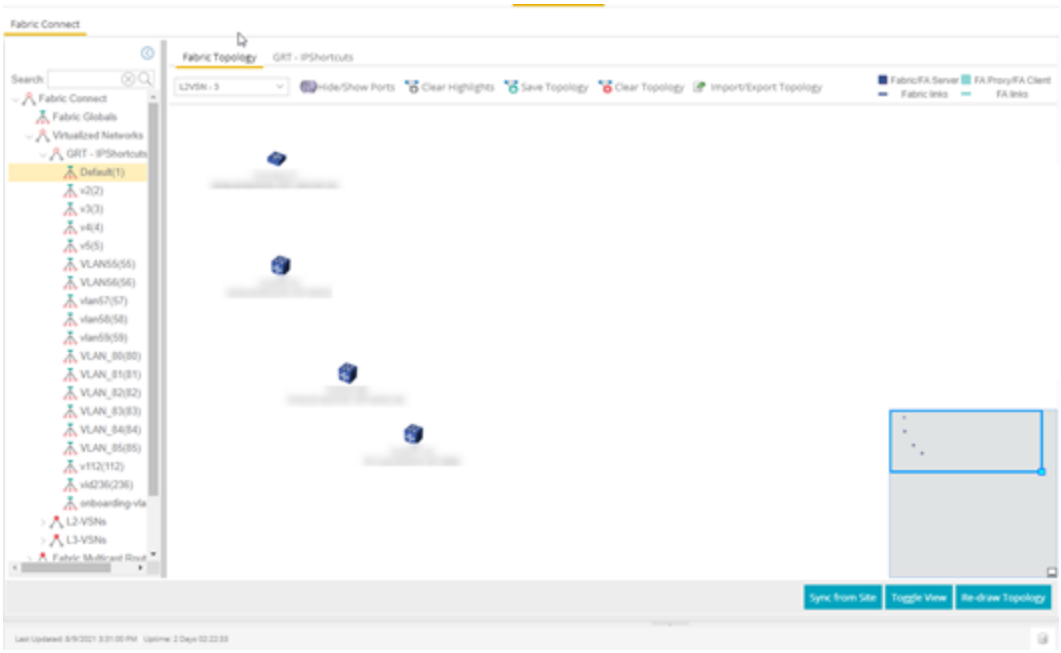
- How to Upgrade Firmware in ExtremeCloud IQ - Site Engine
- Fabric Manager ZTP+ Configuration in ExtremeCloud IQ - Site Engine
- ExtremeCloud IQ - Site Engine Fabric

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.



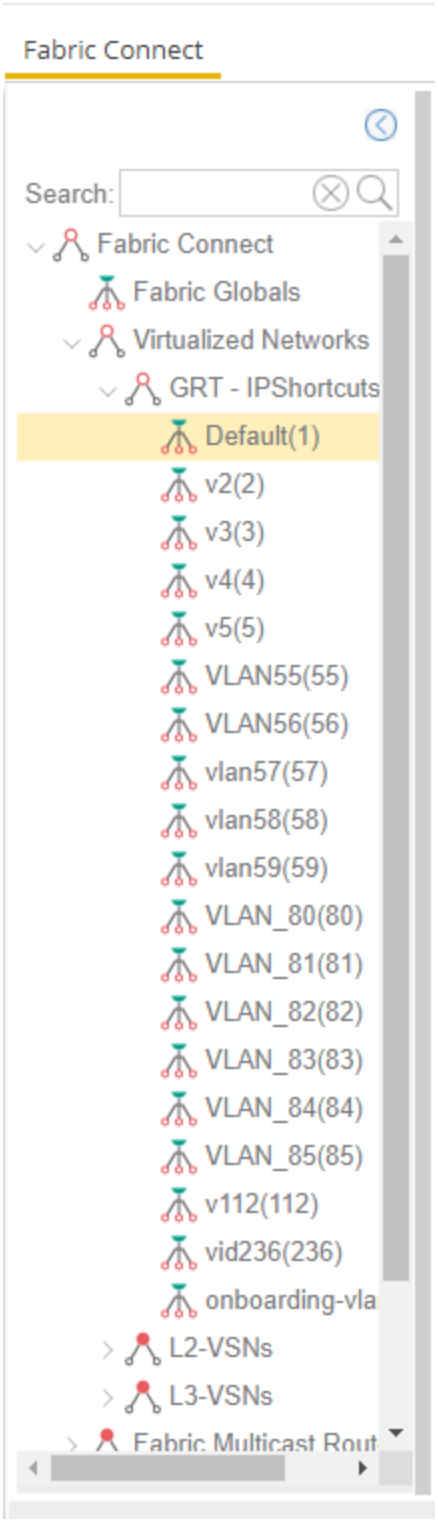
The Fabric Connect tab is divided into two sections: the left-panel tree view and a Fabric Topology right-panel map view.

Left-Panel Tree

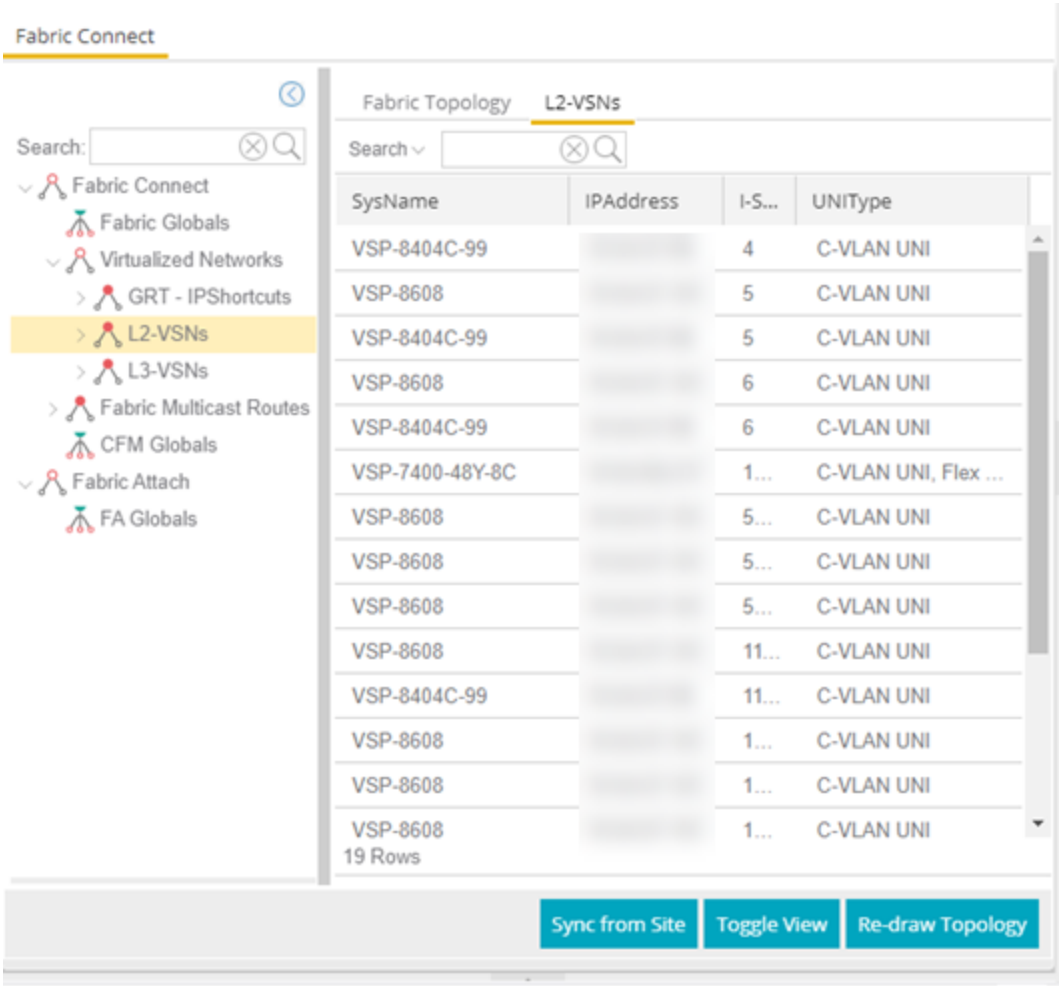
Beginning in version 21.11.10, ExtremeCloud IQ - Site Engine supports two Fabric technology infrastructures: Fabric Connect and Fabric Attach (FA). The left-panel tree includes Fabric Connect and Fabric Attach folders that expand to display all fabric services you have configured in your network.

Fabric Connect Folder

Select the Fabric Connect tab to display the fabric topologies configured on the devices in the site.


Fabric Connect
Search:
Fabric Connect
Fabric Globals
Virtualized Networks
GRT - IPShortcuts
Default(1)
v2(2)
v3(3)
v4(4)
v5(5)
VLAN55(55)
VLAN56(56)
vlan57(57)
vlan58(58)
vlan59(59)
VLAN_80(80)
VLAN_81(81)
VLAN_82(82)
VLAN_83(83)
VLAN_84(84)
VLAN_85(85)
v112(112)
vid236(236)
onboarding-vla
L2-VSNs
L3-VSNs
Fabric Multicast Rout

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.



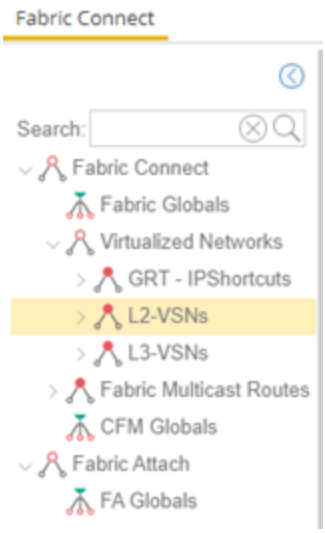
Select the **Toggle View** button to display Fabric Connect fabric services for individual devices.

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:

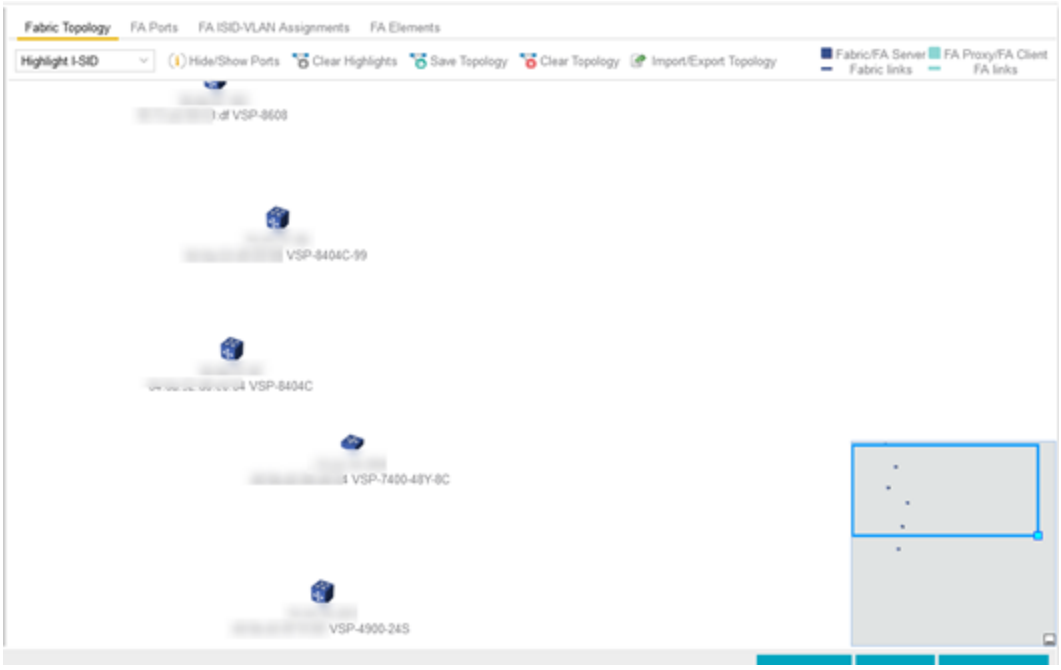
FA Server —for VOSS, ERS 49xx v5.9.2 and later, ERS 4850 v5.9.2 and later, and ERS 59xx series devices; FA Proxy (client proxy) —for ERS 35xx, ERS 48xx, ERS 49xx, ERS 55xx, ERS 56xx, ERS 59xx, and VSP 70xx series devices; FA Standalone Proxy (client proxy) — for ERS 35xx, ERS 48xx, ERS 55xx, ERS 56xx, 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.

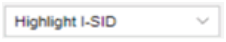
Right-Panel Topology Map

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

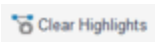
The Fabric Topology tab includes the following tools:

Fabric Service 

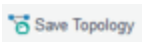
Lists fabric services in your network. Select a service from the drop-down list to display it in the topology map.

Hide/ Show Ports

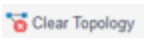
Use to hide or display fabric enabled ports in your network.

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.

Related Information

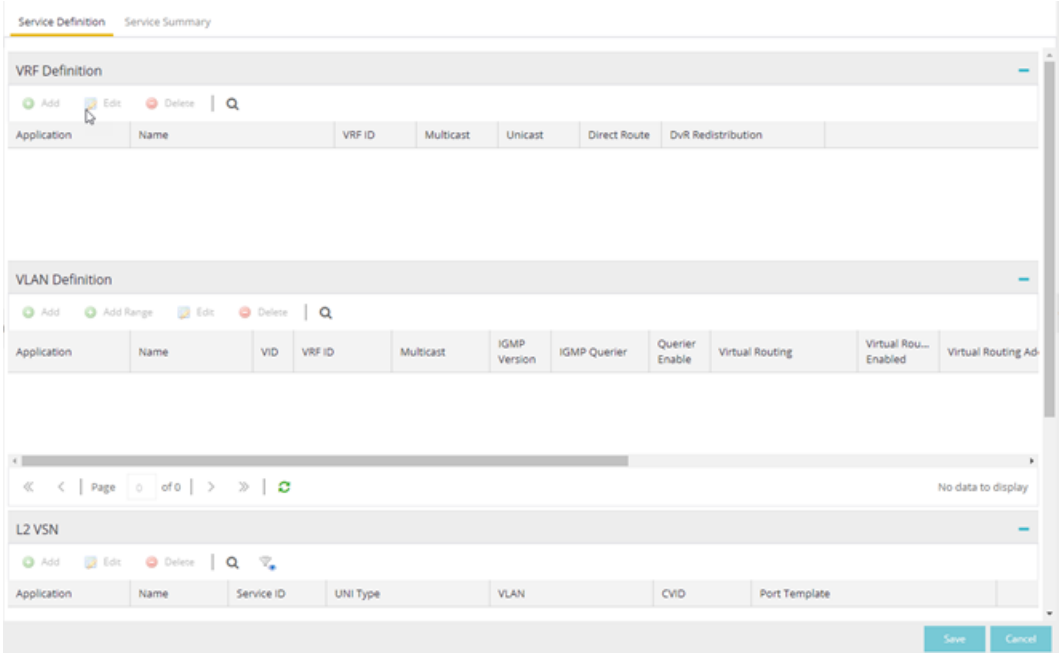
For information on related topics:

- 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.

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 1or 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 VOSS 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.

Flex UNI
Indicates that the fabric service is using the User-Network-Interface (UNI).

The following interface types are available:

- Switched —A VLAN-ID and a given port (VID, port) maps to a Layer 2 VSN I-SID. With this UNI type, VLAN-IDs can be reused on other ports and therefore mapped to different ISIDs.
- Transparent —A physical port maps to a Layer 2 VSN I-SID (all traffic through that port, 802.1Q tagged or untagged, ingress and egress is mapped 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.

VLAN

The VLAN assigned to the fabric service.

CVIDs

Specifies the customer VLAN ID of the associated switched UNI port.

Port Template

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** —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 that 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.

DVR Enable

Select to enable distributed virtual routing.

IMPORTANT: A device on which you enable DVR Leaf mode does not support all ExtremeCloud IQ - Site Engine features. DVR Leaf mode is a constrained operating mode for the device and previous configurations defined on a device may no longer function properly.

DVR Gateway

Enter the gateway address of the DVR device.

Multicast Snooping

Select to configure the service to listen to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers.

Multicast Routing

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

The version of IGMP the service is using: Version 1, 2, or 3.

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.

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.

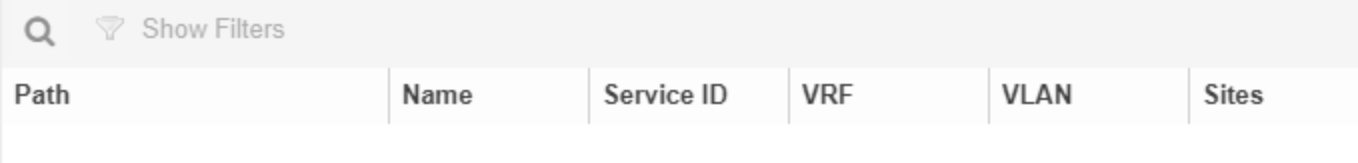
Related Information

For information on related topics:

- Service Summary
- Fabric
- Sites

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.

Related Information

For information on related topics:

- Services
- Fabric
- Sites

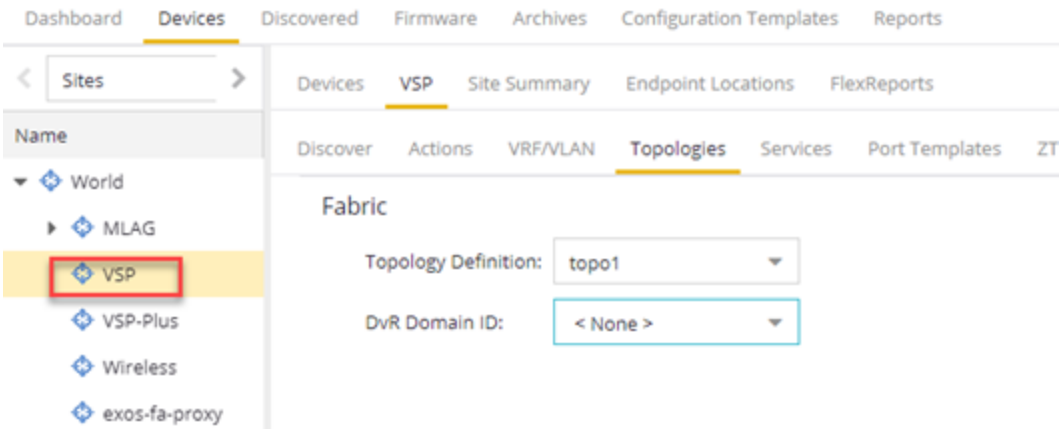
Applying Fabric Services

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.

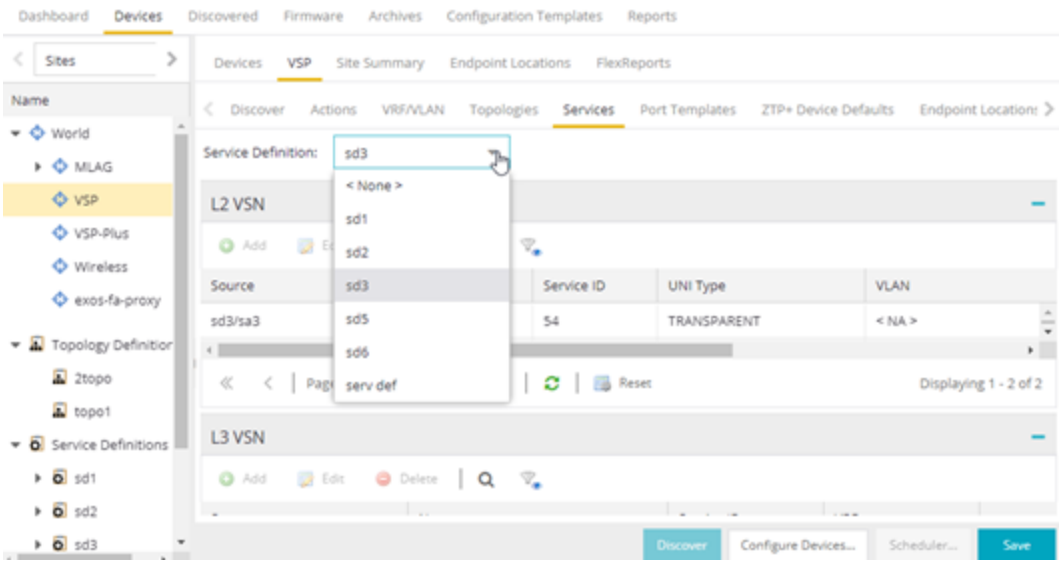


5. Select the **Topologies** tab.
6. Select the topology you want to apply to the site from the **Topology Definition** drop-down list.
7. Select the DVR Domain from the **DVR Domain** drop-down list.
8. Select **Save**.

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

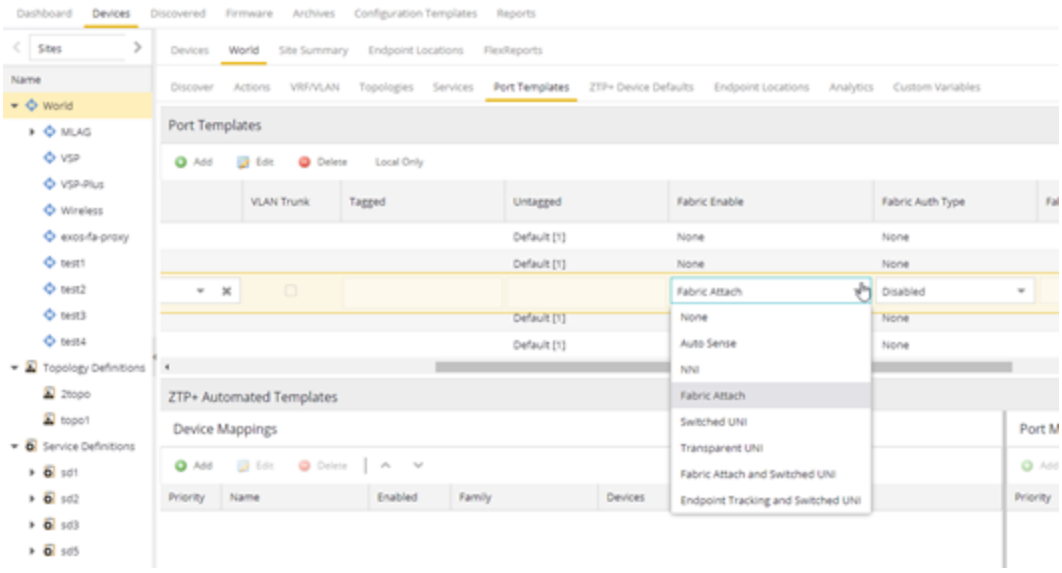
The Port Templates Configuration window enables you to configure ports with a Fabric role. When complete, you can apply the Port Templates configuration to a device.

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 (

) 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 Topologies** 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.

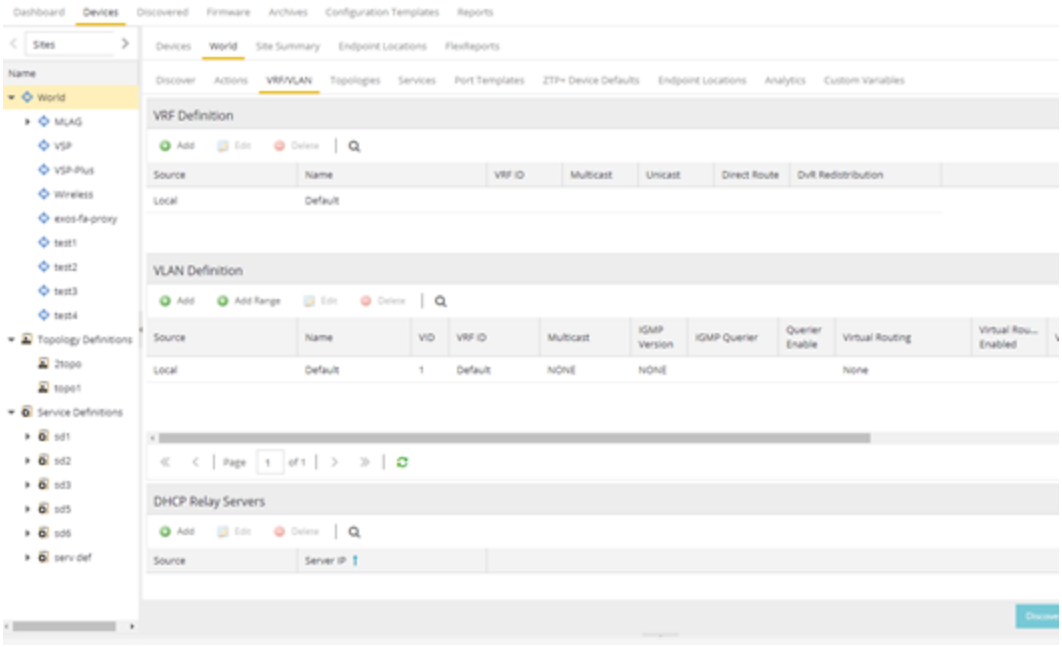
Applying Fabric Services to a Device

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 **Topologies**, **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 Topology

1. Select **Enforce Preview** on the **Topologies** tab in the **Configure Device** window.
2. The **Compare Device** window opens.
3. Select the Topologies 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**.

Related Information

- Services
- Fabric
- Sites
- Devices

Fabric Manager ZTP+ Configuration

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.

Related Information

For information on related topics:

- Sites
- Profiles
- Add Device
- Edit Device
- Devices

How to Add Fabric Manager

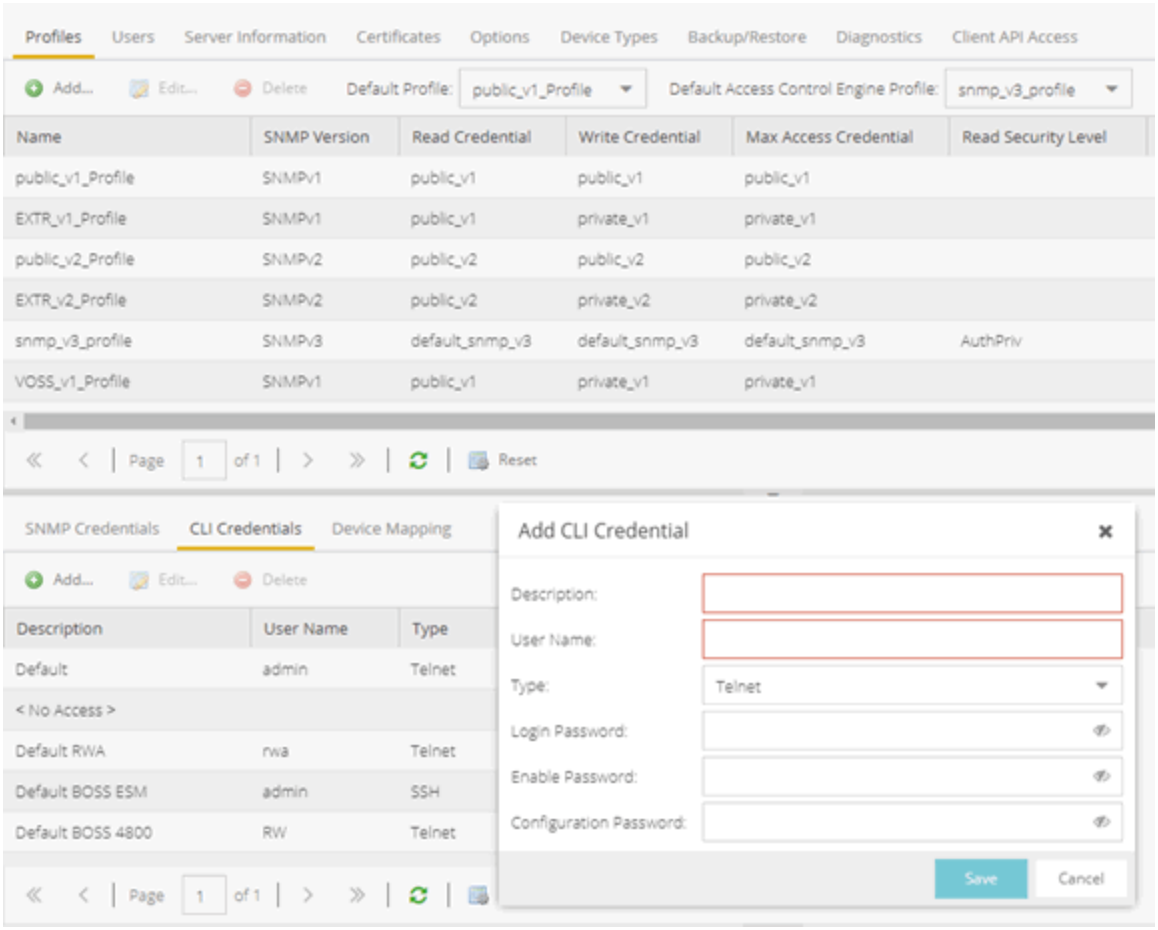
Once you install the Fabric Manager virtual machine (VM), you can add it to ExtremeCloud IQ - Site Engine and enable it via ZTP+ (Zero Touch Provisioning Plus) functionality.

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

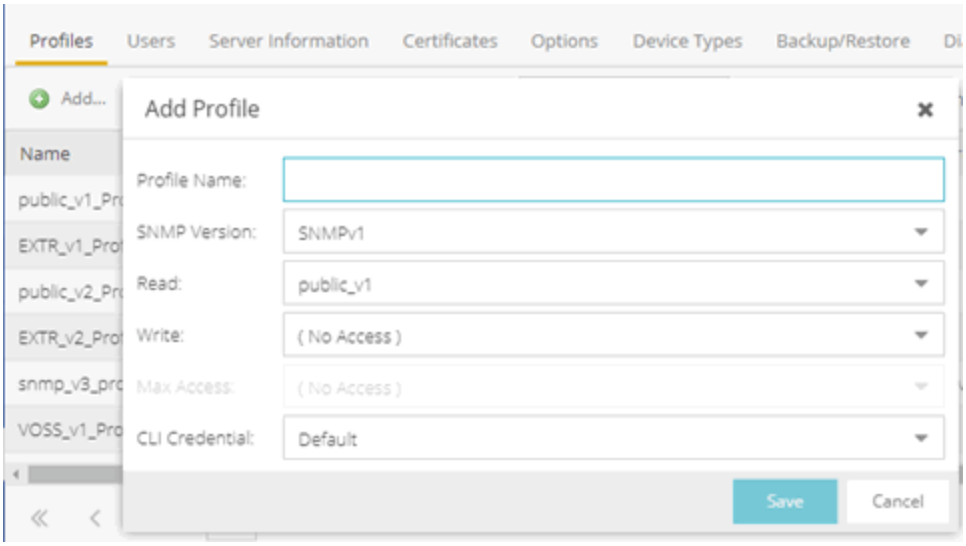
1. Launch ExtremeCloud IQ - Site Engine.
2. Open the **Administration > Profiles** tab.
3. In the bottom panel, select the **CLI Credentials** tab.



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**.

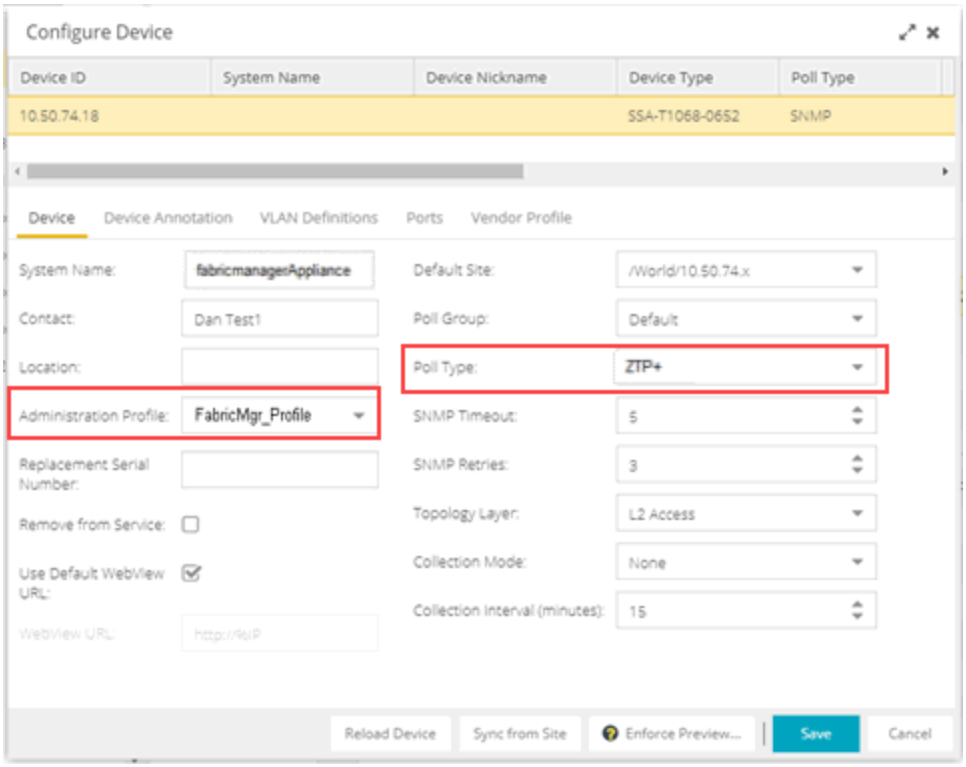
Add Administration Profile to the Fabric Manager engine

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**.

Related Information

- 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.

Related Information

For information on related topics:

- Services
- Fabric
- Sites
- Devices

How to Create a Fabric Service Definition

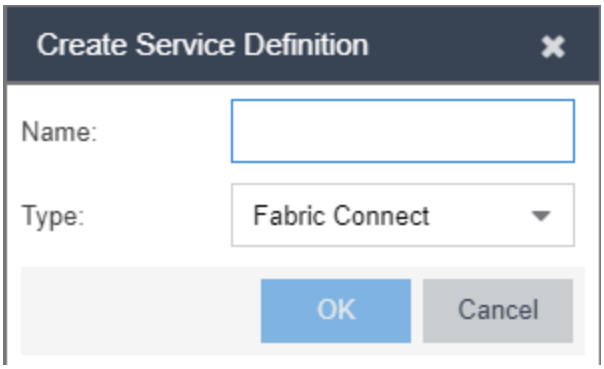
You can create a service definition in the **Sites tab** in ExtremeCloud IQ - Site Engine. Service definitions display information configured in service applications definitions. When created, service definitions are added to sites in your network and are used to build a fabric topology map.

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.

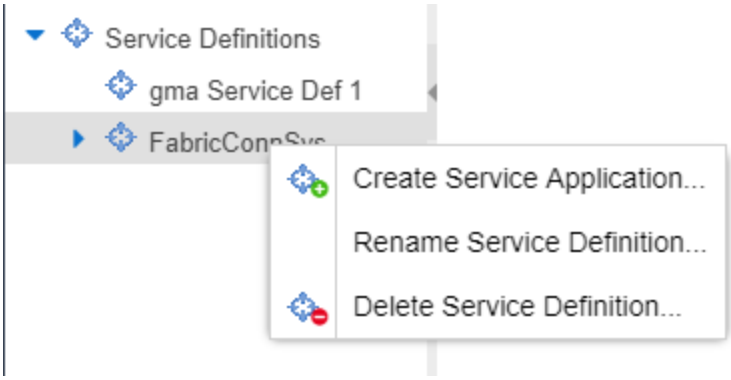
After the service definition is created and configured, you can apply it to a site within your network. When fabric services have been assigned to a site, they cannot be deleted.

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.

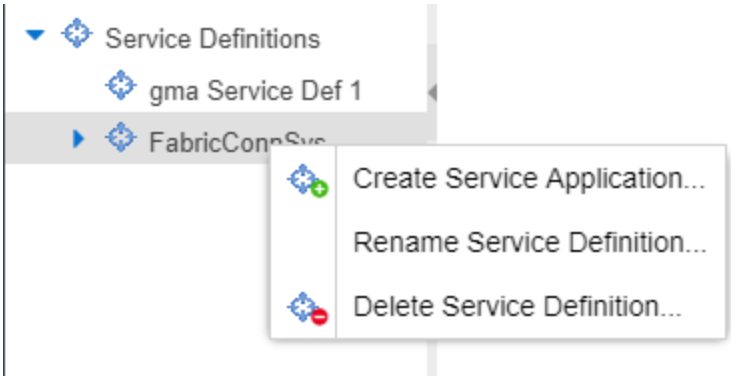


To rename a service definition:

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.

Related Information

For information on related topics:

- Services
- Fabric
- Sites
- Devices

How to Create a Service Application

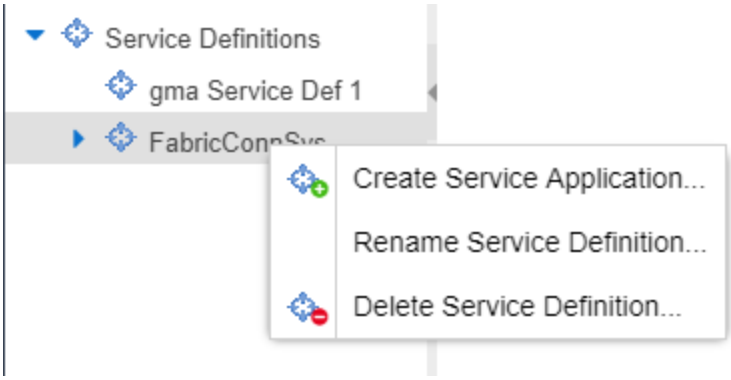
You can create a service application via the **Sites** tab in ExtremeCloud IQ - Site Engine. Service definitions display information from service applications. When created, service applications are added to sites in your network and are used to build a topology map.

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.

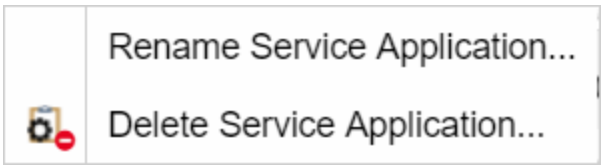
After the service application is created, it is available in the left-panel tree and a new right panel opens that includes a Services tab and a Service Summary tab.

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.

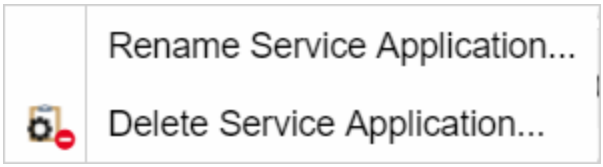
4. Right-click the service application you are renaming.



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.

Related Information

For information on related topics:

- Services
- Fabric
- Sites
- Devices

Configure Fabric Attach Proxy for ExtremeXOS Devices

ExtremeCloud IQ - Site Engine can extend Fabric Attach (FA) functionality to ExtremeXOS devices and provision them as FA Proxy devices.

NOTE: FA proxy is supported on the following ExtremeXOS devices: X435, X450G2, X460G2, X670G2, X440G2, X465, X590, X620, X690, X695, X870, EXOS Stack, 55XX series.

Configure on Services Tab

ExtremeXOS devices that have been provisioned as FA Proxy devices use a VLAN:NSI association, which devices use for their FA Proxy static assignments.

To configure a VLAN:NSI binding for ExtremeXOS devices that are provisioned as FA Proxy devices, create a VLAN in the VLAN tab on the Network > Devices > Configure Device tab. Then create a binding in the Services tab, which requires you to select the VLAN you created. When the binding is established, you can configure CVLAN UNI services to the FA Proxy EXOS device.

Configure Administration Profile

REST API is used to manage VLAN:NSI (network service identifier) bindings used by FA Proxy for an ExtremeXOS device. Because SNMP is used on VLANs and Ports configuration, and because the CLI credentials are reused by the device for REST requests, it is important to make sure that both credentials (SNMP and CLI) for a device profile are correct.

For supported ExtremeXOS devices that have ExtremeXOS Version 31.1.1 firmware, the VLAN and Services tabs are available on the Configure Device tab . If a device is not an FA Proxy-supported device and does not have ExtremeXOS Version 31.1.1 firmware, only the VLAN tab is available.

If a device is enabled as an FA Proxy, only CVLAN UNI services are available for use as VLAN:NSI Fabric Attach Proxy static assignment bindings.

ExtremeXOS devices do not support Fabric Connect; therefore, the Topology tab will not display for these devices. To apply VLANs and L2 services from a service definition to

ExtremeXOS devices within a site, a topology definition and a service definition must be applied to the site.

Related Information

Configuring a Device

Upgrading Fabric Manager

Use the following procedure to upgrade your version Fabric Manager.

Prerequisites

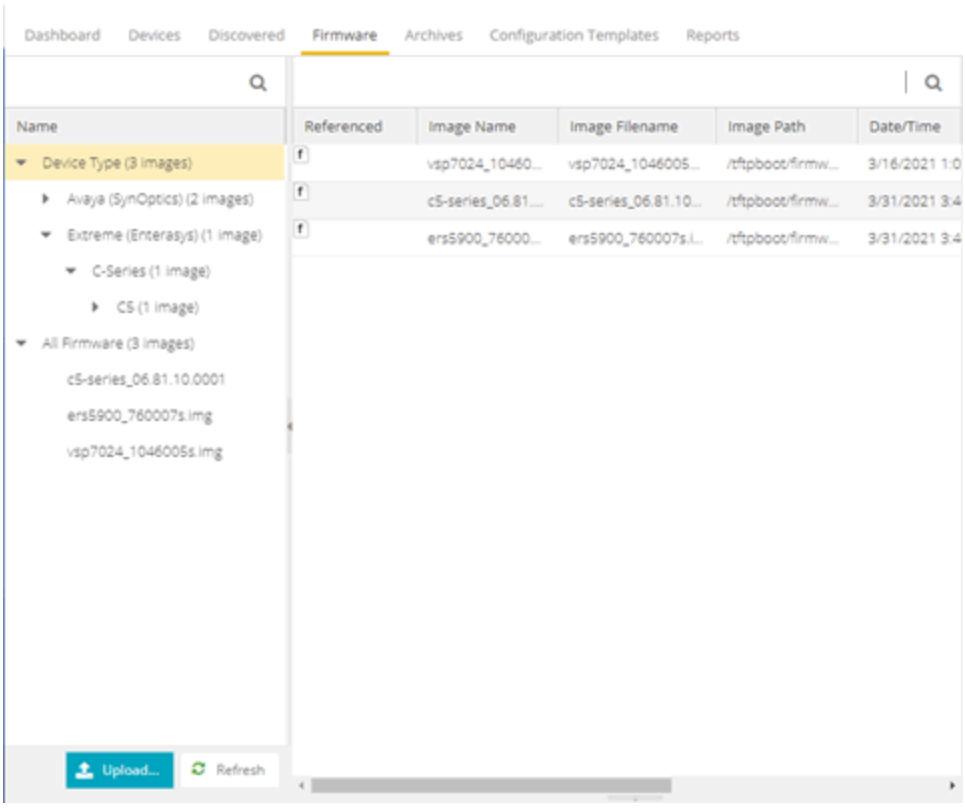
- Upgrade ExtremeCloud IQ - Site Engine to the later version before you upgrade Fabric Manager to the corresponding build number.
- Ensure that both the current and target ExtremeCloud IQ - Site Engine and Fabric Manager build numbers are the same.
- Download the latest upgrade bundle from the Extreme 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.

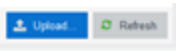
NOTE: After you deploy Fabric Manager and then register with ExtremeCloud IQ - Site Engine, only the user credential associated with the Fabric Manager profile has SSH login access.

Upgrade Procedure

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

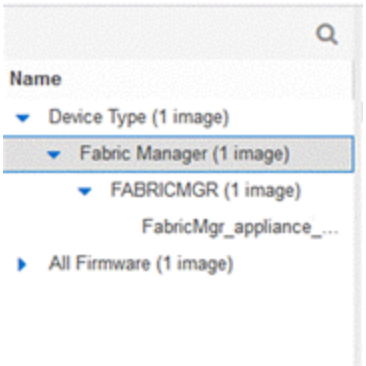
2. Select the **Firmware** tab.



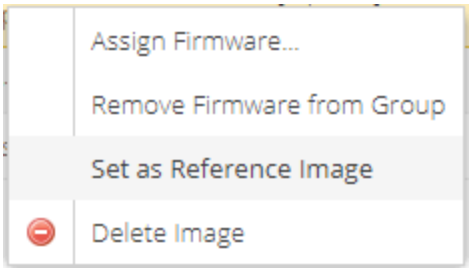
3. On the left panel, select **Upload**  .
4. In the Directory field, select the **SCP** radio button and select **Upload**.

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.

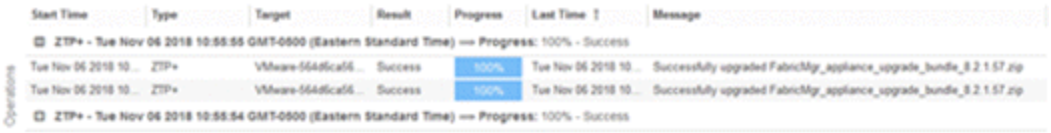


7. Navigate through the newly added Device type until you see the bundle image listed.
8. Right-click the bundle listed on the main panel and select **Set as Reference Image**.

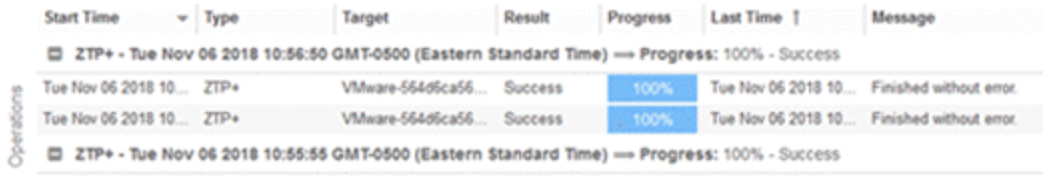


This step sets this image bundle as the Reference upgrade image for Fabric Manager. The upgrade process to get triggered by default can take **up to five minutes** depending on the poll interval set on ExtremeCloud IQ - Site Engine.

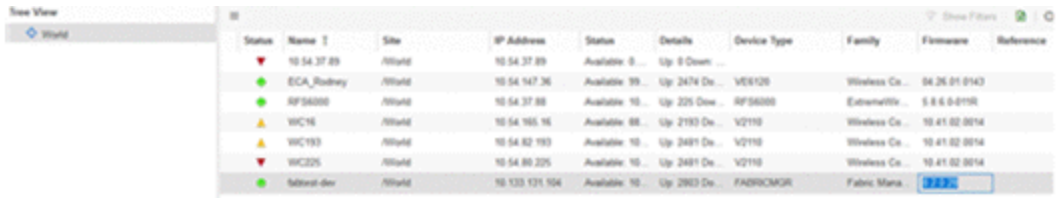
9. Open the **Operations** log on ExtremeCloud IQ - Site Engine and wait until a log of type 'ZTP+' with the message `Successfully upgraded FabricMgr_appliance_upgrade_bundle_<version_number>.zip` appears.



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**.

Related Information

- 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.

Related Information

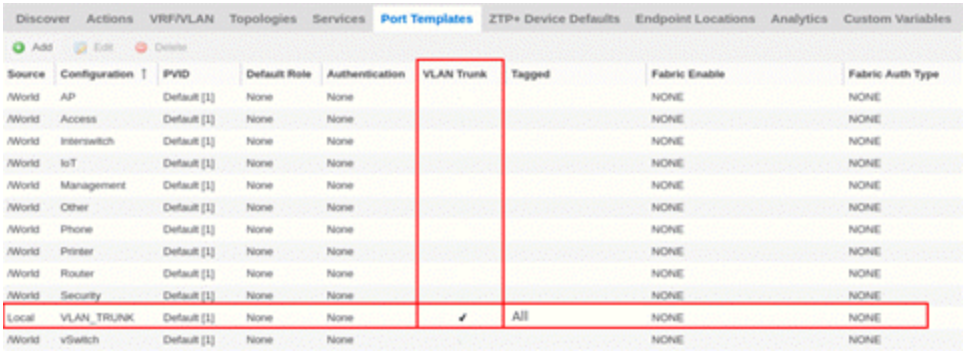
For information on related topics:

- 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.

Related Information

For information on related topics:

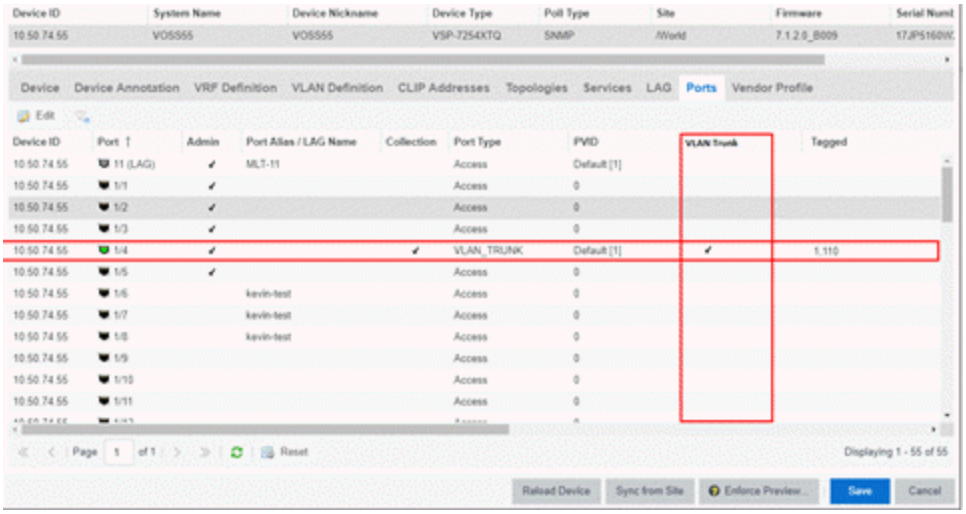
- Provision VLAN Trunks Automatically
- How to Edit a Port Template

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:

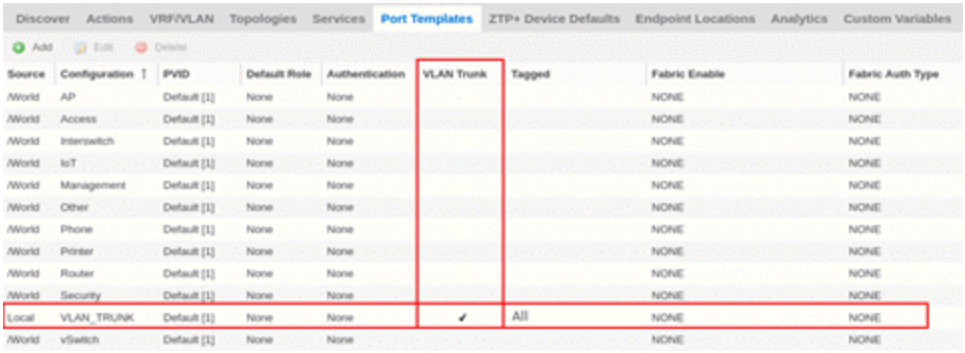
1. Open **Devices > Devices**.
2. Right-click on a specific device, and then select **Configure**.
   The system displays the **Configure Device** dialog.
3. In the Configure Device dialog, select **Ports**.



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

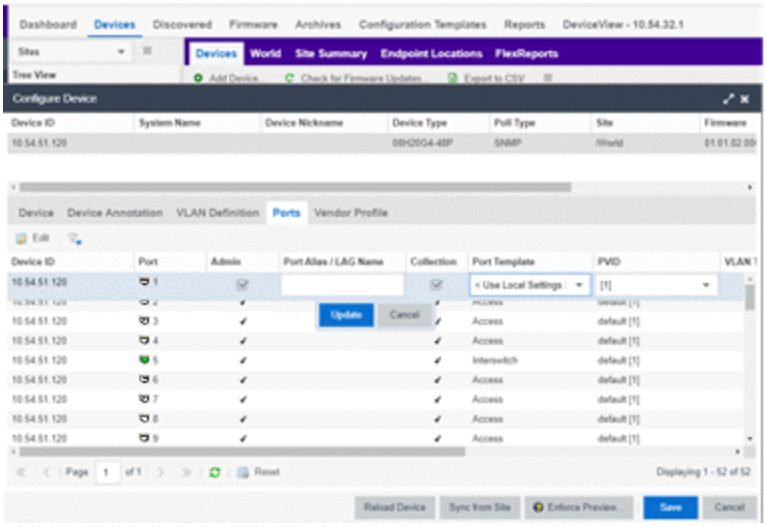
You cannot edit all the fields for a port that is bound to a template. If you want to edit all the fields, you must change the Port Template type to **<Use Local Settings>**. This Port Template type value is available only in the Device Port grid.

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

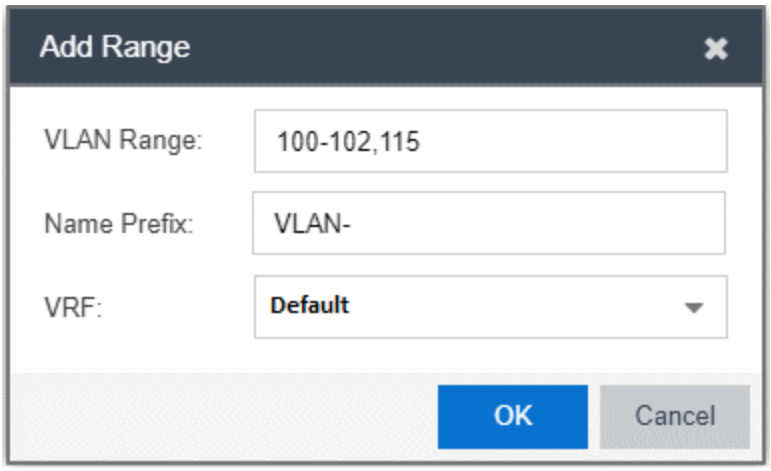
VLAN Range makes it easy to add many VLANs to a device. To add VLANs in a group, instead of manually adding and editing one entry at a time, provide the VID range, Name prefix, and VRF ID for all newly imported VLANs.

You can provision VLANs from three different levels (device, site, service definition):

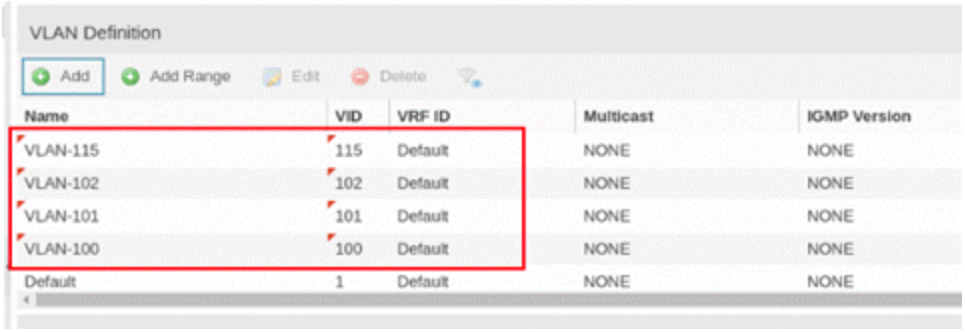
- **Device Level** – Use this level to configure a VLAN on an individual device.
- **Site Level** – Use this level to configure VLANs for all the devices that belong to a site.
- **Service Definition Level** – Use this level to configure VLANs on a Service Definition, which serves as a container for 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).



Related Information

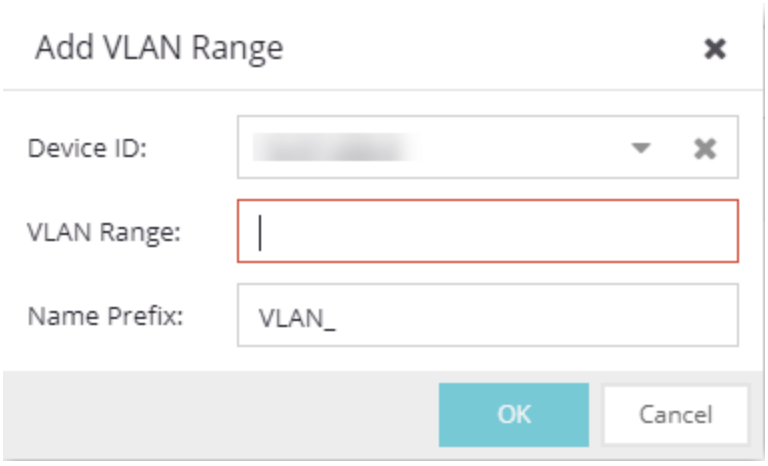
For information on related topics:

- 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.

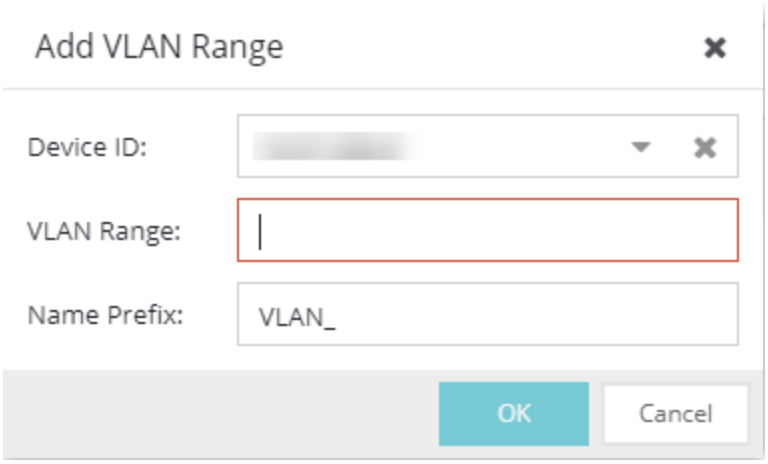
   NOTE: If the selected device does not support VRFs, the VRF field does not display.

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 .

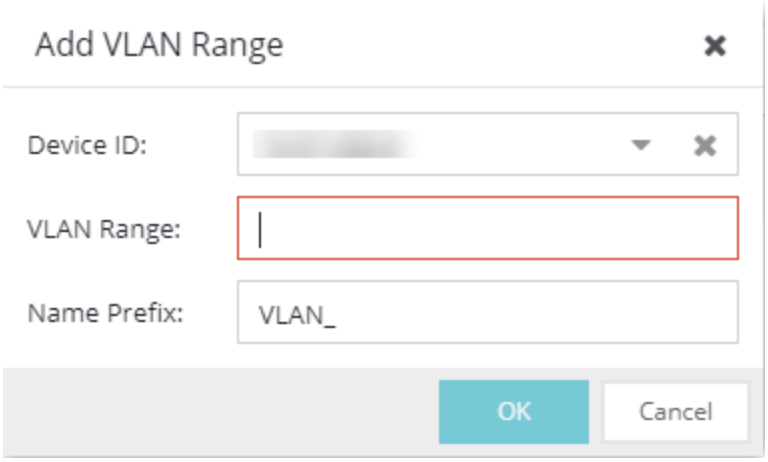
7. Select **OK**.

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.

Related Information

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.

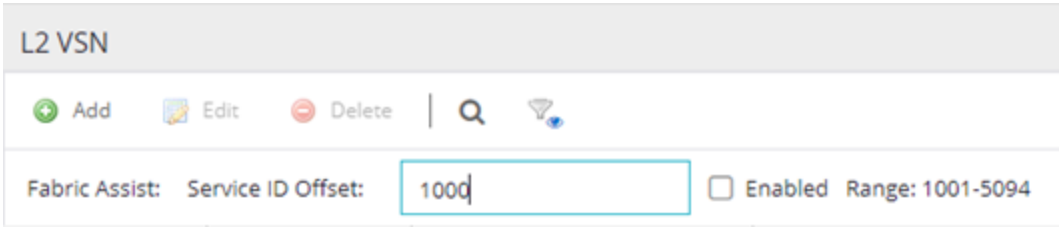
To enable the automatic creation of L2 VSN services, you must enter a Service ID Offset in the L2 VSN dialog.

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.

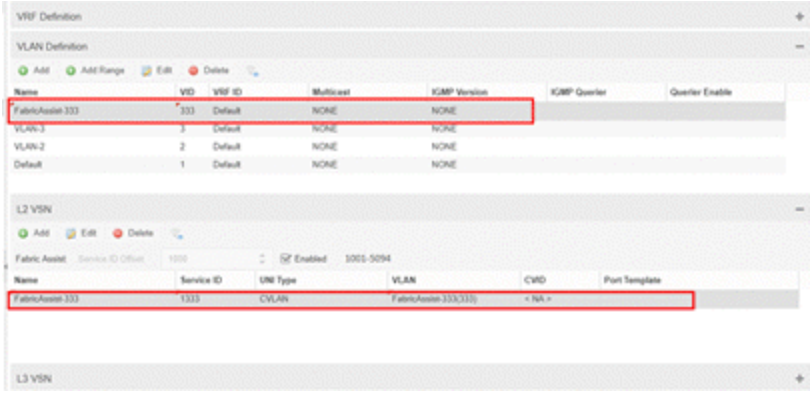
NOTES:

- 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.

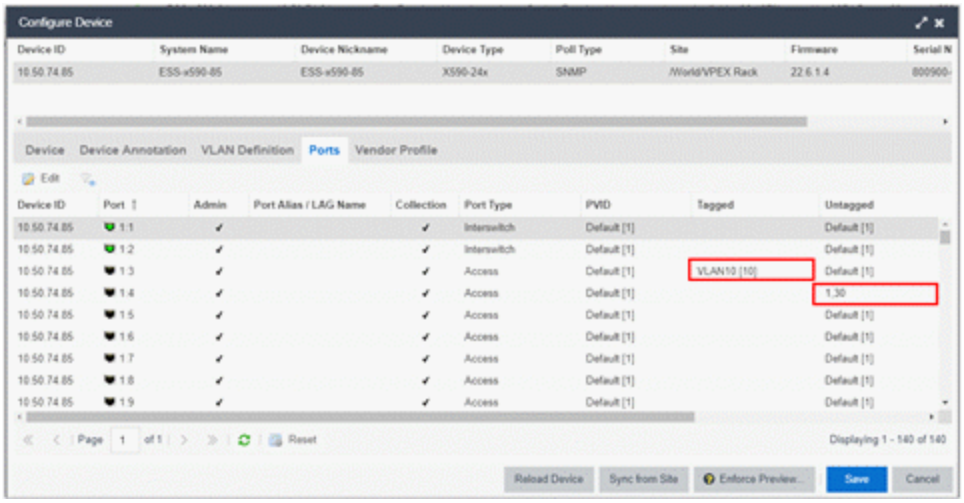
Devices inherit VLAN definitions configured in a site or inherited from a service application that is mapped to a site. Devices in a site also inherit the Enable Pruning value from the site:

- 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.

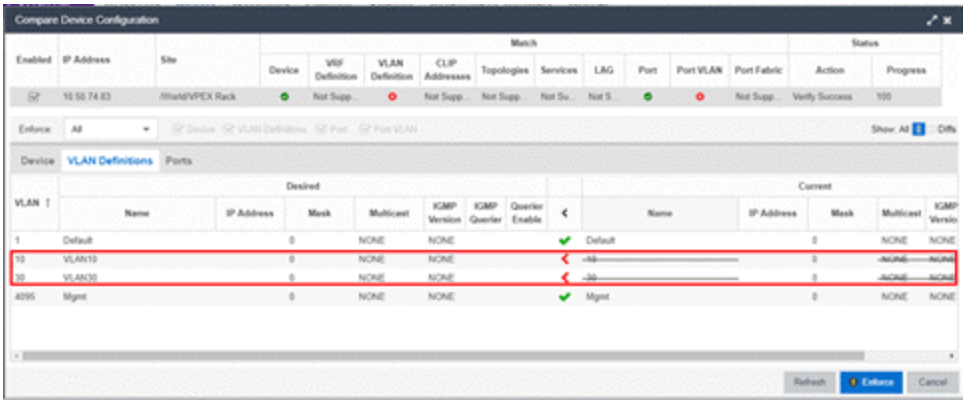
The device VLAN Definition window shows all inherited VLANs so that you can configure tagged or untagged egress on ports. VLAN pruning takes place when you launch the enforce preview. The Enforce Preview window shows only the VLANs that have egress configured on the device.

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.



Related Information

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 devices, ExtremeCloud IQ - Site Engine provides **VLAN provisioning support** so only the VLANs from the device will be imported into the Service Definition.
- For VOSS 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.

Related Information

For information on related topics:

- Fabric Assist

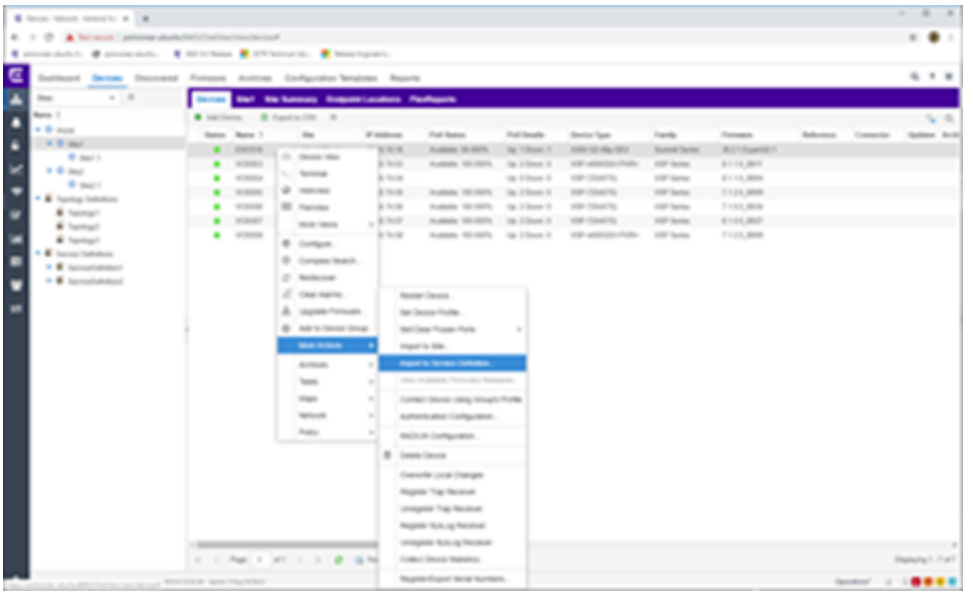
Prerequisites

Before you begin the import process, you must do the following:

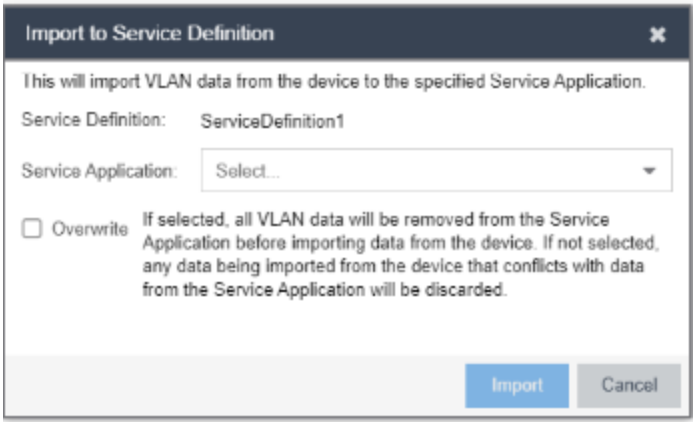
- Identify the target Service Definition and Service Application(s) that you want to import into.
  If the Service Definition and Service Application(s) have not already been created, you must create them before the import process begins.
- Assign the Service Definition to the Site that contains the 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

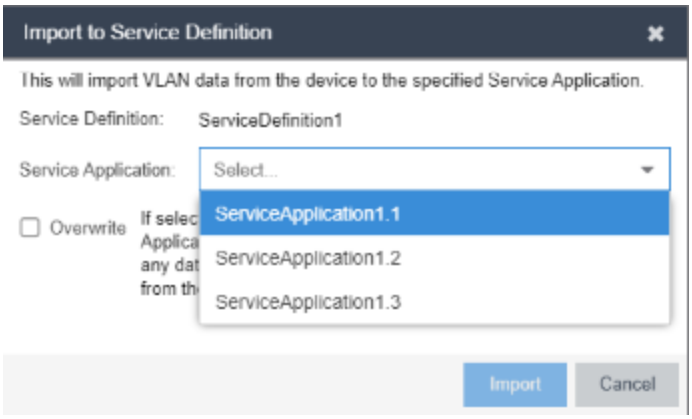
1. Open **Network > Devices > Sites View**.
2. Expand **World**, and then select a site.
3. On the Devices sub-tab, right-click on the device that you want to import from, and then select **More Actions > Import to Service Definition**.



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 ExtremeCloud IQ - Site Engine's ability to provision certain features:

   - For devices that ExtremeCloud IQ - Site Engine has **VLAN provisioning support** (such as EOS and ExtremeXOS), 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 VOSS), the VRFs, VLANs, L2, and L3 services will be imported into the Service Definition.

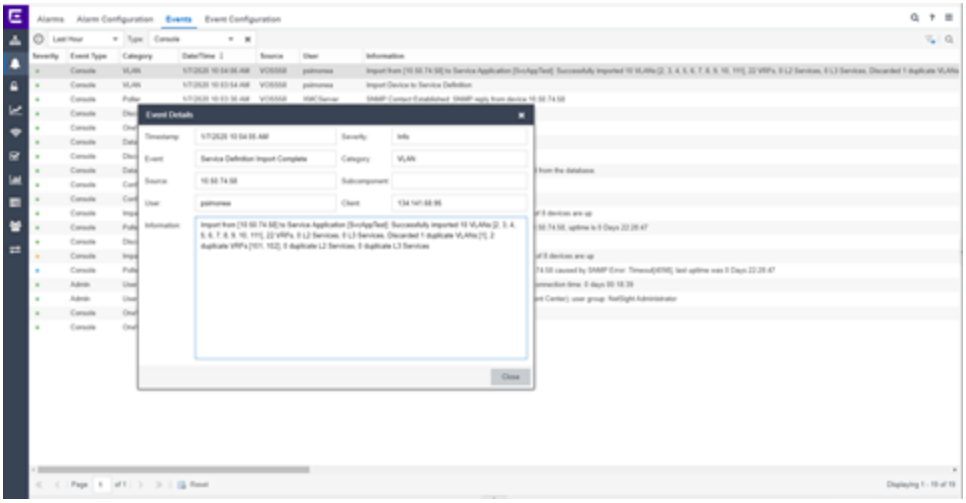
   NOTE: Currently only CVLAN UNI services are supported in Release 8.4. Switched and Transparent UNI support will be added in a future release.

   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.

Related Information

For information on related topics:

- Maps
- Network
- How to Create and Edit a VLAN

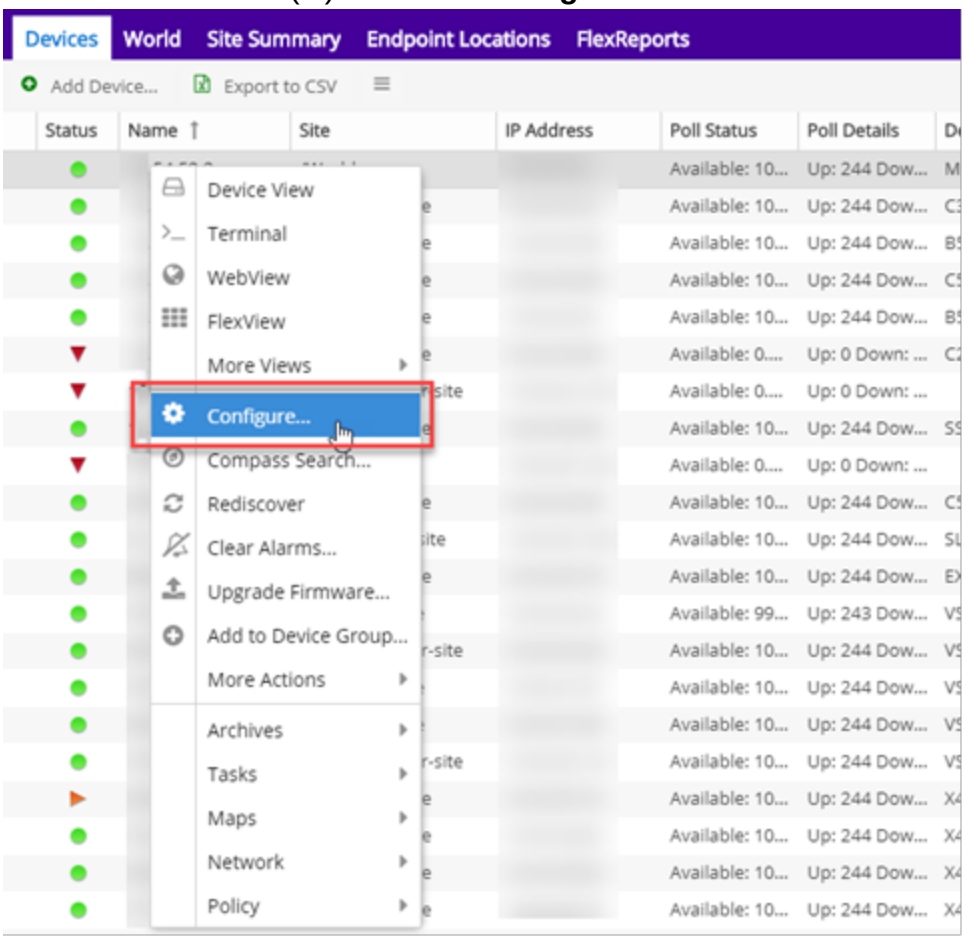
Changing Device Configurations

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.

Related Information

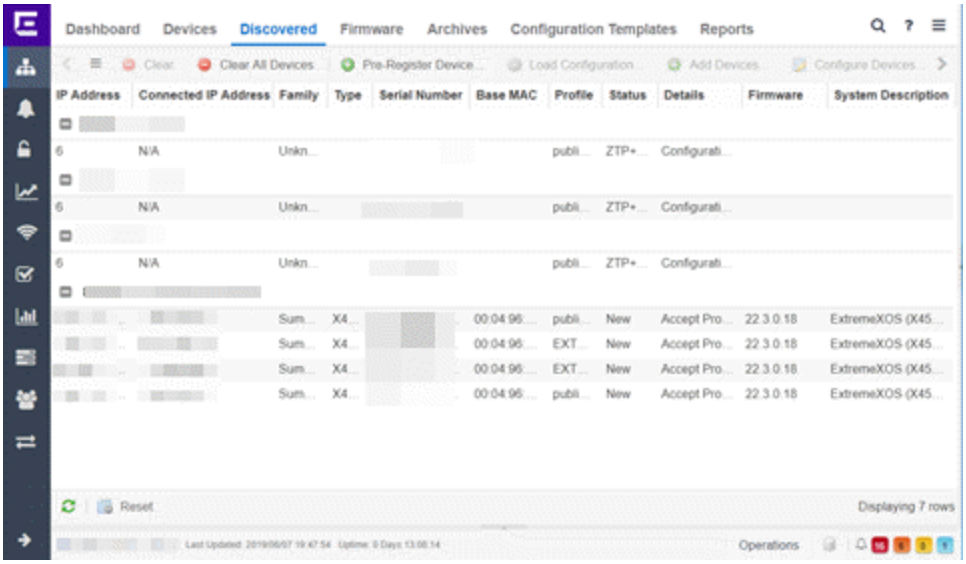
For information on related topics:

- 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 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.

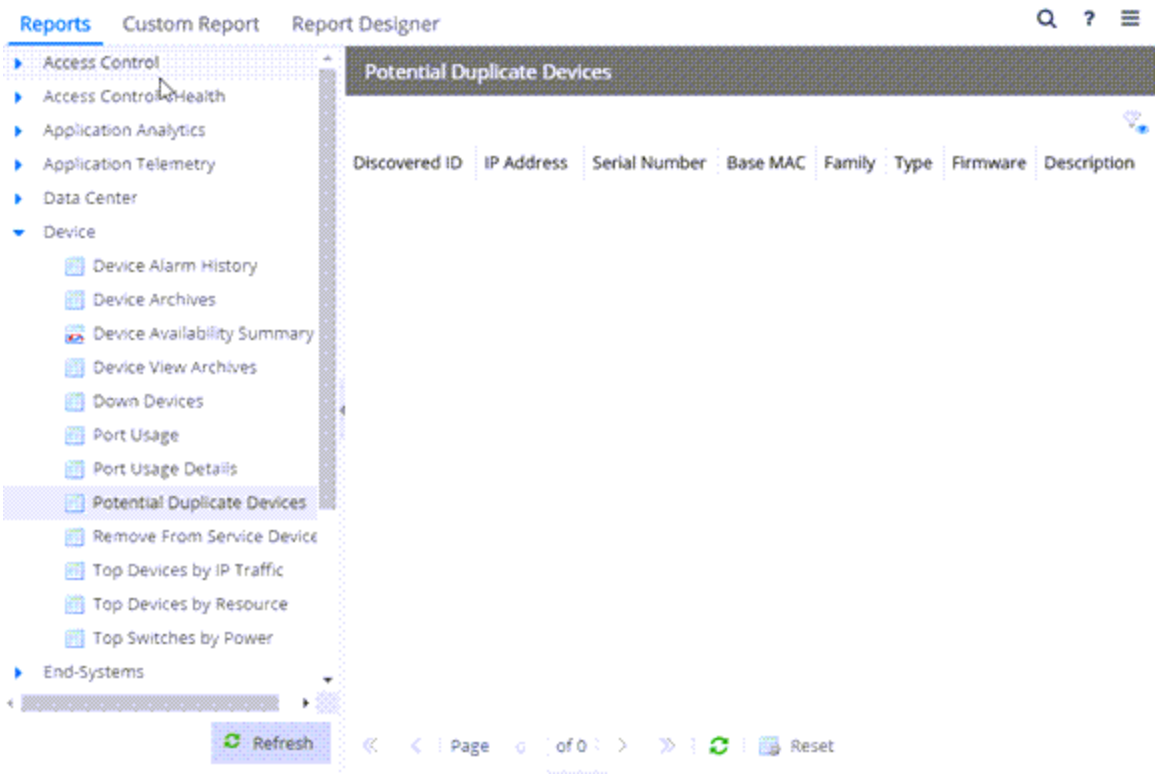
For example, you are adding three devices to ExtremeCloud IQ - Site Engine that appear on the **Discovered** tab. All three devices share the same Serial Number, but have different IP Addresses. The Discovered ID column will display the same serial number. Selecting **Group by This Field** in the menu 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.

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

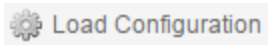
The **Last Seen** column displays the date and time the device last communicated with the ExtremeCloud IQ - Site Engine server.

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 

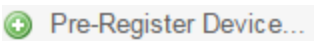
Select to open the Load a configuration on a Discovered Device window, which allows you to use a saved configuration for an existing device on a ZTP (zero touch provisioning) enabled device.

Clear 

Select to remove the currently selected device from the **Discovered** tab.

Clear All Devices 

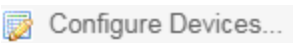
Select to remove all devices listed on the **Discovered** tab.

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.

Related Information

For information on related windows:

- Network Tab
- Devices Tab

For information on related tasks:

- How to Discover Devices in ExtremeCloud IQ - Site Engine
- How to Upgrade Firmware

Load Configuration on a Discovered Device

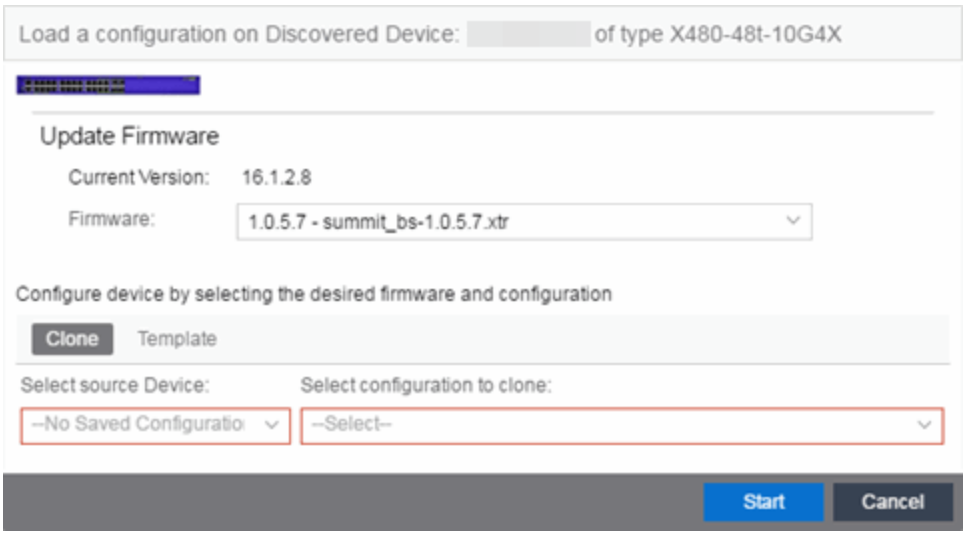
Use this window to use a saved device configuration on a device you are adding to ExtremeCloud IQ - Site Engine. Devices to which you load a saved configuration must have ZTP (Zero Touch Provisioning) enabled.

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.

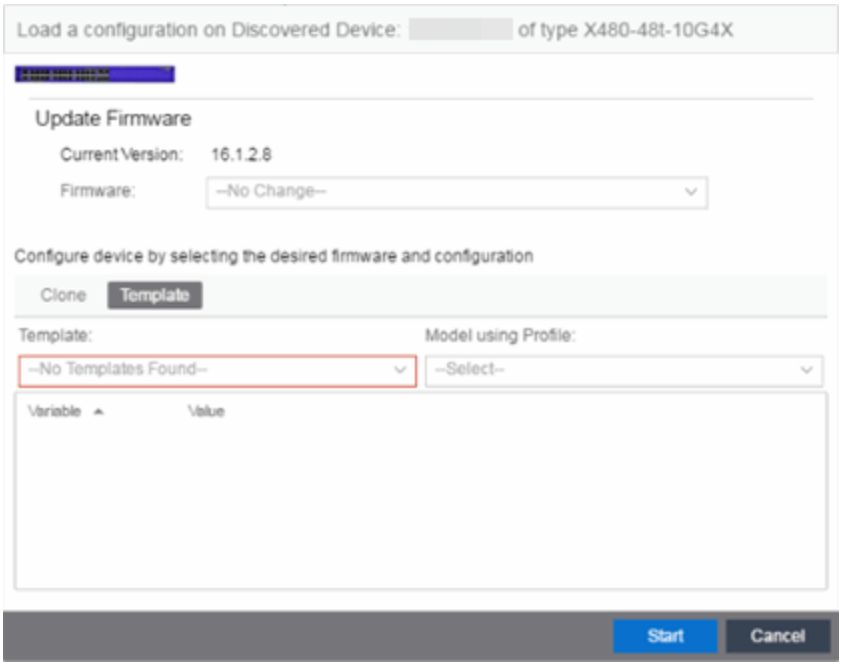
Start

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.

Related Information

For information on related windows:

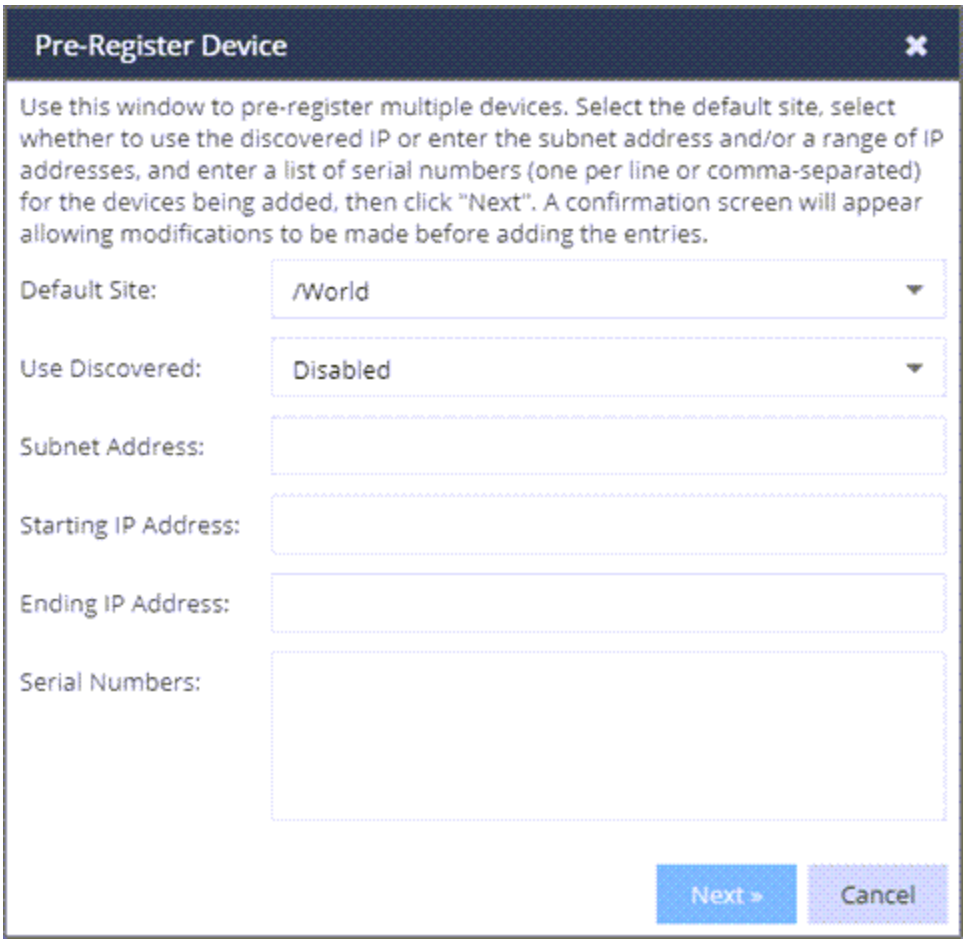
- Discovered

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

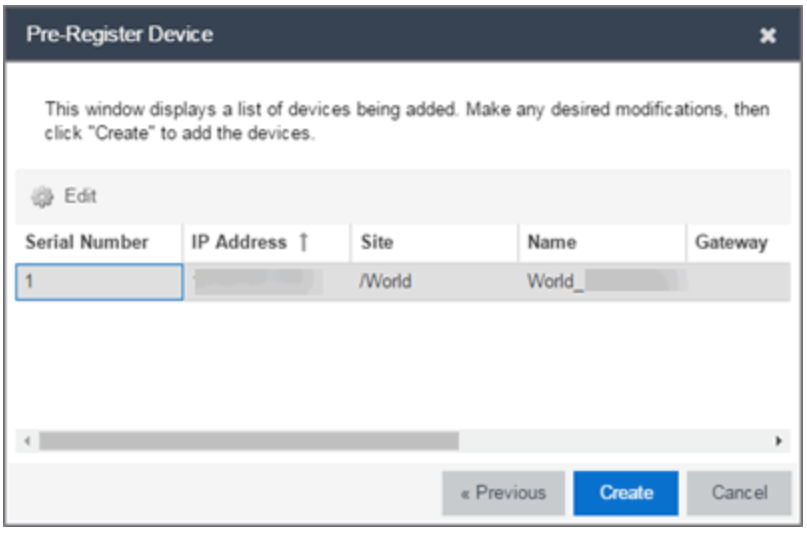
Select the **Next** button to open a confirmation window allowing you to verify the device information entered. Although it is recommended you enter device information in the site's **ZTP+ Device Defaults** window, you can also use this window to enter the Gateway, Domain Name, and DNS Server information 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.

Related Information

For information on related windows:

- Discovered

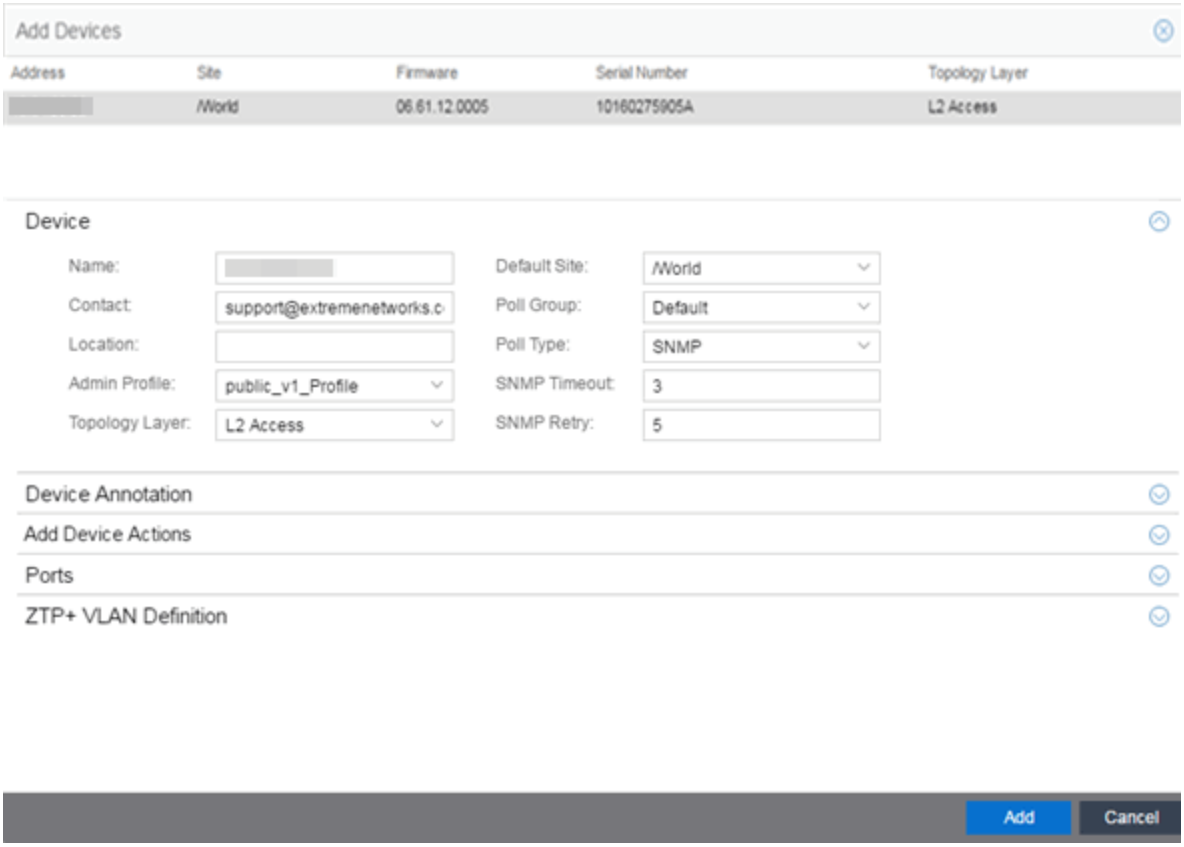
Add Devices

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 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.

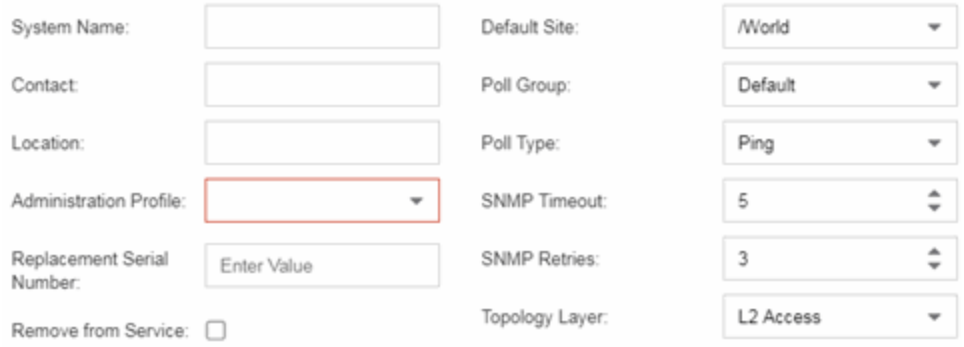
When you first open the window, only the Device section is expanded. Select a section heading to expand that section.

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 (SNMPv1or 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.

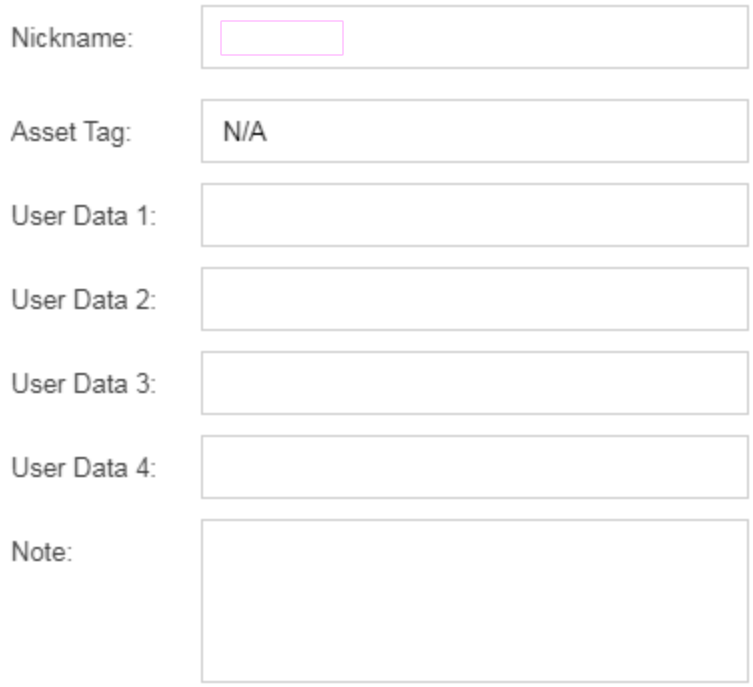
SNMP Retry

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 1and 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

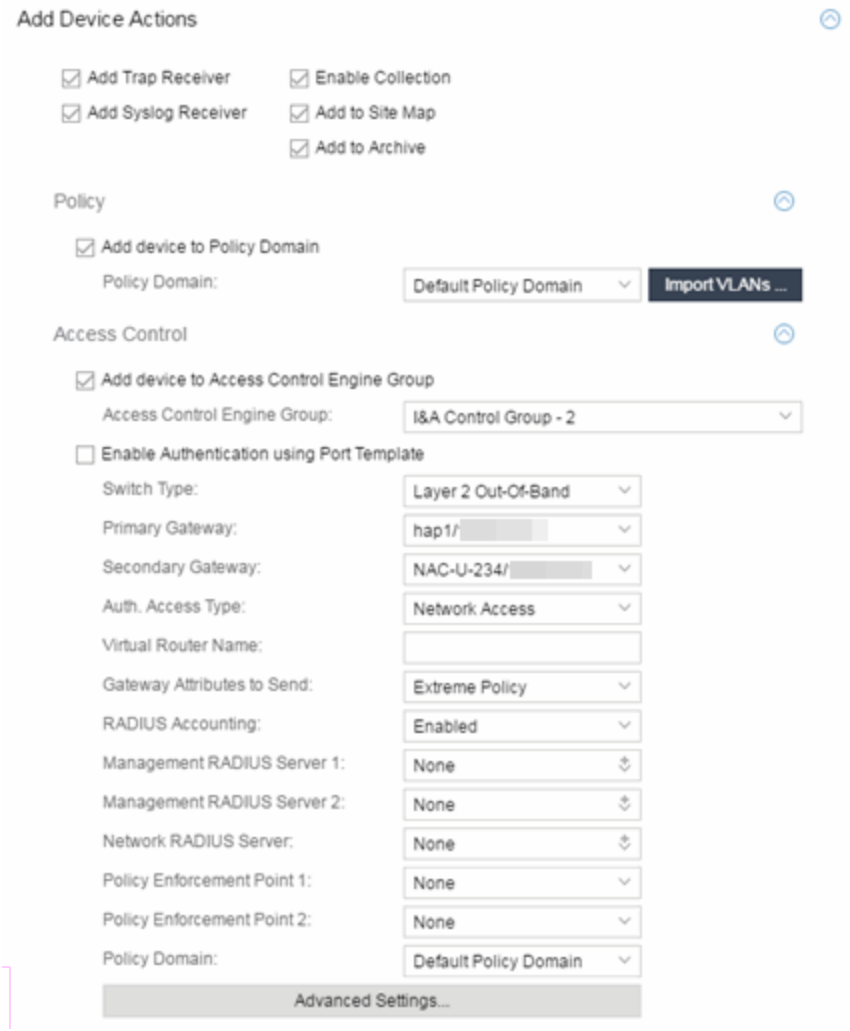
The user-defined information displayed in the devices table in the **User Data** columns.

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.

ExtremeControl

Add device to ExtremeControlEngine Group
Select this checkbox to add the device to an ExtremeControlEngine 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 ExtremeControl gateway.
- **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 ExtremeControl engine, ExtremeControl 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 Gateway

Use the drop-down list to select the primary ExtremeControl Gateway 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 gateways at Enforce, and this field displays **Determined by Load Balancer**.

Secondary Gateway

Use the drop-down list to select the secondary ExtremeControl Gateway 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 gateways at Enforce, and this field displays **Determined by Load Balancer**.

NOTE: To configure additional redundant ExtremeControl Gateways per switch (up to four), use the Display Counts option in the Display Options panel (Administration > Options > ExtremeControl).

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: For ExtremeXOS devices only. ExtremeControl uses CLI access to perform configuration operations on ExtremeXOS devices.

- 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 ExtremeControl 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 ExtremeControl 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 ExtremeControl 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 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.

Gateway RADIUS Attributes to Send

Use the drop-down list to select the RADIUS attributes included as part of the RADIUS response from the ExtremeControl 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 ExtremeControlengine, providing real-time connection status in ExtremeCloud IQ - Site Engine.

Management RADIUS Server 1and 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 ExtremeControlengine. (This option is only available if a Secondary Gateway 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 1and 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 ExtremeControl is unable to apply policies to restrict end user access after the user is granted access.

Policy Domain

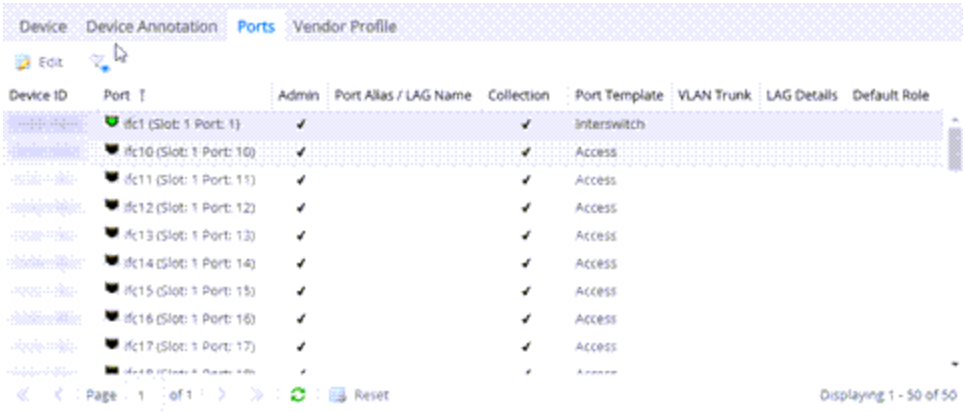
Use this option to assign the switch to a policy domain and enforce the domain configuration to the switch. The switch must be an Extreme Networks switch.

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 1and 4094 that identifies a particular VLAN. VID 1is 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 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.

Related Information

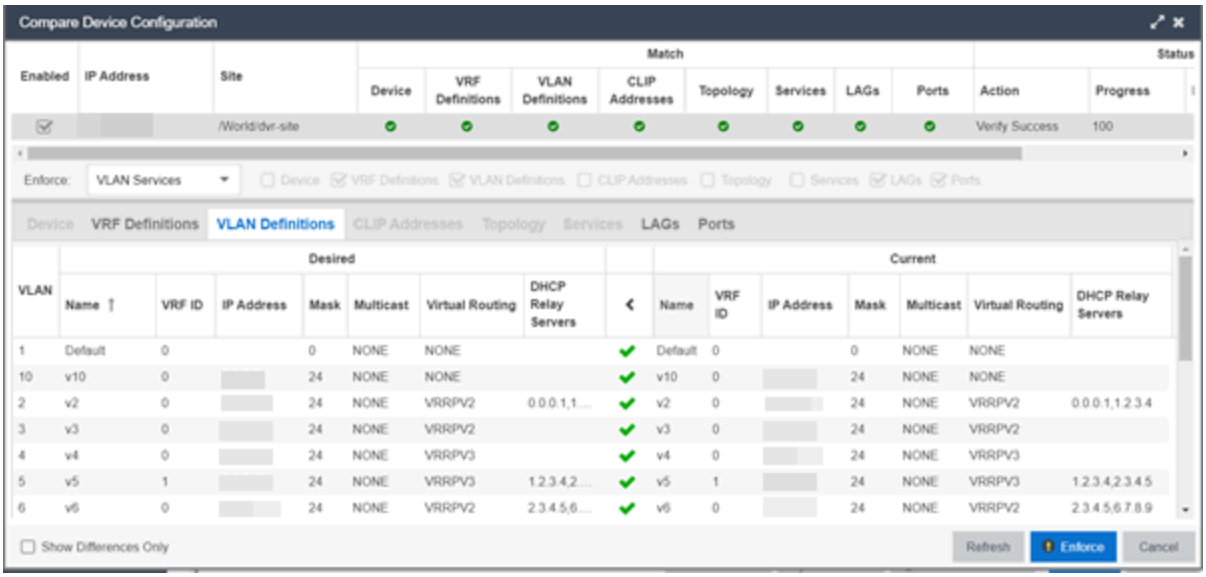
For information on related windows:

- Discovered

Compare Device Configuration

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

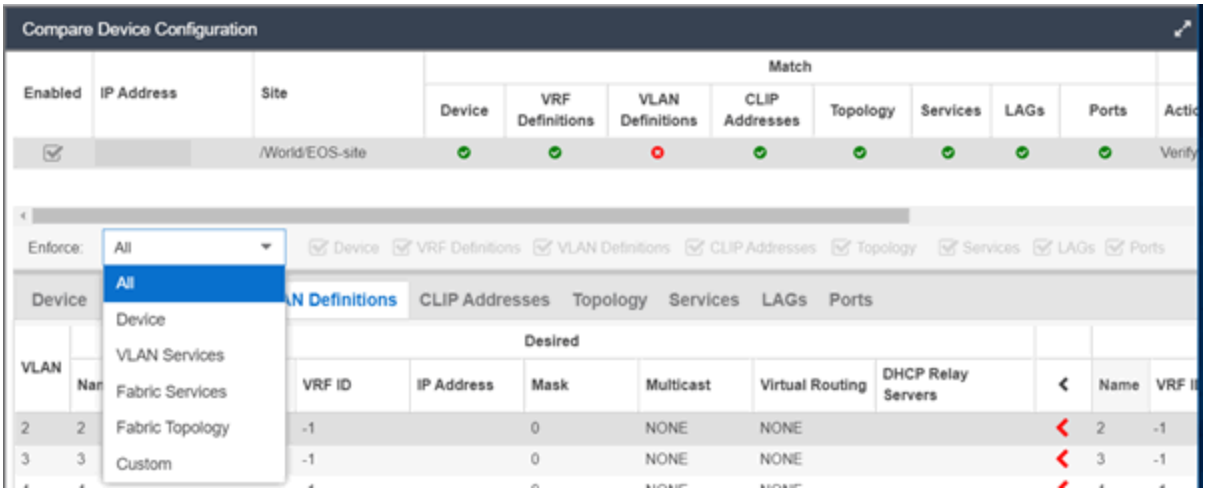
Devices on which the current configuration matches the desired configuration display a check icon (✔), while devices on which differences are detected display a red x (✖).

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.

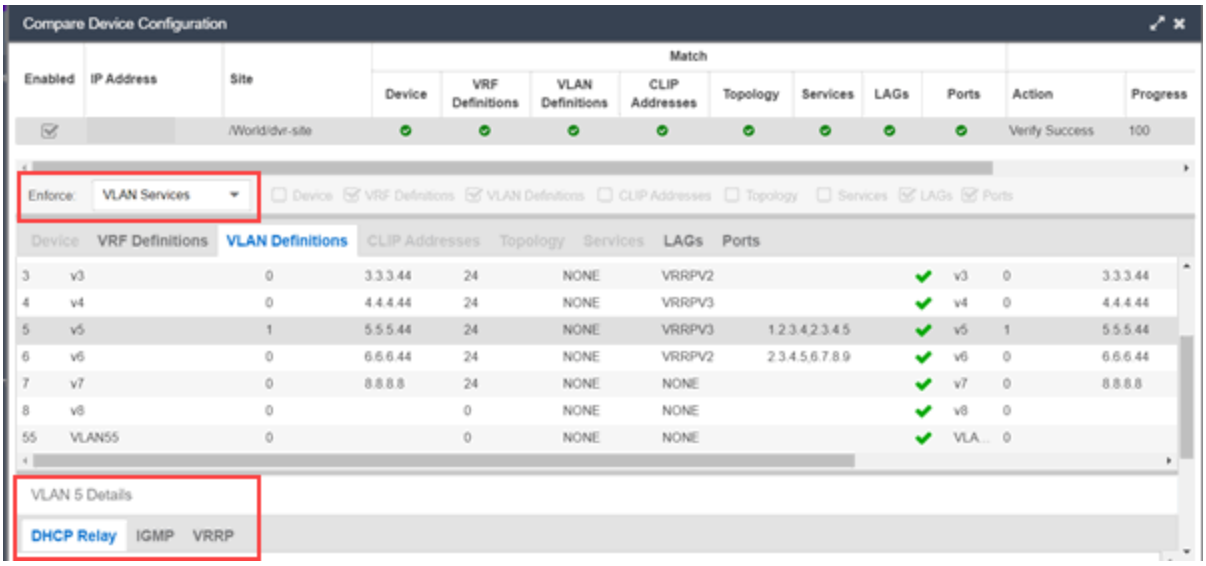
Device

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 Topology 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
- Topology Services

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
- Topology
- 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.

Mask
Displays the IP/ subnet mask.

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 1or 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 VOSS devices.

VOSS 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 VOSS 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

Topology

The **Topology** 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.

System ID

The system-defined fabric service identifier assigned to the device. The default is the MAC address for the device.

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.

Primary BVLAN

The Primary Backbone VLAN. This information is configured on the **Sites > Topology Definition** tab.

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.

System Name

The system name of the device.

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.

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.

SPBM Nickname
A value that other fabric devices use to identify the device. The SPBM nickname must be unique within the 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
Displays the identifying number for the DvR domain.

Fabric Attach
The check box is selected if Fabric Attach functionality is supported.

IP Shortcuts
The check box is selected if IPv4 Shortcuts are enabled for the device.

Multicast
The check box is selected if Multicast is enabled for the device.

IPv6 Shortcuts
The check box is selected if IPv6 Shortcuts are enabled for the device.

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

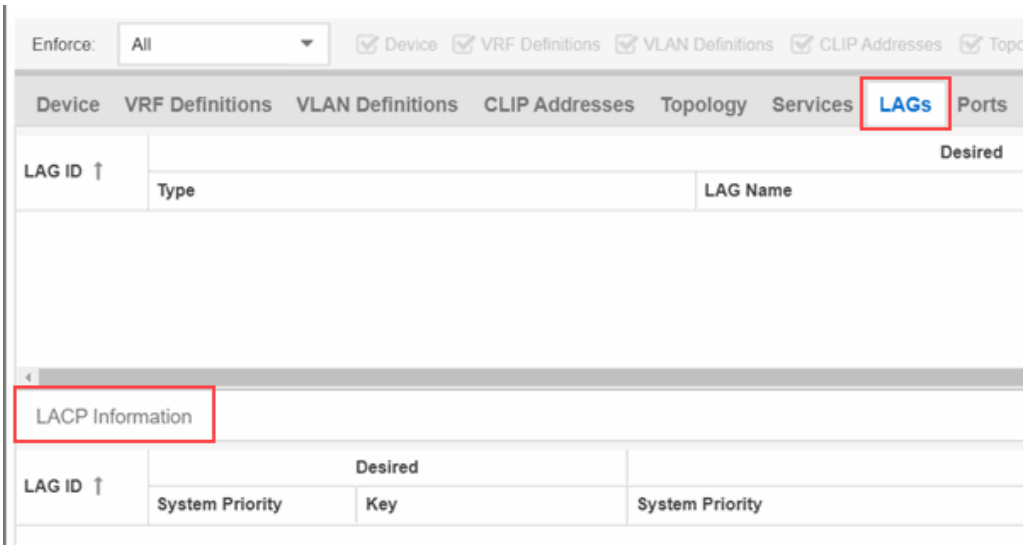
Displays the ports that are included in the LAG.

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 1and 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 1through 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 devices and provision them as FA Proxy devices. Select "Fabric Attach" or "" from the drop-down list to enable the port on a VOSS device (acting as FA Server) to connect to an ExtremeXOS device (acting as FA Proxy).

- **Fabric Attach** - Enable Fabric Attach server functionality on the port of a VOSS device acting as a Fabric Attach server) to connect to an ExtremeXOS device (acting as a Fabric Attach proxy).
- **Fabric Attach and Switched UNI** - Enable Fabric Attach server functionality on the port of a VOSS device acting as a Fabric Attach server) to connect to an ExtremeXOS 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 VOSS 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

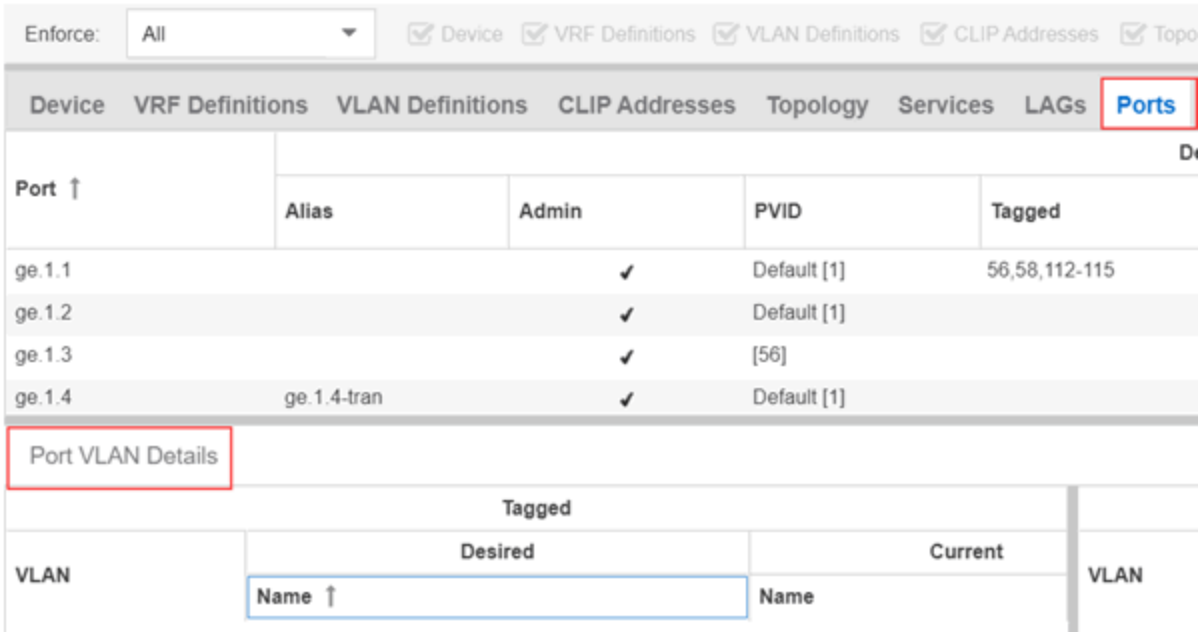
Indicates whether SLPP Guard is enabled on the port. Use SLPP Guard to provide additional loop protection to protect wiring closets from erroneous connections. SLPP Guard requires **SLPP** to be enabled. SLPP detects loops in an SMLT network. Because SMLT networks disable Spanning Tree (STP), Rapid Spanning 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 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.

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.

Related Information

For information on related topics:

- VLAN Concepts
- Configure Device
- Site Tab

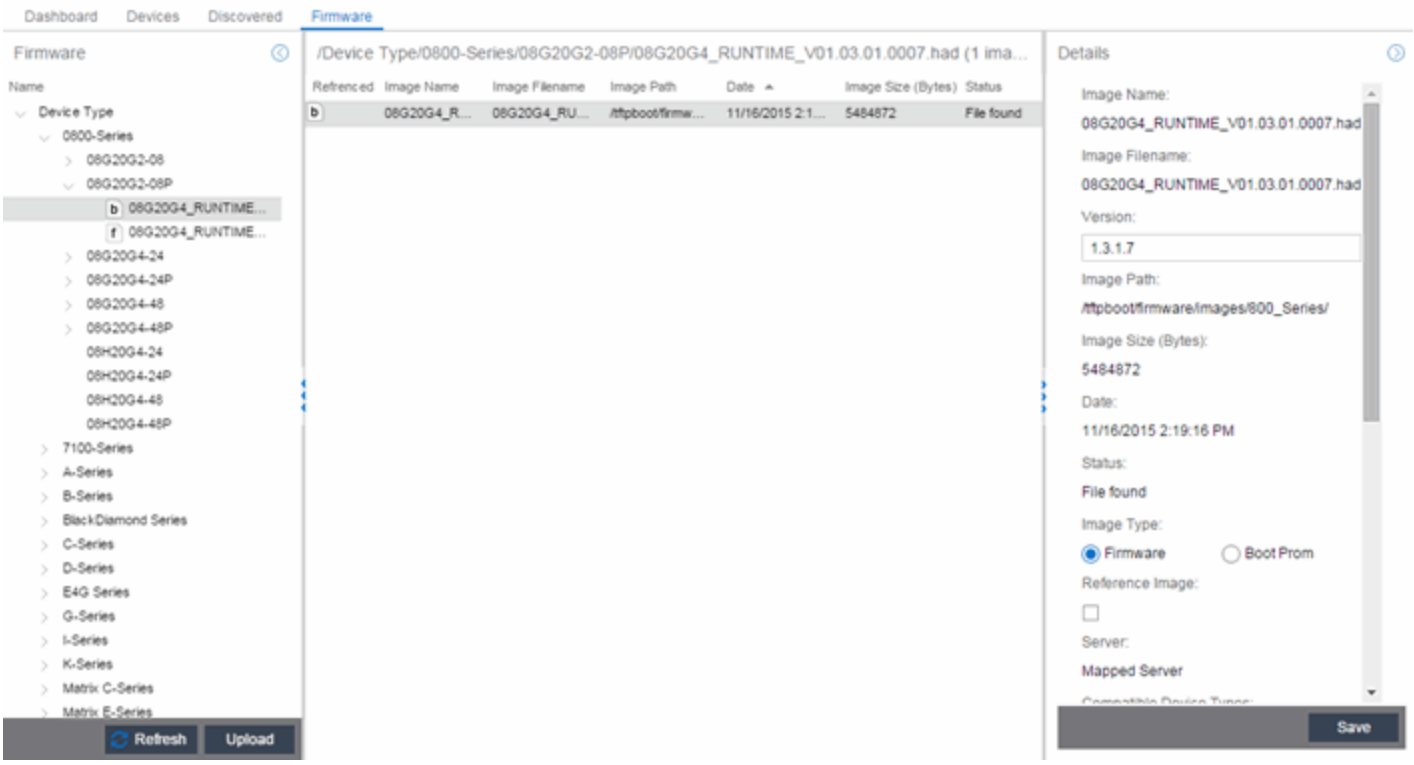
Firmware

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

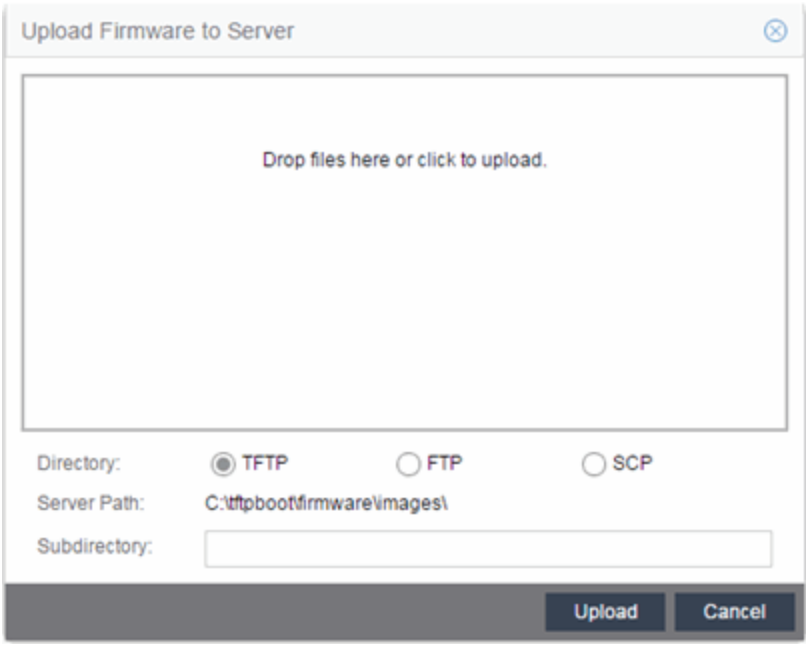
The **Firmware** tree in the left panel displays firmware and boot PROM images grouped according to product family and device type. It provides pre-defined firmware groups and automatically organizes the images stored in your firmware directory under the appropriate group when you perform a firmware 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.



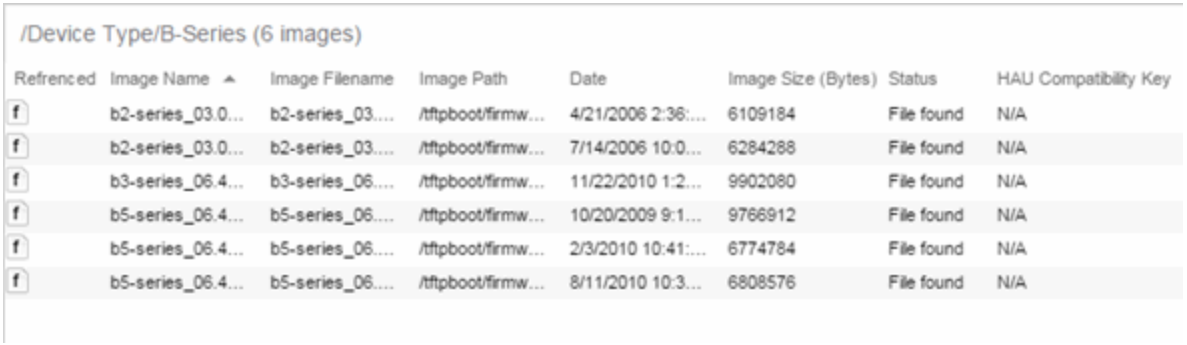
For additional information on how to upload a firmware or boot PROM image, see How to Upgrade Firmware.

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

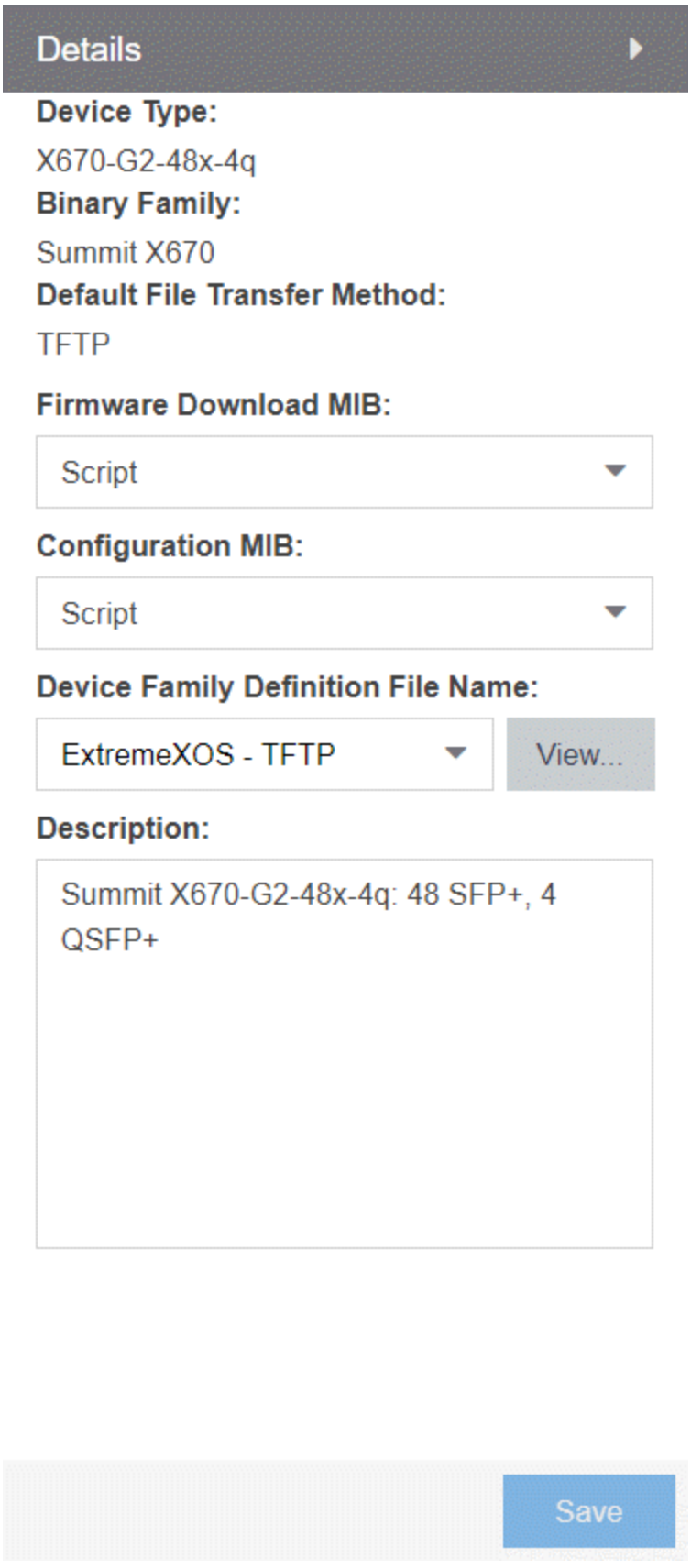
NOTE: Firmware images that were discovered with a NetSight version prior to 4.4 need to be removed from ExtremeCloud IQ - Site Engine (right-click the image on the **Firmware** tab and select **Delete Image**) and then rediscovered in order to populate the compatibility key field.

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.

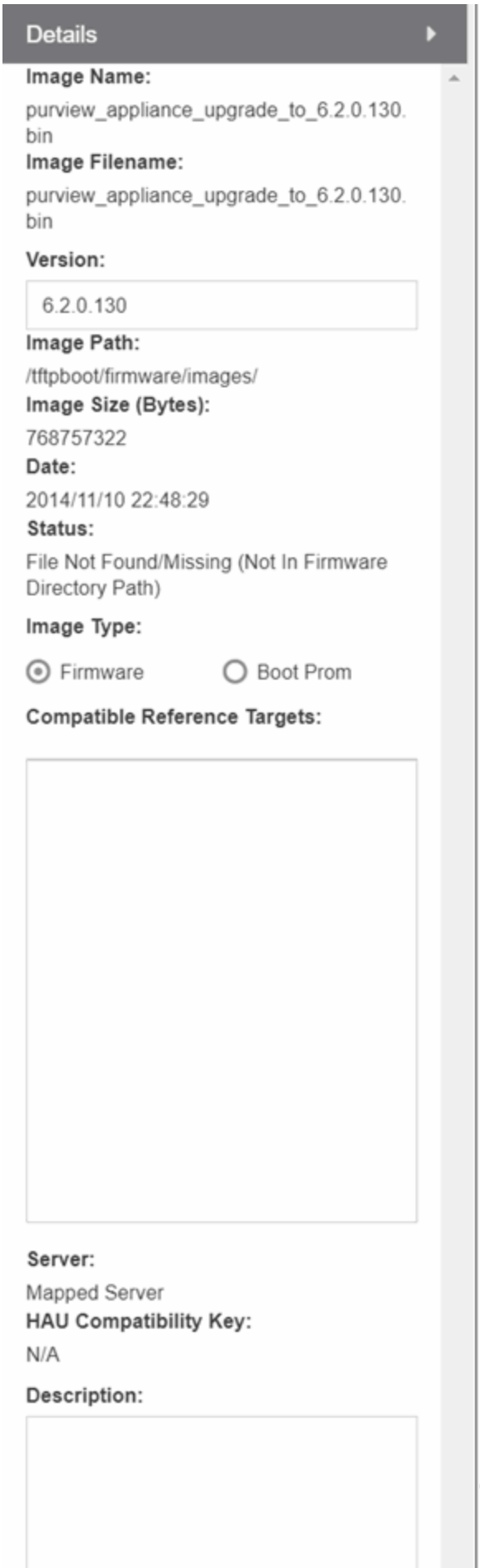

Details
Image Name:
purview_appliance_upgrade_to_6.2.0.130.bin
Image Filename:
purview_appliance_upgrade_to_6.2.0.130.bin
Version:
6.2.0.130
Image Path:
/tftpboot/firmware/images/
Image Size (Bytes):
768757322
Date:
2014/11/10 22:48:29
Status:
File Not Found/Missing (Not In Firmware Directory Path)
Image Type:
Firmware
Boot Prom
Compatible Reference Targets:
Server:
Mapped Server
HAU Compatibility Key:
N/A
Description:

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.

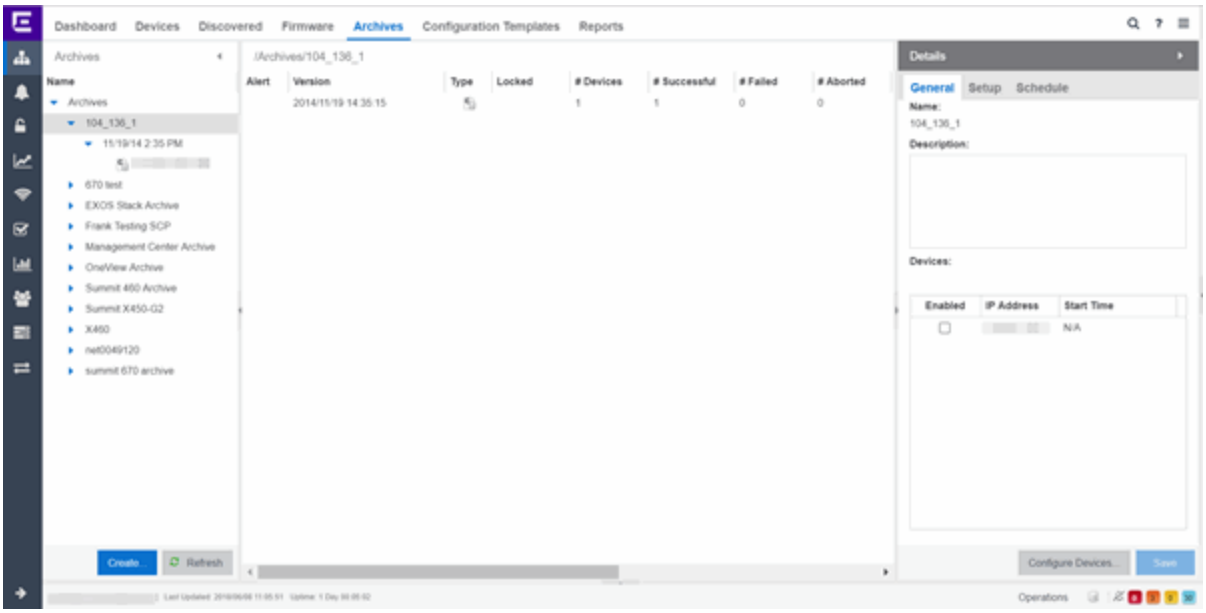
Related Information

For information on related windows:

- Network
- Devices
- How to Upgrade Firmware

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.

Related Information

For information on related tabs:

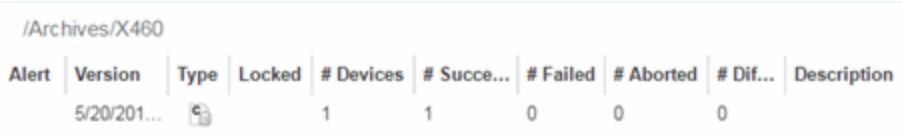
- Archive Name Panel
- Archive Version Panel
- Archive File Panel

For information on related tasks:

- How to Archive
- How to Restore an Archive
- How to Compare Archives

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.

Related Information

For information on related tabs:

- Archive Name right-panel
- Archive Version right-panel

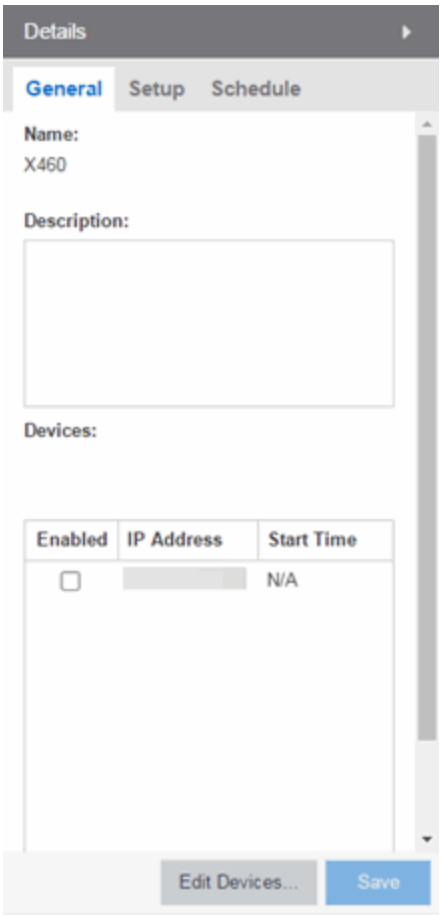
For information on related tasks:

- How to Archive
- How to Restore an Archive

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**.

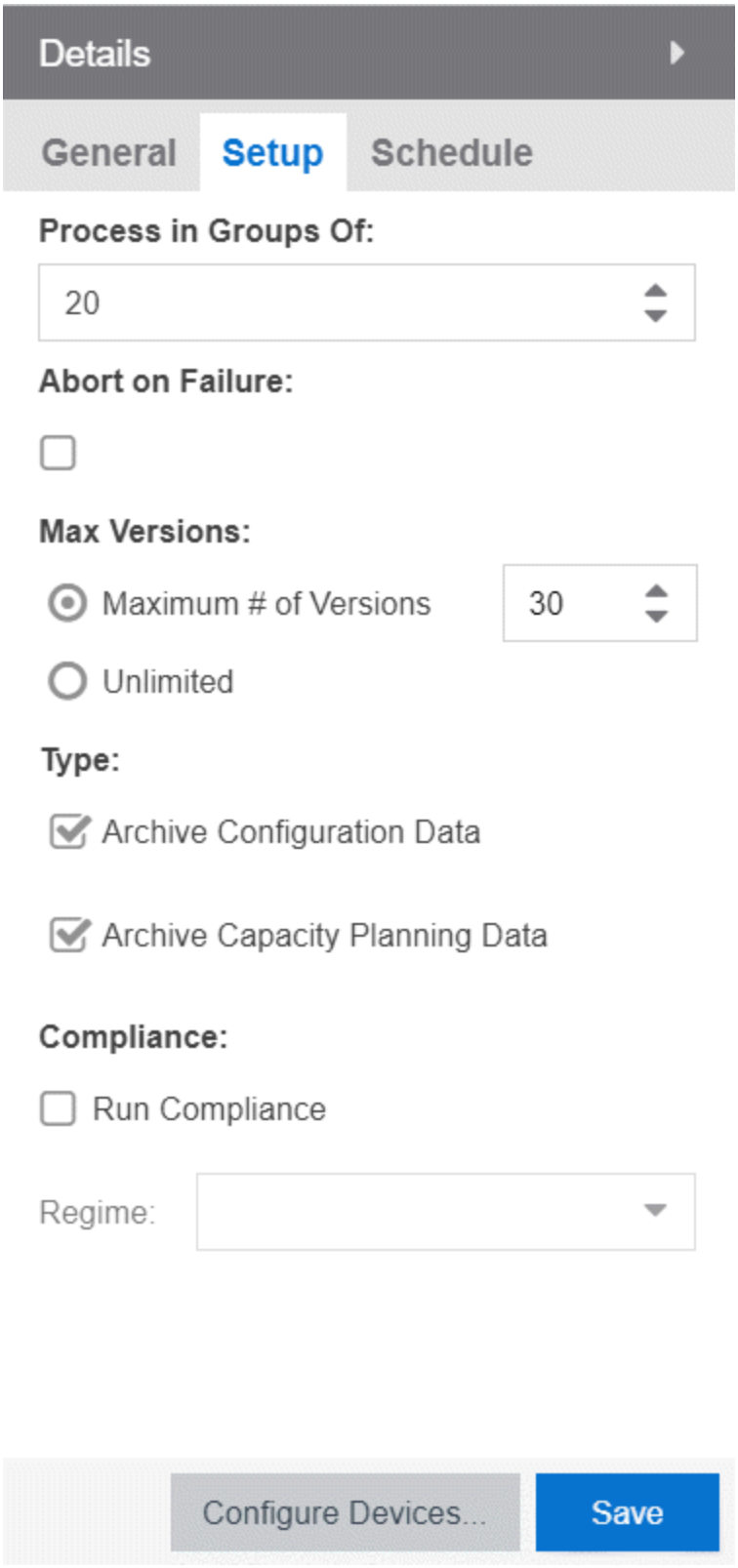
Description

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.

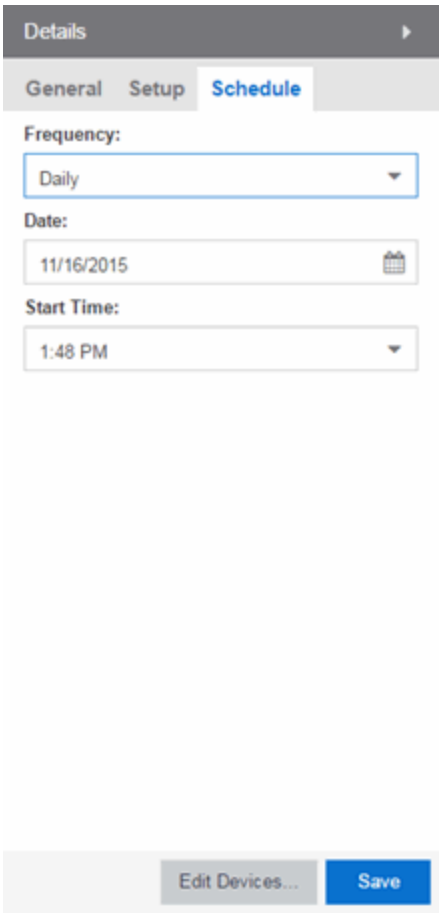
Save

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.)

Related Information

For information on related tabs:

- Archive Name Main Panel

For information on related tasks:

- How to Archive
- How to Restore an Archive

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 checkmark 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.

Related Information

For information on related tabs:

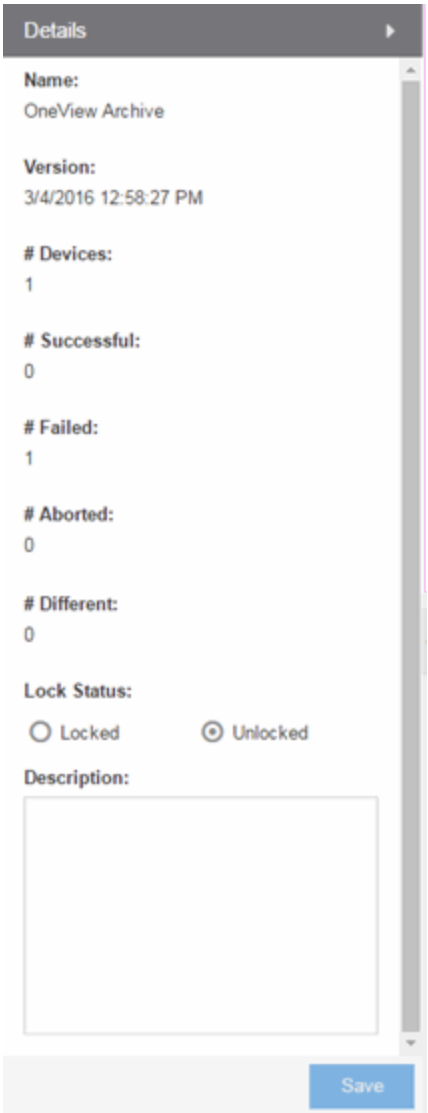
- Archive Version Right-Panel
- Archive File Right-Panel

For information on related tasks:

- How to Archive
- How to Restore an Archive

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.

Related Information

For information on related tabs:

- Archive Name Panel

For information on related tasks:

- How to Archive
- How to Restore an Archive

Archive File

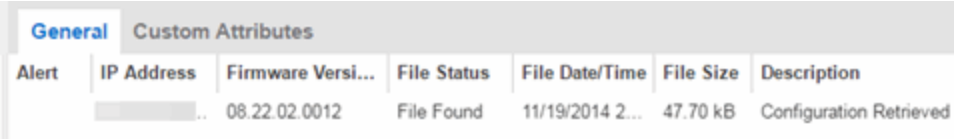
The Archive File panel appears when you select an archive configuration file in the left-panel of the **Archives** tab. It contains information about specific archive configurations.

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 checkmark 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.

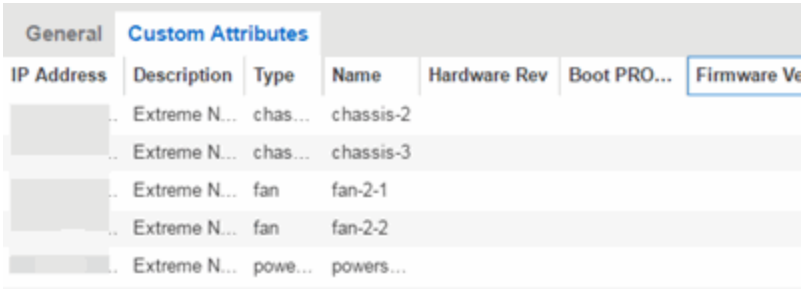
Description

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.

Related Information

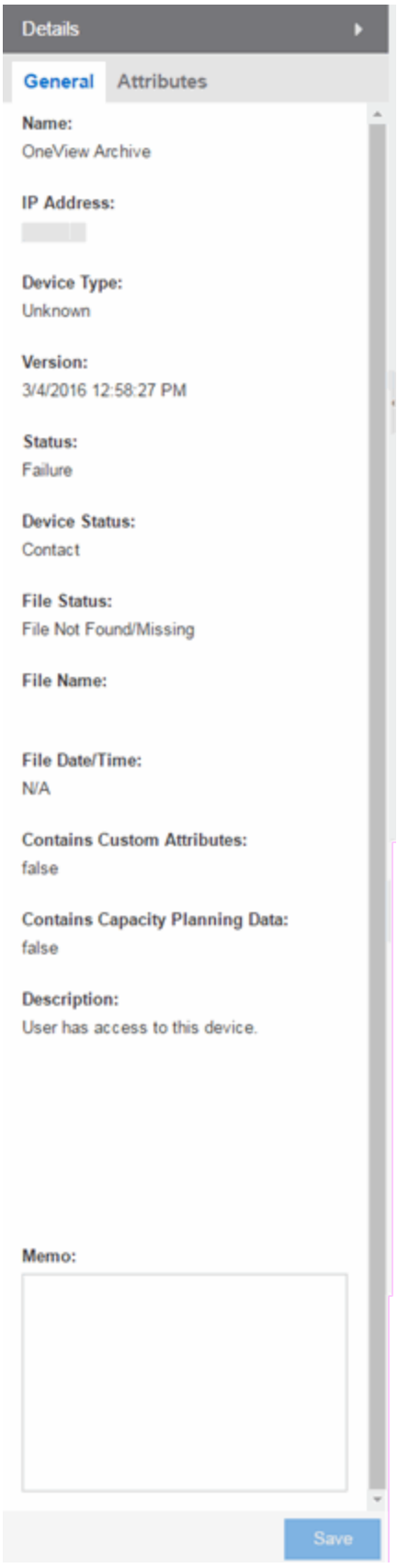
For information on related windows:

- Archive File Right-Panel

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.

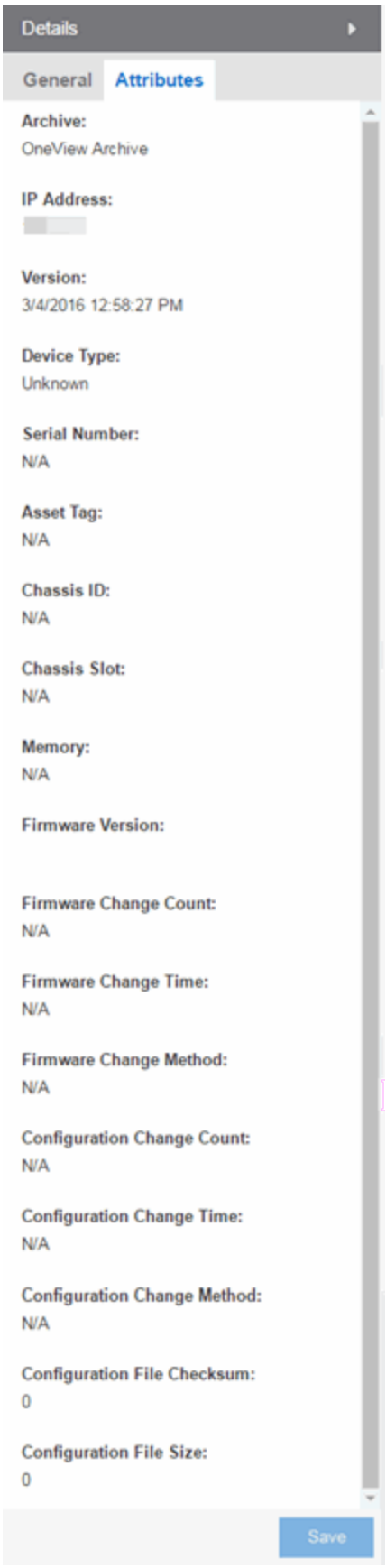
Description

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.

Related Information

For information on related tabs:

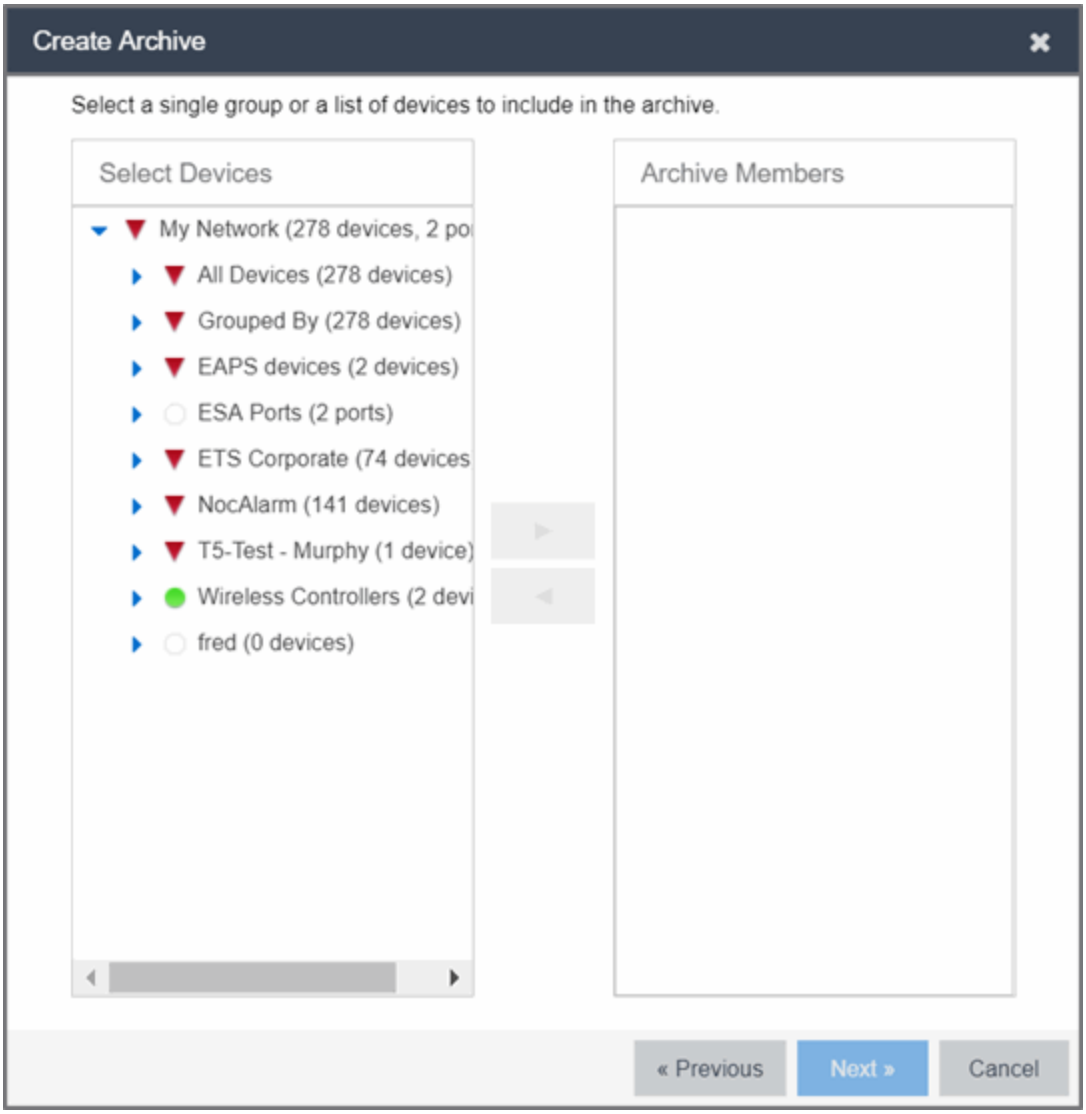
- Archive File Panel

For information on related tasks:

- How to Archive
- How to Restore an Archive

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.

Related Information

For information on related tabs:

- Archive Name Right-Panel

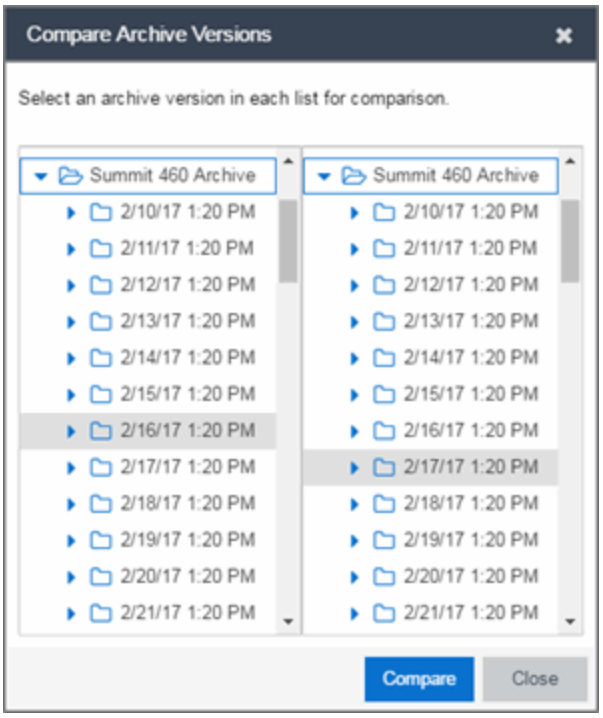
For information on related tasks:

- How to Archive
- How to Compare Archives

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.

Related Information

For information on related windows:

- Compare Configuration Files Window
- Configuration File Viewer

For information on related tasks:

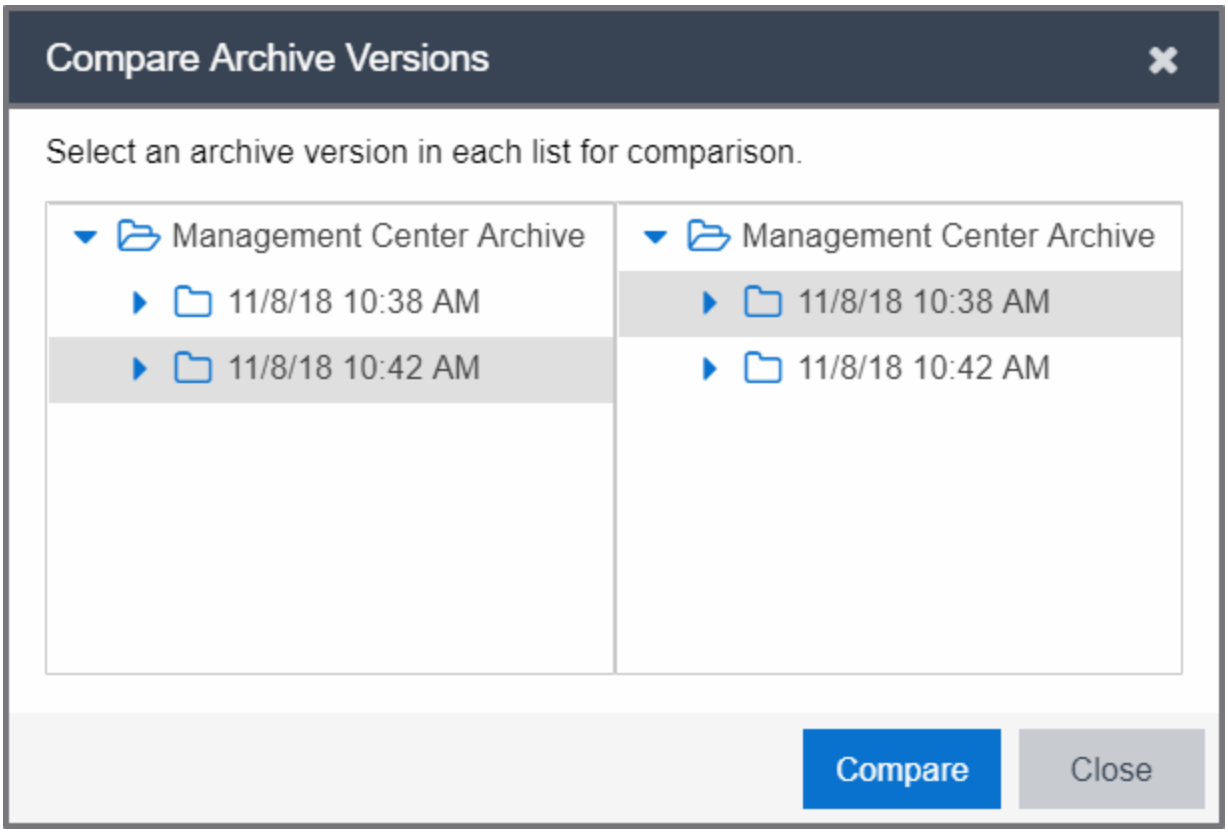
- How to Archive
- How to Compare Archives

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.

Related Information

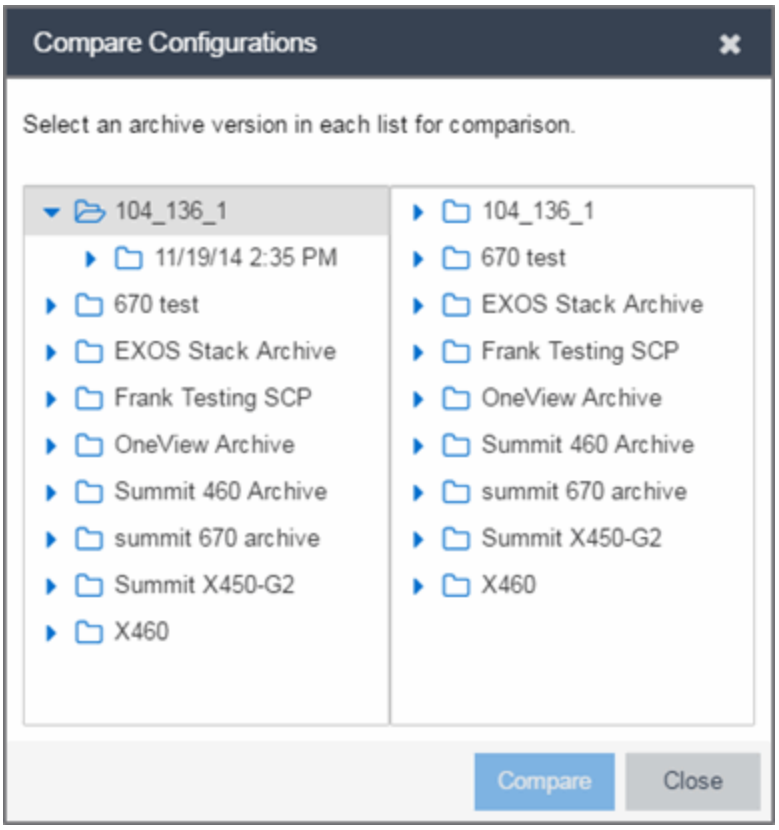
For information on related tasks:

- How to Archive
- How to Compare Archives
- How to Restore an Archive

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.

Related Information

For information on related windows:

- Configuration File Compare Window
- Configuration File Viewer

For information on related tasks:

- How to Archive
- How to Compare Archives

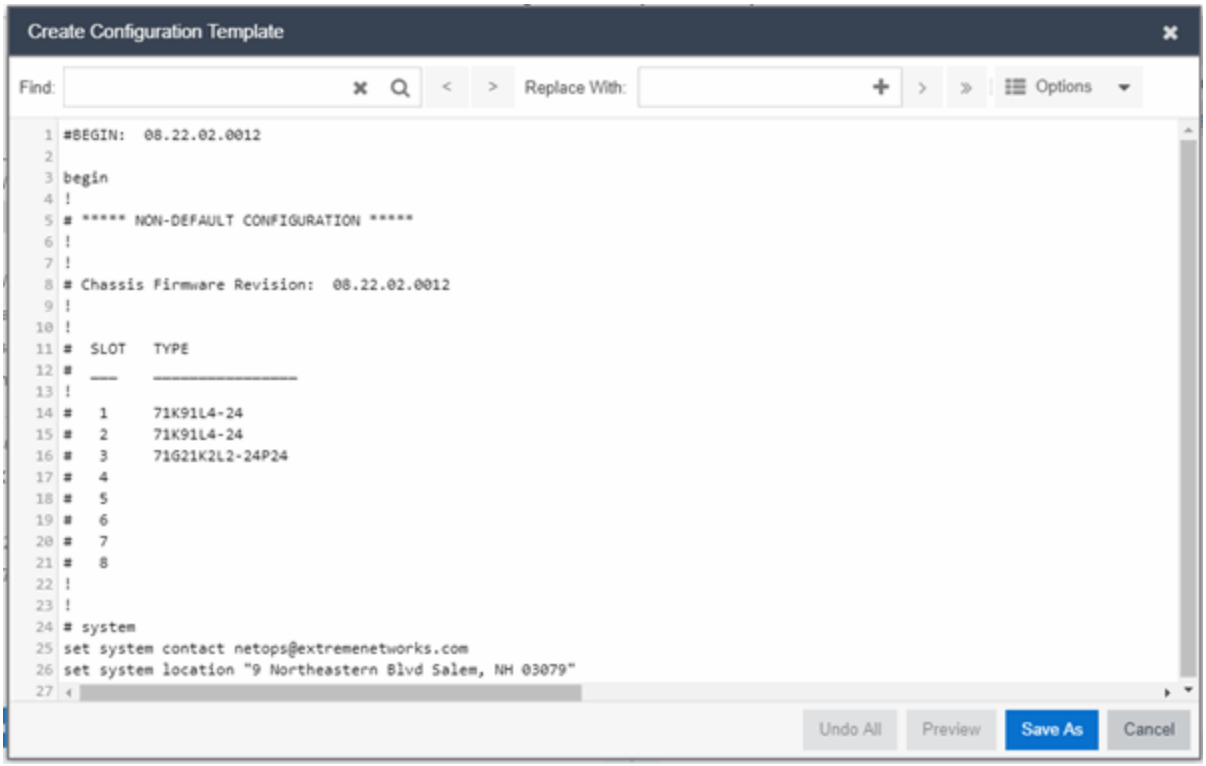
Creating a Configuration Template

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:

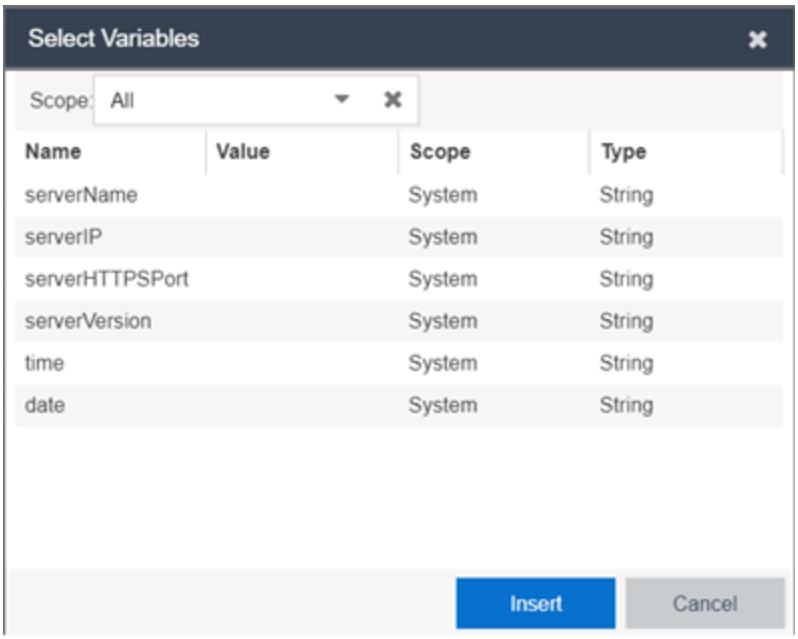
1. Access the **Archives** tab.
2. Right-click an archive file in either the left-panel Archives tree or the **General** tab table and select **Create Configuration Template**.

   The **Create Configuration Template** window opens.

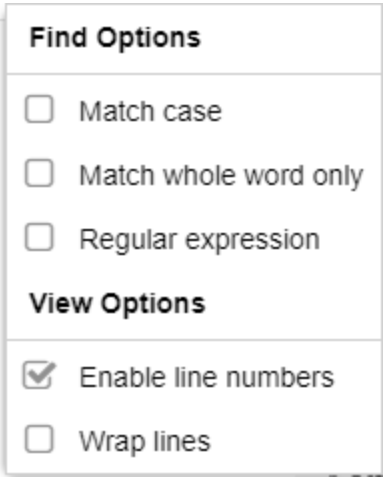


Archived device configuration file data displays in ASCII format or html format, depending on the device family to which the archived device is assigned.

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.

Related Information

For information on related tasks:

- How to Archive
- How to Compare Archives
- How to Create a Custom Variable

Configuration File Compare

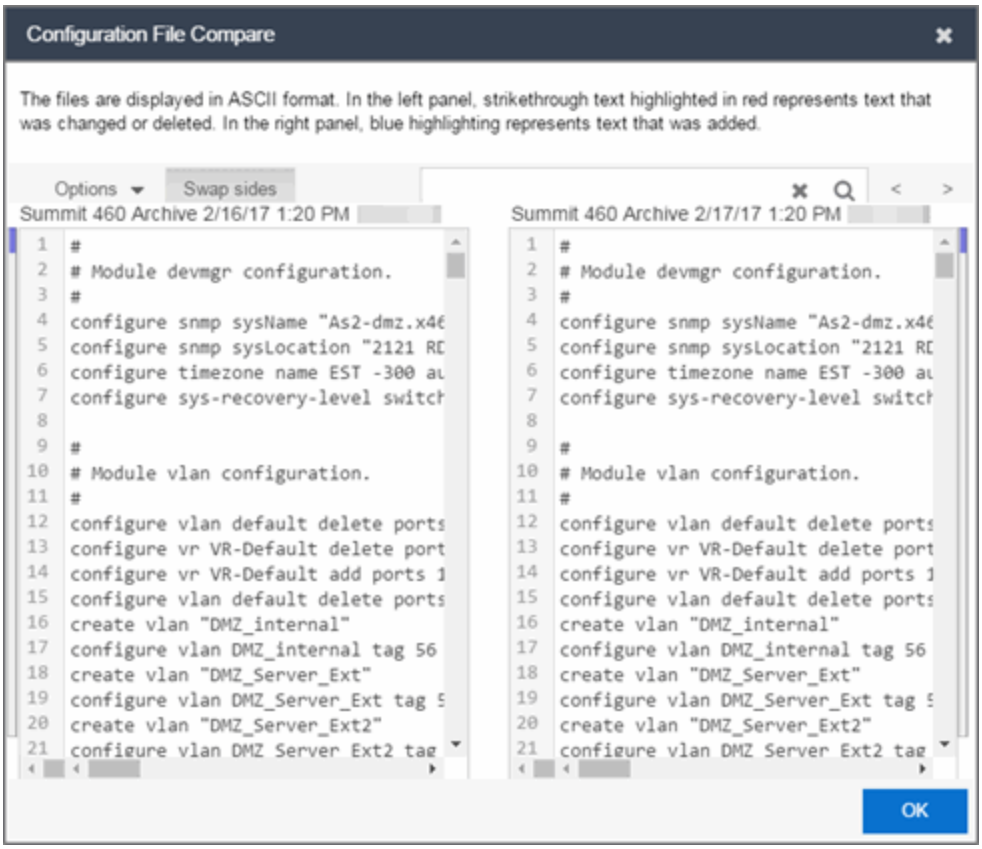
The Configuration File Compare window lets you compare two archived configuration files.

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.

Related Information

For information on related windows:

- Configuration File Viewer

For information on related tasks:

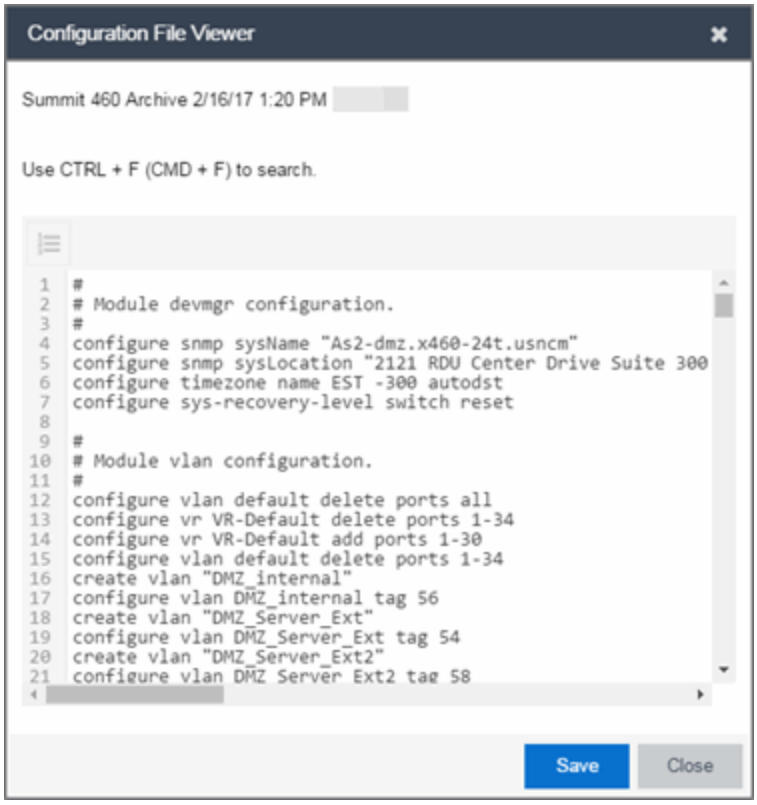
- How to Archive
- How to Compare Archives

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.

Related Information

For information on related windows:

- Configuration File Compare Window

For information on related tasks:

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.

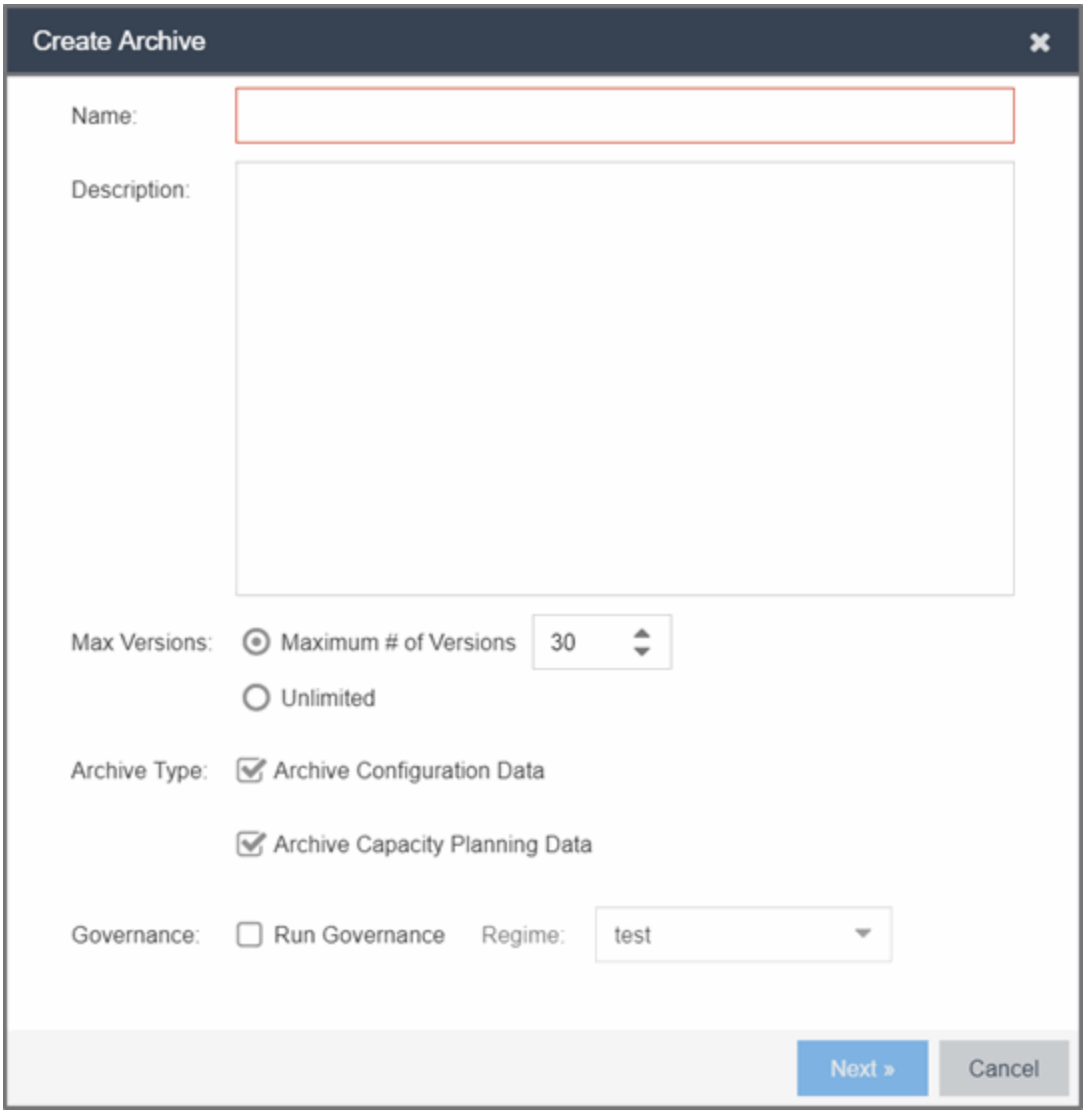
After an archive operation is created, it is listed by name in the left-panel Archives folder. Below the archive name are the archive versions, displayed by the date and time of the creation of the version. Under the versions are individual configurations, listed by the IP address of the device whose 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.

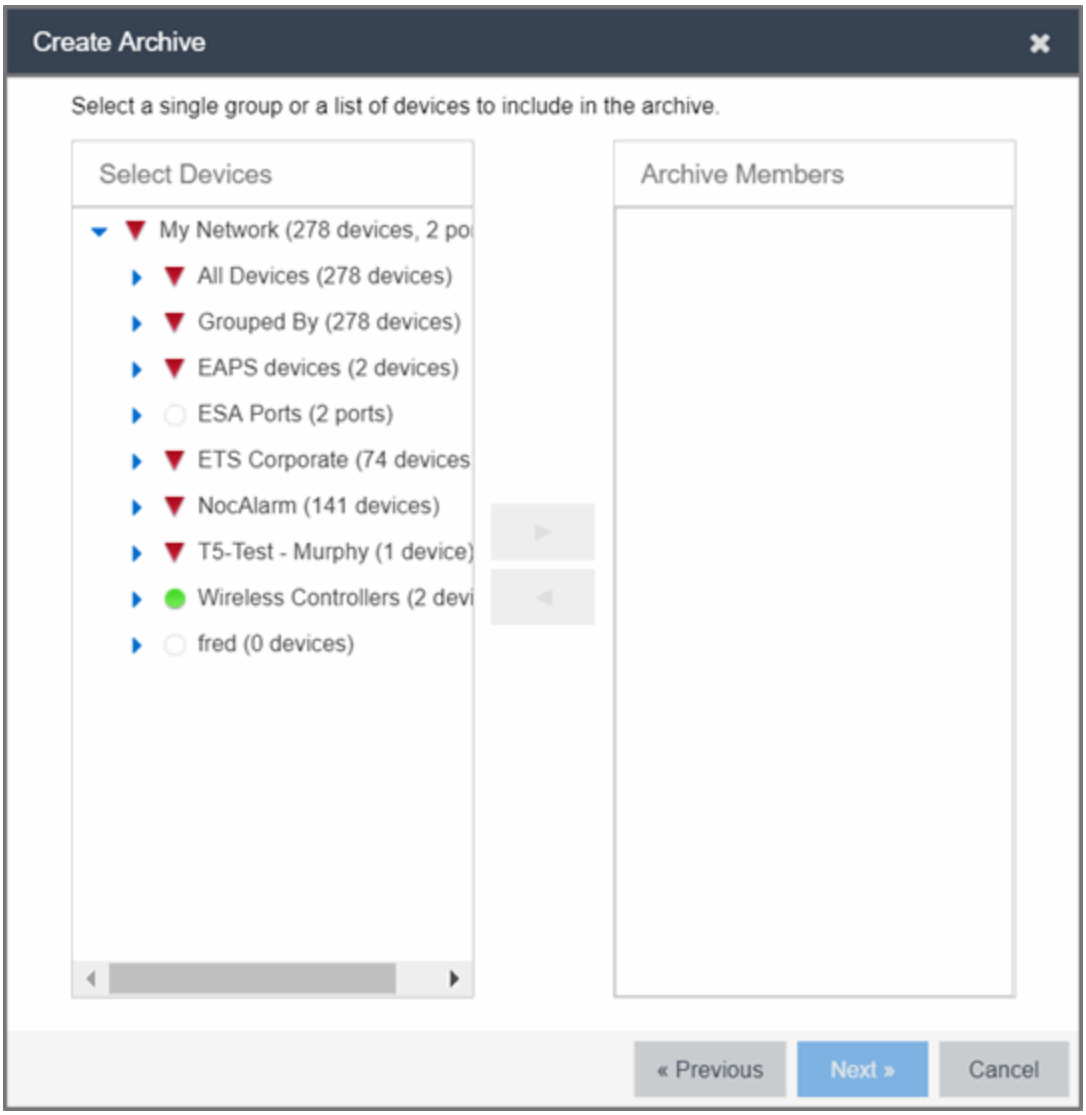
Run Compliance

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

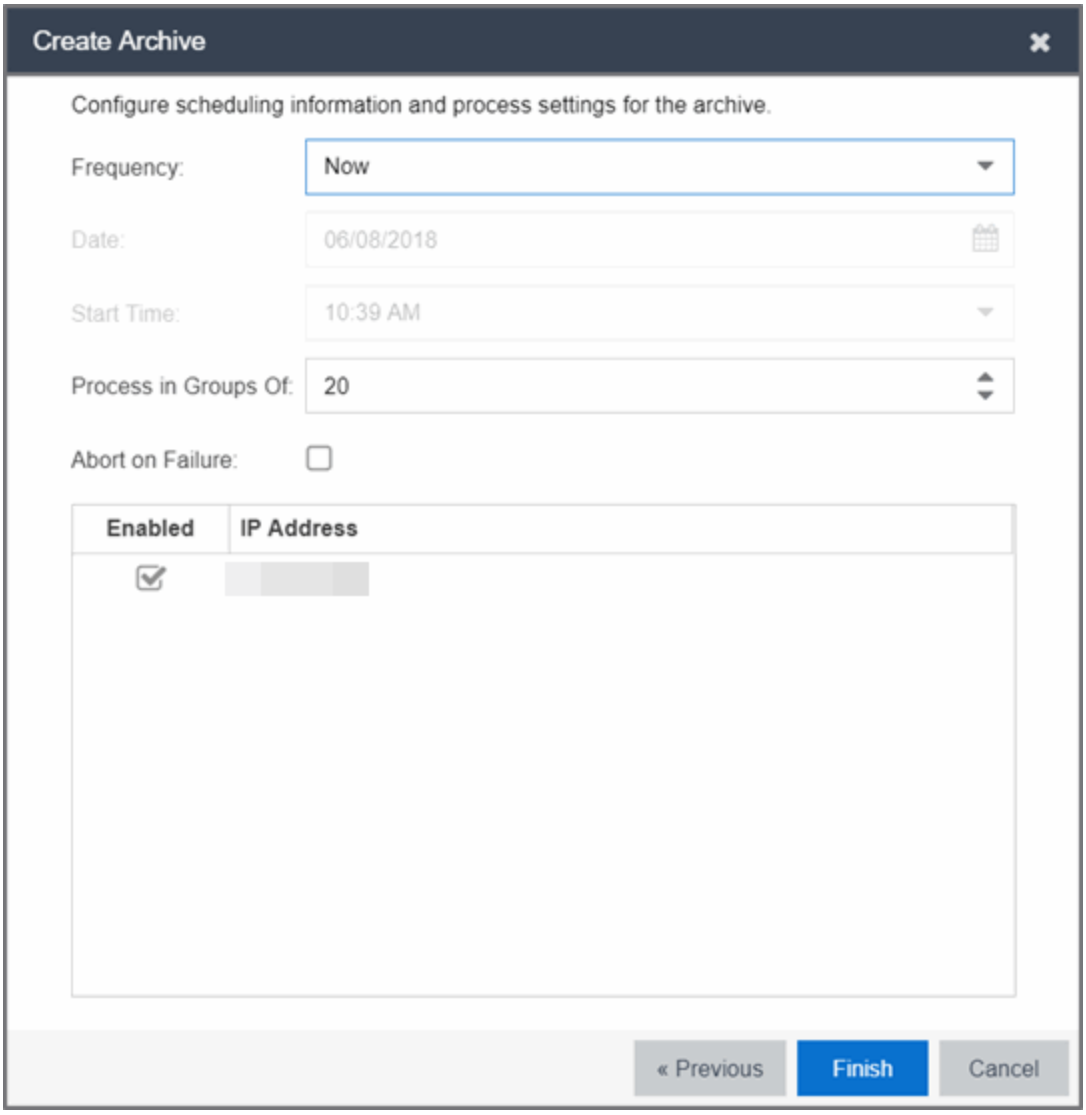
In the Devices tree, select the device(s) or device group you want to archive, and select **>** to add it to the Archive Members list.

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.

Related Information

For information on related tasks:

- How to Archive
- How to Restore an Archive
- How to Compare Archives

Restore Archive

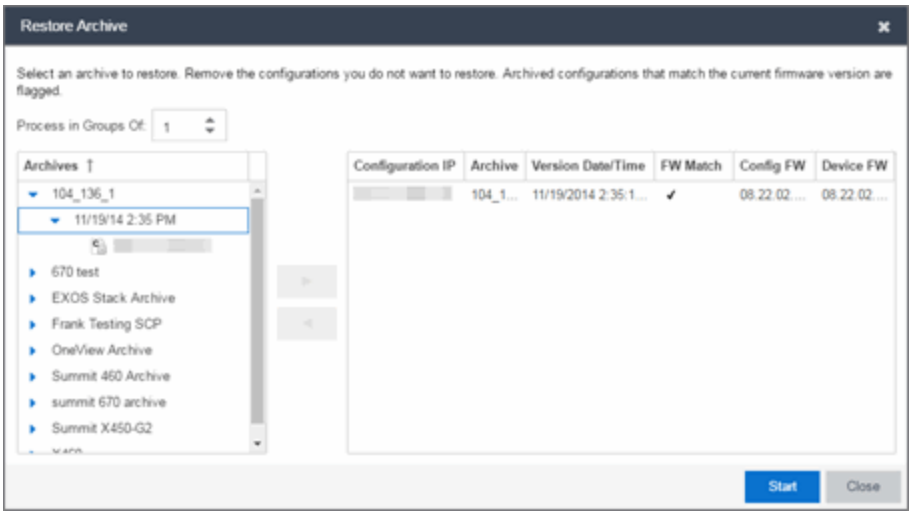
Use the **Restore Archive** window to restore saved (archived) device configuration files to one or more devices. Saved configurations are listed in the left-panel of the **Archive**s tab under the appropriate archive and version. Each configuration displays an icon that identifies the type of saved 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 1may 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.

Related Information

For information on related tasks:

- How to Archive
- How to Restore an Archive

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.

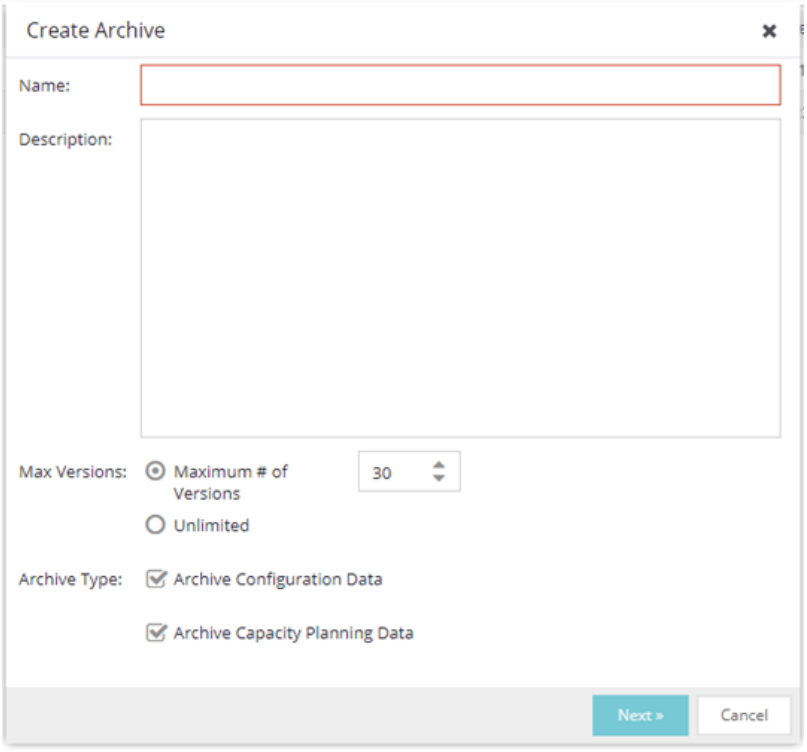
Instructions on:

- 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.

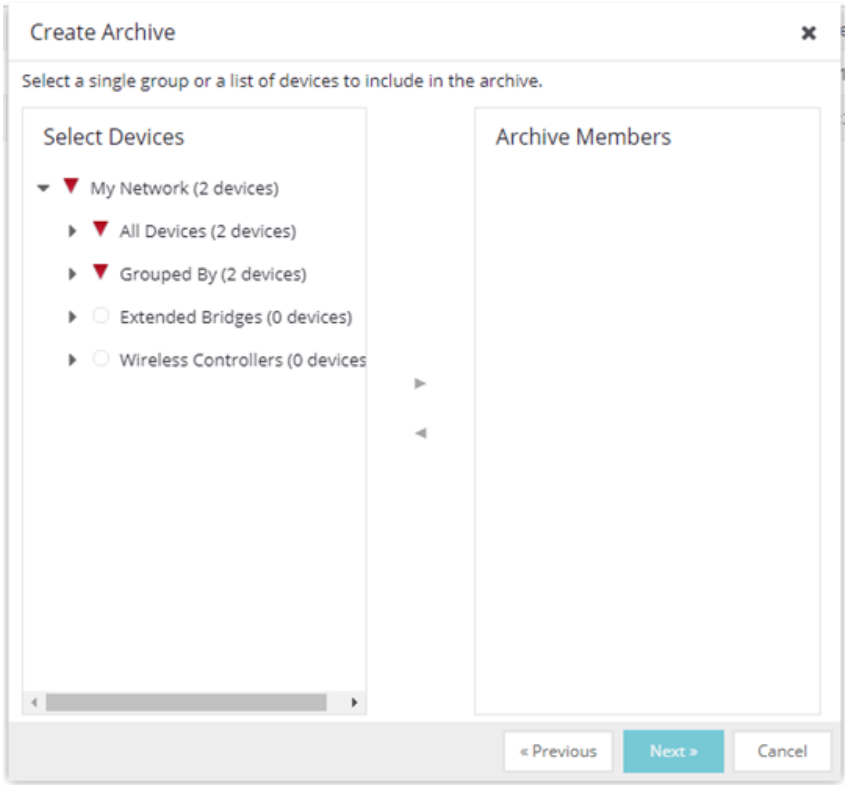
1 Select the **Create** button in the left-panel. The **Create Archive** window displays.



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.)

---

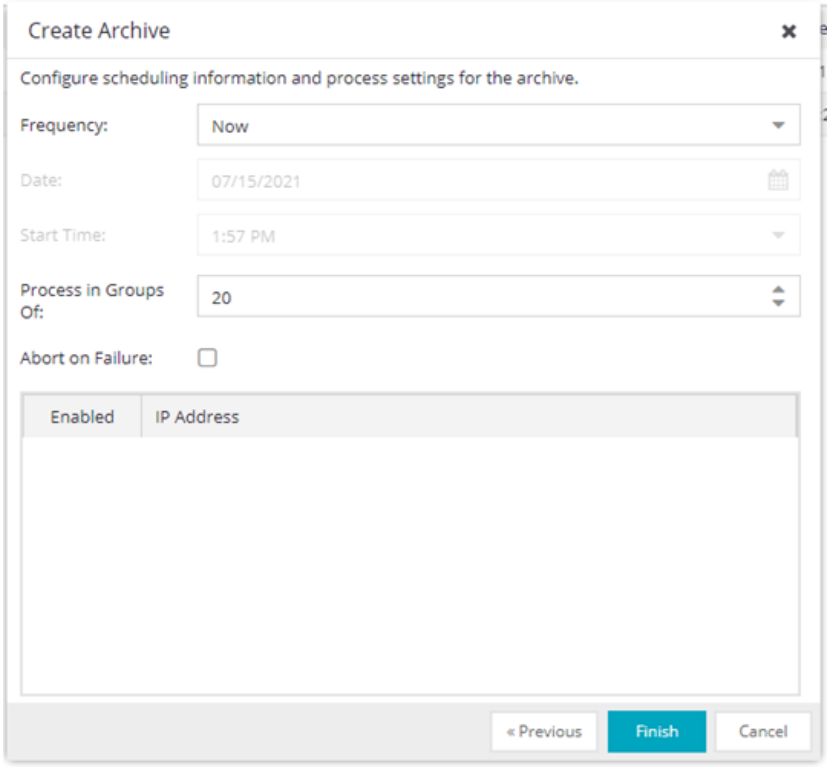
b. If you want to remove a member from the Archive Members list, select the

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.

Related Information

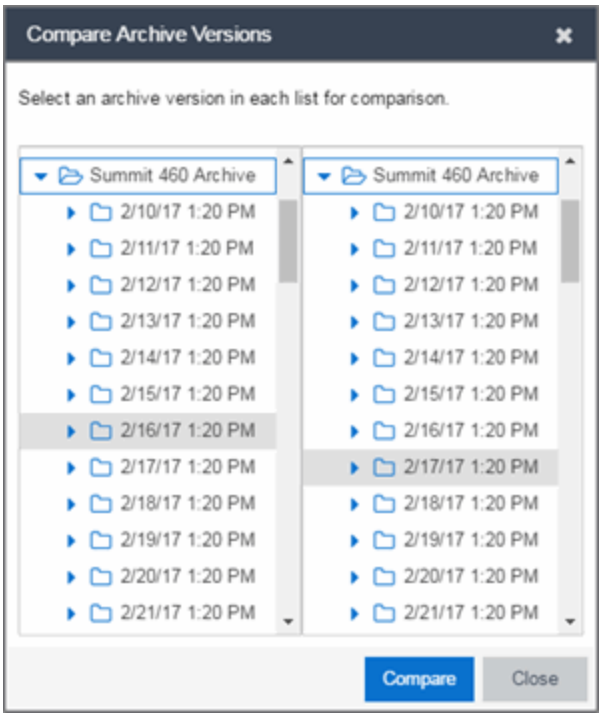
For information on related tasks:

- Create Archive
- How to Restore an Archive
- How to Compare Archives

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.

Related Information

For information on related tasks:

- How to Archive
- How to Restore an Archive

For information on related windows:

- Compare Archives Window

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 1may 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.

Related Information

For information on related tasks:

- Restore Archive
- How to Archive

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.

Related Information

For information on related windows:

- Network Tab
- Devices Tab
- Firmware Tab

Configuration Templates

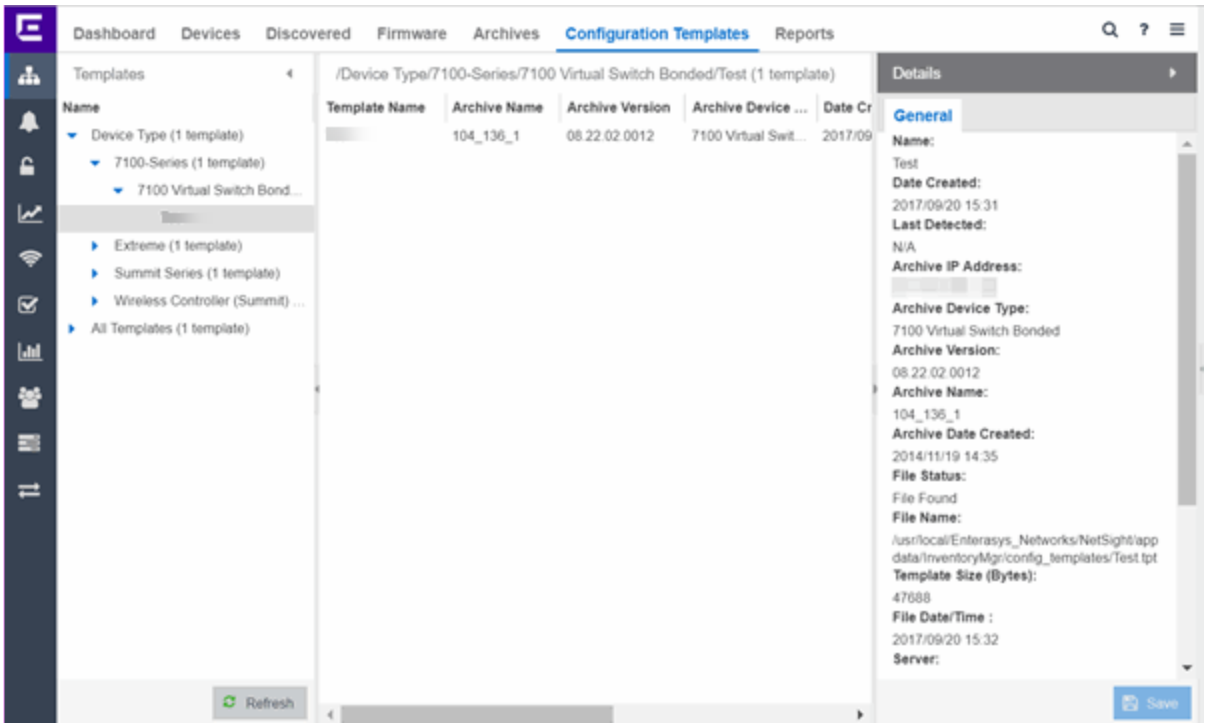
The **Configuration Templates** tab displays configuration templates you create, grouped according to product family and device type. ExtremeCloud IQ - Site Engine provides pre-defined template groups and automatically assigns a template to the appropriate group when you create the template. Each template 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.

Related Information

For information on related topics:

- Network
- Create Configuration Templates

Alarms & 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

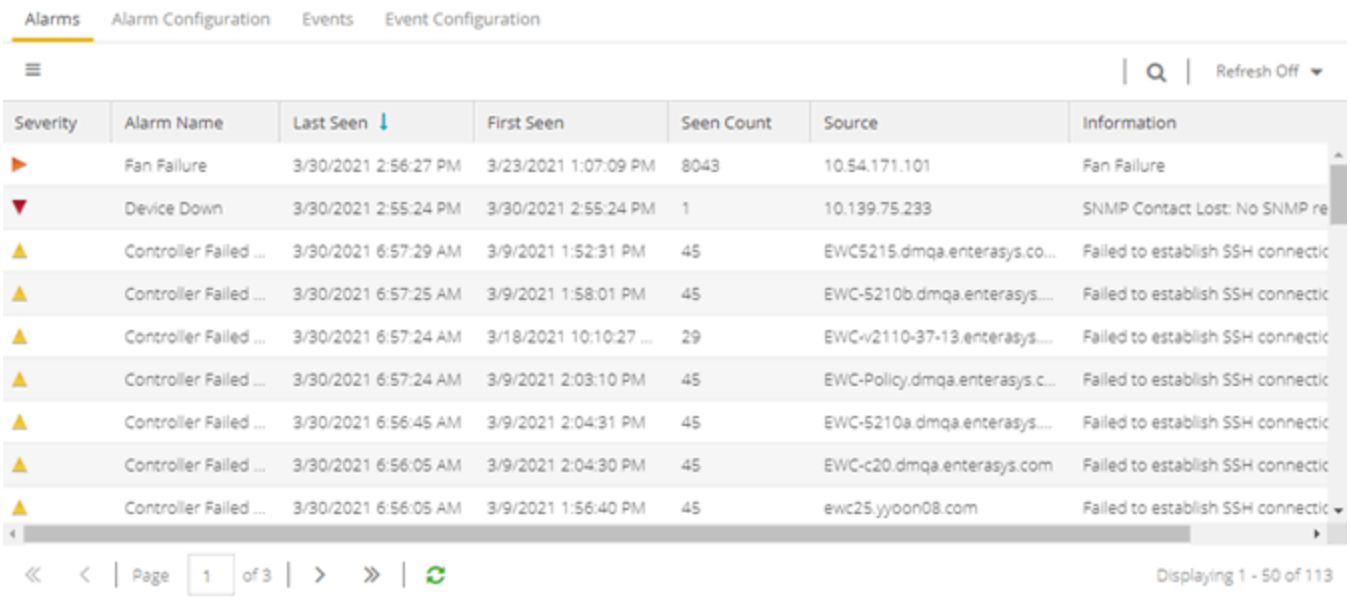
To view the information in the Alarms and Event logs, you must be a member of an authorization group assigned the appropriate ExtremeCloud IQ - Site Engine capabilities:

- NetSight OneView > Access OneView
- NetSight OneView > Events and Alarms > OneView Event Log Access
- NetSight OneView > Events and Alarms > OneView Alarms Read Access or Read/Write Access

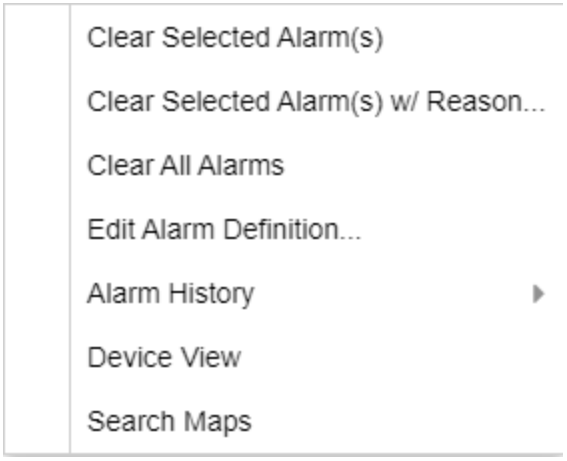
For additional information, see Users and ExtremeCloud IQ - Site Engine Access Requirements.

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:



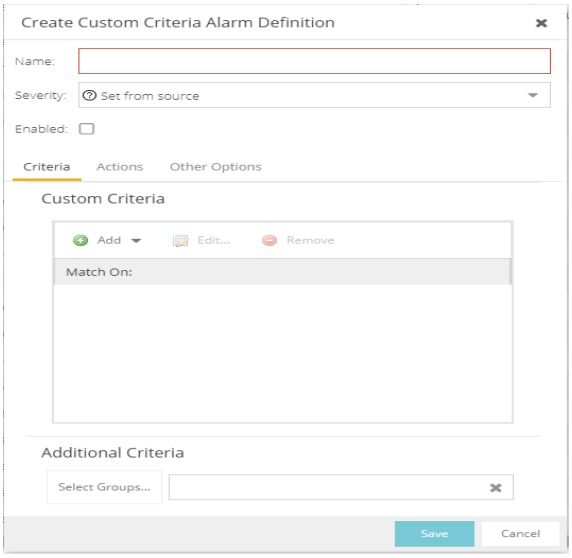
Clear Selected Alarm(s)
Select to clear the selected alarm from the Alarms table.

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:

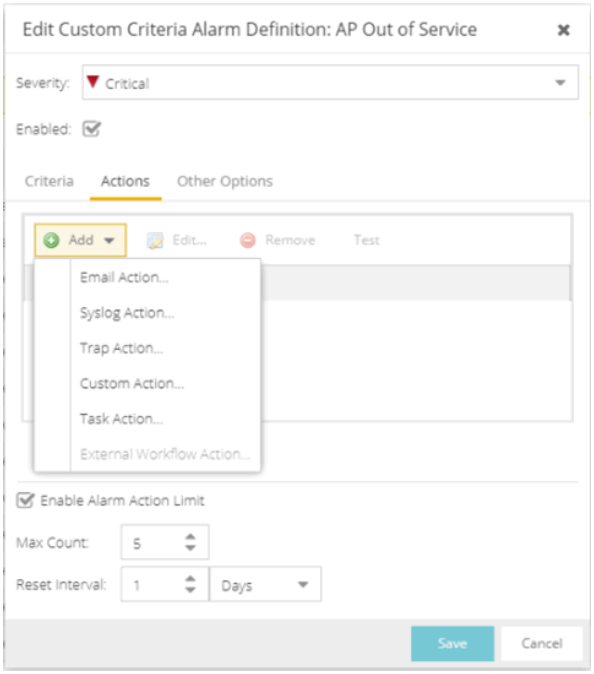


The severity of the alarm displays in the Severity field. Use the drop-down list to change the alarm severity. The Enabled check box indicates if the custom criteria has been enabled.

- 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.

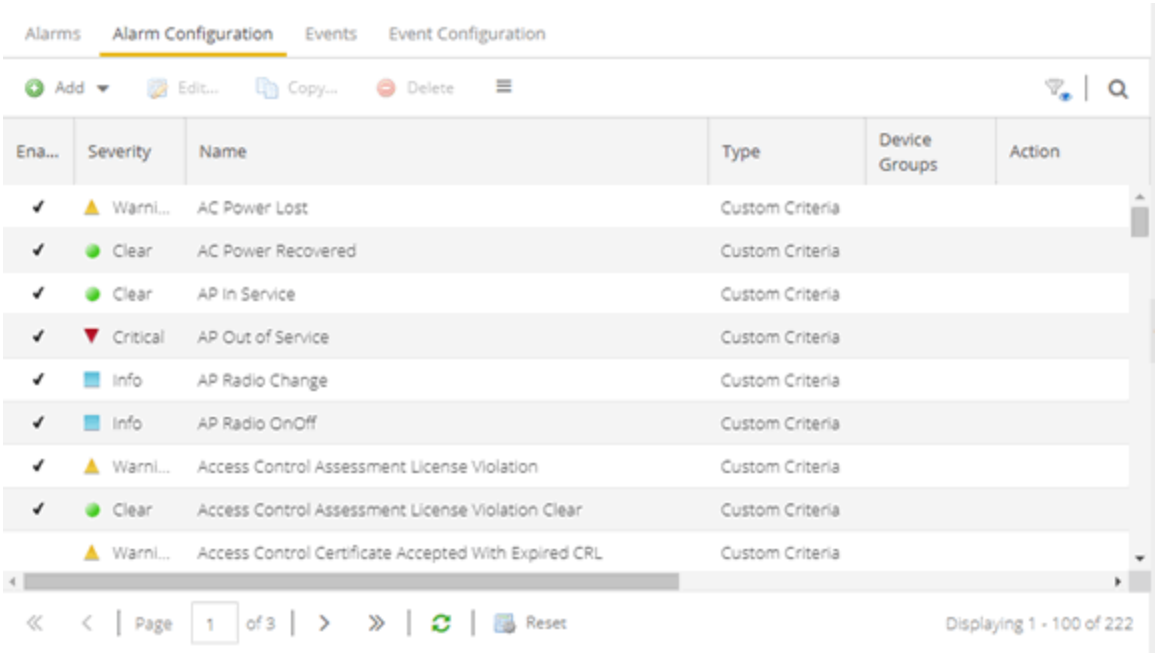
Alarm Summary

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 checkmark 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.

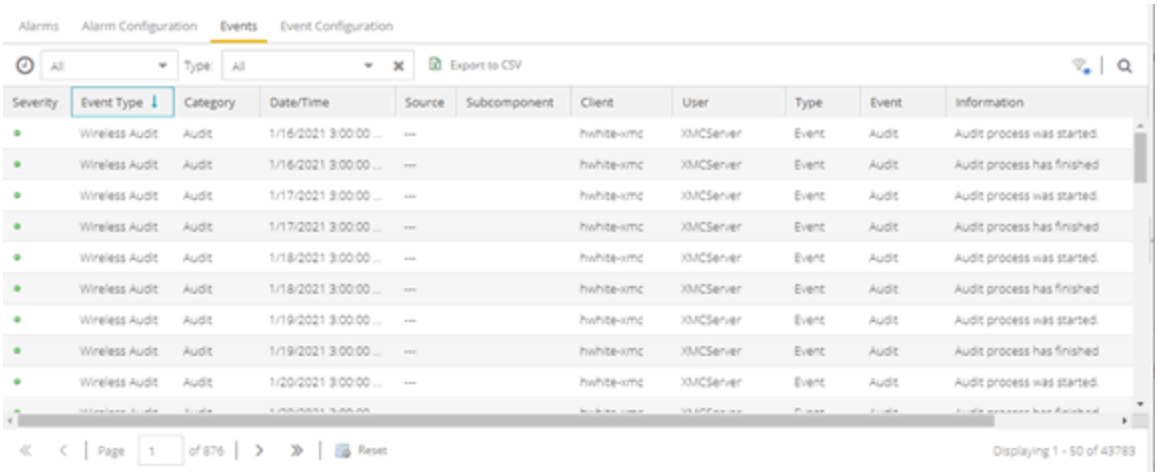
Reset Interval – If Limit Enabled is checked, this column displays the length of time from when the first action is triggered until the count is reset. When the count is reset, actions are executed until the Max Count is reached again. If the reset interval is set to "None", then when the alarm limit 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 legacy components (Console, Inventory, Policy, NAC Manager, and Wireless) present the same data as the event logs in the actual applications.
- The ExtremeControl Audit event log provides information on ExtremeControl 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 ExtremeControl 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.

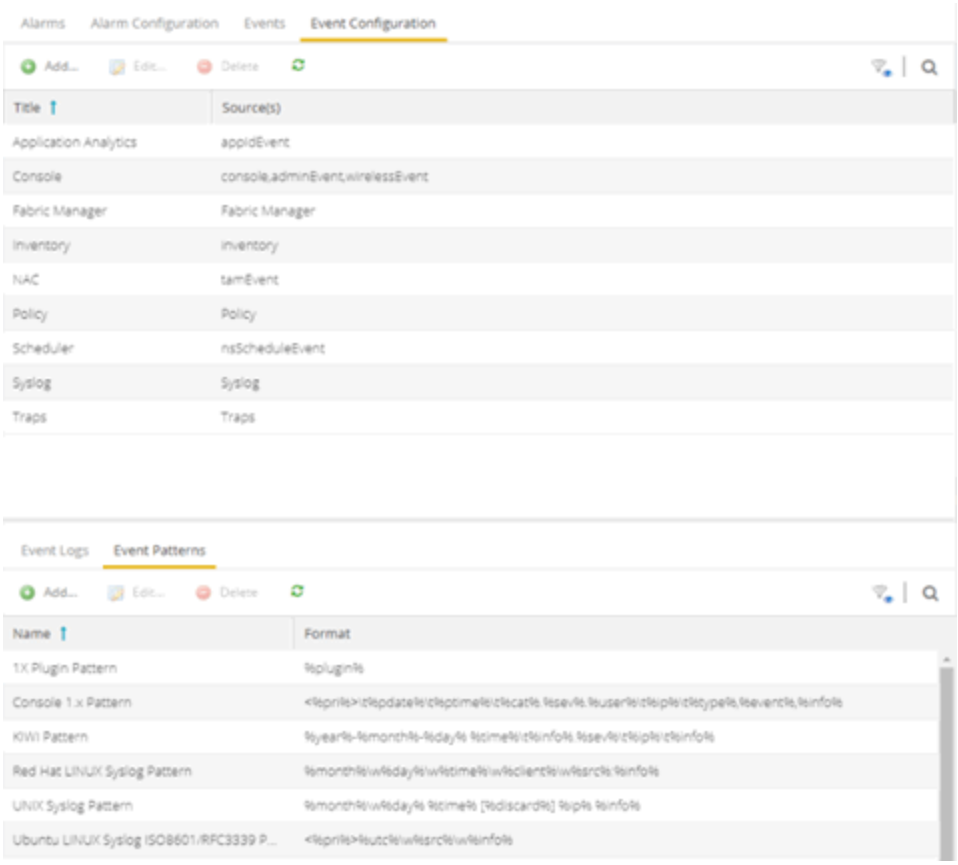
Type – Identifies the type of information for this row (event or trap).

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 & 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 

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.

Related Information

For information on related topics:

- Administration
- Network
- Reports
- Search
- Wireless

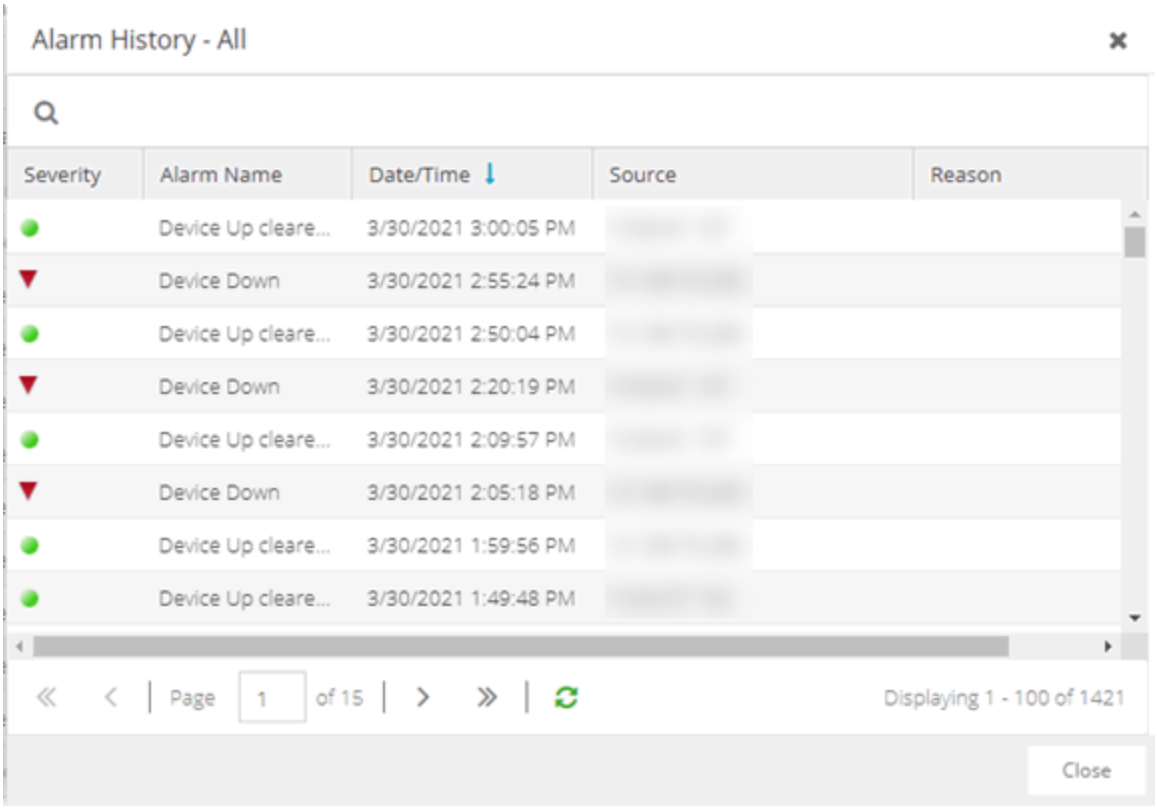
Alarm History

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.

Related Information

For information on related windows:

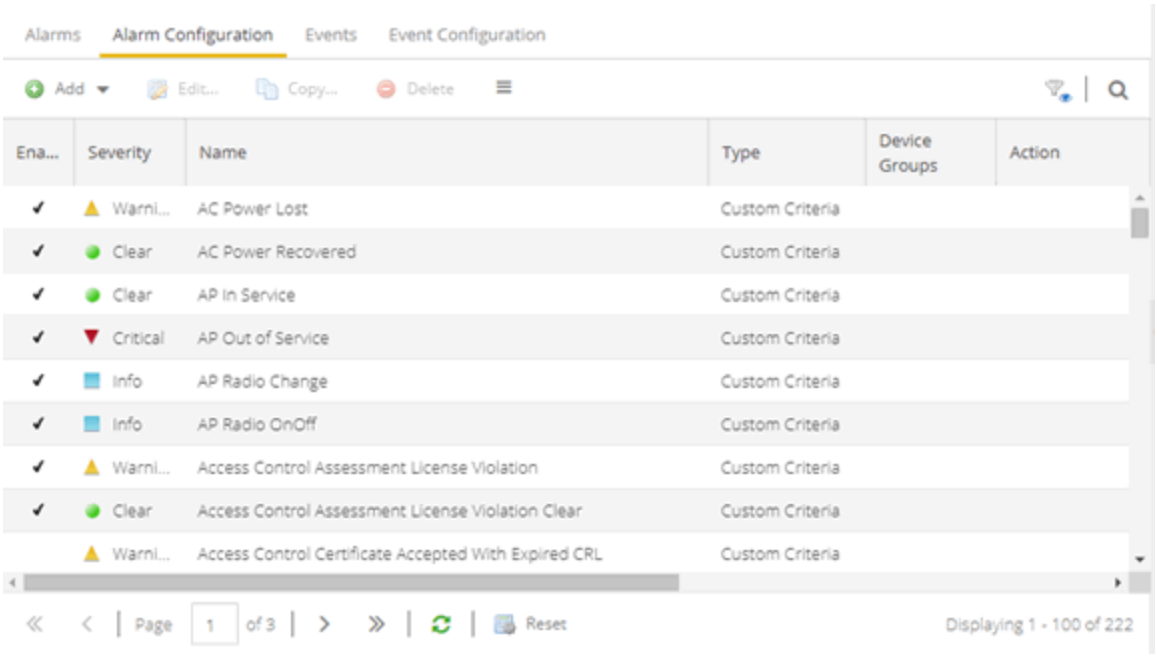
- Alarm Options

For information on related tasks:

- How to Configure Alarms

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

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,

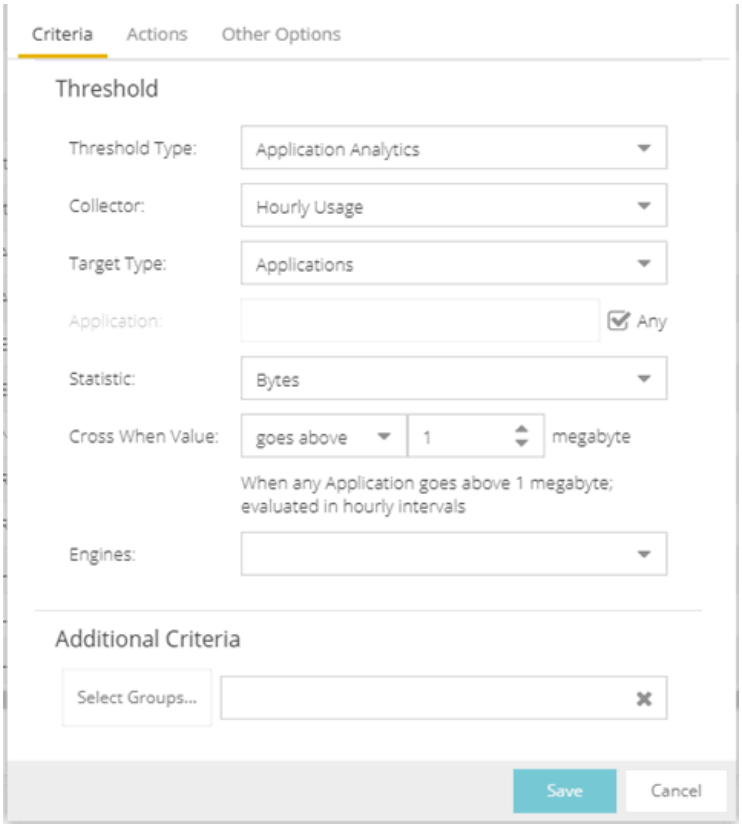
Error, Warning, Notice, or Info) and whether the alarm is triggered by traps, or events, or both.

- **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.

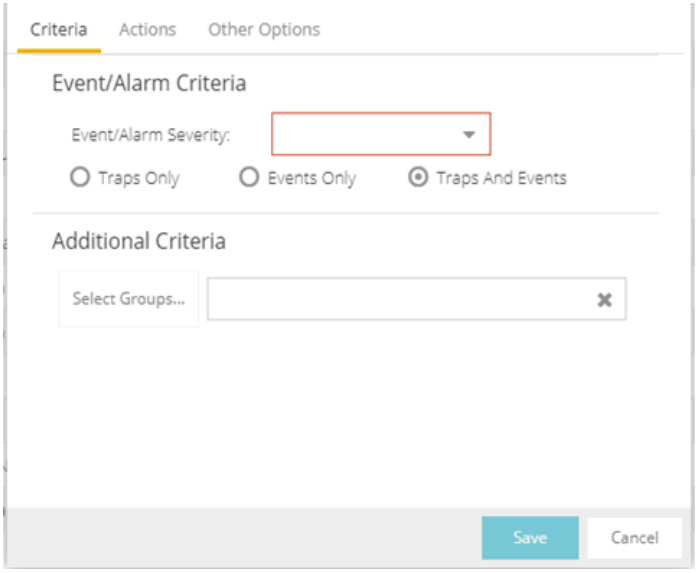
b. Select the traps that trigger the alarm.

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.

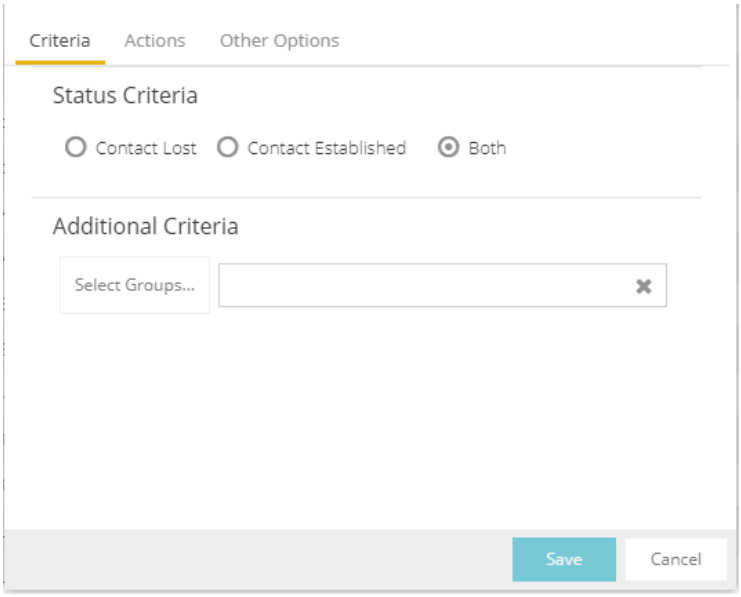
e. Select the **Actions** tab to configure the actions performed when the alarm is triggered.

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

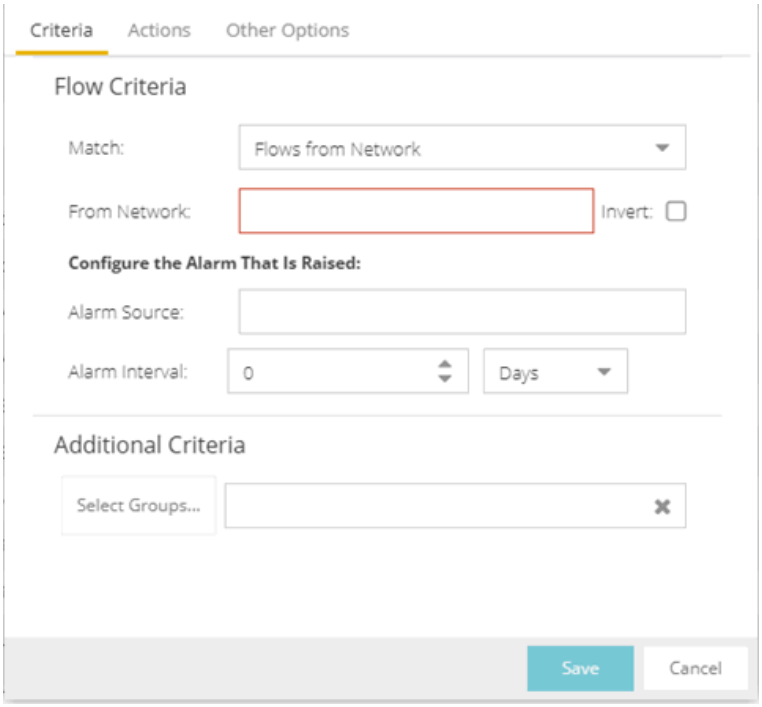


a. Select whether the alarm triggers when contact with a device is lost (Contact Lost), restored (**Contact Established**), or when contact is lost and when contact is regained (**Both**).

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.

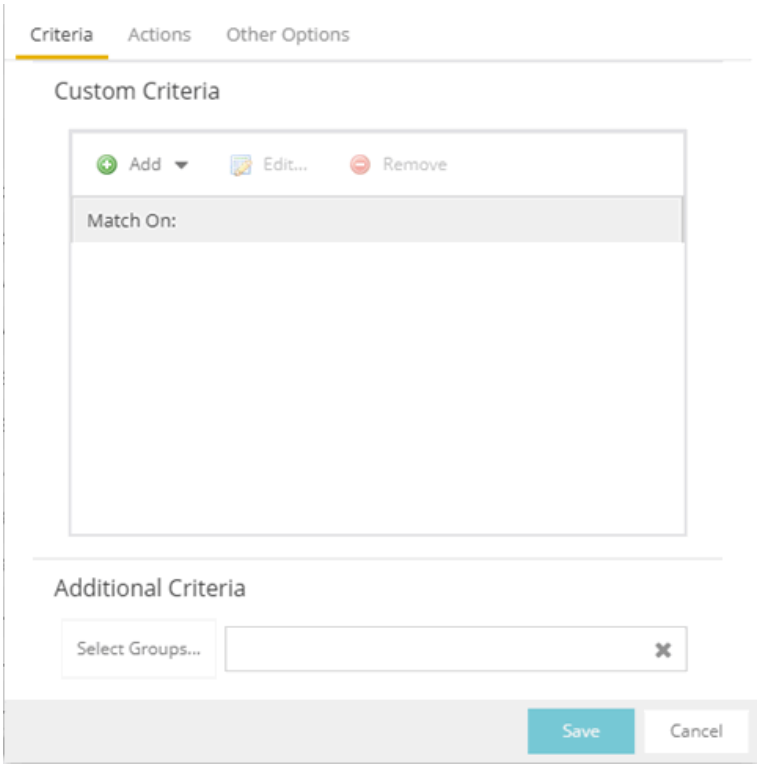
c. Enter a phrase in the **Alarm Source** field used as the source of the alarm.

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.

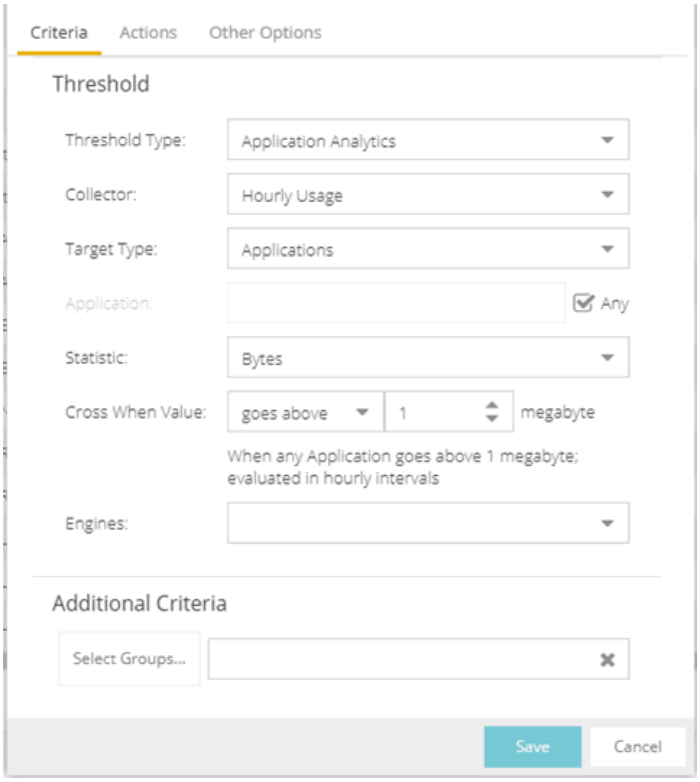
Match Selected – The information text string is matched against one or more phrase selected from the list.

Exclude Selected – The information text string matches if it is not one of the phrases selected from the list.

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.

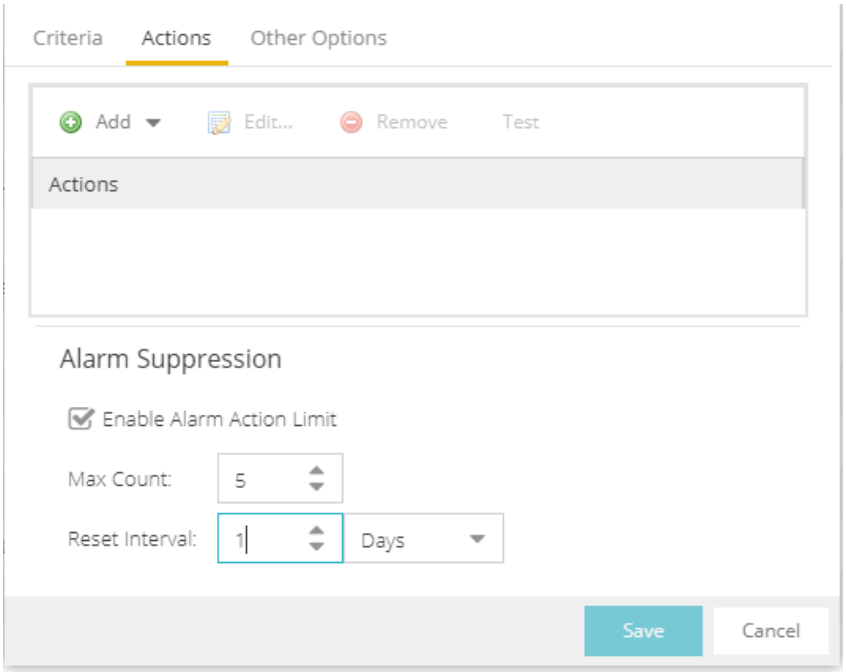
b. Select the criteria against which the threshold is compared.

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.

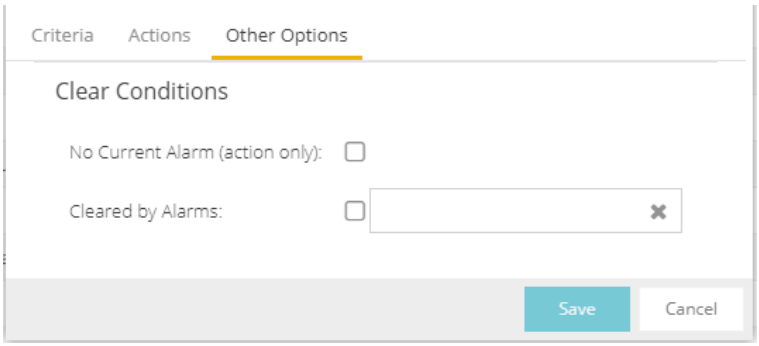
External Workflow Action – Runs a workflow action configured via a third-party application, such as StackStorm, when the alarm is triggered. Select **External Workflow Action** and then select a third-party application workflow.

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.



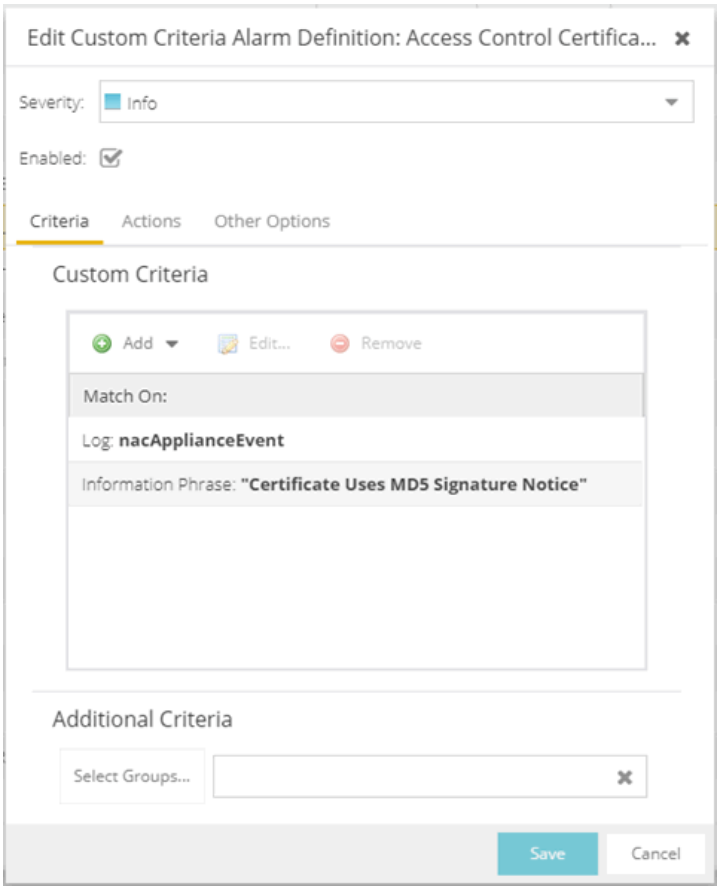
No Current Alarm (action only) – When this option is selected, the trigger event causes the system to perform the configured actions, but does not raise an alarm that becomes associated with the alarm source. The alarm status of the alarm source does not change, and no alarm is added to the system.

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.

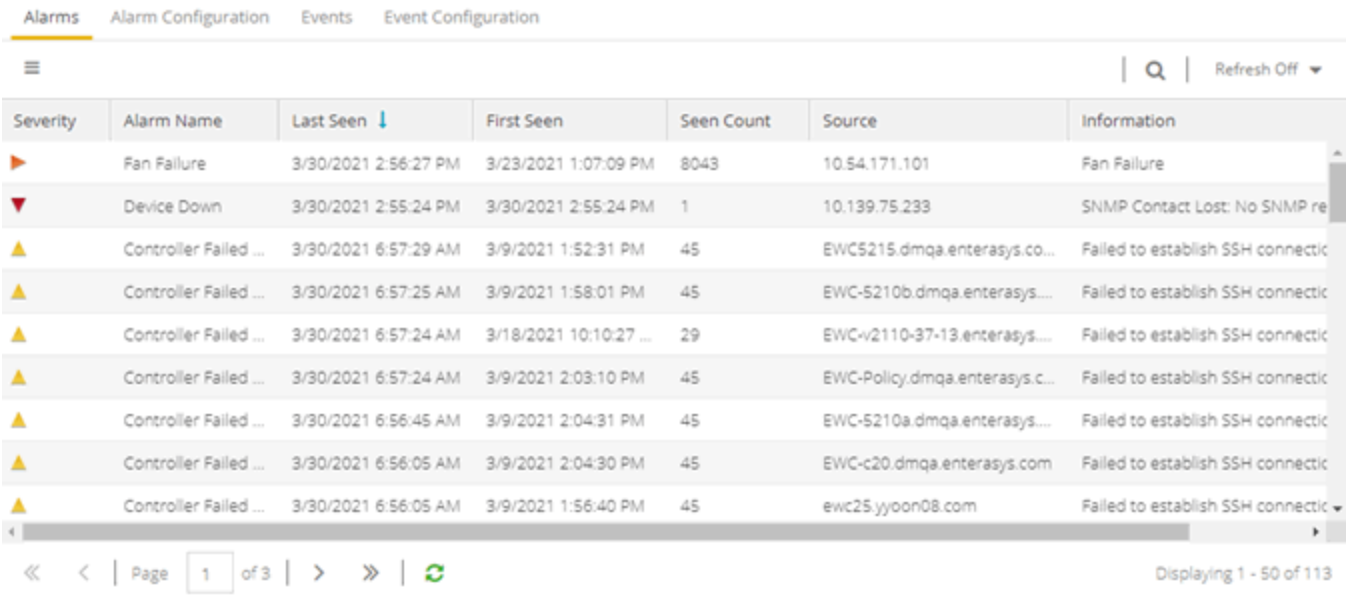
ExtremeCloud IQ - Site Engine

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.

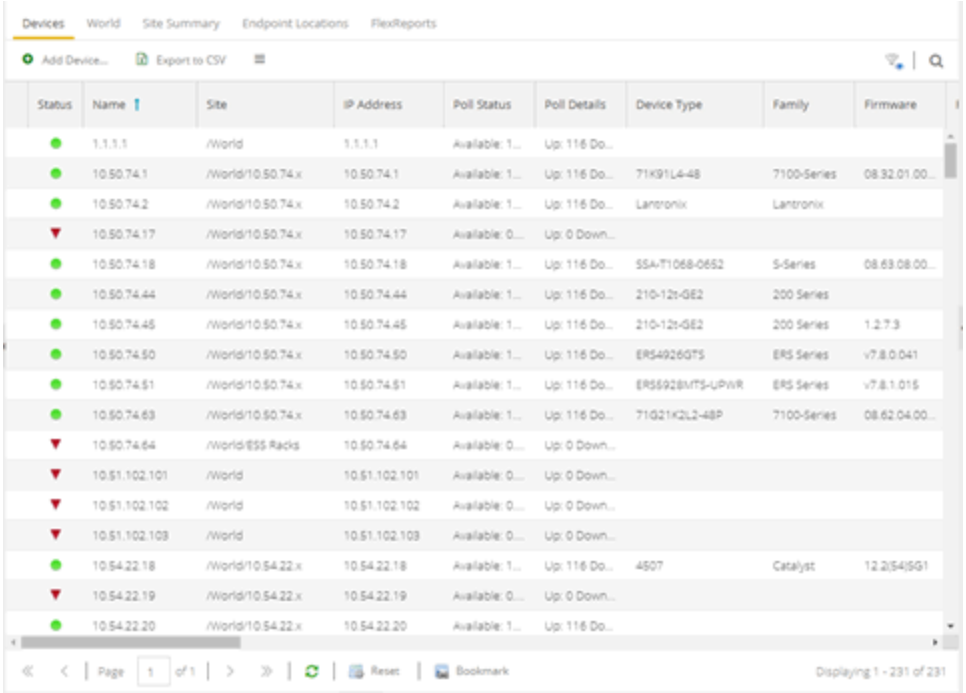
Alarms & Events Tab

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.

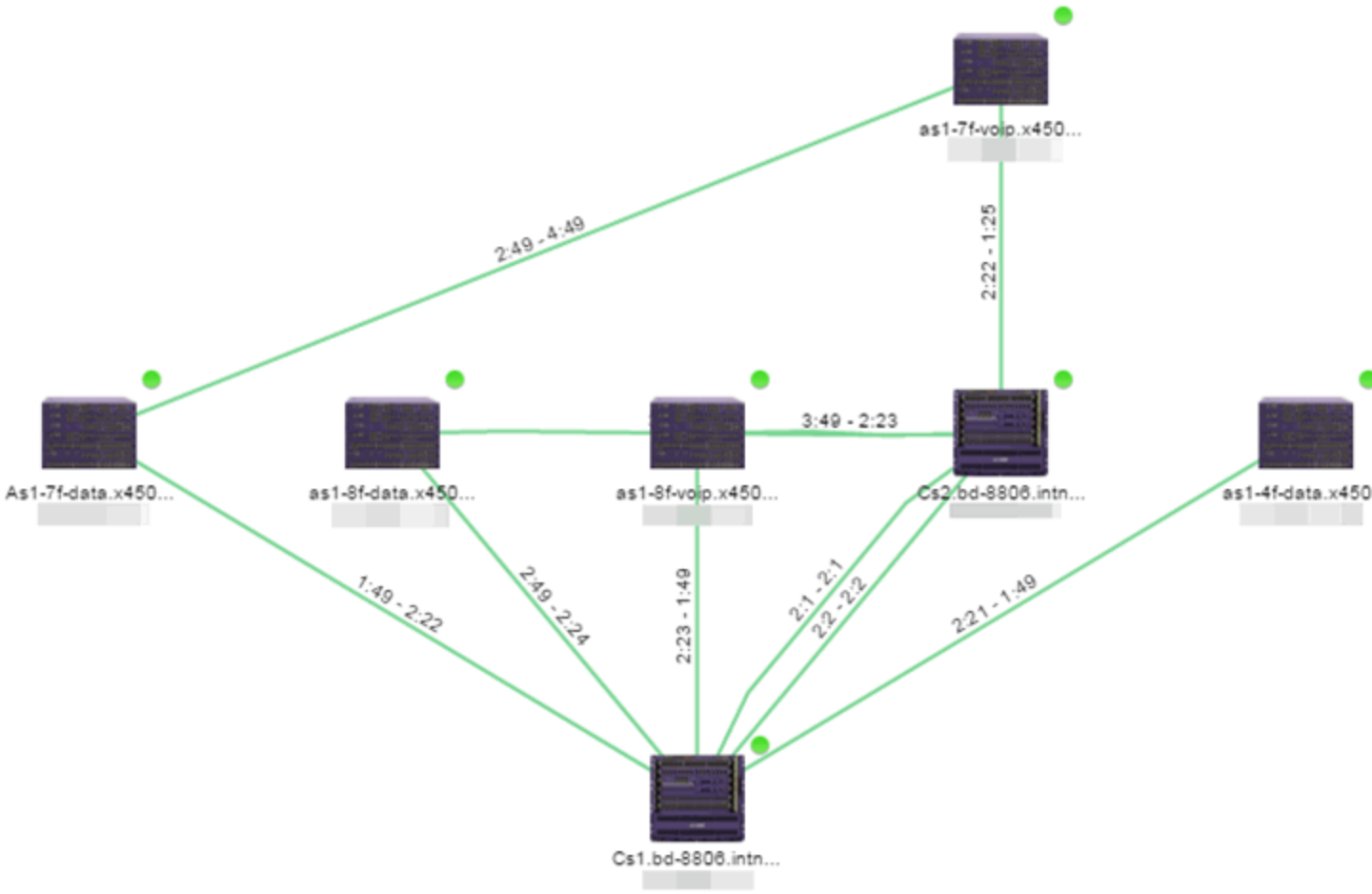


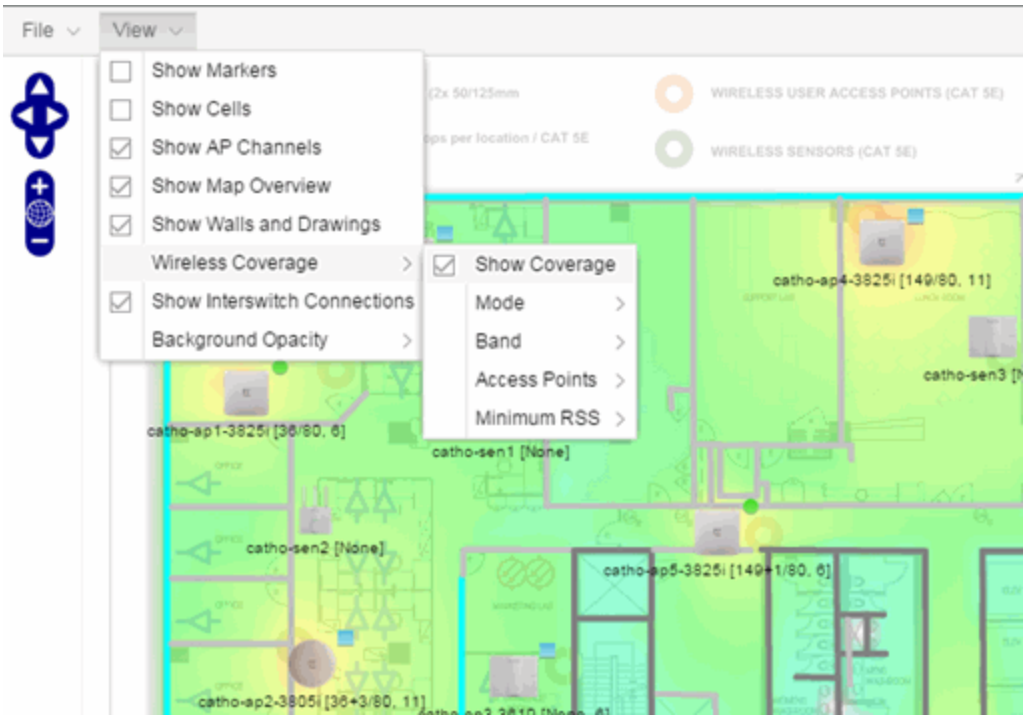
Network Tab

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
As1-7f-data.x450...
as1-8f-data.x450...
as1-8f-voip.x450...
3:49 - 2:23
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...



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.

Related Information

For information on related concepts:

- Alarms & Events

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.

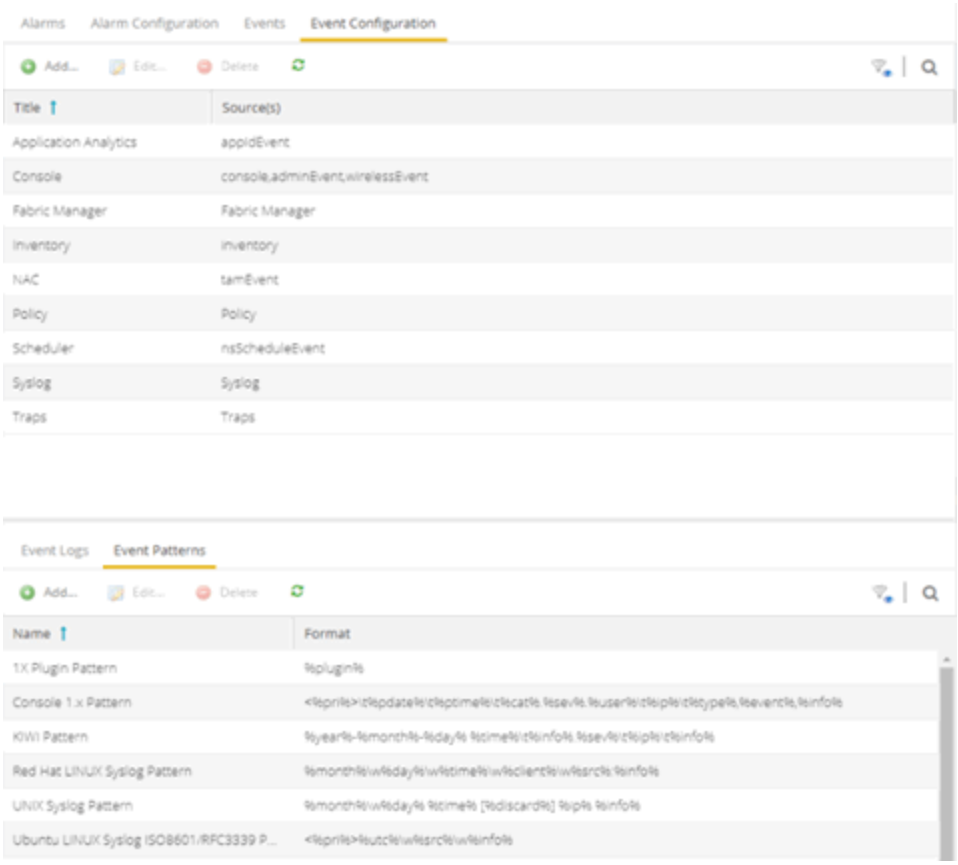
NOTE: **Access Control Audit**, **Access Control Engine**, **Admin**, **Console View**, **Compliance**, **Wireless**, and **Wireless Audit** Event Types are not configurable and not displayed on the **Event Configuration** tab.

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.

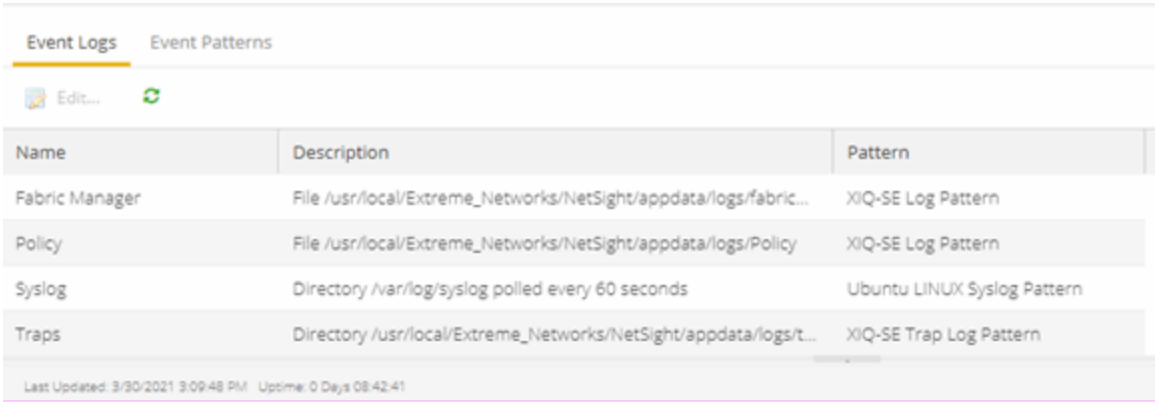
Delete

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.

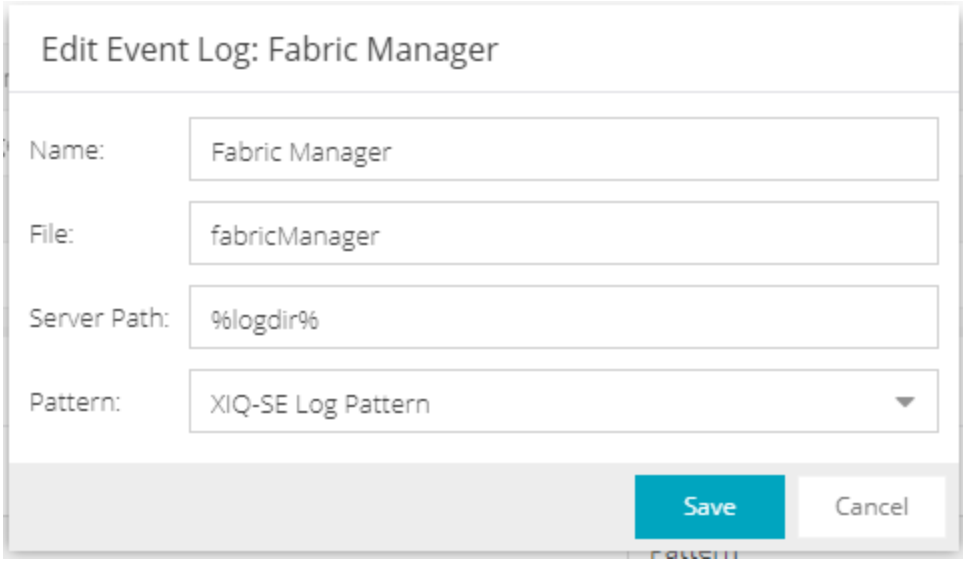
Description

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.

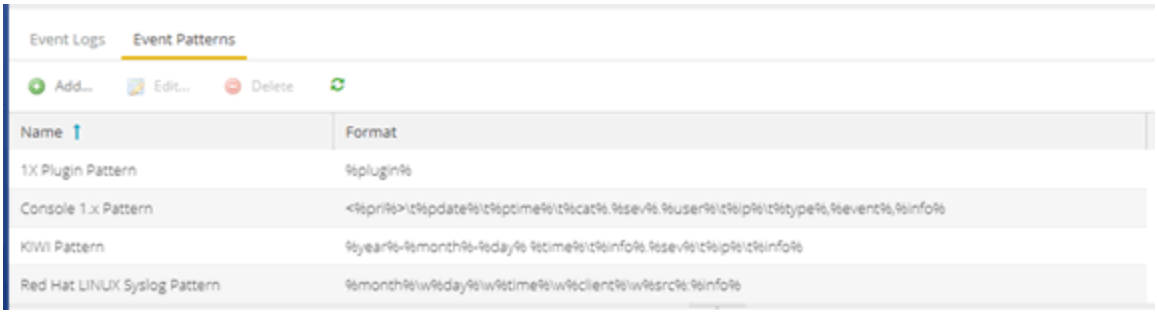
File
: Enter the name of the log file.

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.

Related Information

For information on related tasks:

- How to Configure Events

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.

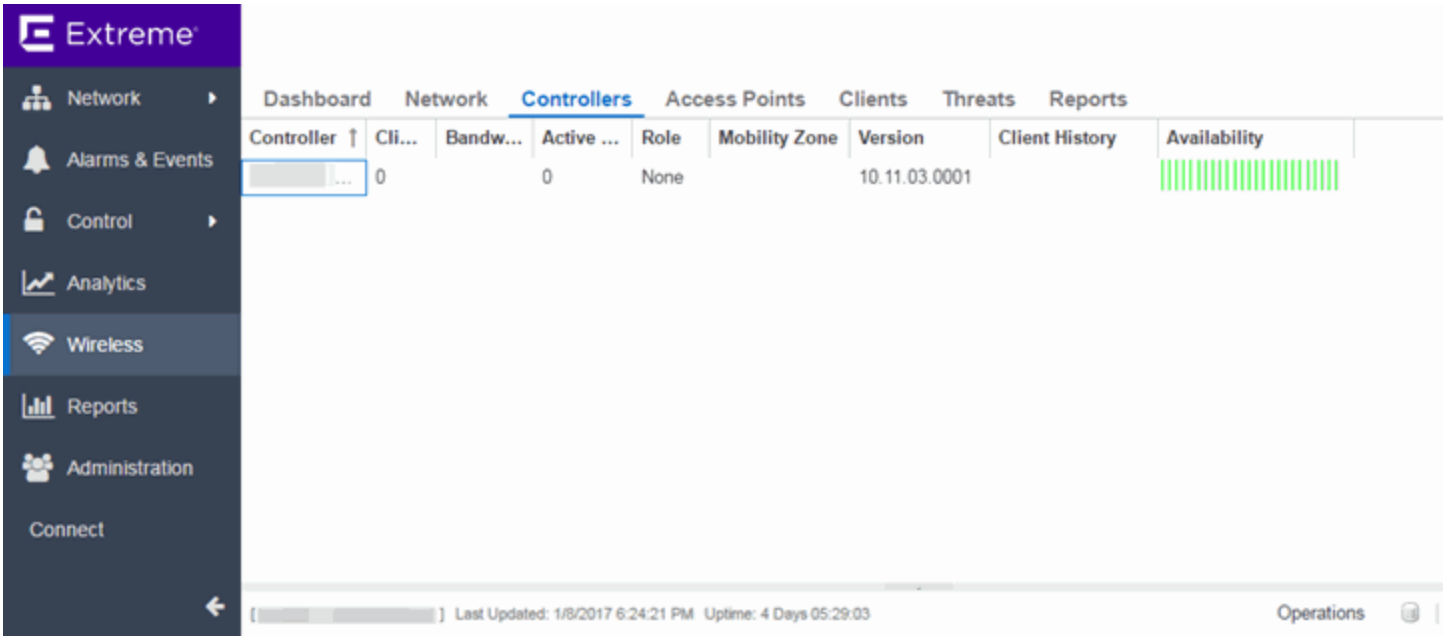
Reports are presented in a familiar wireless component tree structure similar to how components are displayed in Wireless Manager. Selecting any node in the tree provides contextual information for that node.

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

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

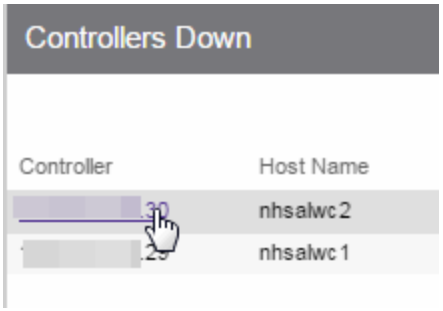
The **Reports** tab allows you to view information about the APs, controllers, and wireless traffic on your network. Available reports are accessible via the **Reports** drop-down list at the top of the tab.

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.

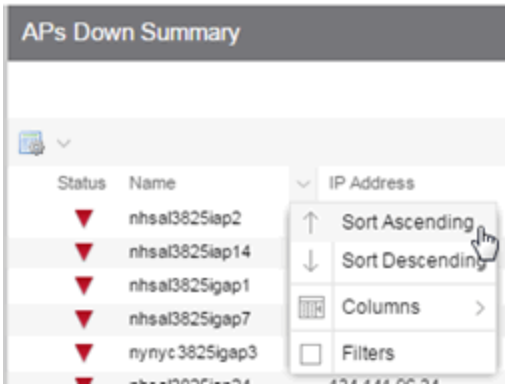
Report Features

ExtremeCloud IQ - Site Engine reports include the following features (depending on the report selected):

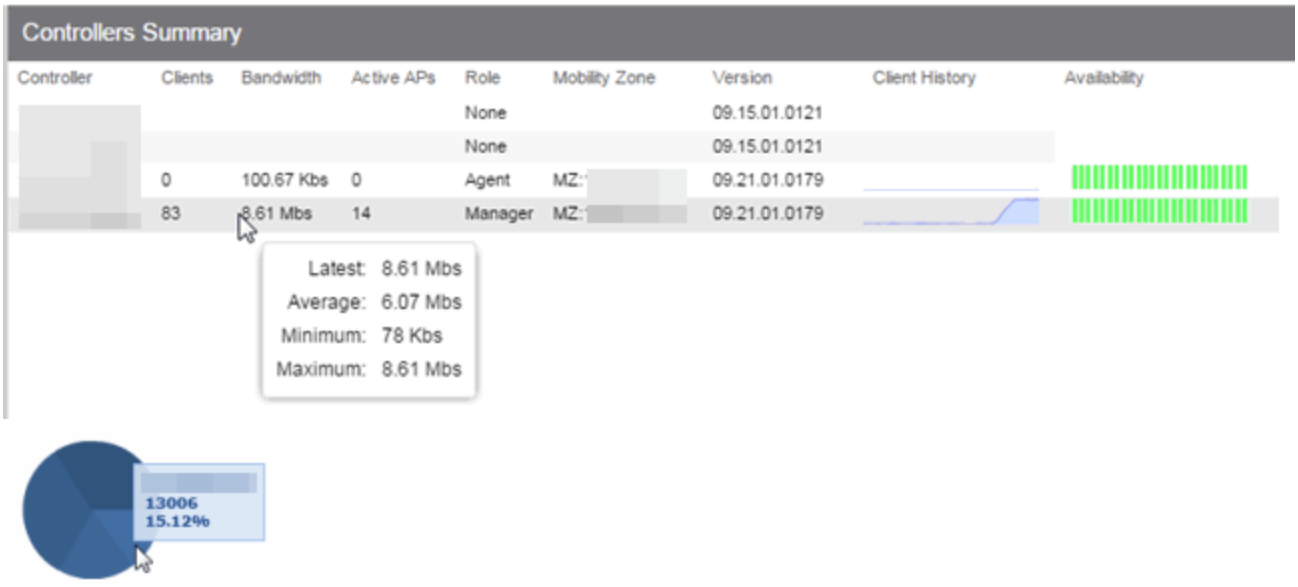
- **Drill-down for Details**—Link to summary reports containing more detailed information. For example, in the Controller Summary report, selecting a controller shows a detailed report for that controller over time.



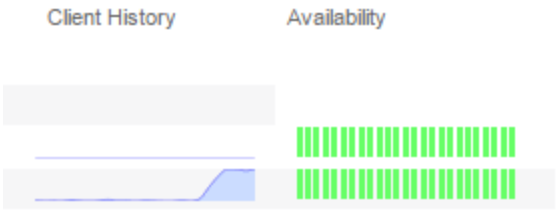
- **Interactive Tables**—Manipulate table data in several ways to customize the view for your own needs:
  - Select the column headings to **perform an ascending or descending sort** on the column data.
  - **Hide or display different columns** by selecting a column heading drop-down arrow and selecting 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.



Related Information

For information on related ExtremeCloud IQ - Site Engine topics:

- Administration
- Network
- Alarms and Events
- Reports
- Search

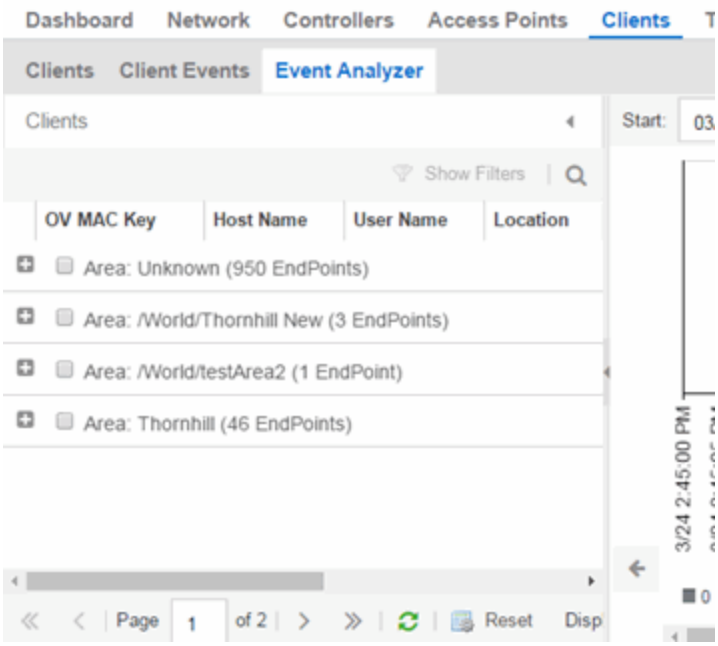
Event Analyzer

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.

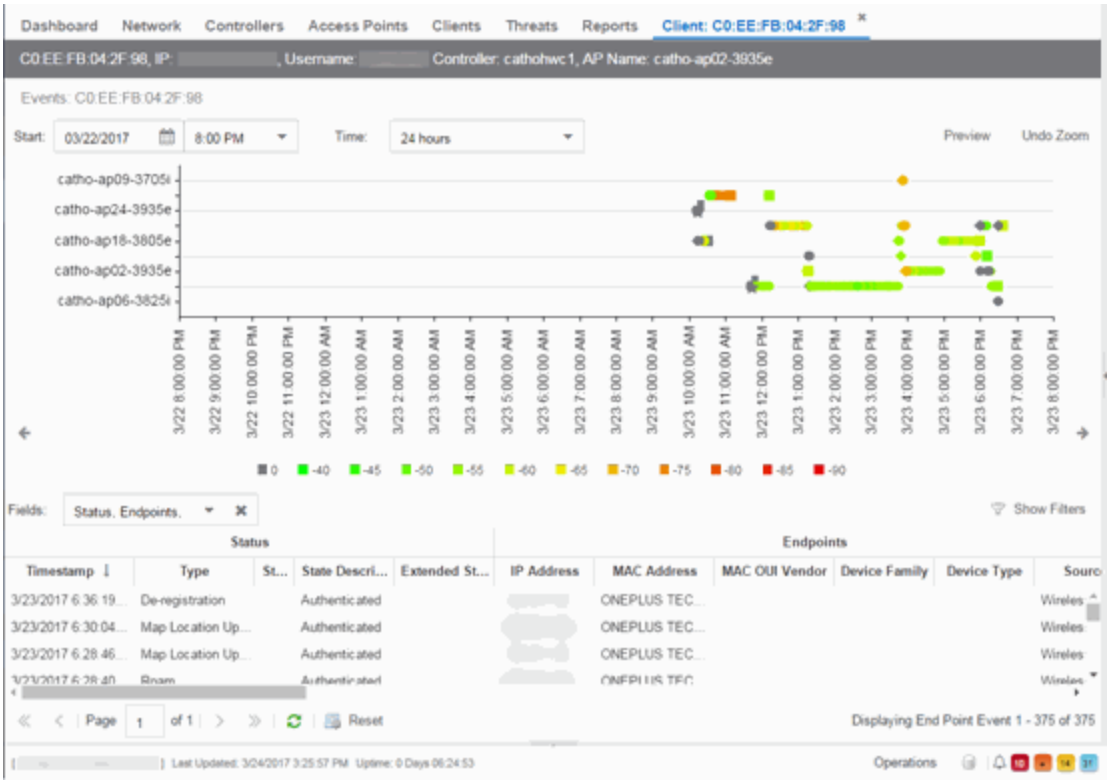
When accessing the tab using the top two methods, a Clients section is available in the left-panel. This section provides you with the ability to display end-point events for specific AP locations.



Once you select the appropriate end-points or areas, this section can be collapsed by selecting the left arrow.

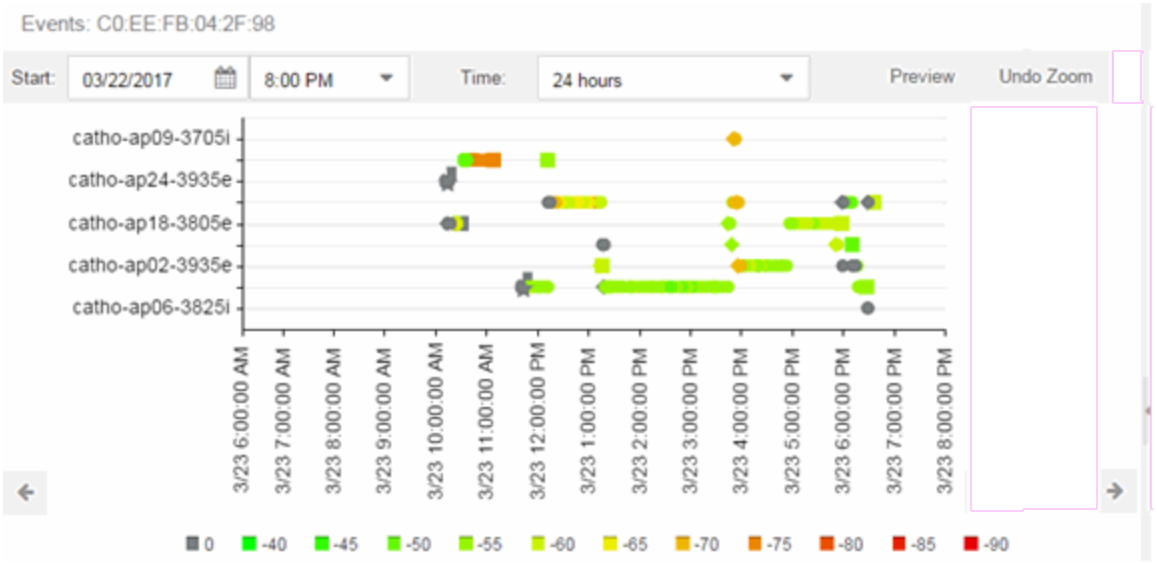
The top of the tab contains a graph displaying the RSS (Received Signal Strength) for the end-point events.

The bottom contains a table showing information about each event.



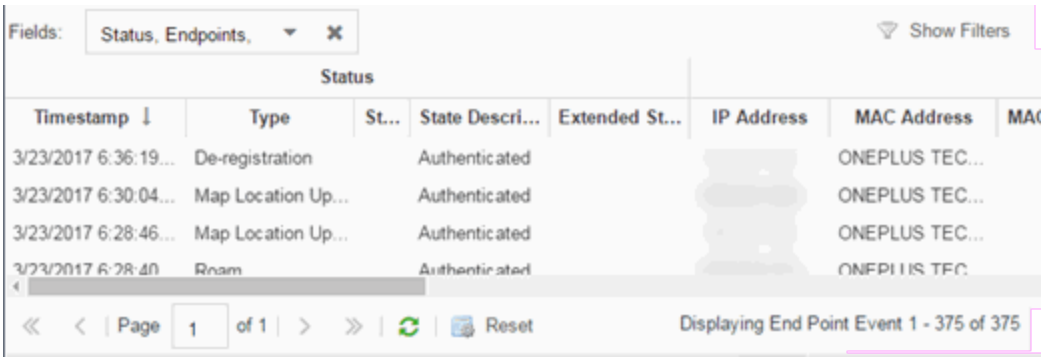
RSS Graph

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
    - ExtremeControl 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

Related Information

For information on related ExtremeCloud IQ - Site Engine topics:

- Wireless

ExtremeCompliance Overview

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 your ExtremeCloud IQ - Site Engine version 21.11.10 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`.

Related Information

For information on related tabs:

- Compliance Dashboard
- Audit Tests
- Archives

ExtremeCompliance® User Guide

12/2021
9037297-00

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

ExtremeCompliance Overview

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 your ExtremeCloud IQ - Site Engine version 21.11.10 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`.

Related Information

For information on related tabs:

- Compliance Dashboard
- Audit Tests
- Archives

How to Obtain and Apply an ExtremeCompliance License

To use the **Compliance** tab in ExtremeCloud IQ - Site Engine, an additional license is required.

To obtain and apply the license in ExtremeCloud IQ - Site Engine:

1. Contact your sales representative to purchase an ExtremeCompliance license.

   An email voucher is generated and sent to you with instructions.
2. Create an Extreme Networks Support Portal account, if necessary.
   a. Open a browser and go to https://secure.extremenetworks.com/.
   b. Enter your information and select **Create An Account**.

      An email is sent to you with instructions to activate your account.
   c. Select the link in your email.

      The Portal - Account Activation web page displays.
   d. Enter your **Email Address** and the **Activation Code** included in your activation

email, if they do not automatically populate.

e. Select **Activate**.

3. Access the Extreme Networks Support Portal at https://extremeportal.force.com/ExtrLicenseLanding.
4. Enter your **Email** and **Password** and select **Log In**.
5. Select **Generate License**.

   The Generate License window displays.
6. Enter your **Voucher ID** from the email voucher sent to you and select **Next**.
7. Select the **Terms and Conditions** checkbox and select **Submit**.

   A window displays with your software license key.
8. Copy the license key from the window.
9. Open ExtremeCloud IQ - Site Engine.
10. Access the **Administration** > **Licenses** tab.
11. Select **Add**.

    The **Add License** window displays.
12. Paste the license key you copied in Step 8 and select **OK**.
13. Restart ExtremeCloud IQ - Site Engine.
14. The **Compliance** tab is now available in the menu, allowing you to use ExtremeCompliance audit functionality.

Related Information

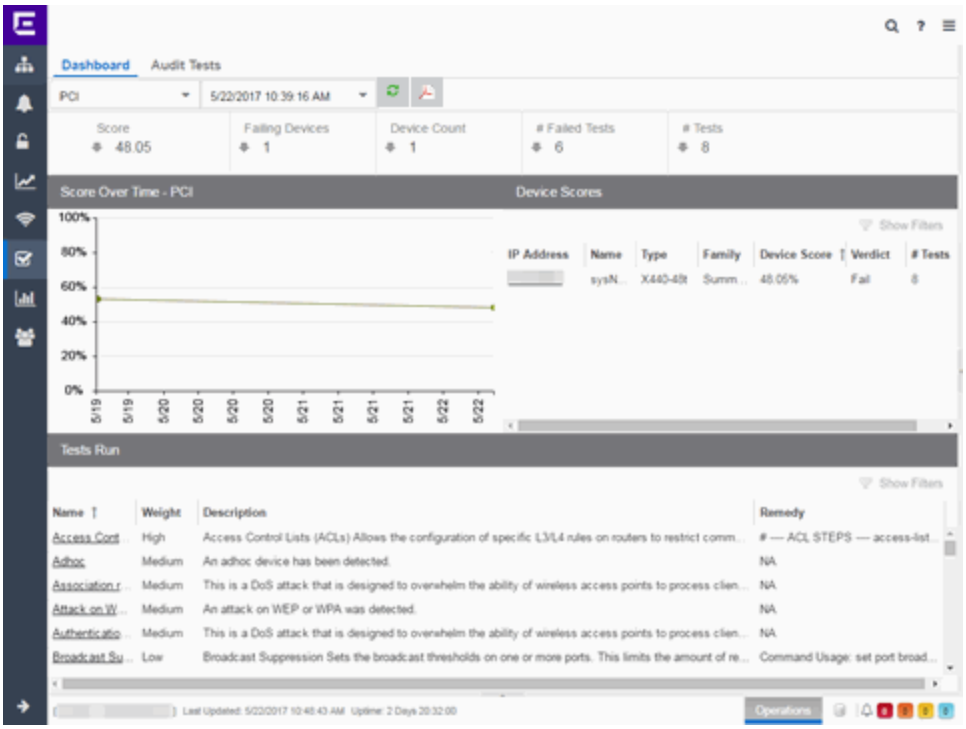
For information on related tabs:

- ExtremeCompliance Overview
- Administration

Compliance Dashboard

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.

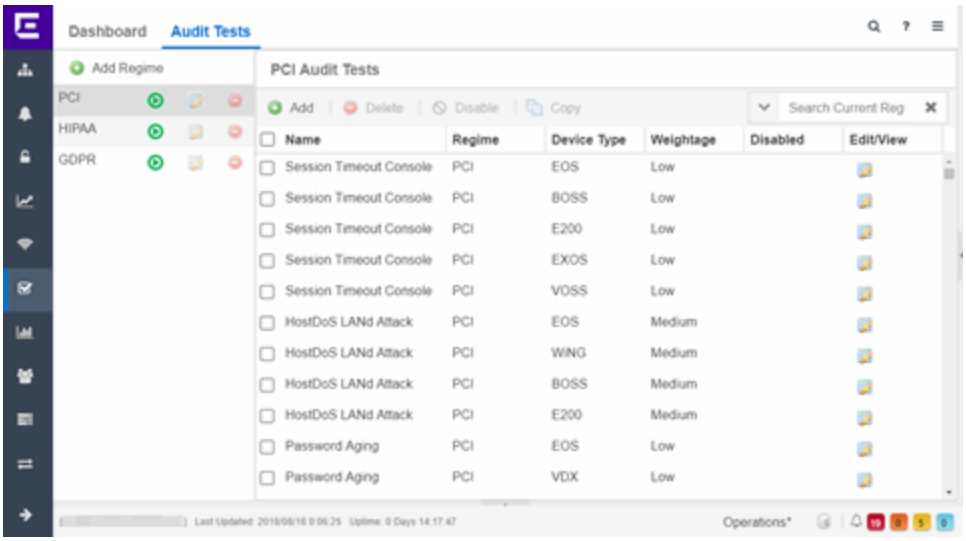
Related Information

For information on related topics:

- ExtremeCompliance Overview
- Audit Tests
- Configure Device

Audit Tests

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 checkmark 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.

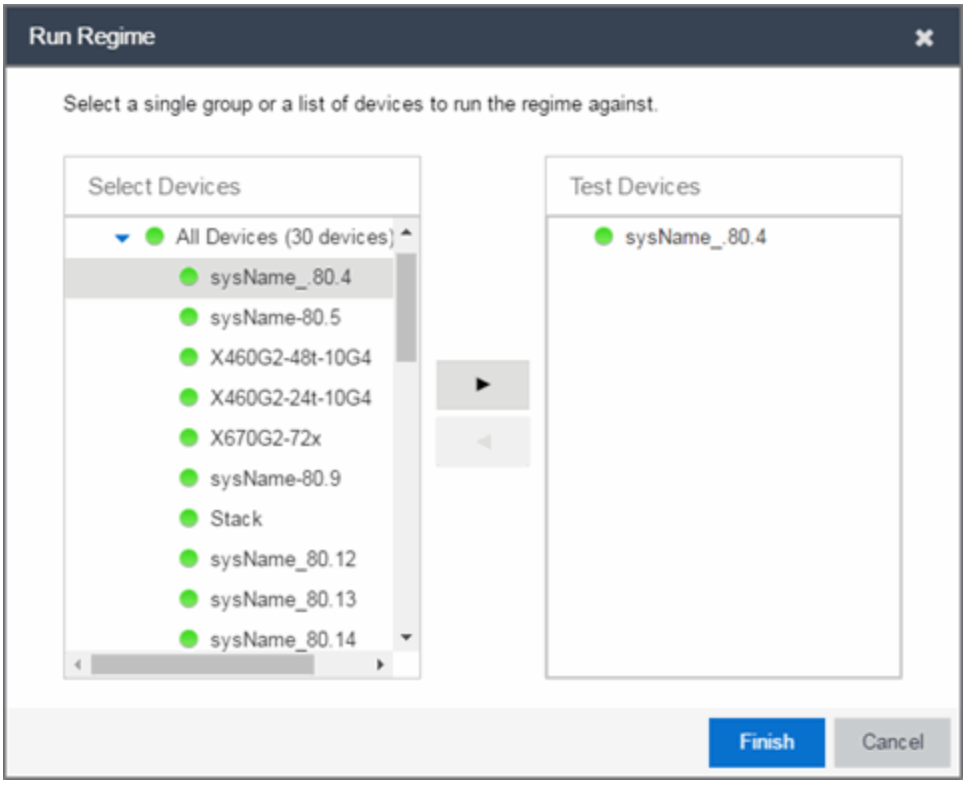
Related Information

For information on related tabs:

- ExtremeCompliance Overview
- Scheduled Tasks

Run Regime

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.

Related Information

For information on related tabs:

- ExtremeCompliance Overview
- Scheduler

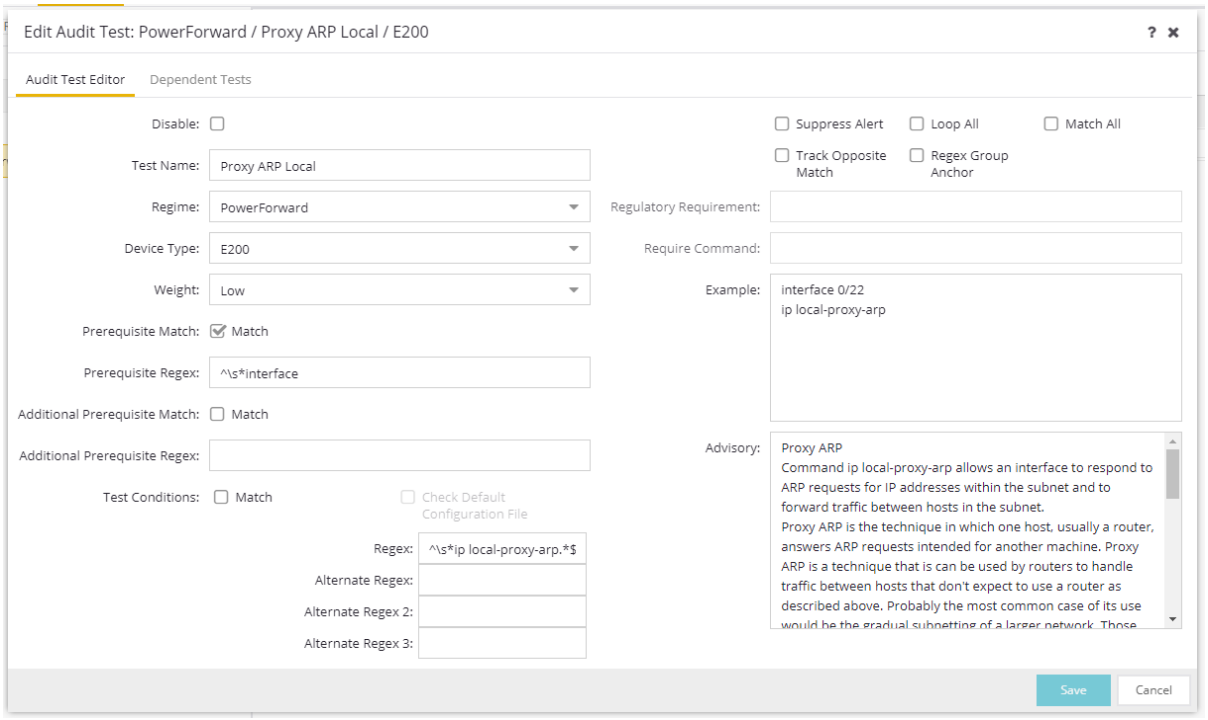
Create/Edit Audit Test

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 21.11.1.0, ExtremeCloud IQ - Site Engine supports multiple Device Types, including **E200**, **EXOS**, **EOS**, **BOSS**, **VOSS**, 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 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 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 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.

Related Information

For information on related topics:

- Audit Tests
- Dependent Tests

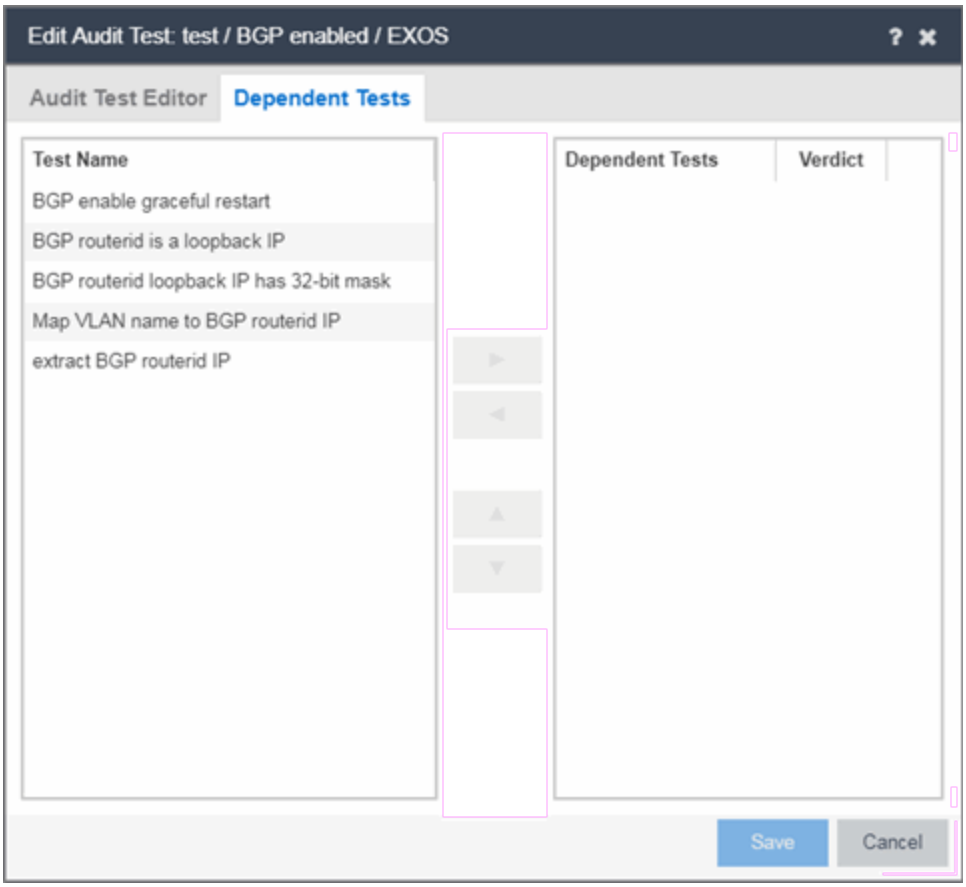
Dependent Tests

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.

Related Information

For information on related topics:

- Audit Test Editor
- Audit Tests

How to Add a New Regime

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.

Related Information

For information on related tabs:

- ExtremeCompliance Overview
- Diagnostics

Third Party Device Support in ExtremeCompliance

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

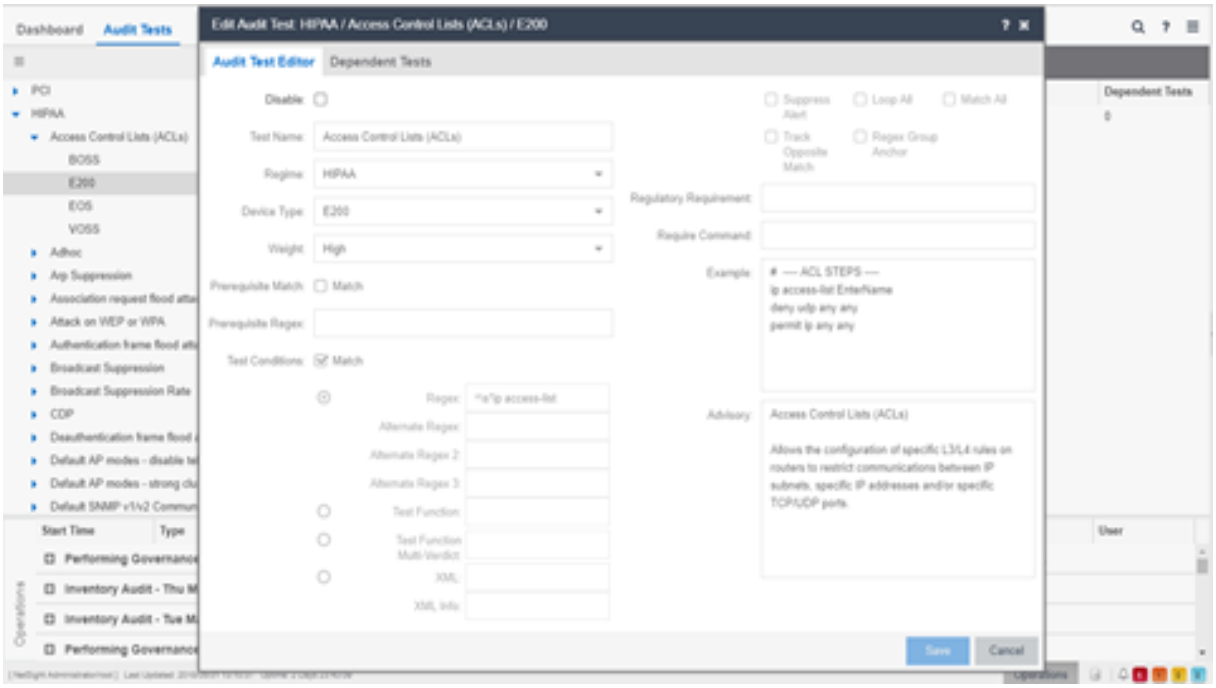
1. Login to ExtremeCloud IQ - Site Engine server as a user with write permissions on the installation.
2. Edit the following file: `<Installation_Directory>/GovernanceEngine/thirdPartyDevices.properties`

3. Follow the instructions given in the file to add SysOIDs. Multiple SysOIDs can be mapped to one user-defined Device Type (for example, 13.6.14.19.11745=XYZ, where 13.6.14.19.11745 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 VOSS) 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.

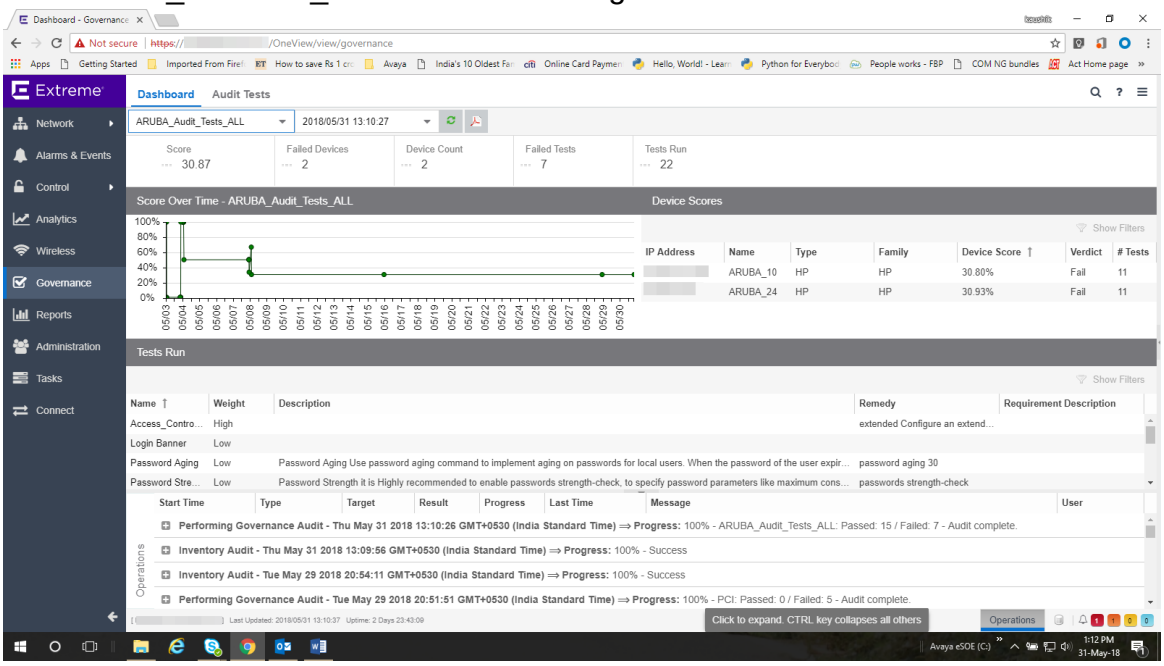
d. Verify the panel displays an **Inventory Audit** entry.

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

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

Extreme Networks tested the following devices:

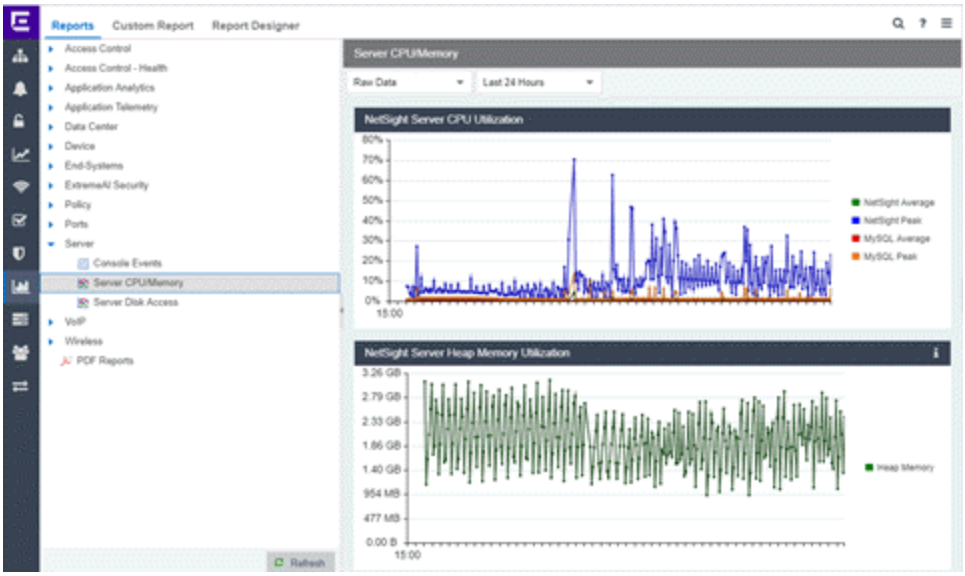
- Cisco IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22) EA2
- Cisco IOS Software, C3750 Software (C3750-IPBASE-M), Version 12.2(35) SE5

#	**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.

Related Information

- Report Designer

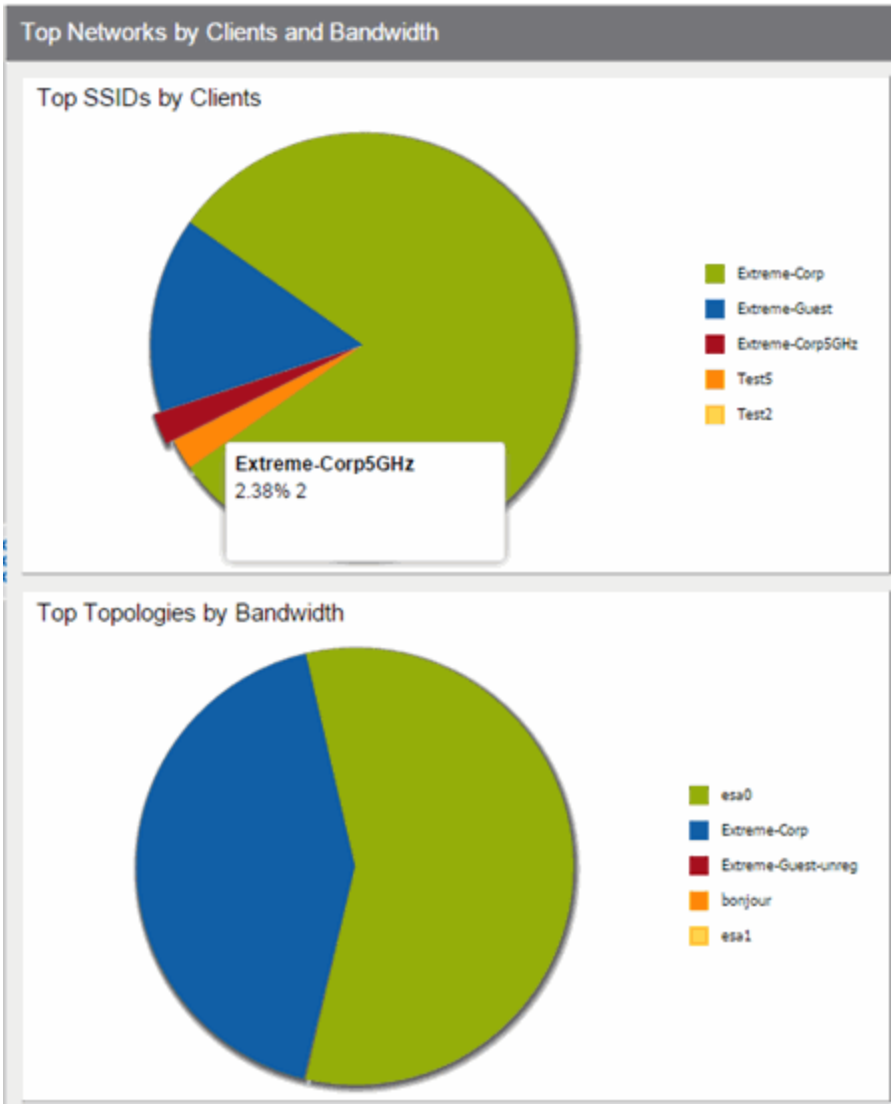
Reports Features

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.

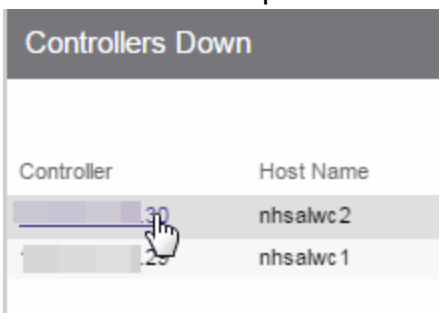
Reports Features

ExtremeCloud IQ - Site Engine reports include the following features (depending on the report selected):

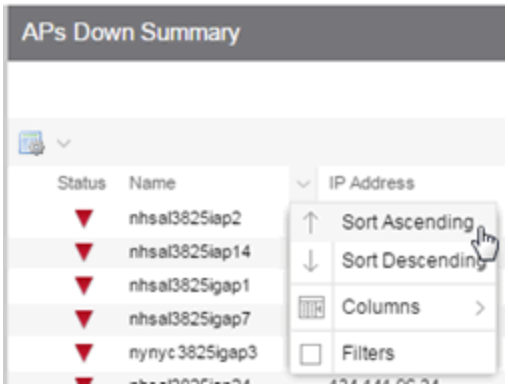
- **Hover Over for Info** —Hover over a pie section to display the name of the segment, the percentage represented by the segment and the number of elements. for some reports, selecting a pie section opens a filtered end-systems grid for more detailed information.



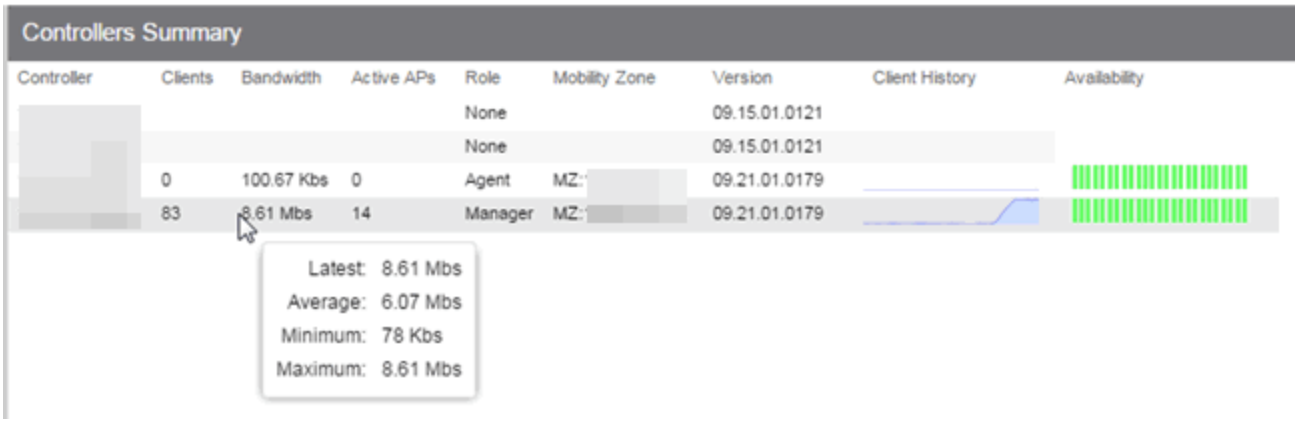
- **Drill-down for Details**—Link to summary reports containing more detailed information. For example, in the Controller Summary report, selecting a controller shows a detailed report for that controller over time.



- **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.

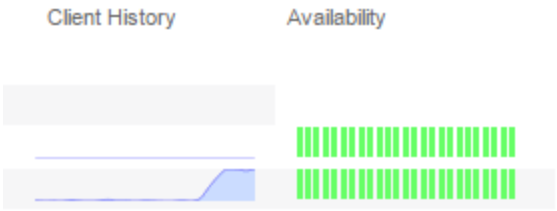


- **Interactive Charts**—Use data-point rollovers for quick information on chart data. For example, in the Controller Summary report, rolling over the value reported for Bandwidth provides additional bandwidth statistics over time.



- **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.

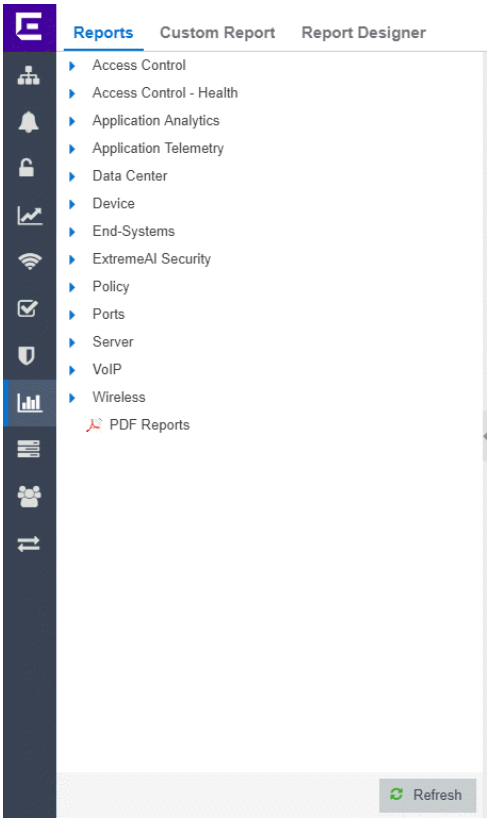
Related Information

- ExtremeAnalytics tab

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.
- **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.

Related Information

- ExtremeAnalytics

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 ExtremeCloud IQ - Site Engine OneView > Access OneView and NetSight 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.

Related Information

- 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.

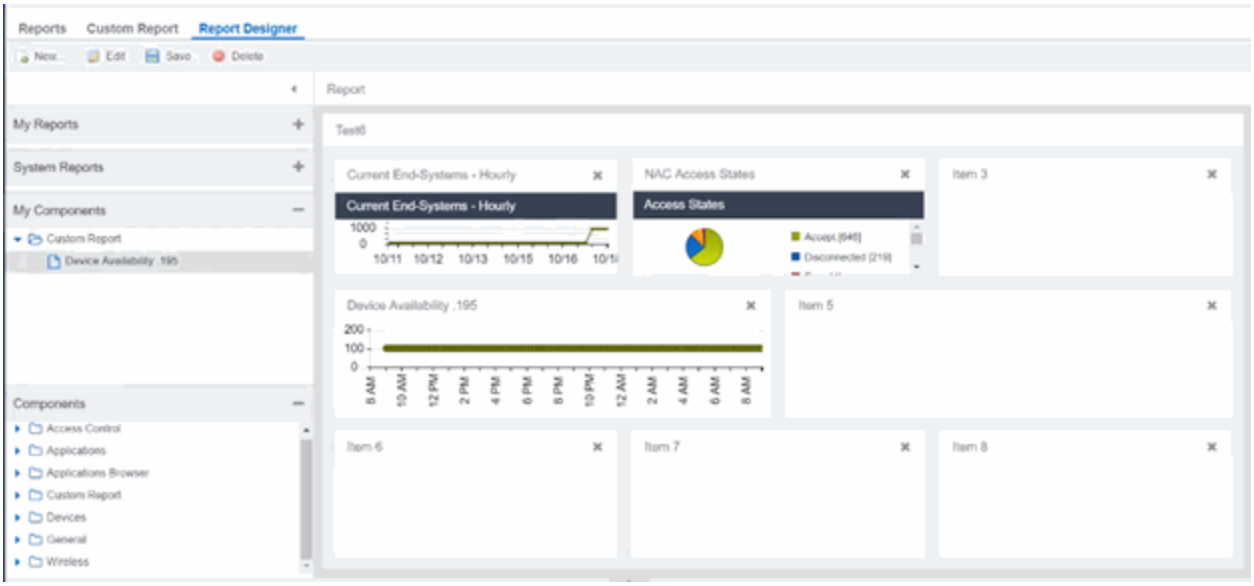
In order to use the Report Designer, you must be a member of an authorization group that is assigned the ExtremeCloud IQ - Site Engine OneView > Access OneView and NetSight OneView > Access OneView Administration capabilities.

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.

Related Information

- 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.

Related Information

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.

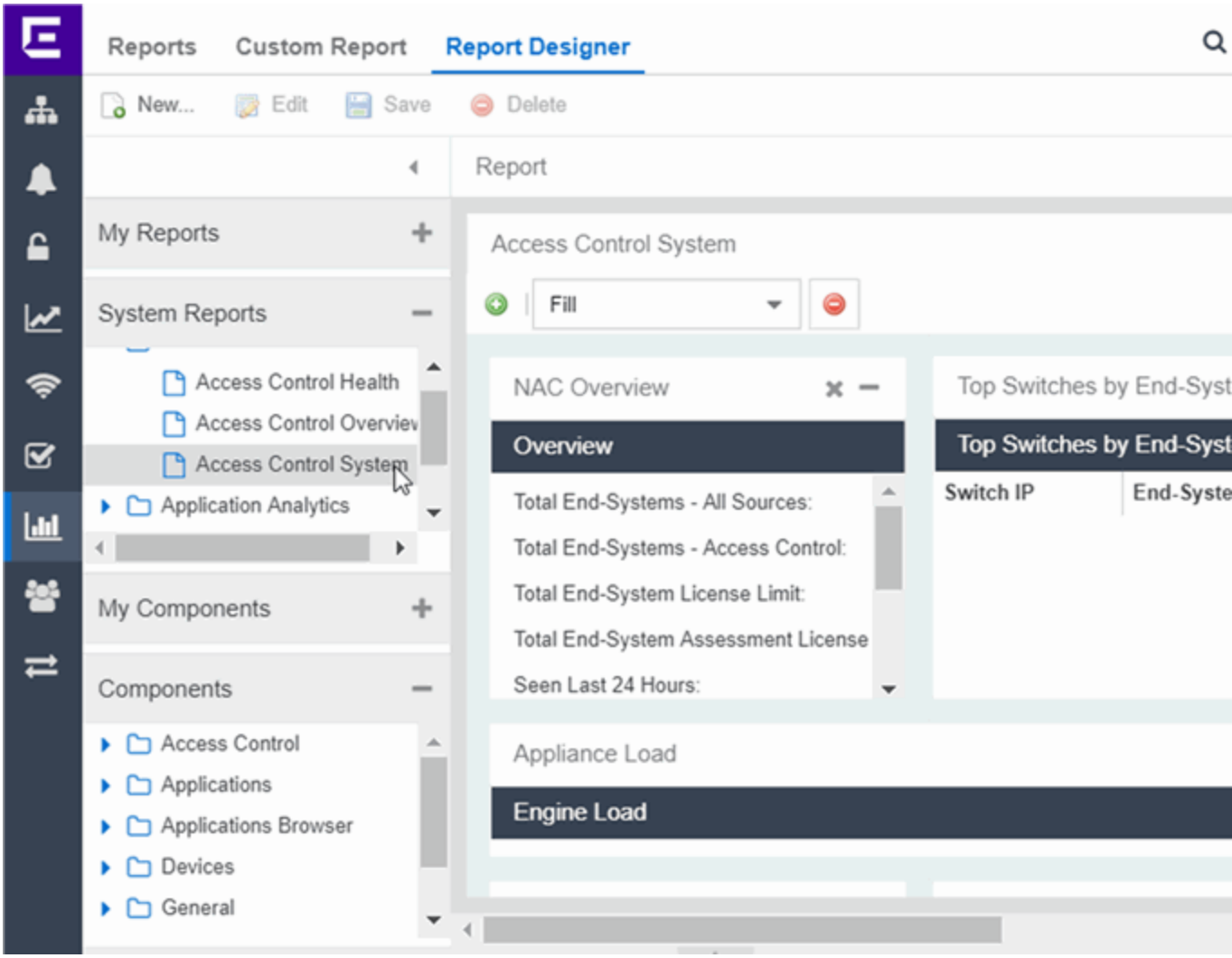
The Report Designer can be accessed from the **Reports** tab. In order to use the Report Designer, you must be a member of an authorization group that is assigned the ExtremeCloud IQ - Site Engine OneView > Access OneView and NetSight OneView > Access OneView Administration capabilities.

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 ExtremeControl 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, ExtremeControl > ExtremeControl 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.

Related Information

- Reports Catalog

Custom Components in Report Designer

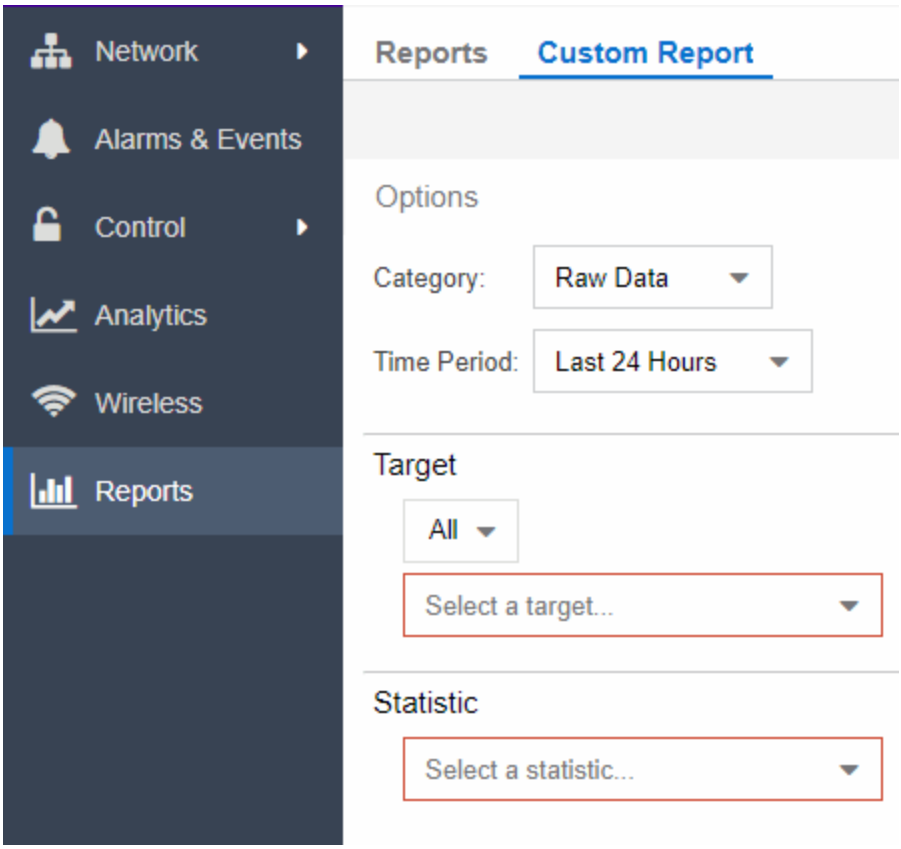
When you create an Advanced Browser report in the ExtremeAnalytics Browser, you can save it to the **Report Designer** to use as a custom component. The custom component uses the target, statistic, start time, and search criteria you defined in the Advanced Browser report.

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.

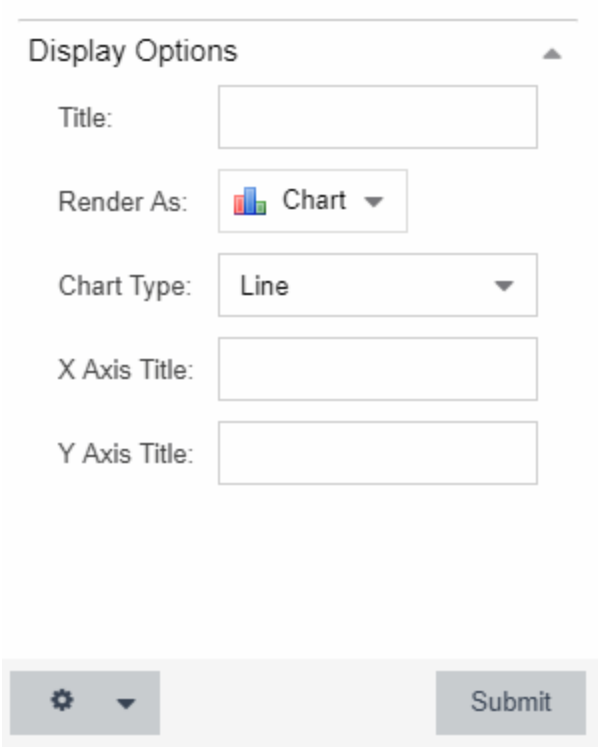
Create a New Component

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.

Related Information

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

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 three authentication methods available: OS Authentication (the default), LDAP Authentication, RADIUS Authentication, and TACACS+ 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 three tiers of licenses for ExtremeCloud IQ - Site Engine and devices:

- Pilot
- Navigator
- No License

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 **Used Pilot**, **Used Navigator**, and **Used NAC** boxes show the total number of devices used against each type of license.

Via the **Licenses** tab, you can add licenses by adding license keys manually.

Source
The origin of the license. Licenses can be managed in ExtremeCloud IQ or in Management Center, when added manually.

Feature
The feature in ExtremeCloud IQ - Site Engine for which the license is providing access. This column displays XIQ-PIL-S-C for Pilot licenses, XIQ-NAV-S-C for Navigator licenses, NetSightEval for evaluation licenses, and XIQ-NAC-S for Access Control licenses.

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 the **Options** tab (**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

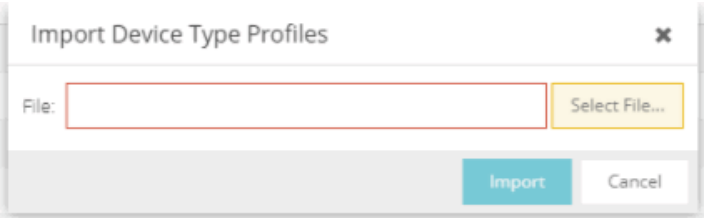
Select a the arrow at the right of a column heading in the table to expand a column function drop-down list. This column heading drop-down list includes Sort, Columns, and Filter column functions, as well as the following functions:

- **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. It provides a Server Licenses report that displays all server licenses and enables you to export end-system events for a particular date range in a log file.
- **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.

Related Information

For information on the other ExtremeCloud IQ - Site Engine tabs:

- Alarms and Events
- Devices

- Reports
- Wireless

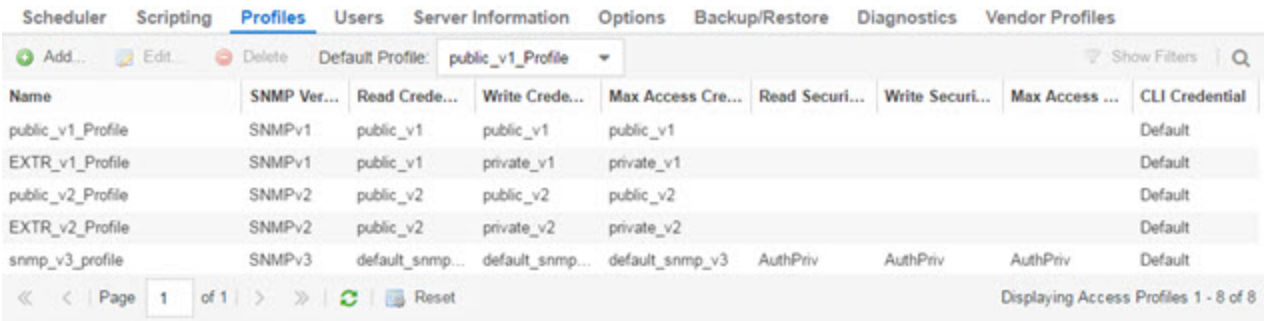
Profiles

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 SNMPv1or 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 SNMPv1or SNMPv2c, these columns do not apply.

CLI Credential
The CLI credential specified for the profile.

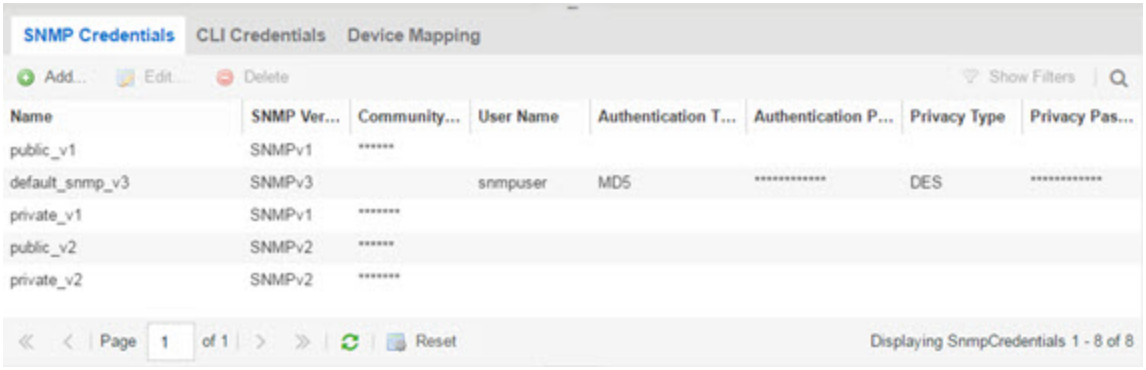
Add Button
Opens the Add/ Edit Profile window where you can select the SNMP version and define the profile name and passwords/ community names used by the profile.

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 SNMPv1or 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 or DES) and passwords used by the credential.

Add Button

Opens the Add/ Edit SNMP Credential window where you can define new SNMP credentials.

Edit Button

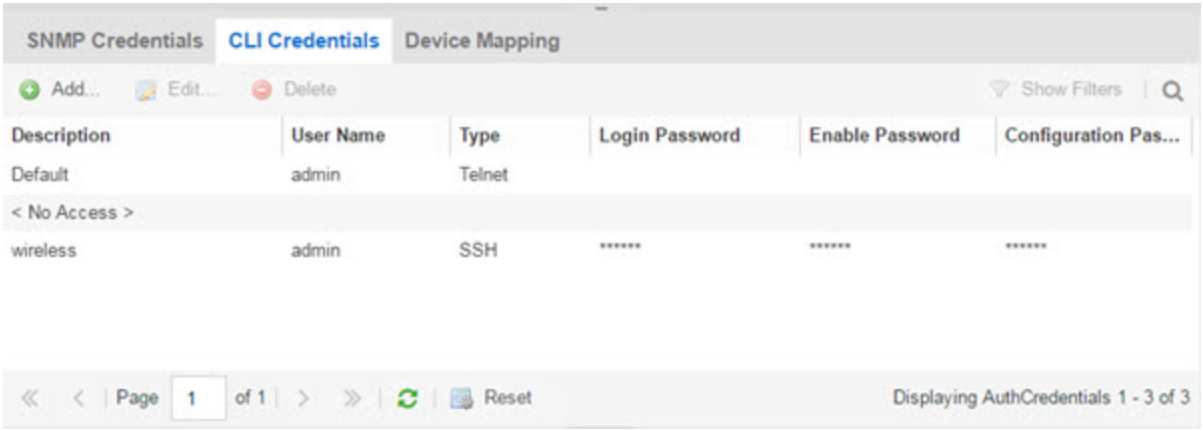
Opens the Add/ Edit Credential window where you can modify a credential selected from the SNMP Credentials table.

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.

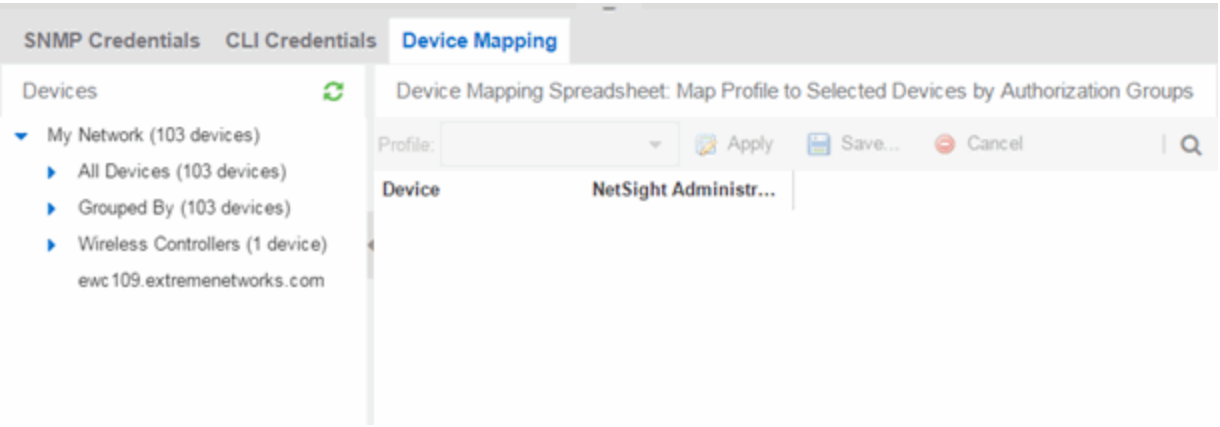
Edit Button
Opens the Add/ Edit CLI Credential window where you can modify a CLI credential selected from the CLI Credentials table.

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.



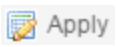
Device Tree

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 Save...

Saves your changes on the device or devices selected.

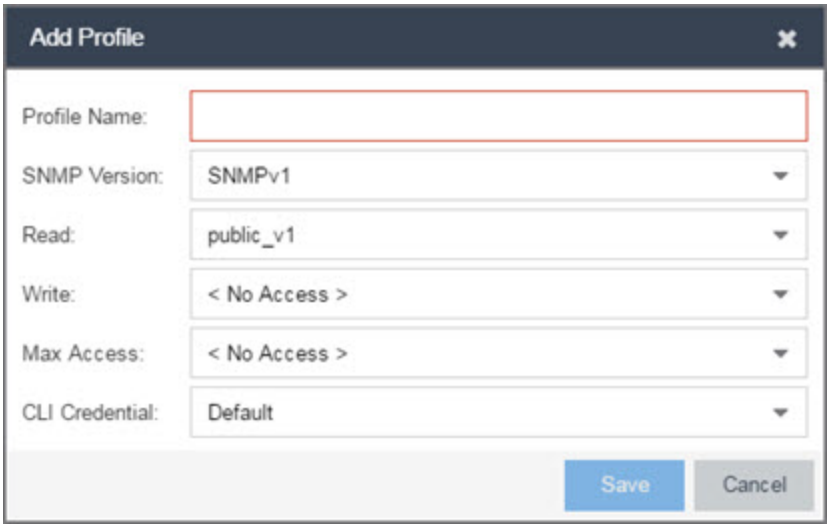
Cancel Button Cancel

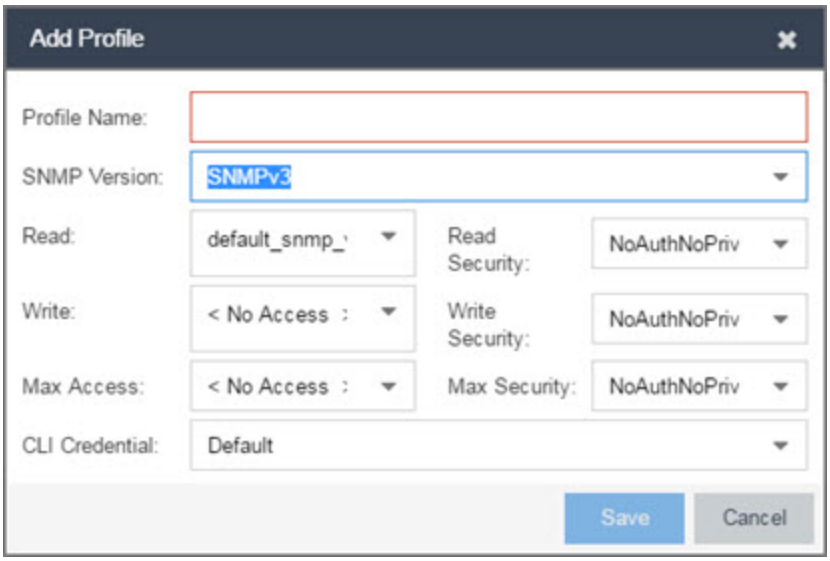
Discards your unsaved changes.

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 contain SSH CLI credentials for the controller. 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 SNMPv1or 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:

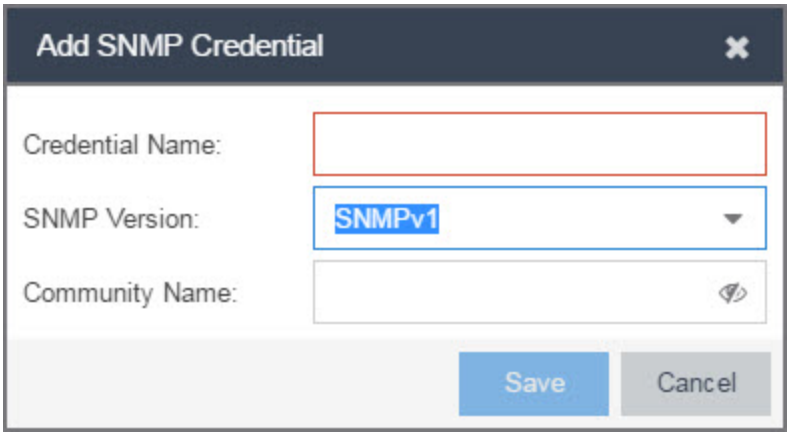
- AuthPriv —Highest security level requiring authentication and privacy (encrypted information).
- AuthNoPriv —Requires authentication, but unencrypted information.
- NoAuthNoPriv —Neither authentication nor privacy required.

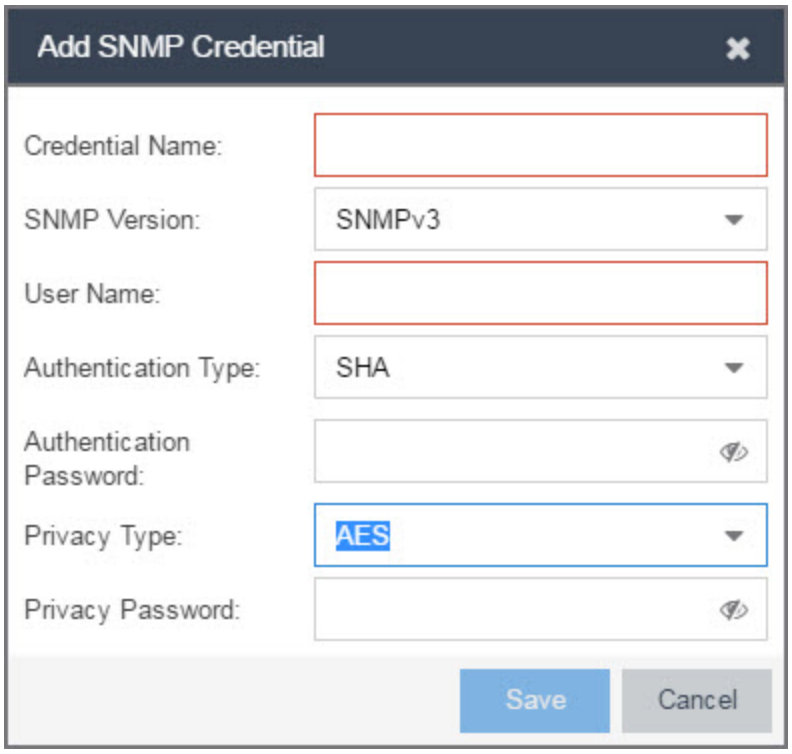
CLI Credential

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 SNMPv1or 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 SNMPv1or 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 1and 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

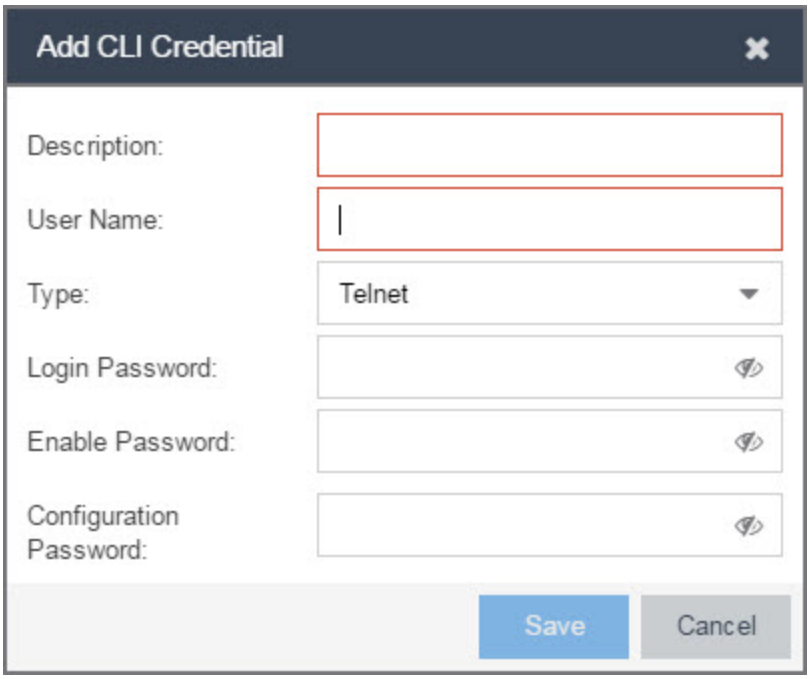
For SNMPv3 credentials, select DES or None from this drop-down list.

Privacy Password

This is the password (between 1and 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 Login password must be added 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.

Related Information

For information on related windows:

- Users/ Groups Tab
- Site Tab

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.

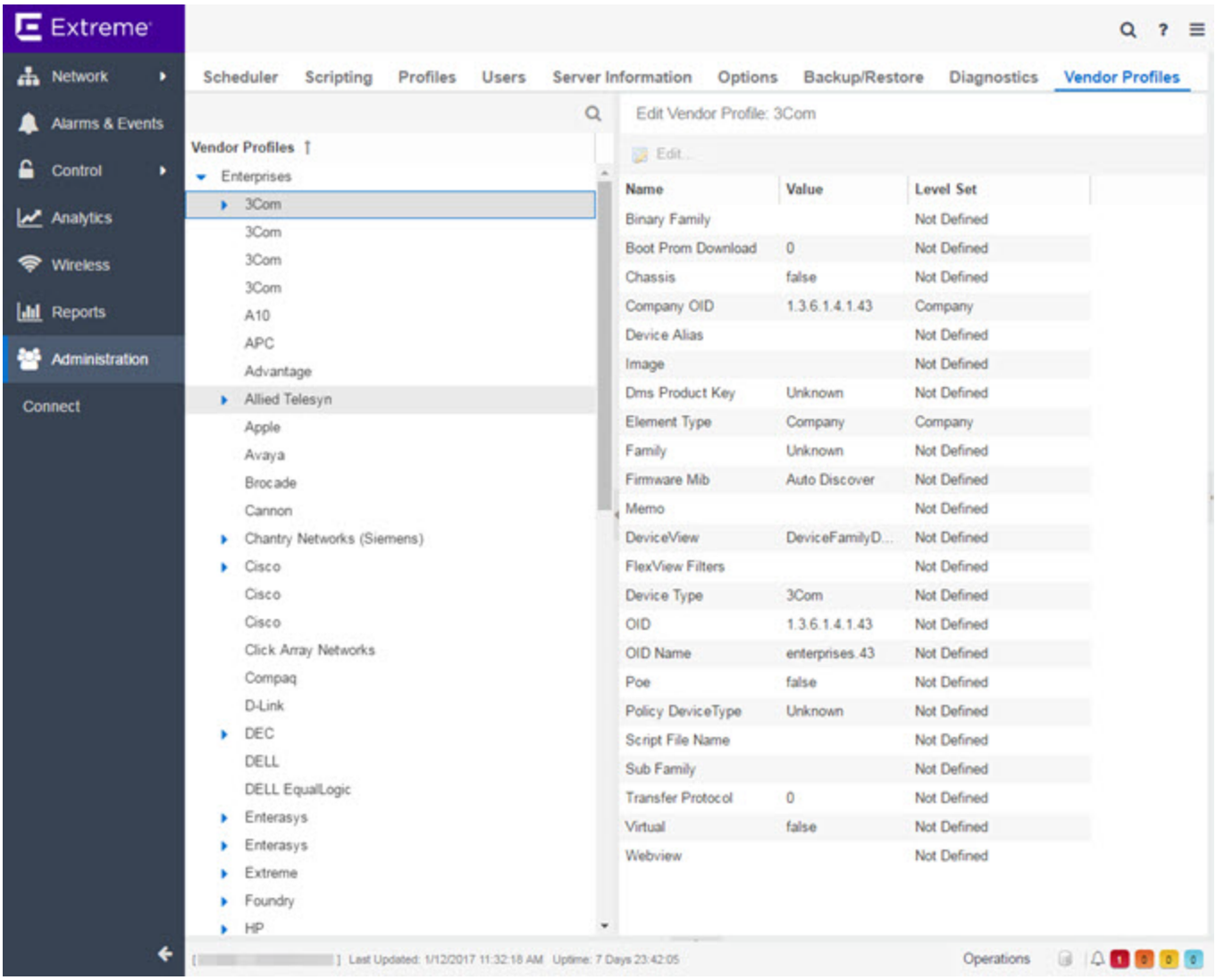
Vendor Profiles are a beta feature. To enable vendor profile functionality, contact Extreme Networks' Global Technical Assistance Center (GTAC).

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.

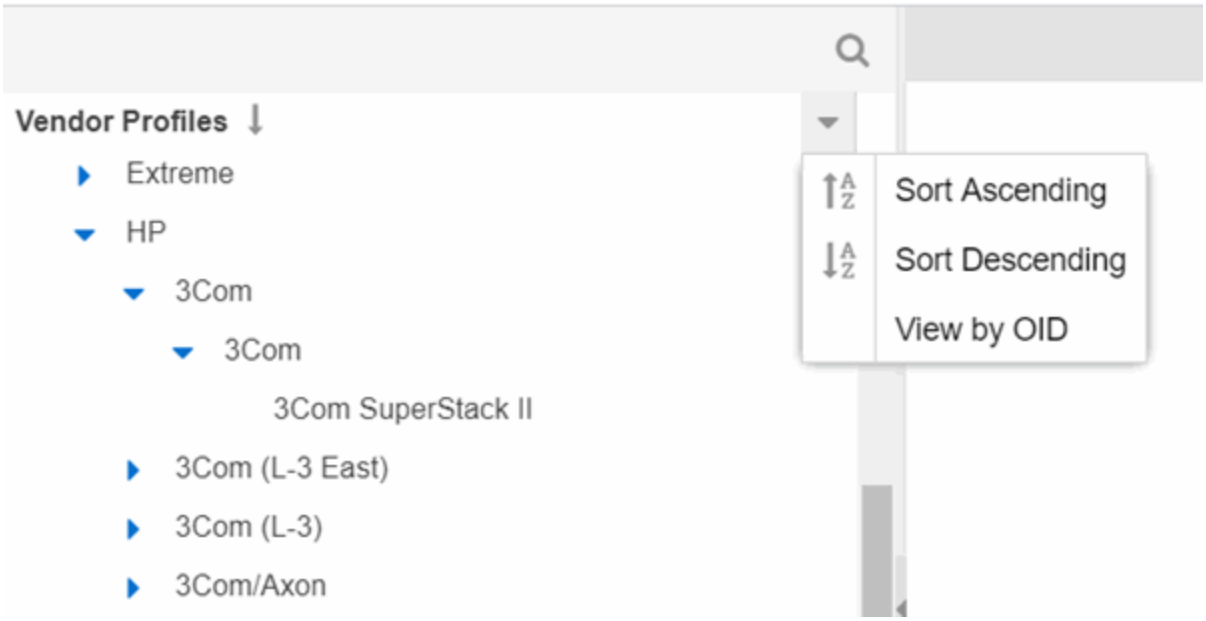
The **Vendor Profiles** tab is organized into two panels. The left panel contains a list of vendors and companies that manufacture networking devices. Nested within the company folder, if a device is part of a series of devices (known in ExtremeCloud IQ - Site Engine as a device family), are folders 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

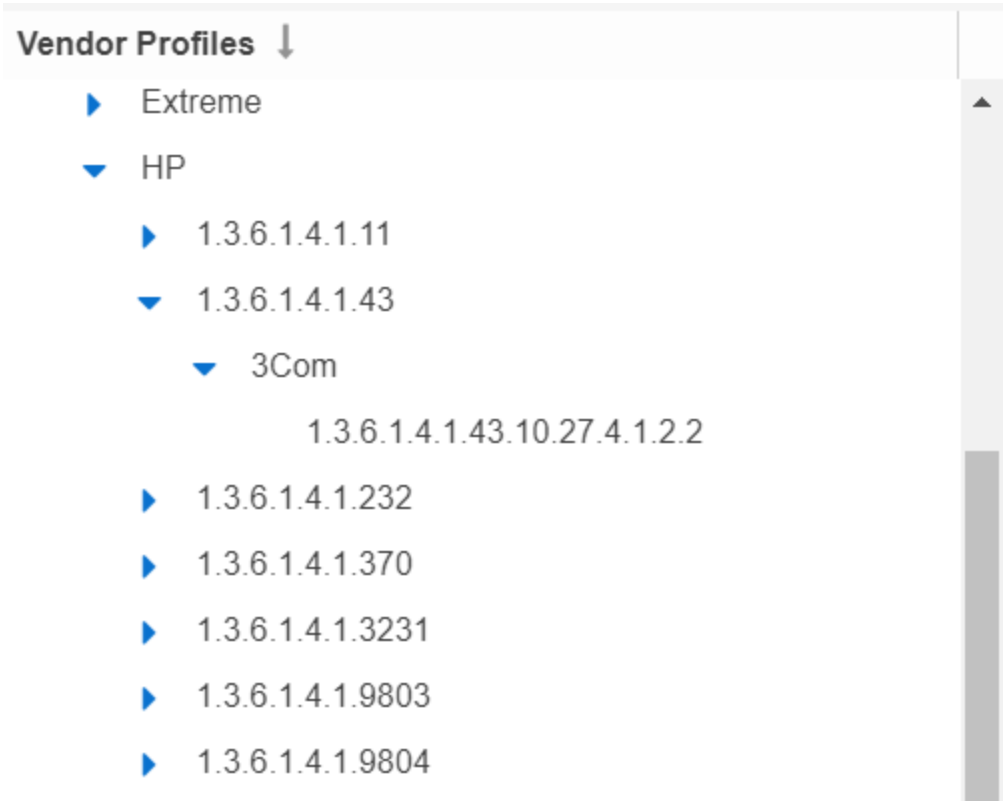
The left-panel of the **Vendor Profiles** tab contains a list of device vendors, displayed in alphabetical order. Select the drop-down list in the left-panel Vendor Profiles field to display the following options:



- **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.

Related Information

For information on related windows:

- Users/ Groups Tab
- Site Tab

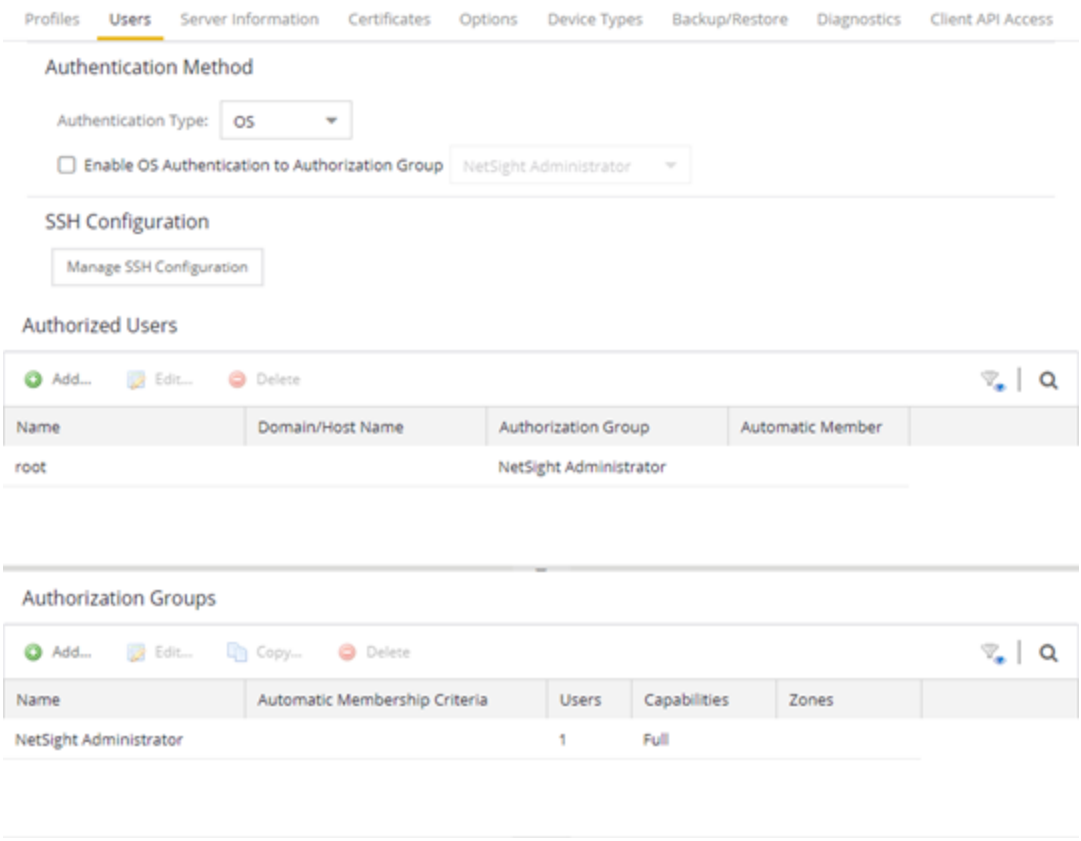
Users

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 four authentication methods available: OS Authentication (the default), LDAP Authentication, RADIUS Authentication, and TACACS+ 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.

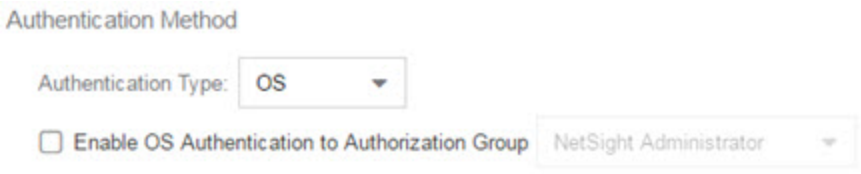
The following authentication methods are available:

- OS Authentication *(the default)*
- LDAP Authentication
- RADIUS Authentication
- TACACS+ Authentication

WARNING: Changes to the **Authentication Type** are automatically saved to the server, which can prevent access to users.

OS Authentication (Default)

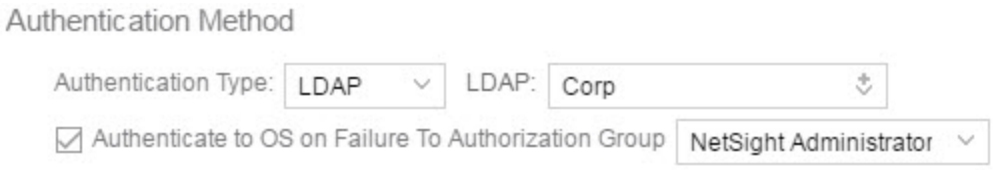
With this authentication method, the ExtremeCloud IQ - Site Engine Server uses the underlying host operating system to authenticate users. Use the Authorized Users table to create a list of users allowed access and define their access capabilities.



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 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.

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.

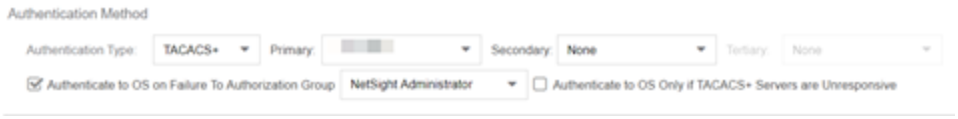
With RADIUS Authentication, configure dynamic assignment of users to authorization groups based on the attributes associated with a user in Active Directory. When a user authenticates, the attributes associated with that user are matched against a list of criteria specified as part of each authorization 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.

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.

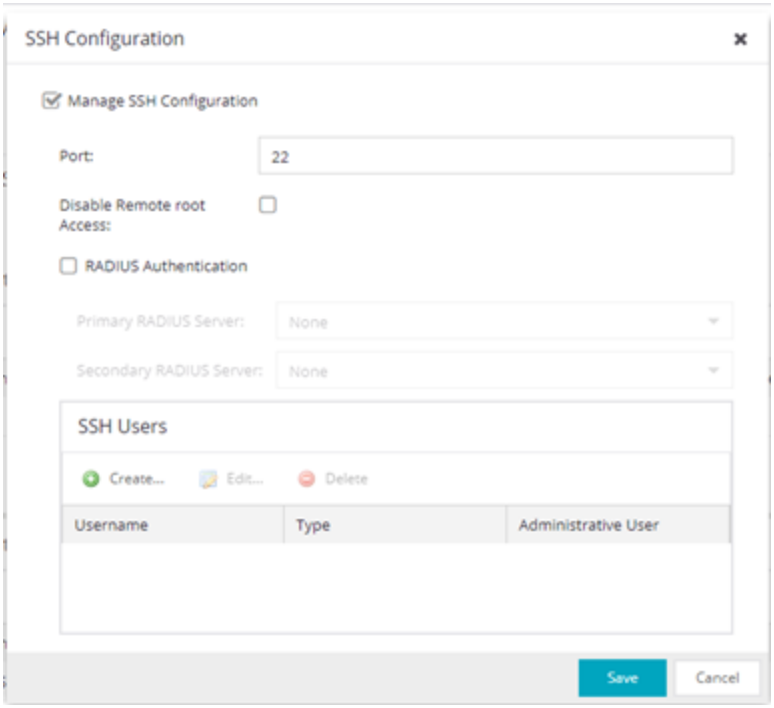
ExtremeCloud IQ - Site Engine attempts to authenticate a client from the primary to the secondary and to the tertiary server in the event of communicating to the TACACS+ server. However, if a TACACS+ server responds with any status, the client does not fall through to the next server.

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.

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.



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.

SSH Users Table

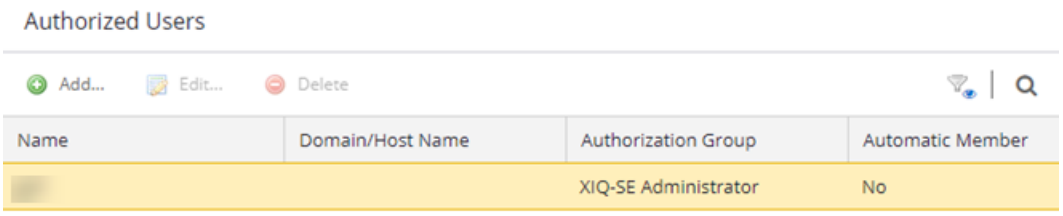
Use the toolbar buttons to create a list of users allowed to log in to the ExtremeCloud IQ - Site Engine engine using SSH. You can add Local and RADIUS users and grant the user Administrative privileges, if appropriate. A user that is granted administrative rights can run sudo commands and commands that 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 via LDAP, RADIUS, or TACACS+ 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.

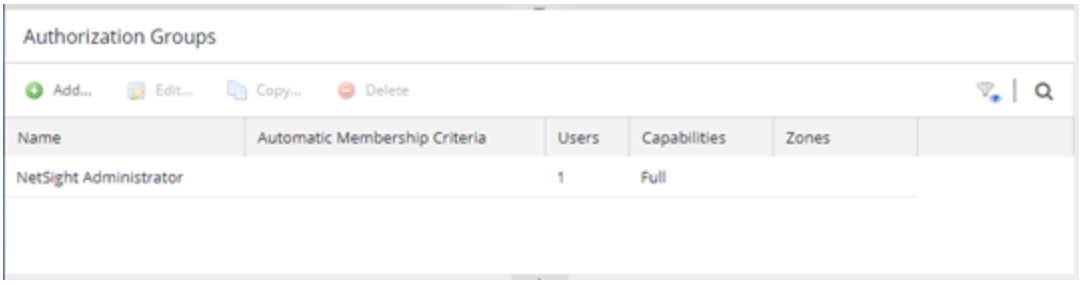
Add
Opens the Add/ Edit User window, which allows you to define the username, domain, and authorization group for a new authorized user.

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.

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.

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.

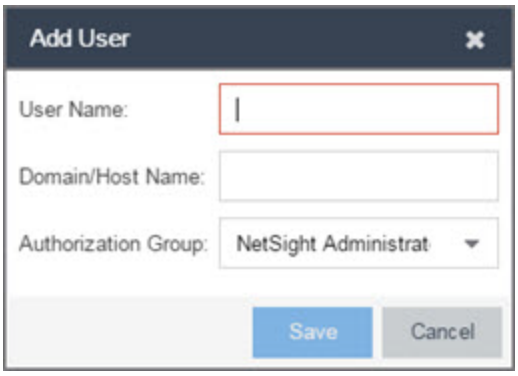
Delete
Removes the selected group from the Groups table.

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

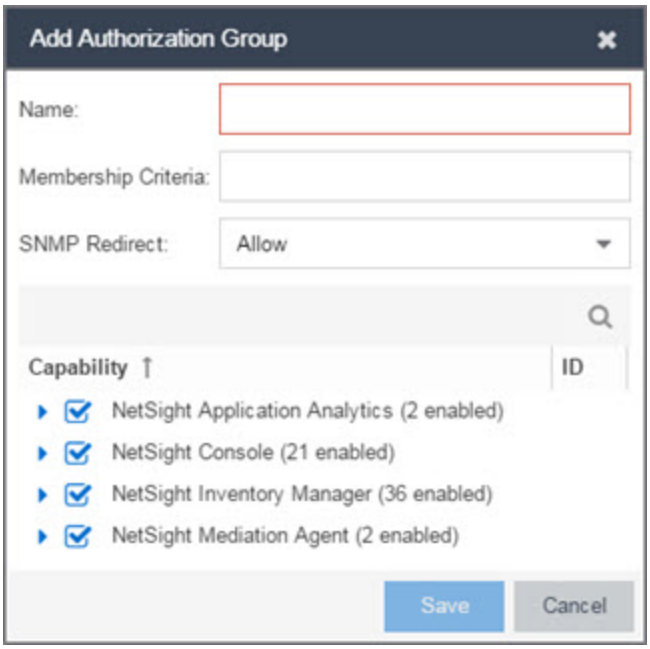
The user's domain/ hostname used to authenticate to the ExtremeCloud IQ - Site Engine database.

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.

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.

Related Information

For information on related windows:

- Profiles/ Credentials Tab
- Site Tab

How to 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 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.

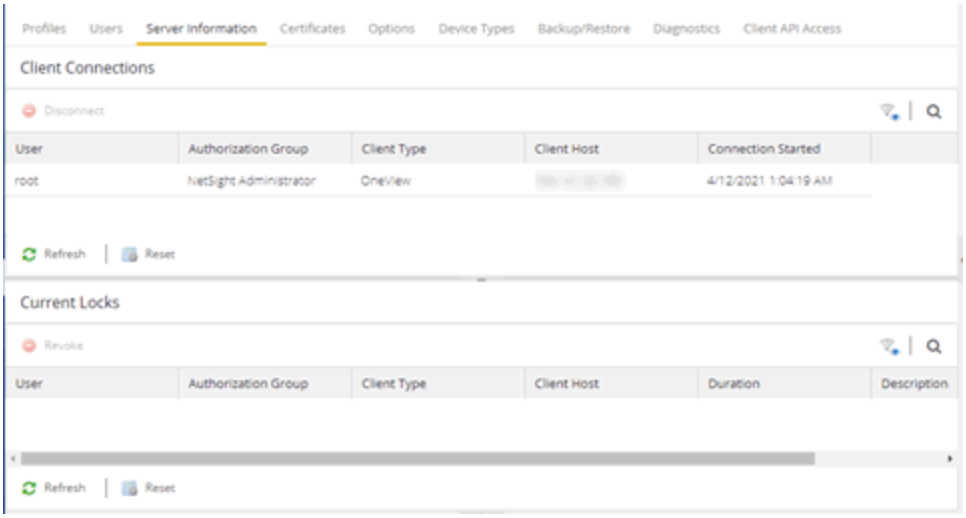
Related Information

For information on related topics:

- Users
- Authorization Group Capabilities

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.

Related Information

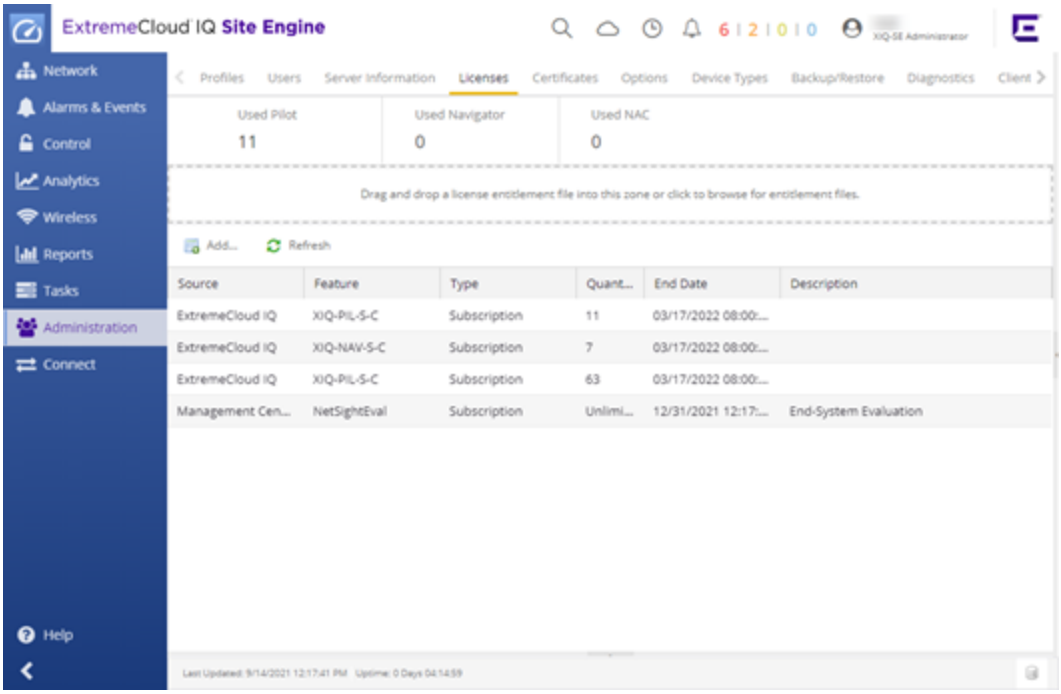
For information on related tabs:

- Users

Updating a License

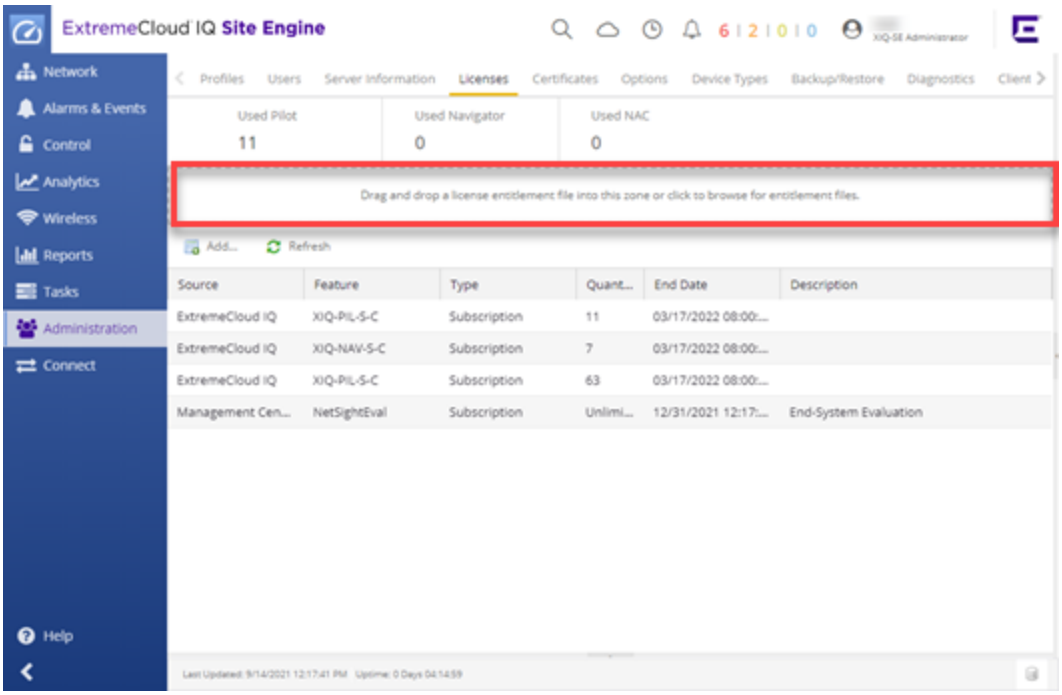
This Help topic provides instructions for updating a license in ExtremeCloud IQ - Site Engine.

1 In ExtremeCloud IQ - Site Engine, access the **Administration** > **Licenses** tab.



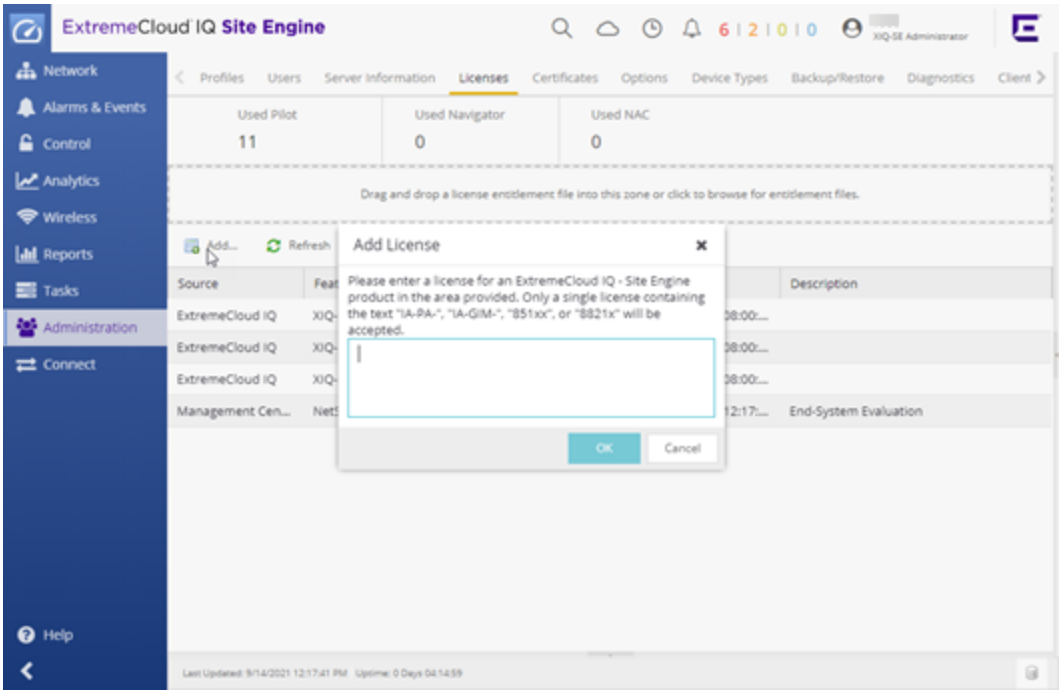
2. Drag and drop any license entitlement files in the open box above the table.

NOTE: License entitlement file functionality (Air Gap mode licensing) is not available in this release.



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-", "IA-GIM", "851xx", or "8821x".

3. Select **OK**.
4. Select the **Add** button and continue entering additional licenses one at a time.

Your licenses are updated.

Related Information

For information on related windows:

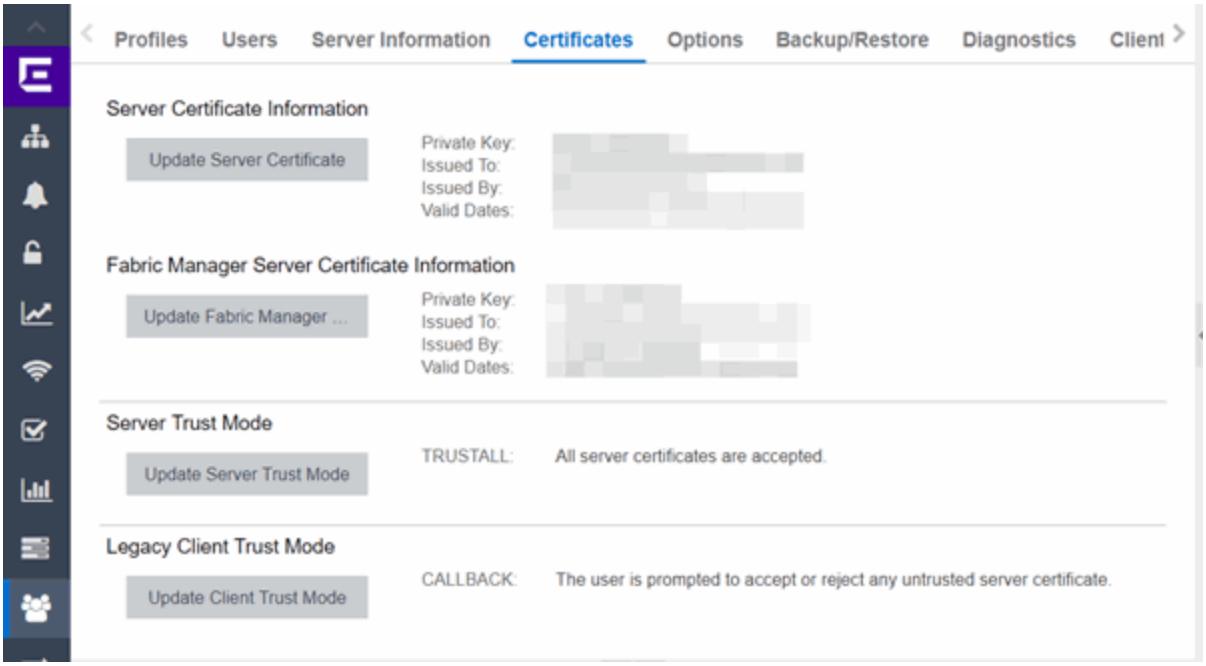
- Administration

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.

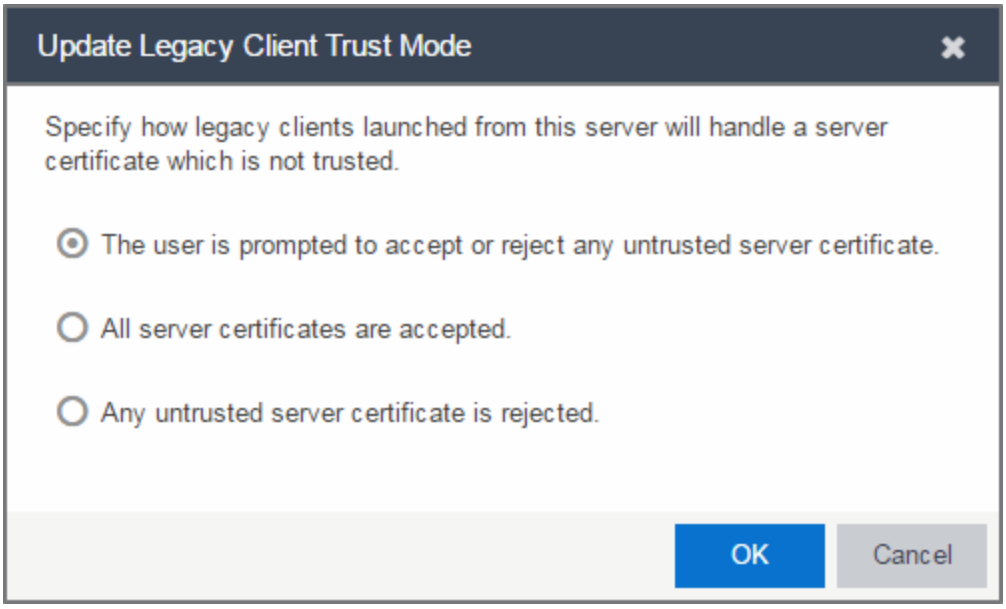
Related Information

For information on related windows:

- 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.

Related Information

For information on related windows:

- 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.

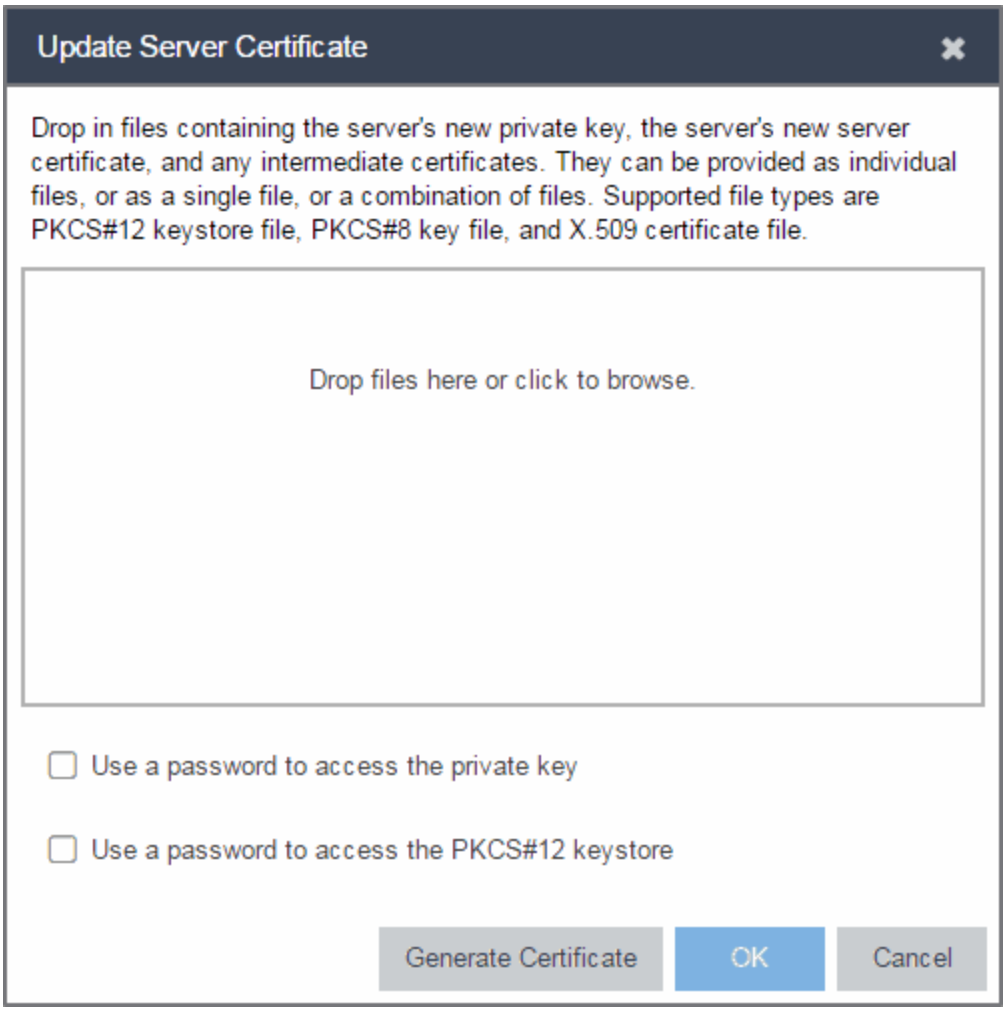
During installation, ExtremeCloud IQ - Site Engine generates a unique private server key and server certificate. While these provide secure communication, there can be cases where you want to update the ExtremeCloud IQ - Site Engine server certificate to a custom certificate provided from an external 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.

Related Information

For information on related topics:

- Certificates Tab
- Update Server Certificate Trust Mode Window
- Update Client Certificate Trust Mode Window

Add Fabric Manager Certificate Window

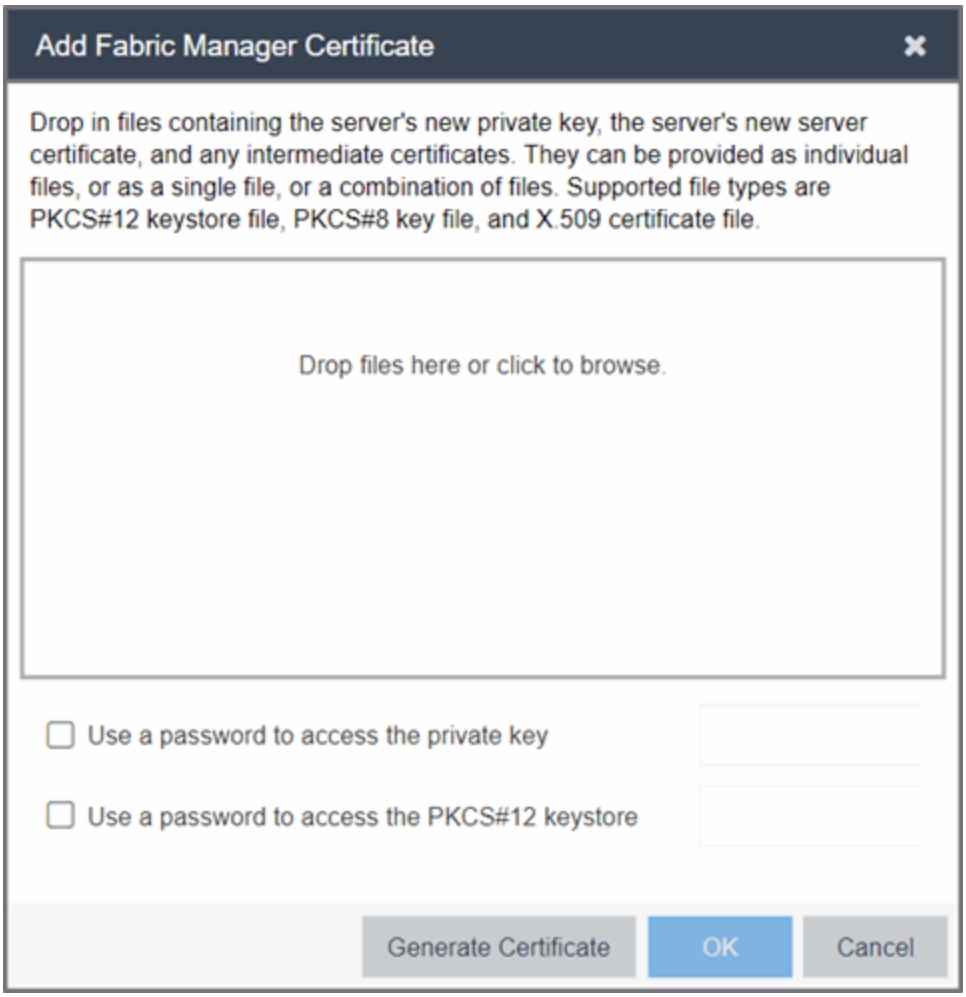
The Fabric Manager server uses a private key and server certificate to provide secure communication for administrative web pages, ExtremeCloud IQ - Site Engine Dashboard tools, and for internal communication between servers. Use the Add Fabric Manager Certificate window to replace the Fabric Manager 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.

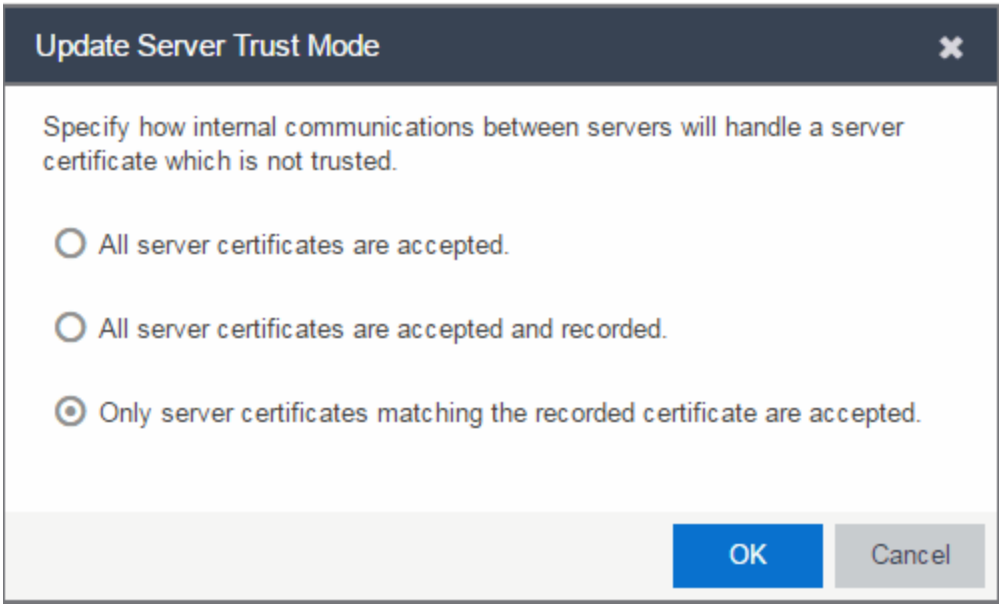
Related Information

For information on related topics:

- 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 ExtremeControl. For example, there is the ExtremeCloud IQ - Site Engine server, the ExtremeControl engine servers, and ExtremeControl assessment servers. In addition, there can be external servers such as LDAP servers with which both ExtremeCloud IQ - Site Engine and ExtremeControl 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/ ExtremeControl 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 ExtremeControl 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 ExtremeControl.

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. ExtremeControl 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.

Related Information

For information on related topics:

- 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

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.

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 -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://<NetSight Server FQDN>:8443/Monitor/jsp/nac/dashboard.jsp`. or the ExtremeCloud IQ - Site Engine web page at `https://<NetSight 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: View > Security Report > View Certificates
   - Mozilla Firefox 3.5 or later: Tools > Page Info > Security > View Certificates

Use OpenSSL

1. Use OpenSSL to test the server connection with the following command:
   ```
   openssl s_client -connect <NetSight 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.

You need to:

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 -out <file_name>.key
      ```

      For example:

      ```
      openssl genrsa 2048 | openssl pkcs8 -v1 PBE-SHA1-RC4-128 -topk8 -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 v15 format using the following command:

```
openssl pkcs8 -v1 PBE-SHA1-RC4-128 -in <original_key_
file> -topk8 -out <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 1above as the input file, and specify the output file name you prefer:

   ```
   openssl req -new -key <input file> -out <output
   file>
   ```

   For example:

   ```
   openssl req -new -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.

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:

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 and changing an end-system's group membership.
- 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.
- 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:

NetSight (ExtremeCloud IQ - Site Engine) Console > Wireless Manager > Launch
Adds the ability to view the **Wireless** tab.

NetSight (ExtremeCloud IQ - Site Engine) Suite > Devices > Add, Discover and Import
Adds the ability to add devices in the **Network** tab.

NetSight (ExtremeCloud IQ - Site Engine) 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

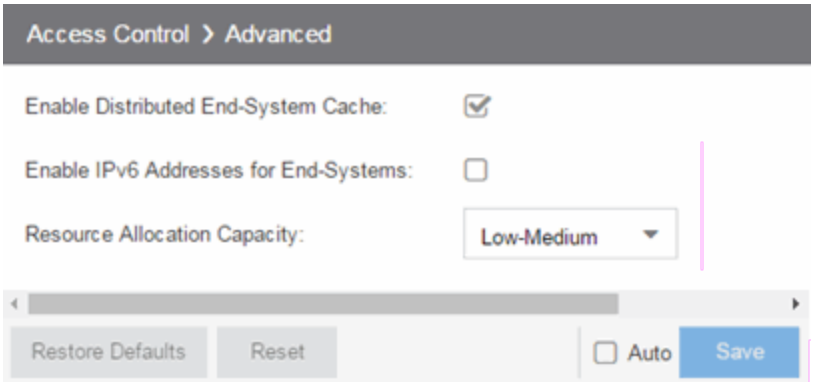
Selecting Access Control in the left panel of the **Options** tab provides the following view, where you can edit settings associated with the **Control** > **Access Control** tab. The right-panel view changes depending on what you select in the left-panel tree. Expand the Access Control tree to view 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

Use this view to configure advanced settings for the Access Control tab.



Enable Distributed End-System Cache

The **Enable Distributed End-System Cache** option is intended for large enterprise environments as a way to improve response times when handling end-system mobility. Enabling this option improves ExtremeControl performance when discovering new end-systems as they connect, or when end-systems move from one place to another in the network.

To use the end-system cache feature, it must be enabled on both the ExtremeCloud IQ - Site Engine Server (using this option) and on the ExtremeControl engines using the cache.

When this feature is enabled, the ExtremeCloud IQ - Site Engine Server and the ExtremeControl engine exchange additional data each time end-system data is updated. This feature is **not** recommended unless there is sufficient network bandwidth for the additional data, a fast connection between the ExtremeCloud IQ - Site Engine Server and the ExtremeControl engine, and end-systems are adding or moving frequently.

Enable IPv6 Addresses for End-Systems

The **Enable IPv6 Addresses for End-Systems** option enables ExtremeControl 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.

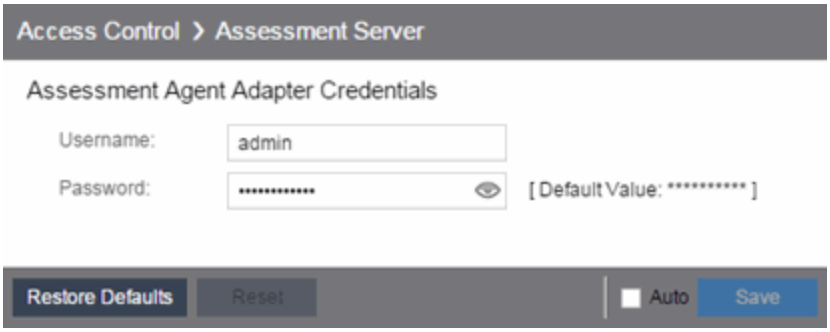
Resource Allocation Capacity

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 ExtremeControl 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 Server

Use these options to provide assessment agent adapter credentials.

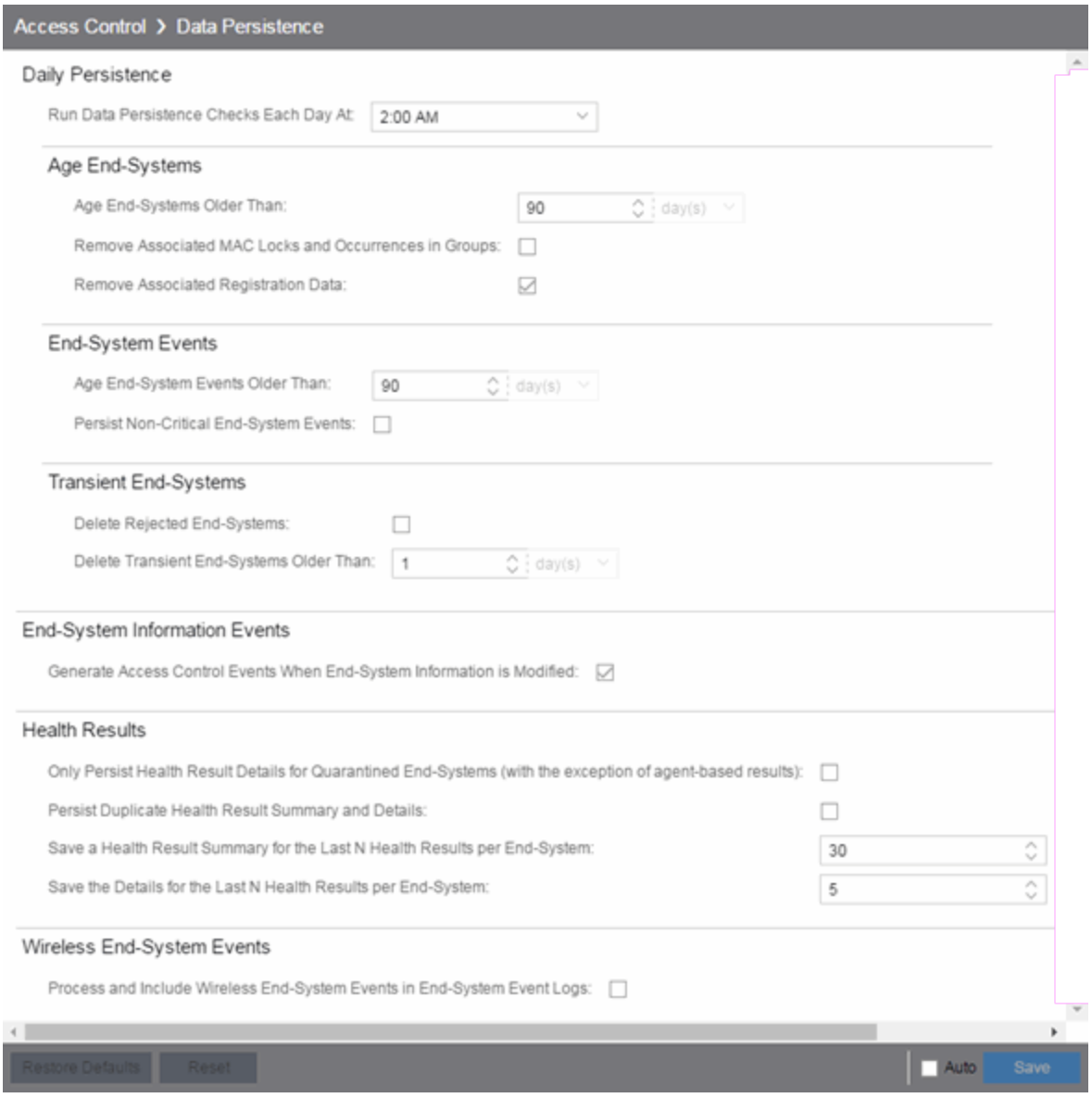


Assessment Agent Adapter Credentials

Specify the username and password the ExtremeControl 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 ExtremeControl 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 1day. 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 ExtremeControl Events When End-System Information is Modified
Select the checkbox if you want ExtremeControl 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.

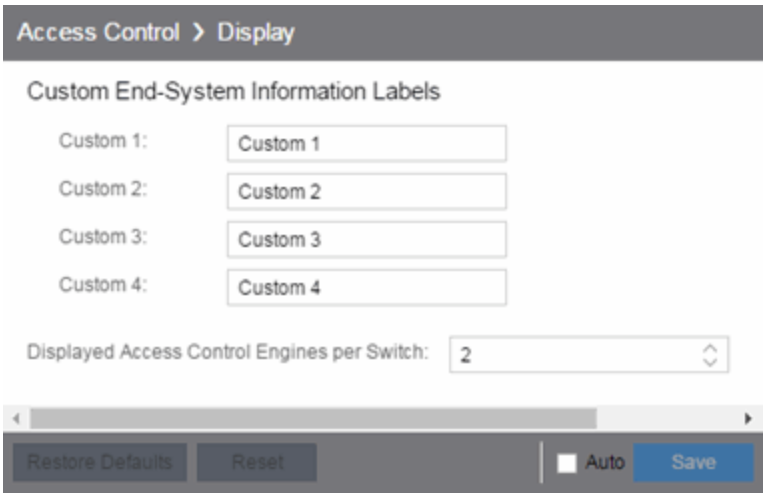
Save the Details for the Last N Health Results per End-System
Specify how many health (assessment) result details are saved and displayed in the End-Systems tab for each end-system. By default, the Data Persistence check saves detailed information for the last five health results per end-system.

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 ExtremeControl Gateways you can select when adding or editing a switch in an ExtremeControl 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.

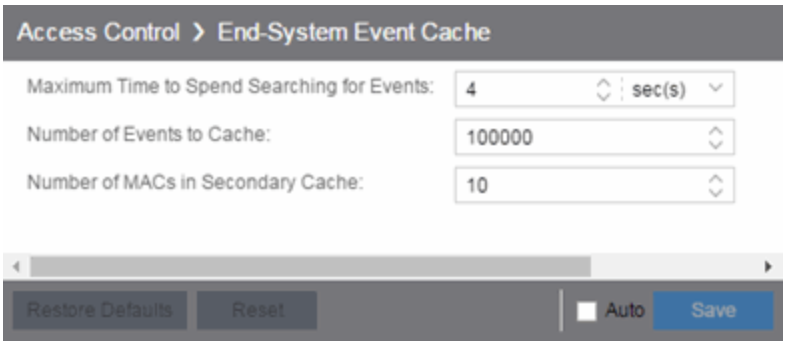
Displayed ExtremeControl Engines per Switch

Select the number of ExtremeControl engines displayed in the Add Switches to Group or Edit Switches in Group windows. By default, these windows enable you to configure two ExtremeControl 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**.

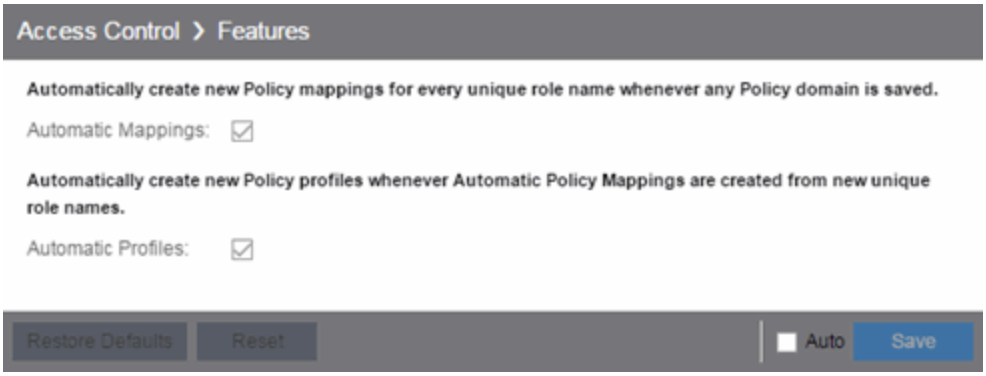
When an engine configuration audit is performed during an Enforce operation, warning messages can display in the audit results listed in the Enforce window. If there is a warning associated with an engine, you are given the option to acknowledge the warning and proceed with the enforce anyway.

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 ExtremeControl 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.

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 ExtremeControl windows.



Notification Engine

Use this panel to define the default content contained in ExtremeControl 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 ExtremeControl 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.

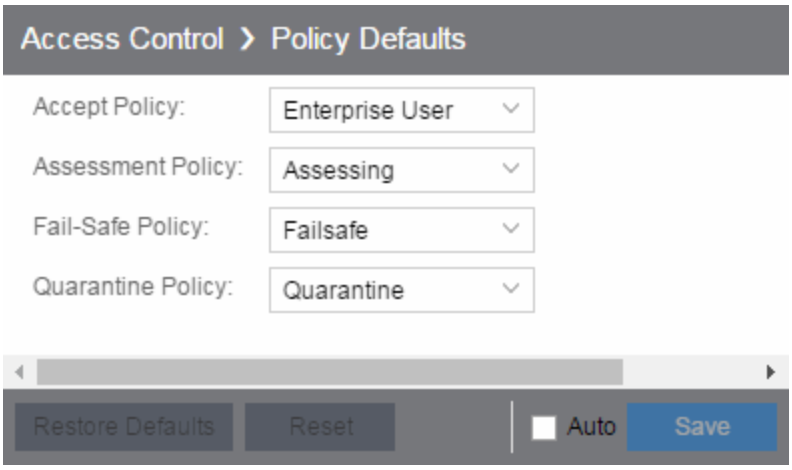
Maximum Events Queuable in Service Period
This limits the rate that events can be added to the queue (not processed from the queue) and protects the event engine against a large amount of events arriving too quickly. If events arrive at a rate that exceeds this amount, they are discarded.

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 ExtremeControl 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 ExtremeControl 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

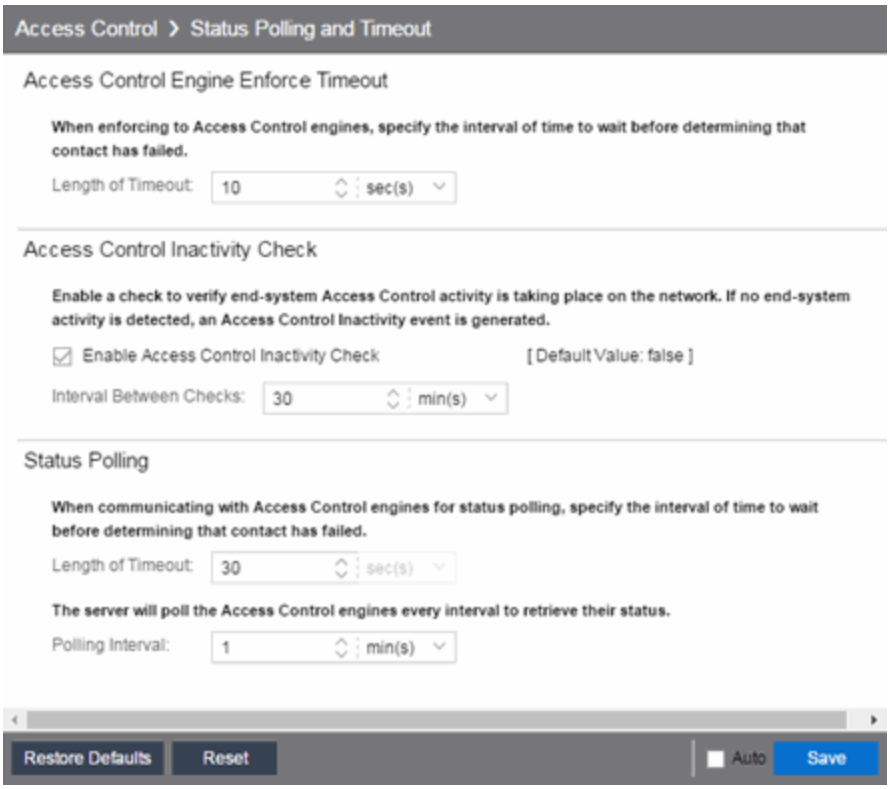
Select the default fail-safe policy. The fail-safe policy is applied to an end-system if the end-system's IP address cannot be determined from its MAC address, or if there is a scanning error and an assessment of the end-system could not take place.

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 ExtremeControl engines.



ExtremeControl Engine Enforce Timeout

When enforcing to ExtremeControl 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.

ExtremeControl 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 ExtremeControl Inactivity event is

sent to the Events view. Use the **Alarms and Events** tab to configure custom alarm criteria based on the ExtremeControl Inactivity event to create an alarm, if desired.

Status Polling

Length of Timeout —When communicating with ExtremeControl 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 ExtremeControl engines to determine engine status.

Related Information

For information on related topics:

- ExtremeControl

Alarm Options

Selecting Alarm in the left panel of the **Options** tab provides the following view, where you can configure alarm settings.

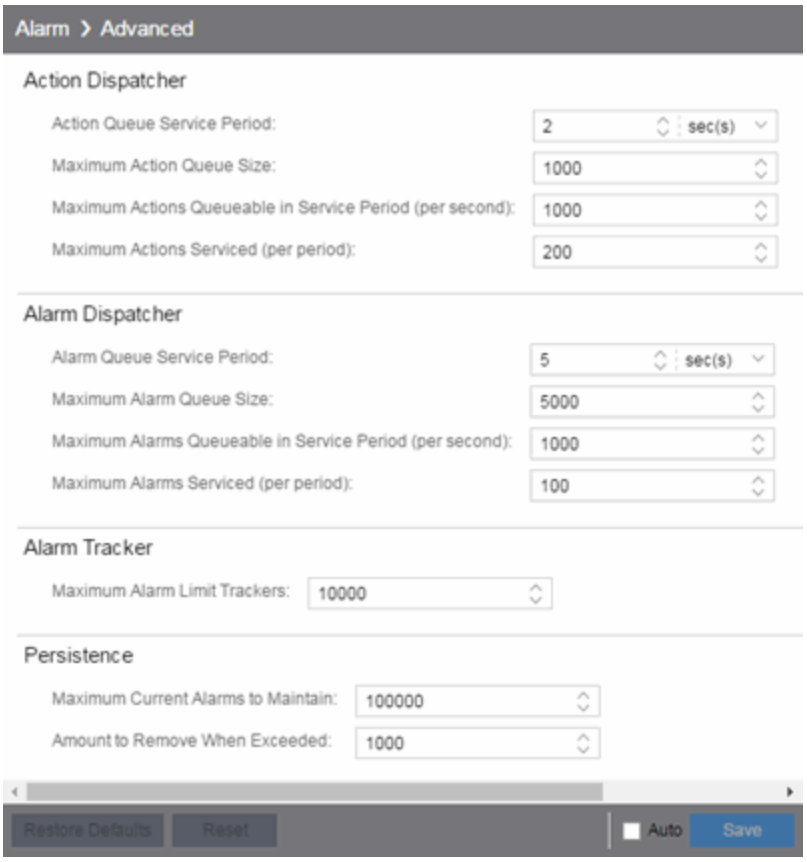
Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.

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

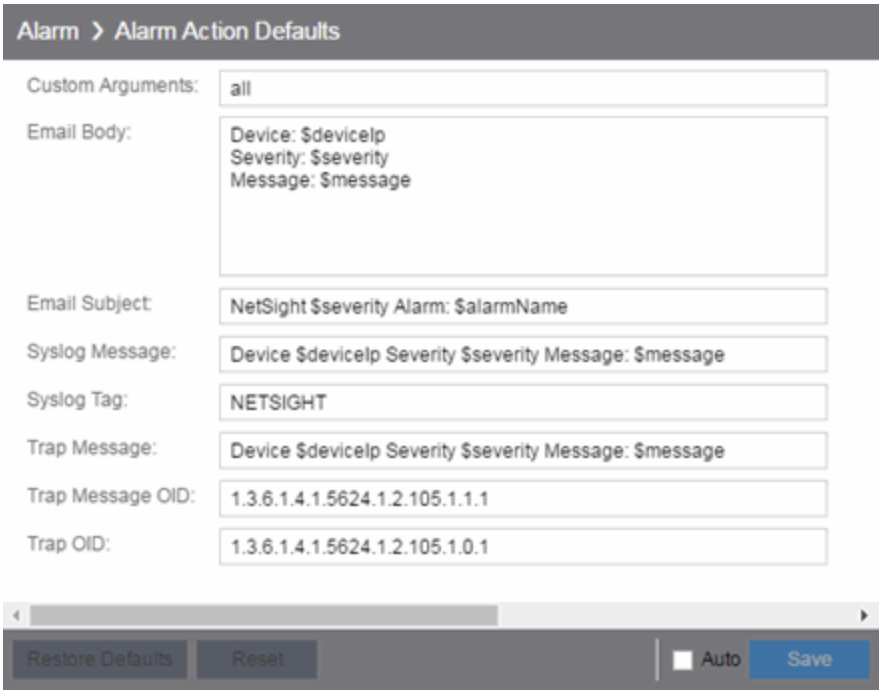
When you define an alarm with a limit, ExtremeCloud IQ - Site Engine tracks whether the limit is exceeded and when to reset the count. Use this option to set the maximum number of alarms that ExtremeCloud IQ - Site Engine tracks. (An alarm limit specifies the number of times the alarm action performed 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.

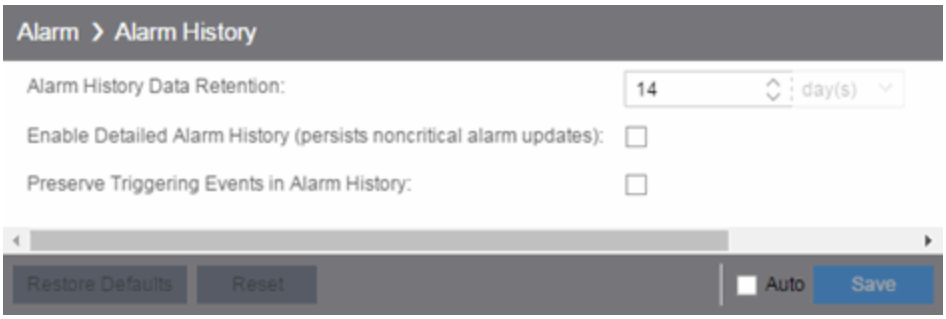
Trap Message
The varbind sent in the trap.

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.

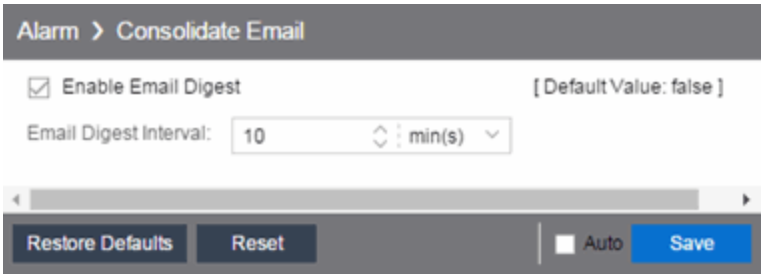
Enable Detailed Alarm History (persists noncritical alarm updates)

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



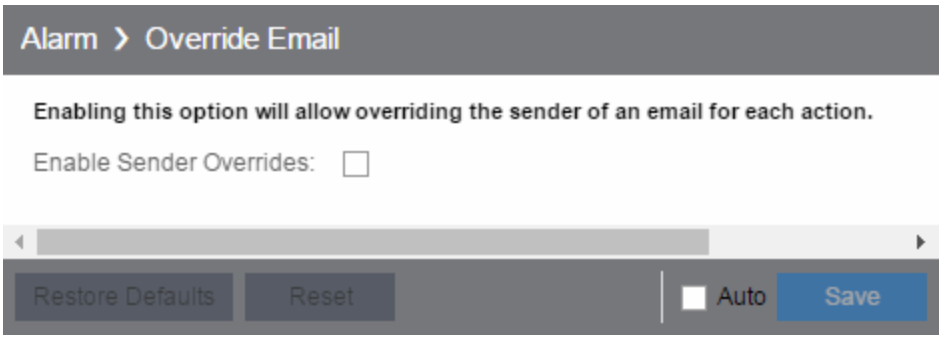
Enable Email Digest

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.

Related Information

For information on related topics:

- Administration

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.

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.

Alarm/Event Logs and Tables

Alarm and Event Host/Port Names

Display Host Name in Source Column When Available: ☐

Resolve Port Name/Alias: ☑

Resolve Source Host Names: ☐

Event Log Entry Date/Time Format

By default, raw timestamp format (1262965697614) is used

Use ISO 8601 Timestamp Format (2010-01-08T18:45UTC): ☐

Event Tables Row Limit (per type)

Retain Rows Count: 9000

Row Count to Remove When Exceeded: 1000

Execute Command Script

Include Script Contents in Execute Command Script Events: ☐

Number of Compliance Engine Logs to Limit

☐ Limit Number of Compliance Engine Log Files Saved

Files to Limit: 20

Number of Event Logs to Limit

☐ Limit Number of Log Files Saved

Files to Limit: 20

Number of Events to Consider for Event Correlation

Number of Events to Consider for Event Correlation: 1000

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 the **Enable Name Resolution** option.)
- **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 the **Enable Name Resolution** option.)

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 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.

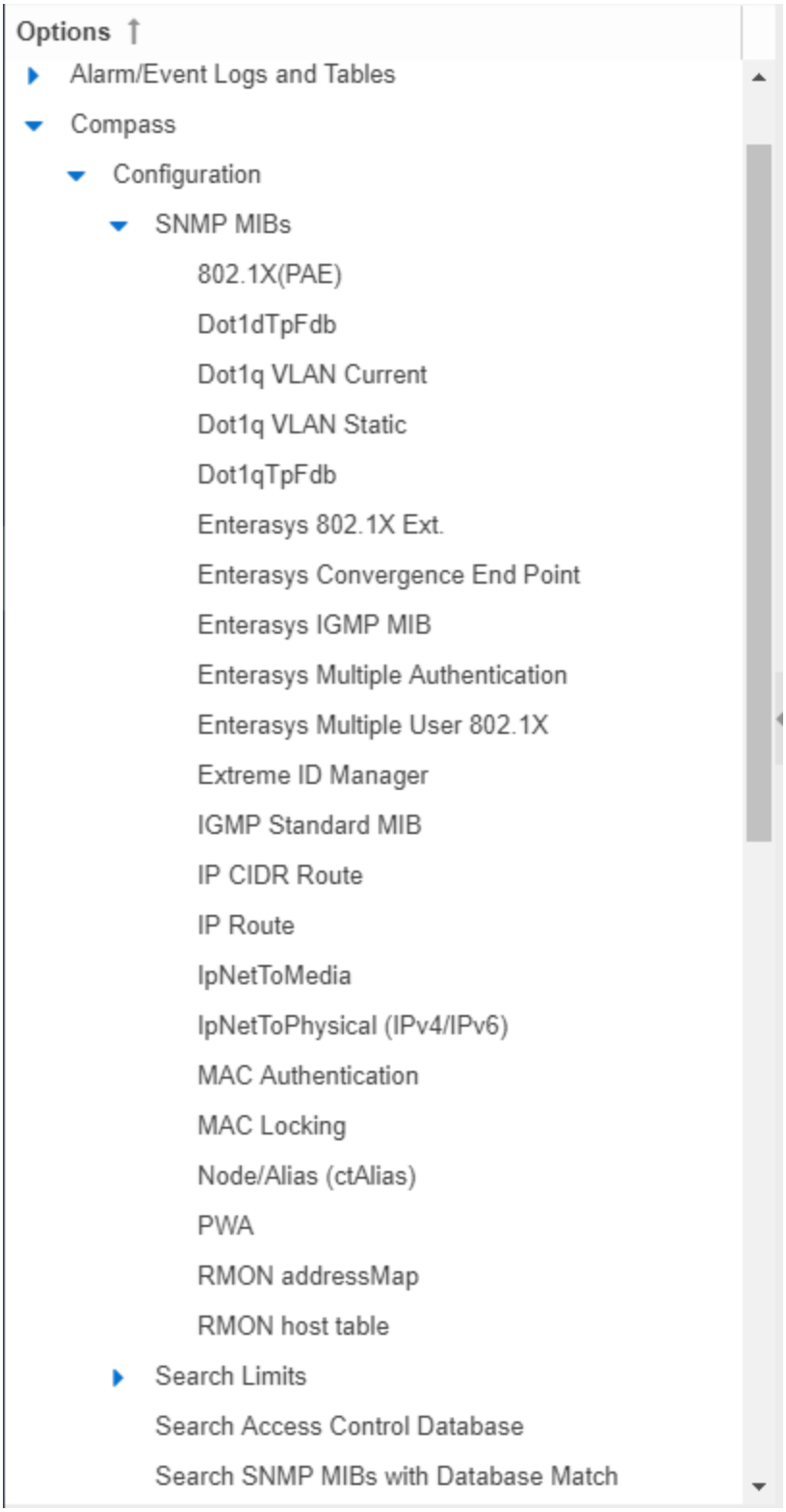
Related Information

For information on related topics:

- Administration

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.


Compass
Configuration
Search Limits
Number of Devices Allowed for a Search: 100
Number of Search Results Allowed: 200
Number of Searches Allowed at Once: 5
Time Limit for a Search: 20 sec(s)
Search Access Control Database
Search SNMP MIBs with Database Match
[Default Value: false]
SNMP MIBs
802.1X(PAE):
[Default Value: true]
Dot1dTpFdb:
[Default Value: true]
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:
Restore Defaults
Reset
Auto
Save

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 ExtremeControl Database

Select this checkbox to include ExtremeControl 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 ExtremeControl Database, the SNMP MIBs are **not** searched unless the **Search SNMP MIBs with Database Match** checkbox is also selected. If the **ExtremeControl** checkbox is deselected, then the ExtremeControl 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.

Related Information

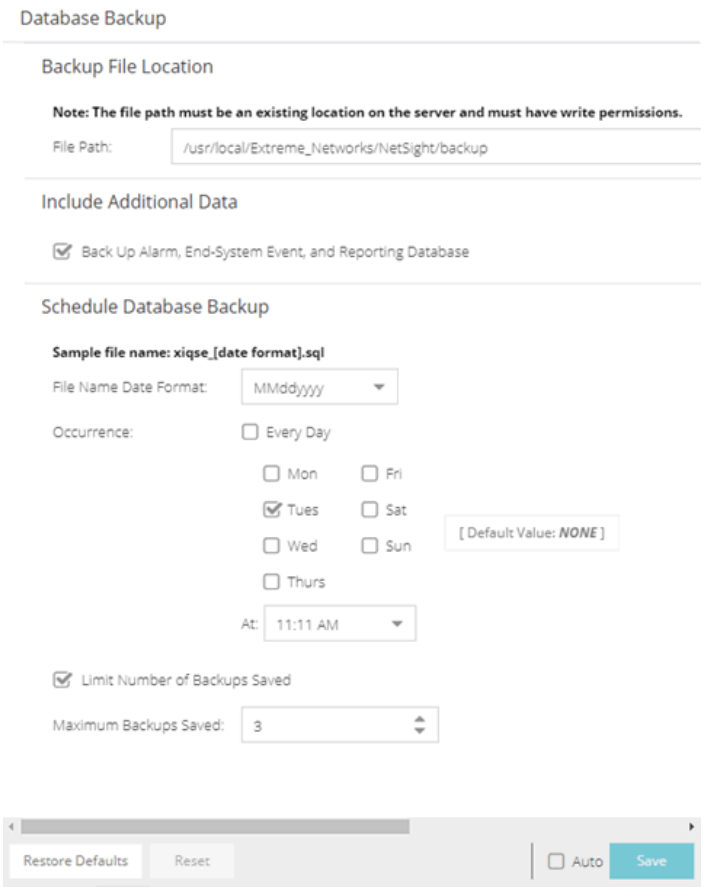
For information on related topics:

- Administration

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 File Location

File Path

The database backup is saved to the directory specified in the **File 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.

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

File 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.

Related Information

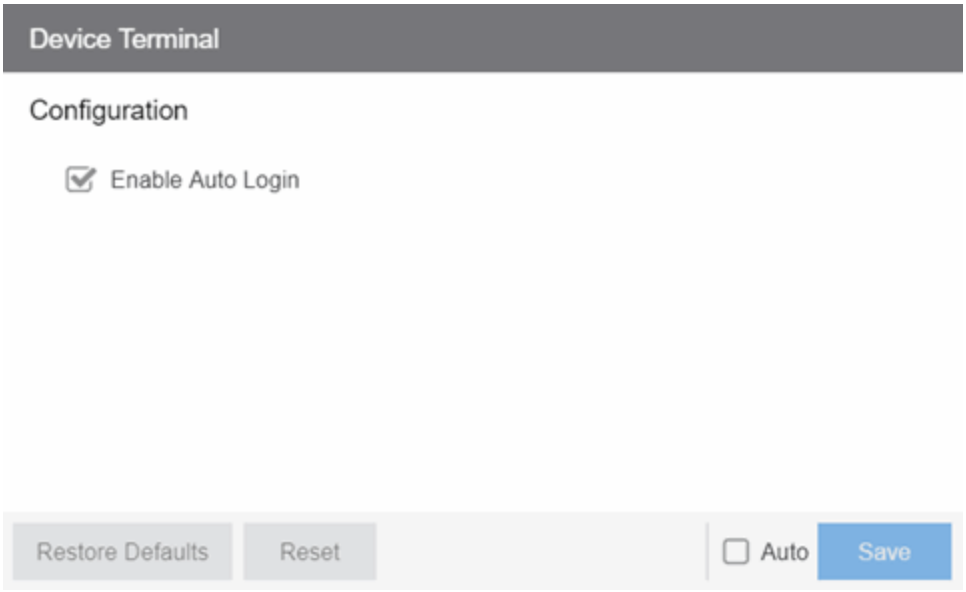
For information on related topics:

- Administration

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.

Related Information

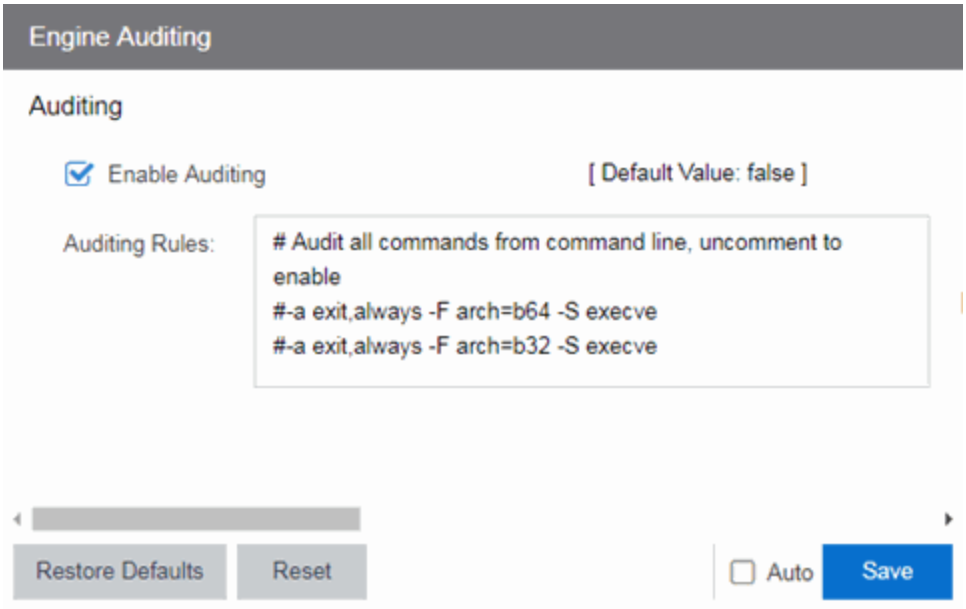
For information on related topics:

- Administration

Engine Auditing Options

Selecting Engine Auditing in the left panel of the **Options** tab provides the following view, where you can enable auditing of users connected to the ExtremeCloud IQ - Site Engine server CLI via SSH.

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 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 users connected to the ExtremeCloud IQ - Site Engine CLI via SSH in the 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 ExtremeCloud IQ - Site Engine CLI.

Related Information

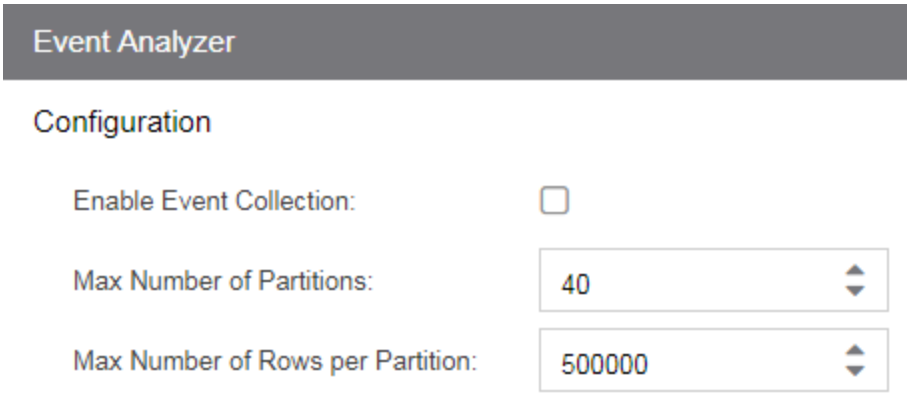
For information on related topics:

- Administration

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.

Related Information

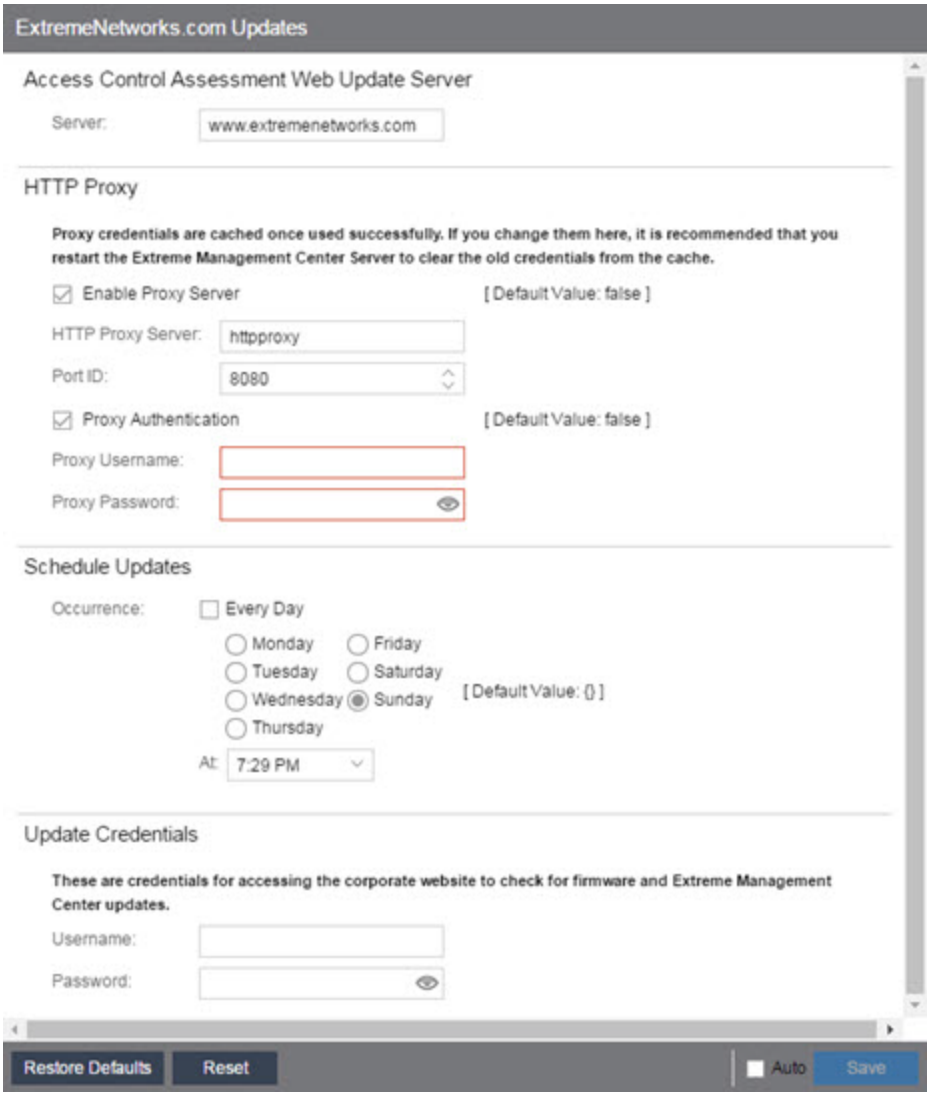
For information on related topics:

- Administration

ExtremeNetworks.com Updates Options

Selecting ExtremeNetworks.com Updates in the left panel of the **Options** tab provides the following view, where you can configure options for accessing the ExtremeNetworks.com website to obtain information about the latest ExtremeCloud IQ - Site Engine product releases and Extreme Networks firmware releases available for download. 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.



ExtremeControl Assessment Web Update Server

Displays the web update server used by ExtremeControl to update ExtremeControl assessment server software. This update operation pertains only to ExtremeControl on-board agent-less assessment servers.

HTTP Proxy Server

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.

Schedule Updates

Use this section to schedule when ExtremeCloud IQ - Site Engine checks for software updates:

- To check for updates every day —Select the **Every Day** checkbox, then select the time to run the check in the **At** drop-down list.
- To check for updates weekly —Select the radio button that corresponds to the day of the week on which you want to run the check, then select the time to run the check in the **At** drop-down list.
- To disable scheduled updates —Do not select the **Every Day** checkbox or any of the radio buttons or select the **Default Value** button to clear your selection.

Update Credentials

Enter the credentials used to access the ExtremeNetworks.com website to obtain firmware and ExtremeCloud IQ - Site Engine update information. You need to create an account at ExtremeNetworks.com and define a username and password for the account, then enter the same credentials here.

Related Information

For information on related topics:

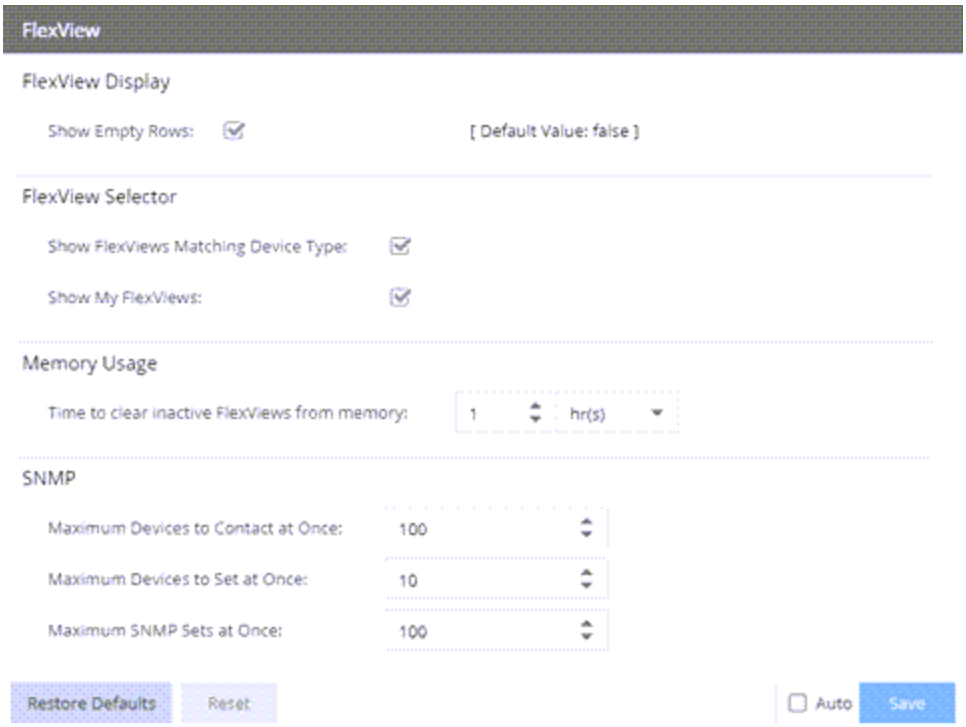
- Administration

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.

Related Information

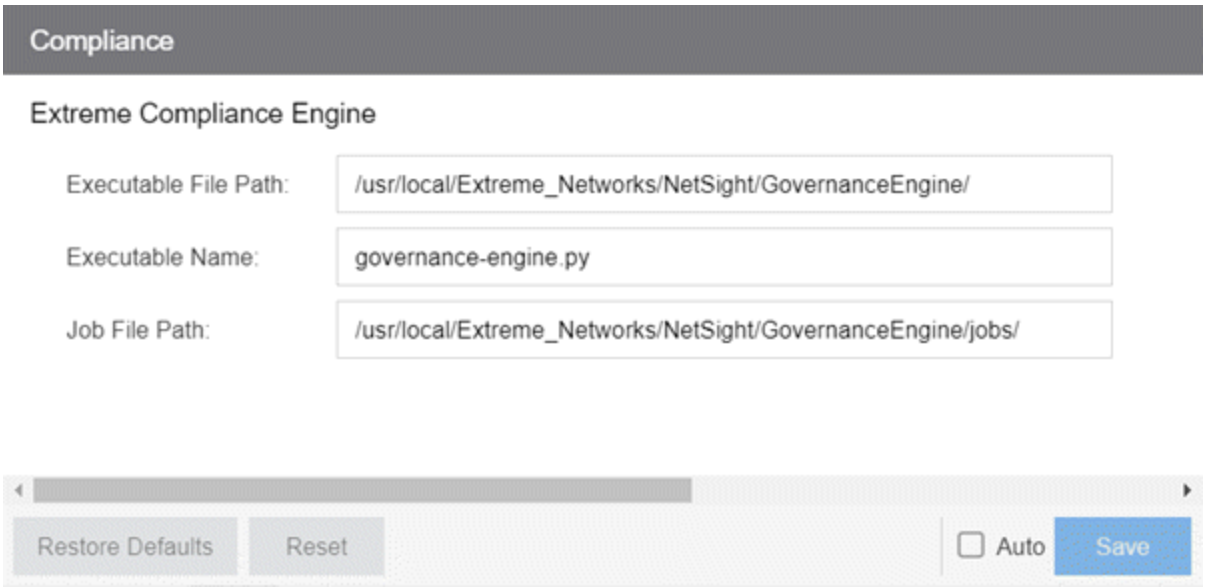
For information on related topics:

- Administration

Compliance Options

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.

Related Information

For information on related topics:

- Administration

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.

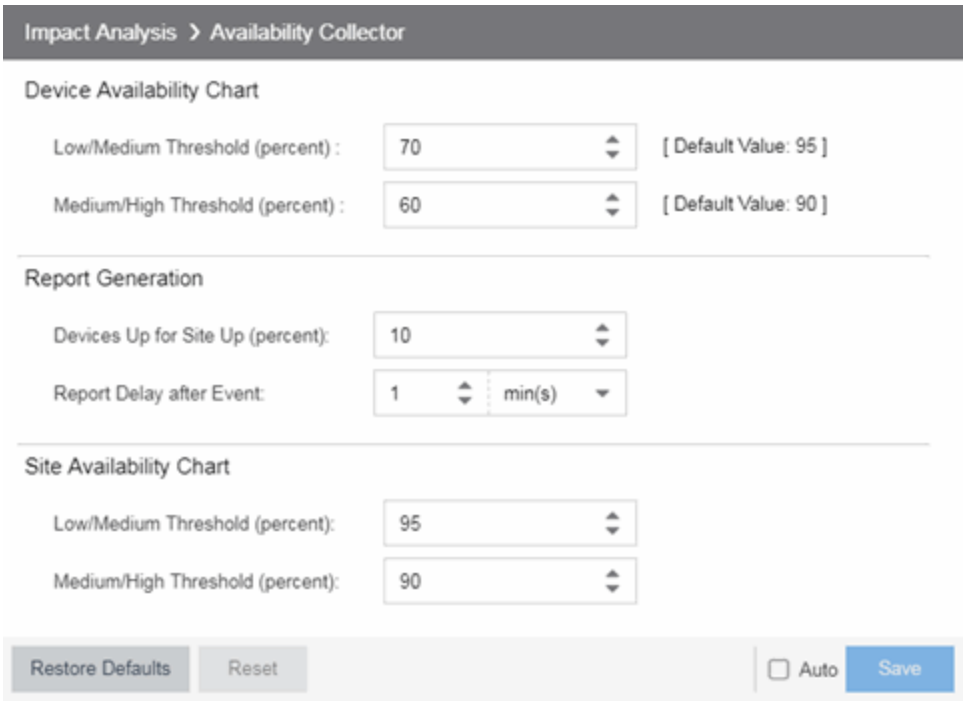
Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.

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)

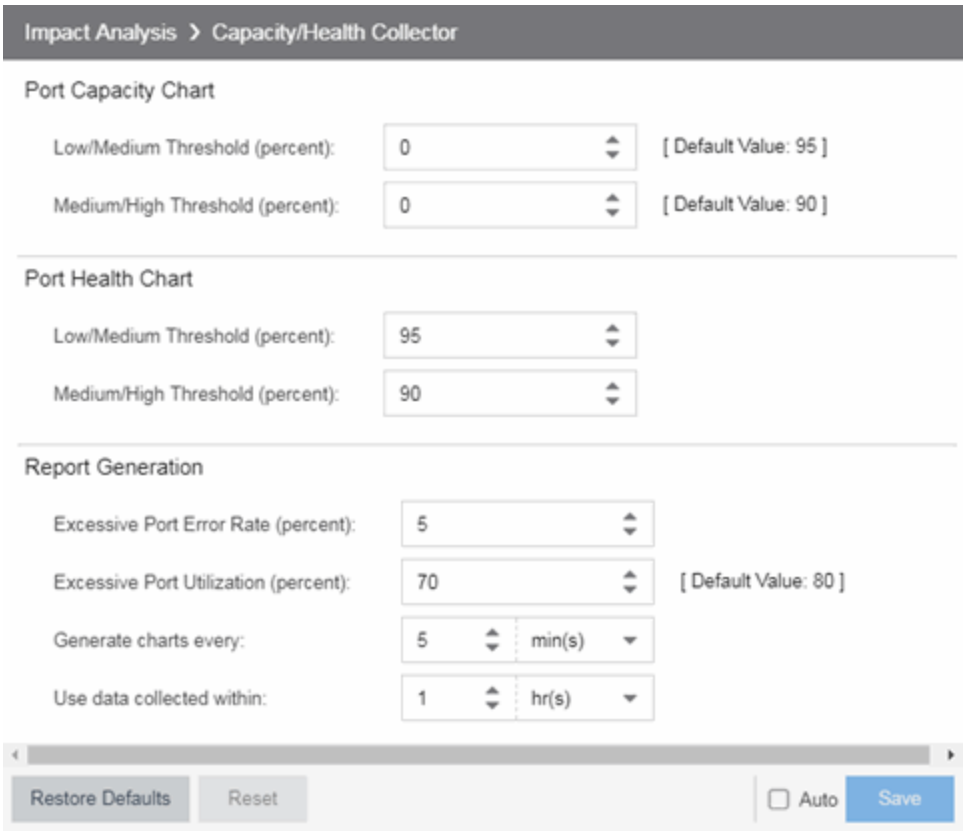
Indicates the percentage of devices included in a site that ExtremeCloud IQ - Site Engine can reach. If the value falls below the percentage entered here, the **Impact Status** of the Site Availability chart moves from **Low** to **Medium**. For devices to be included, data collection must be enabled.

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.

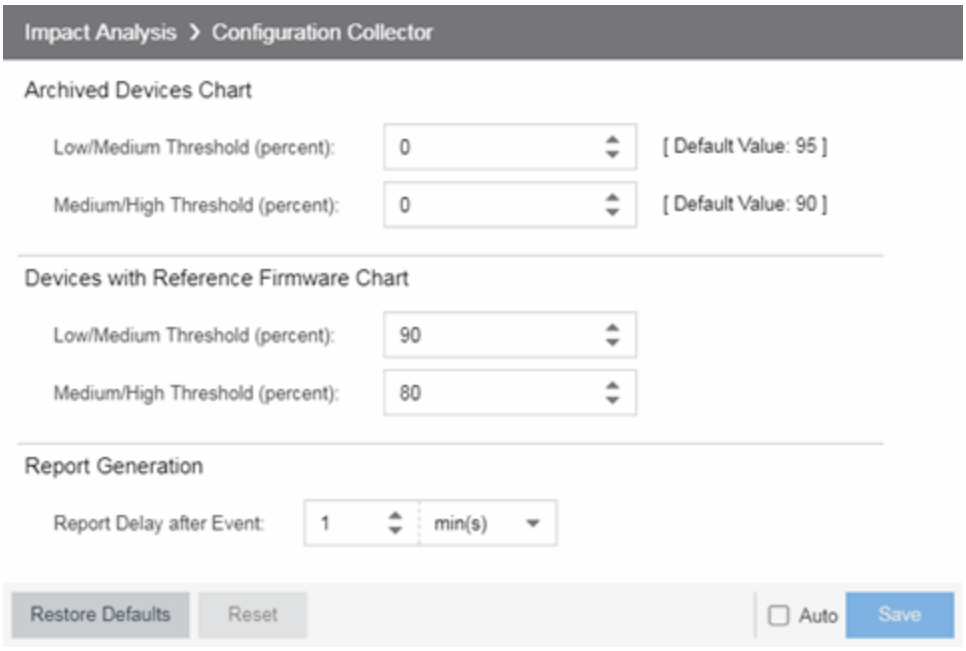
Excessive Port Utilization (percent)
Indicates the port utilization, in percent of total port traffic, above which ExtremeCloud IQ - Site Engine considers the port utilization excessive. A port utilization below the percentage entered here is considered acceptable.

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 1and 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.

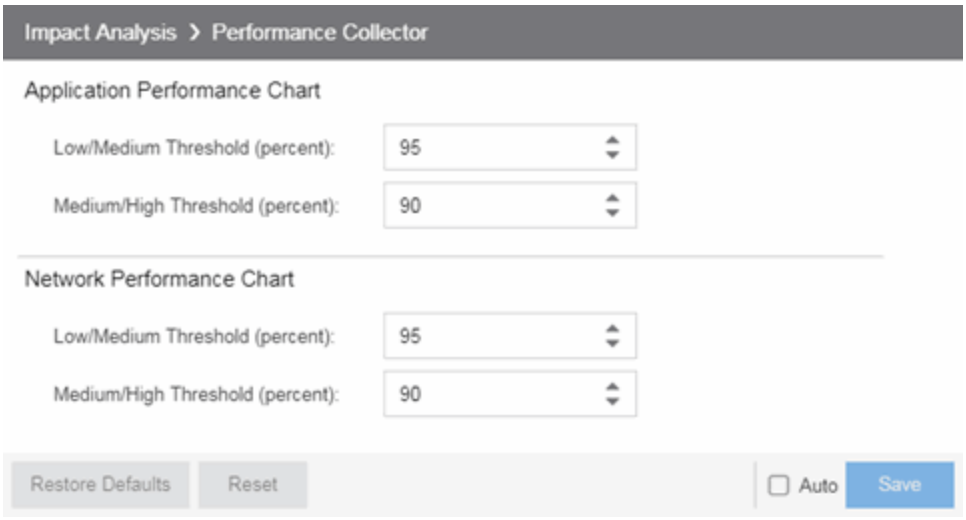
Report Generation

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, or using dynamic thresholding, if enabled.

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, or using dynamic thresholding, if enabled.

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, or using dynamic thresholding, if enabled.

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, or using dynamic thresholding, if enabled.

Related Information

For information on related topics:

- Impact Analysis Dashboard

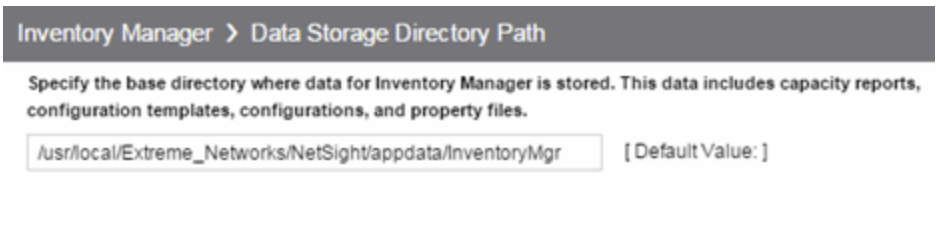
Inventory Manager Options

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

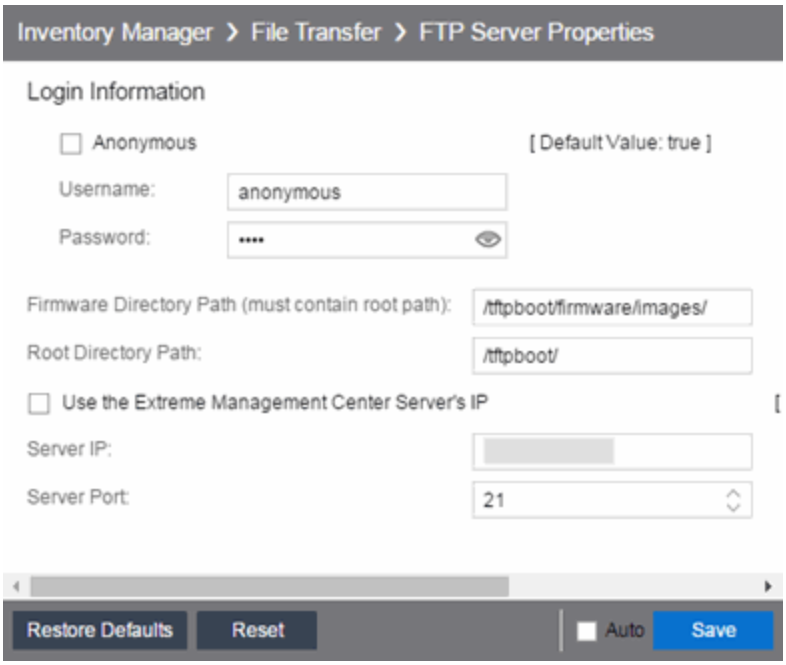
These options specify the FTP, SCP, SFTP, or TFTP file transfer settings used when upgrading firmware.

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 (for example, /root/).
- **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

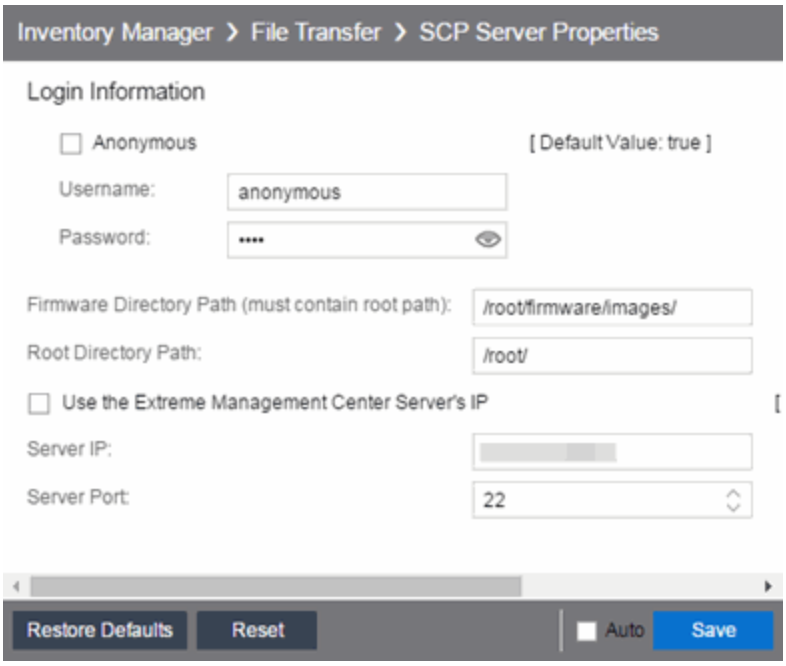
Enter the IP address of the device where the FTP server resides.

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**. On a system with ExtremeCloud IQ - Site Engine installed to be owned as root, the default firmware directory is `/root/firmware/images/`. On a system installed to be owned as netsight, the default firmware directory is `/usr/local/Extreme_Networks/NetSight/home/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 root directory in this 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. On a system with

ExtremeCloud IQ - Site Engine installed to be owned as root, the default root directory is `/root/`. On a system installed to be owned as netsight, the default firmware directory is `/usr/local/Extreme_Networks/NetSight/home/`.

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 (for example, /root/).
- 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.

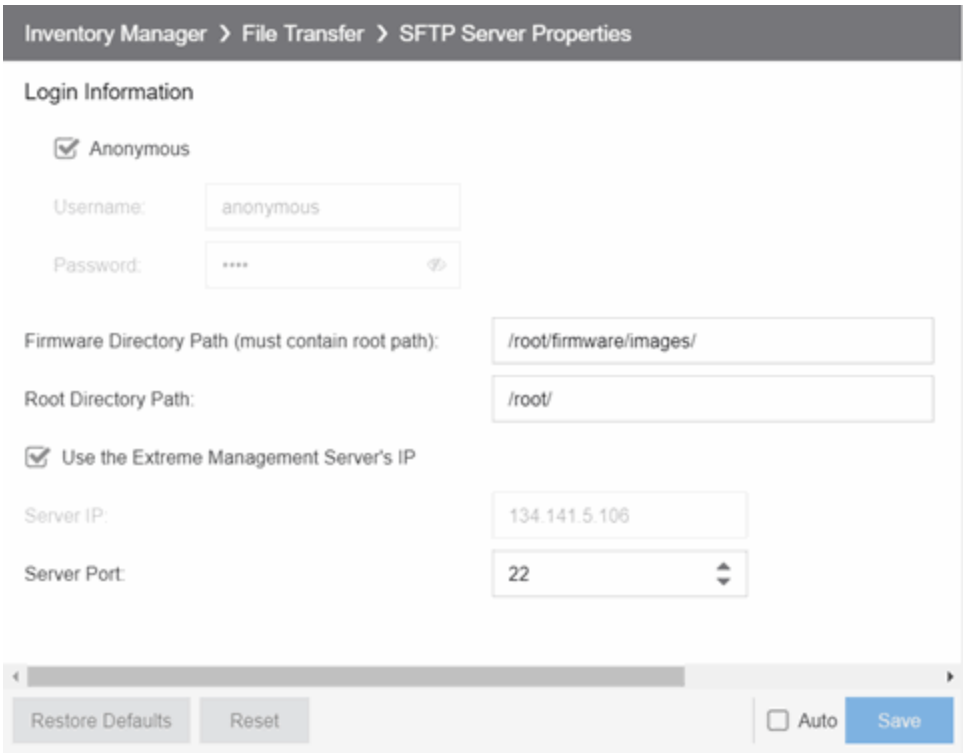
Use the ExtremeCloud IQ - Site Engine Server's IP
Select this checkbox if your SCP server is on the same machine as the ExtremeCloud IQ - Site Engine Server. Selecting this checkbox disables the **Server IP** field.

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**. On a system, the default firmware directory is `/root/firmware/images/`. This path needs to be updated when the SFTP server is installed and a valid directory is created. 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 root directory in this 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. The default root directory is `/root/`. This path needs to be updated when the SFTP server is installed and a valid directory is created.

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 (for example, /root/ .
- 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

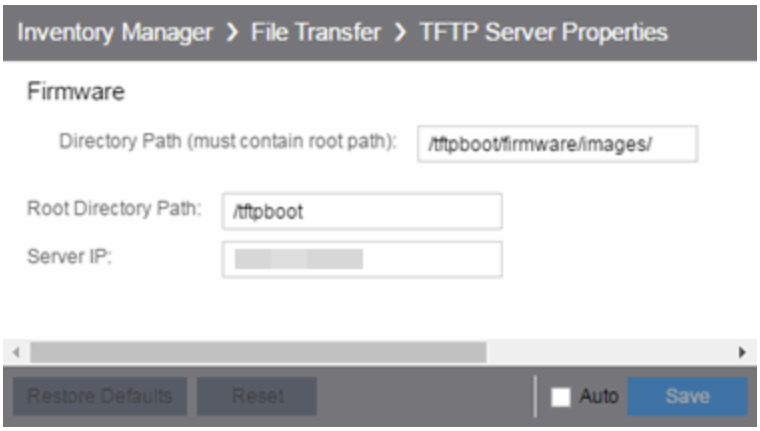
Enter the IP address of the device where the SFTP server resides.

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 (for example, / root/).
- **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.

Related Information

For information on related topics:

- Administration

ExtremeCloud IQ - Site Engine Options

Selecting Site Engine - General 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.


Site Engine - General
Data Display
Auto Group Delimiter:
/
Tooltip
Date Time Format
Use ISO 8601 Timestamp Format (2010-01-08T18:45UTC):
Date:
MM/dd/yyyy
Time:
hh:mm:ss a
Device Tree
Name Format:
Nickname
MAC Address Display
Display By:
Full MAC Address (00:01:F4:22:22:22)
Limit OUI character length
OUI character limit:
8
Unknown MACs as Unknown
[Default Value: false]
Map
Status Refresh Interval:
30
sec(s)
Message of the Day
Enable
Message Title:
Message Body:
Session Limits
Maximum FlexViews Displayable:
10
Maximum PortViews Displayable:
5
Status Bar Message
Status Bar Message:

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)

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.

Map

Status Refresh Interval
Select the interval that determines how often maps are automatically refreshed by ExtremeCloud IQ - Site Engine. If **None** is selected, maps must be manually refreshed.

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.

Related Information

For information on related topics:

- Administration

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.

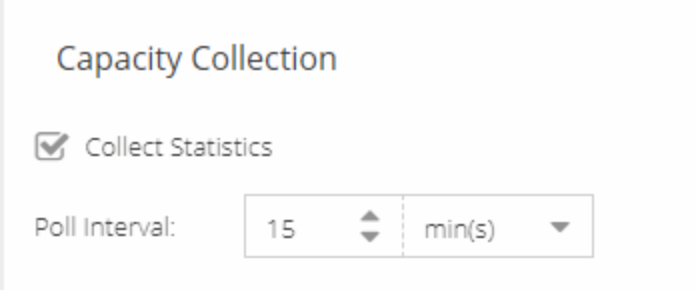
Changing a value from the system default causes a **Default Value** button to appear. Selecting this button changes the field back to the system default value.

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.

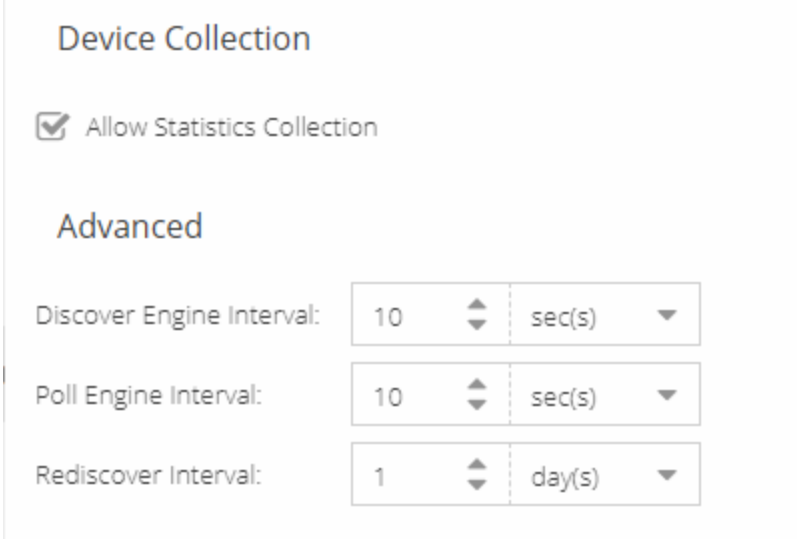
Capacity Collection



Collect Statistics
Enables or disables additional statistics collection.

Poll Interval
The amount of time the data collector waits between polling devices.

Device Collection



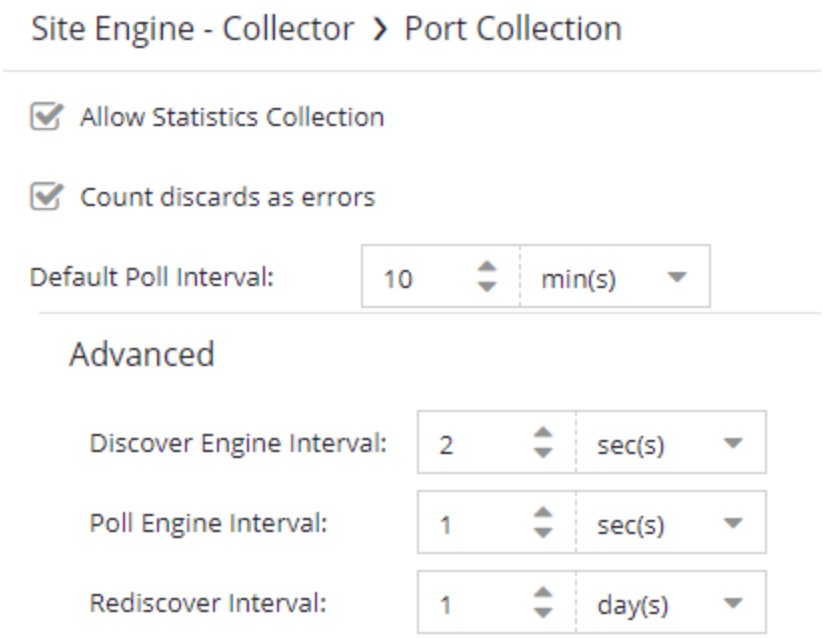
Allow Statistics Collection
Select this check box if you want statistics to be collected when you have enabled statistics collection on the device.

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.

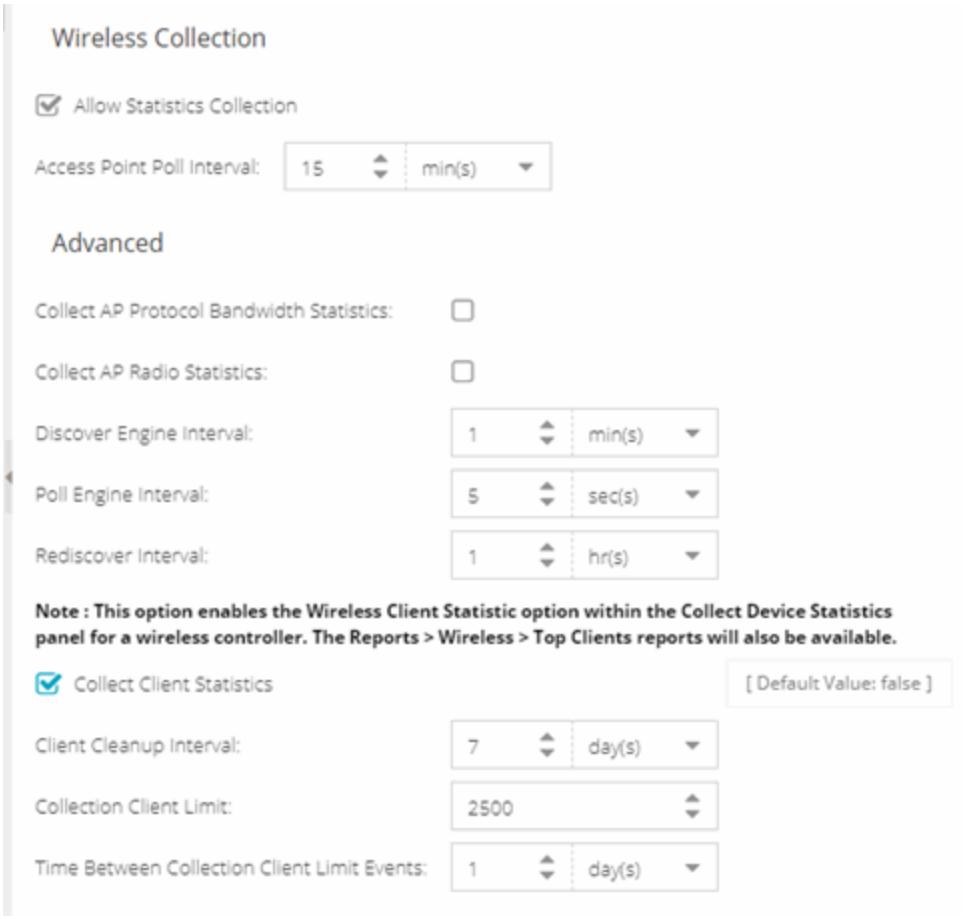
Poll Engine Interval

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.

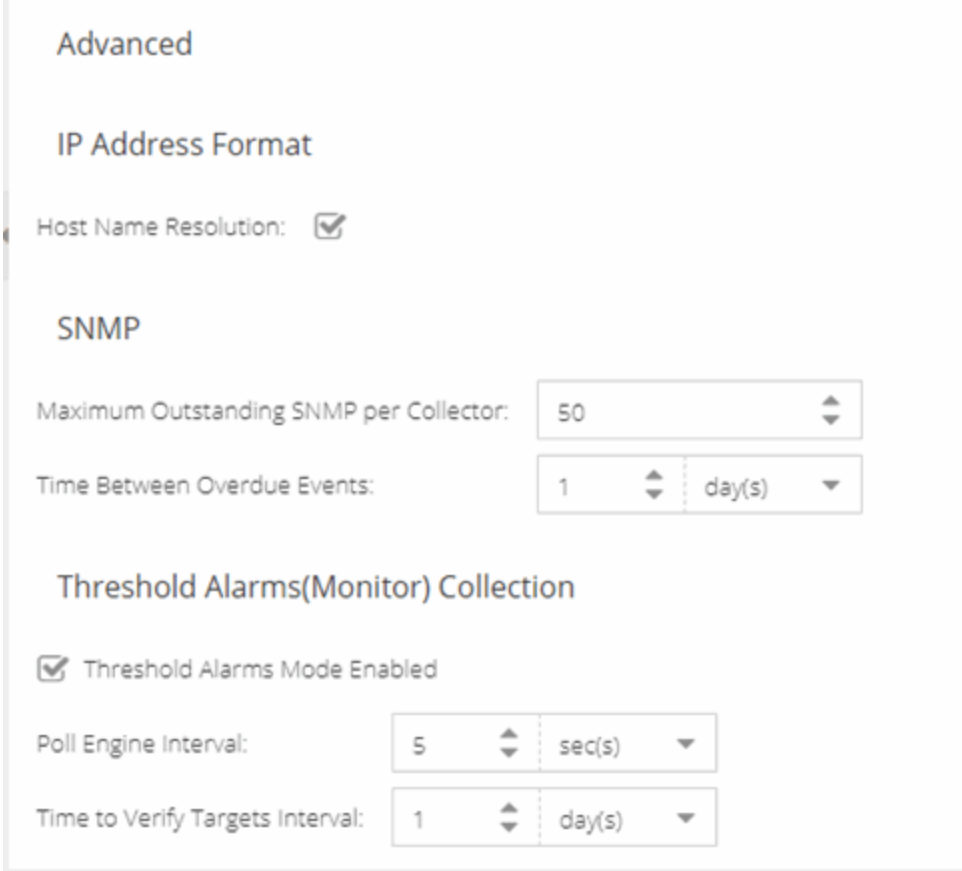
Collection Client Limit

The maximum number of wireless clients for which statistics are stored per collection interval. Valid values are 1to 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.

Related Information

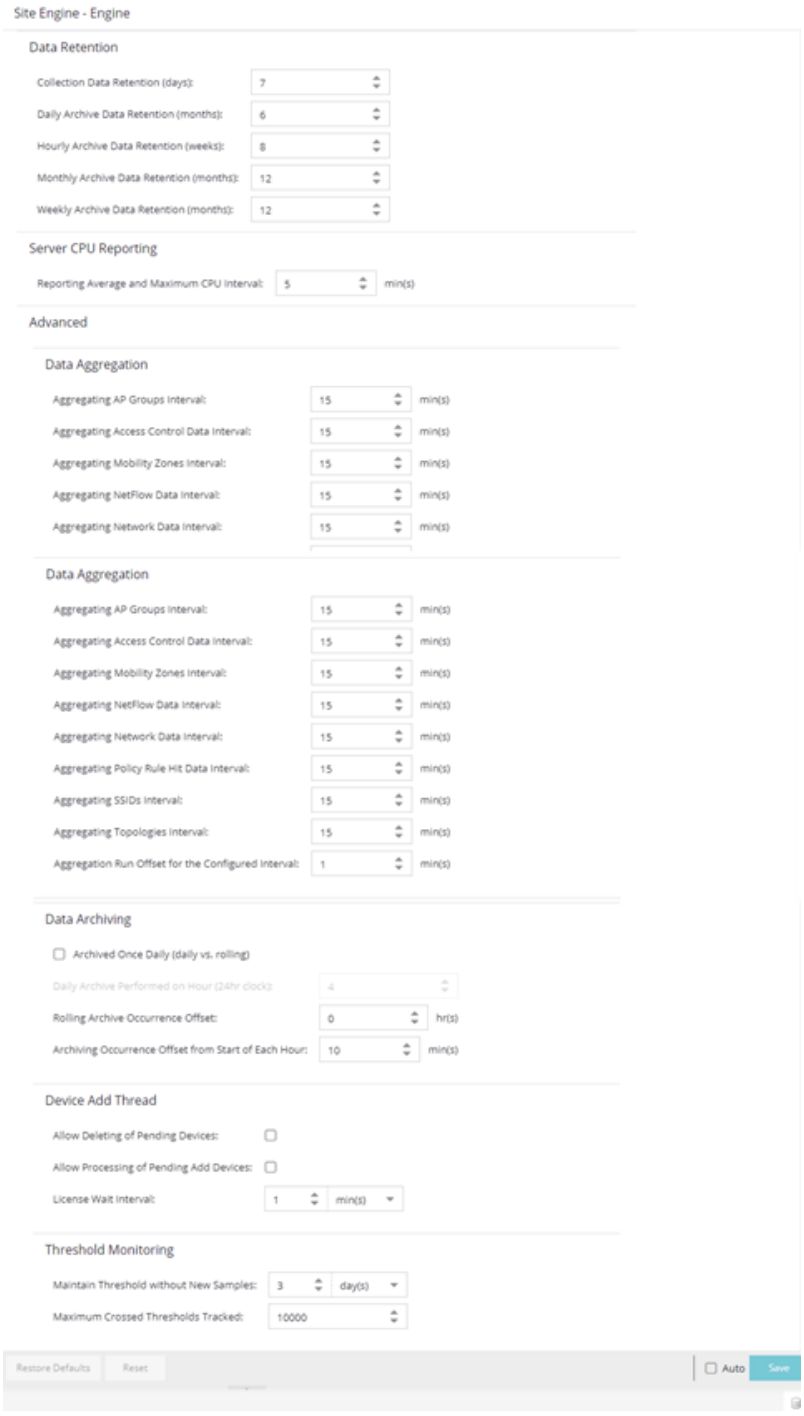
For information on related topics:

- Administration

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
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)
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 Policy Rule Hit 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
Allow Deleting of Pending Devices:
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
Auto
Save

Data Retention

Collection Data Retention (days)

This setting specifies how long (in days) to maintain 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.

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.

Related Information

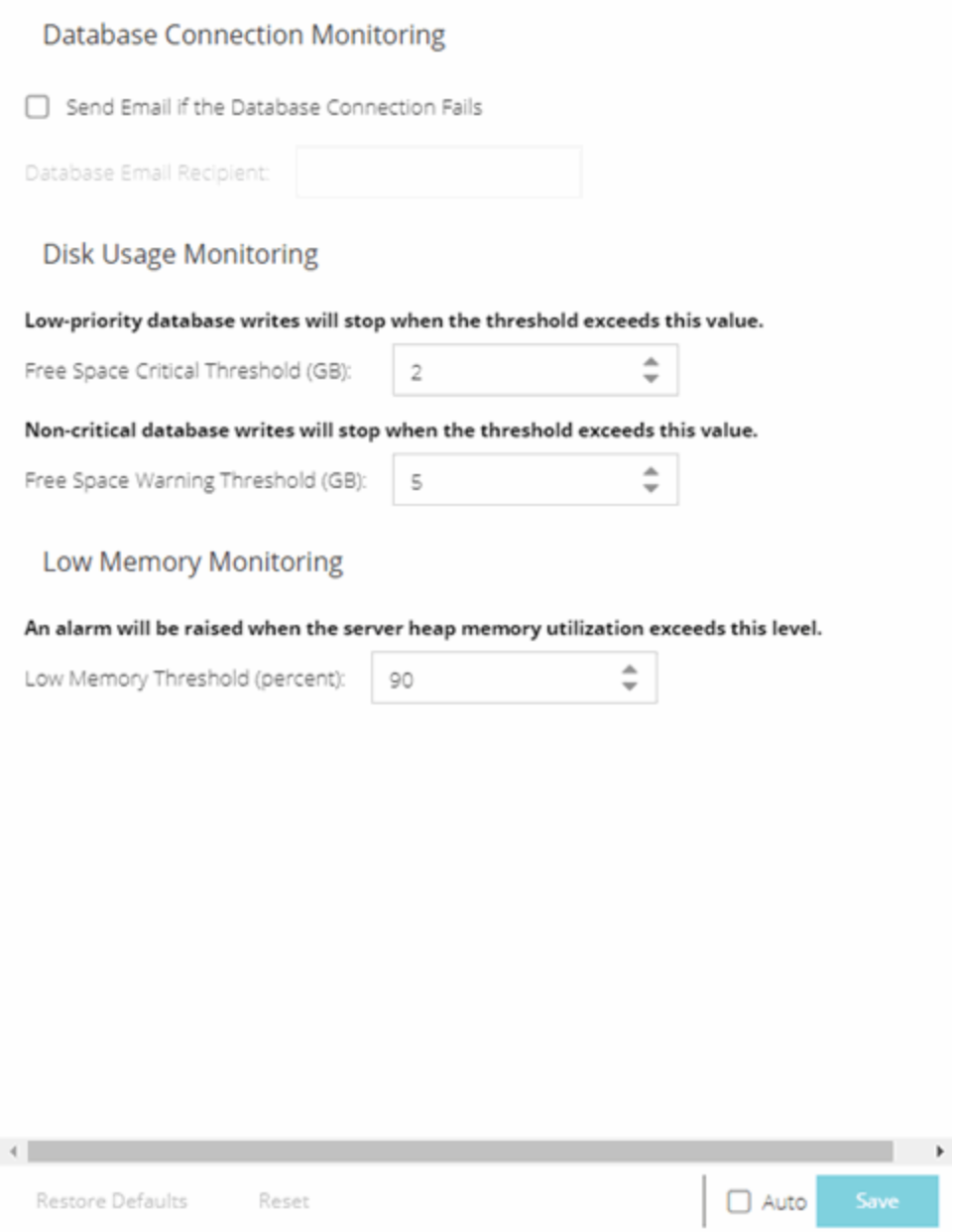
For information on related topics:

- 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.

Related Information

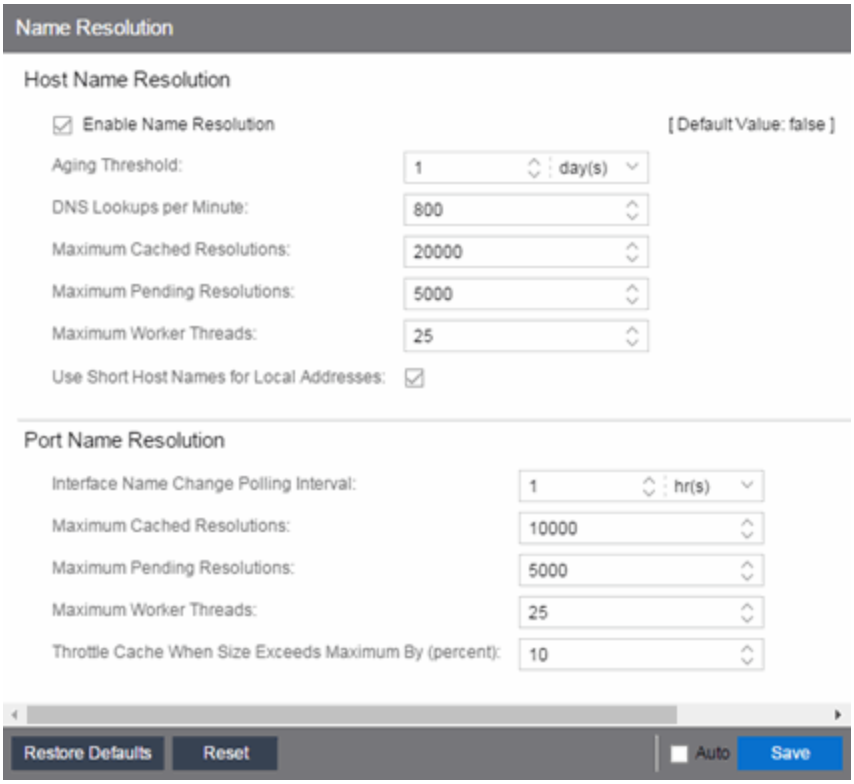
For information on related topics:

- Administration

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 1hour.

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.

Related Information

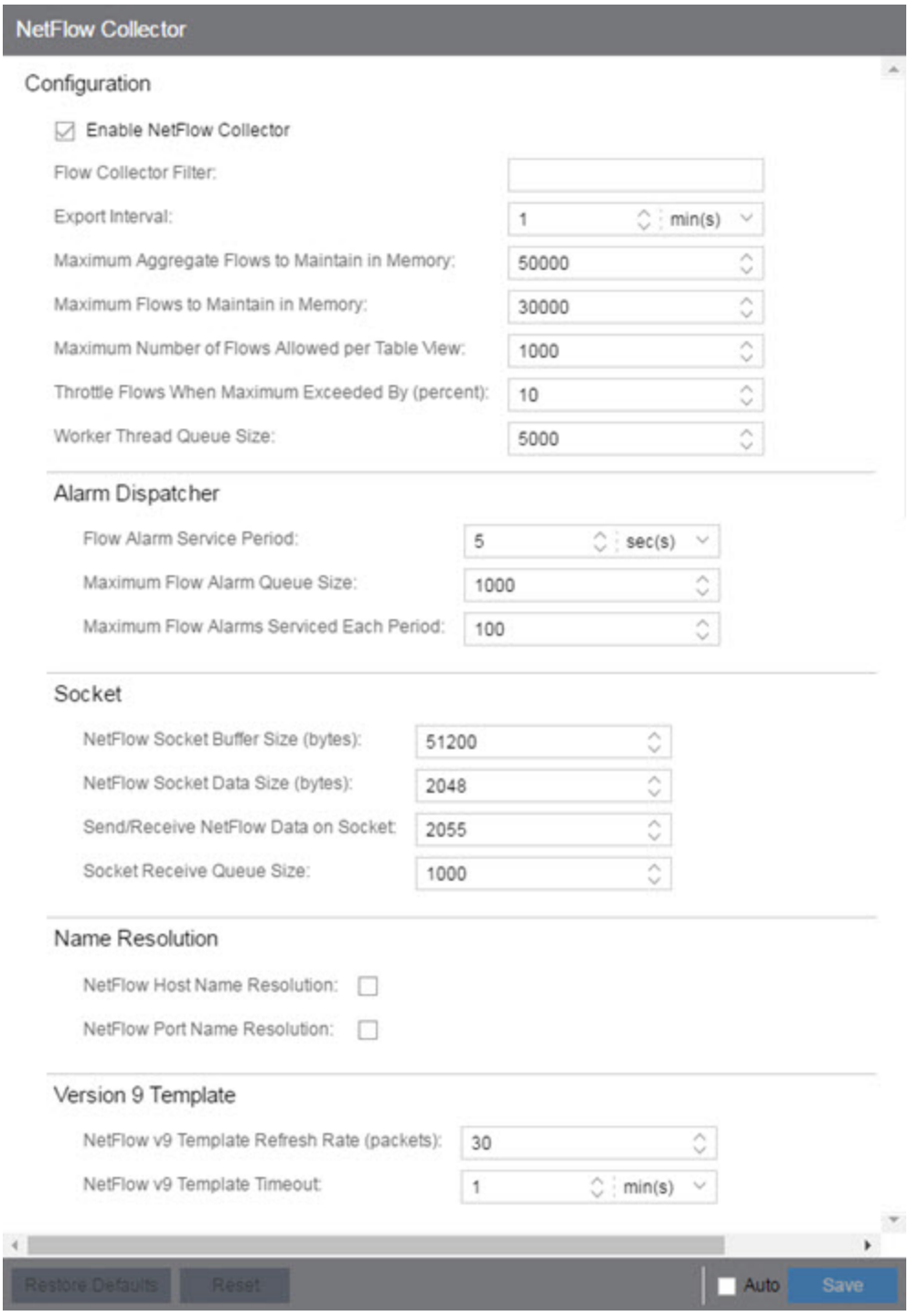
For information on related topics:

- Administration

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.

Related Information

For information on related topics:

- Administration

Network Monitor Cache Options

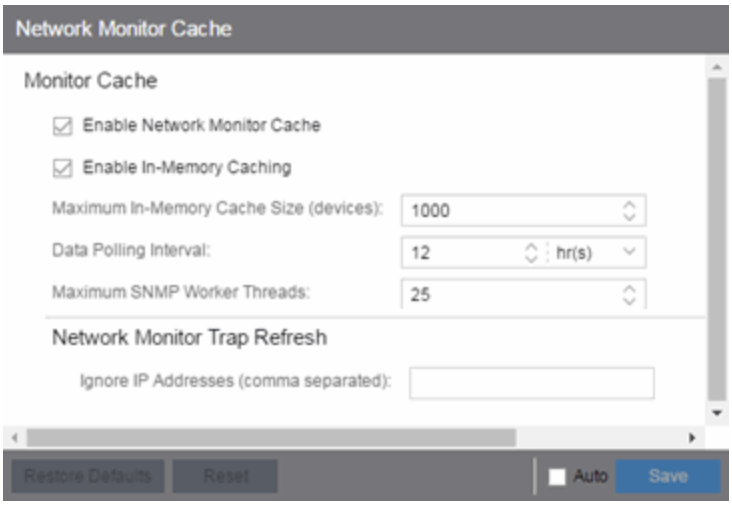
Selecting Network Monitor Cache in the left panel of the **Options** tab provides the following view, where you can edit network monitor cache settings. The network monitor cache stores information about the physical topology of a device, with additional emphasis on port information. Data is pulled from 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.

Related Information

For information on related topics:

- Administration

Policy Options

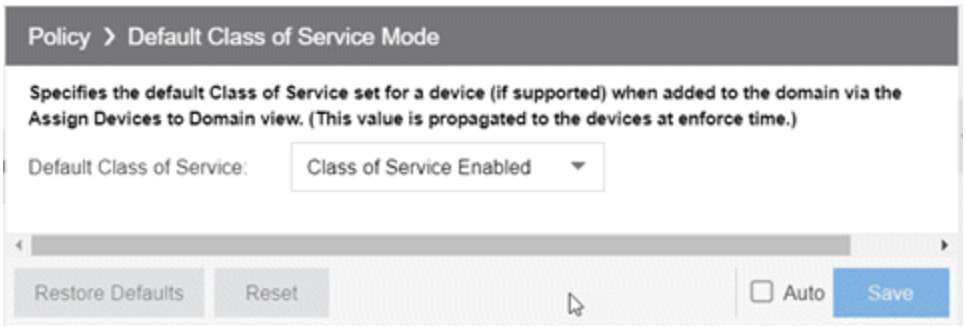
Selecting Policy in the left panel of the **Options** tab provides the following view, where you can edit options that apply to policy functionality found in the **Policy** tab.

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.

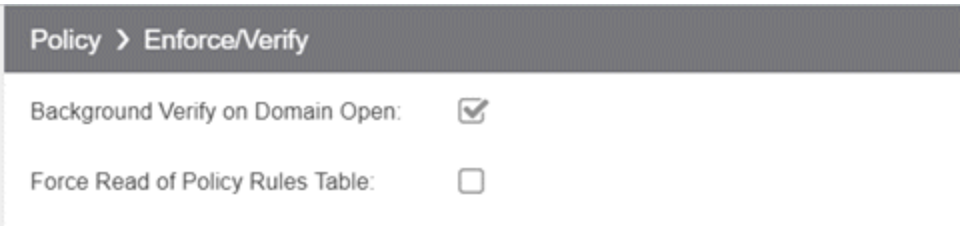
Default Class of Service Mode

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

Selecting **Background Verify on Domain Open** causes 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.

Related Information

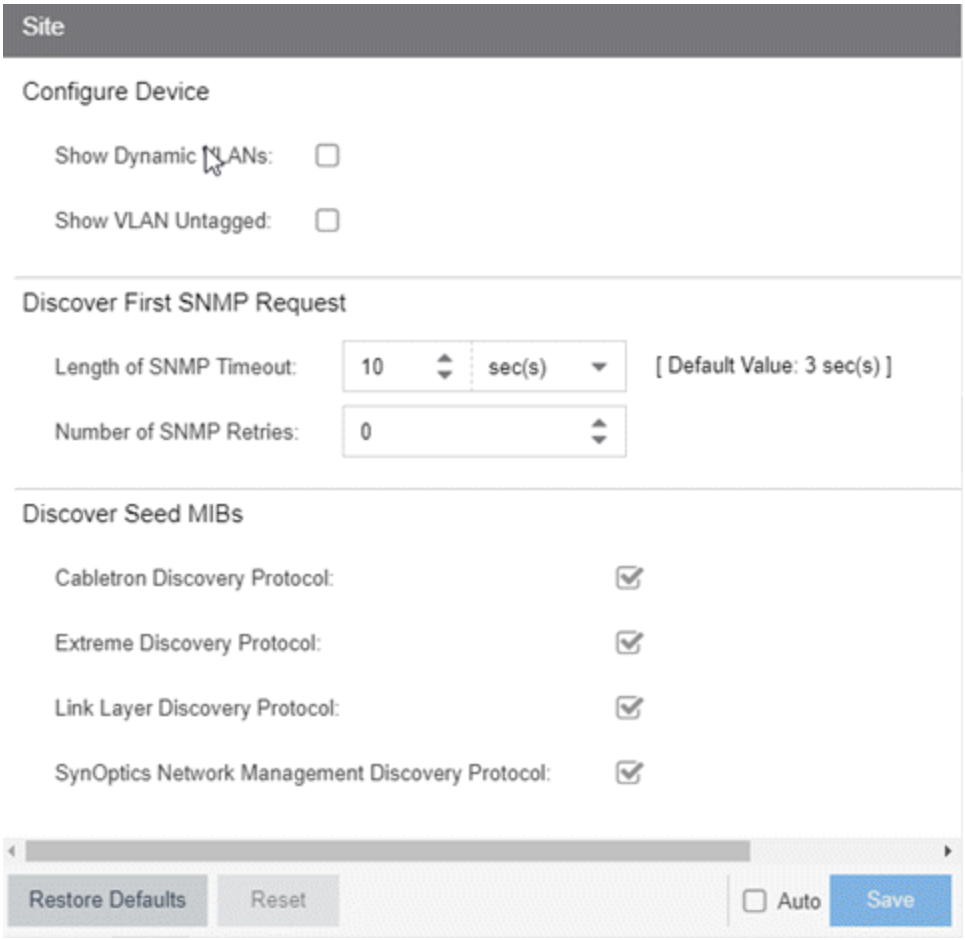
For information on related topics:

- Policy

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 1and 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.

Related Information

For information on related topics:

- Administration

SMTP Email Options

Selecting SMTP Email in the left panel of the **Options** tab provides the following view, where you can specify the SMTP email server used by ExtremeCloud IQ - Site Engine when sending emails to users. ExtremeCloud IQ - Site Engine can be configured 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.

Outgoing Email (SMTP) Server
Identifies the email server used for outgoing messages.

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."

Sender's SMTP Password
The password for the user account entered in the **Sender's Email Address** field. Select the **Eye** icon to display your password.

Related Information

For information on related topics:

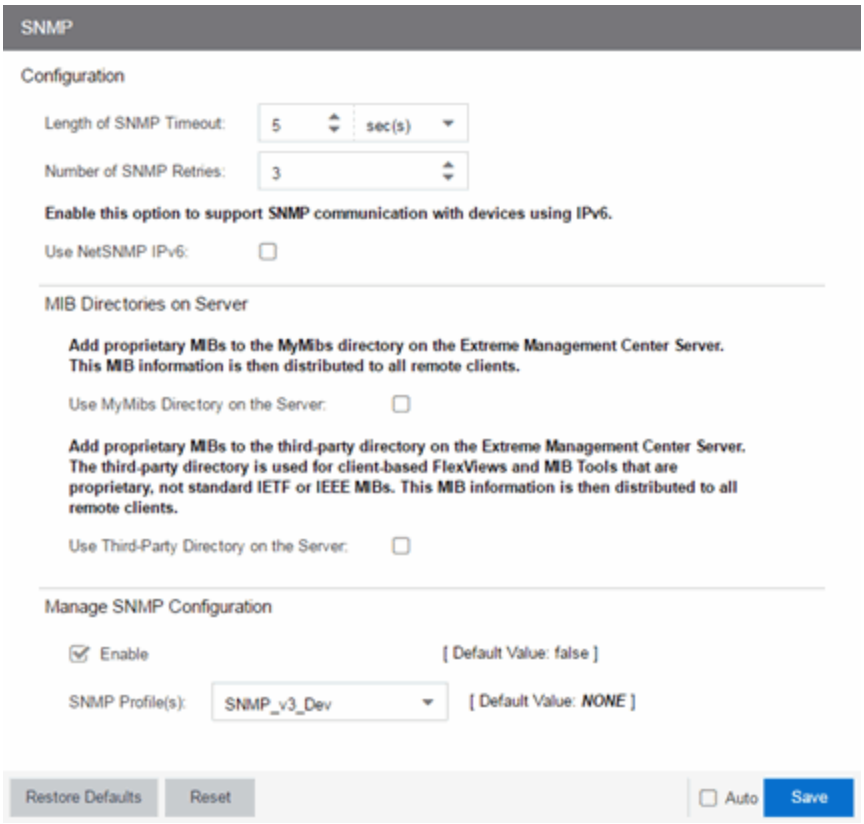
- Administration

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 3 seconds. The value for this setting must be between 1and 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.

Related Information

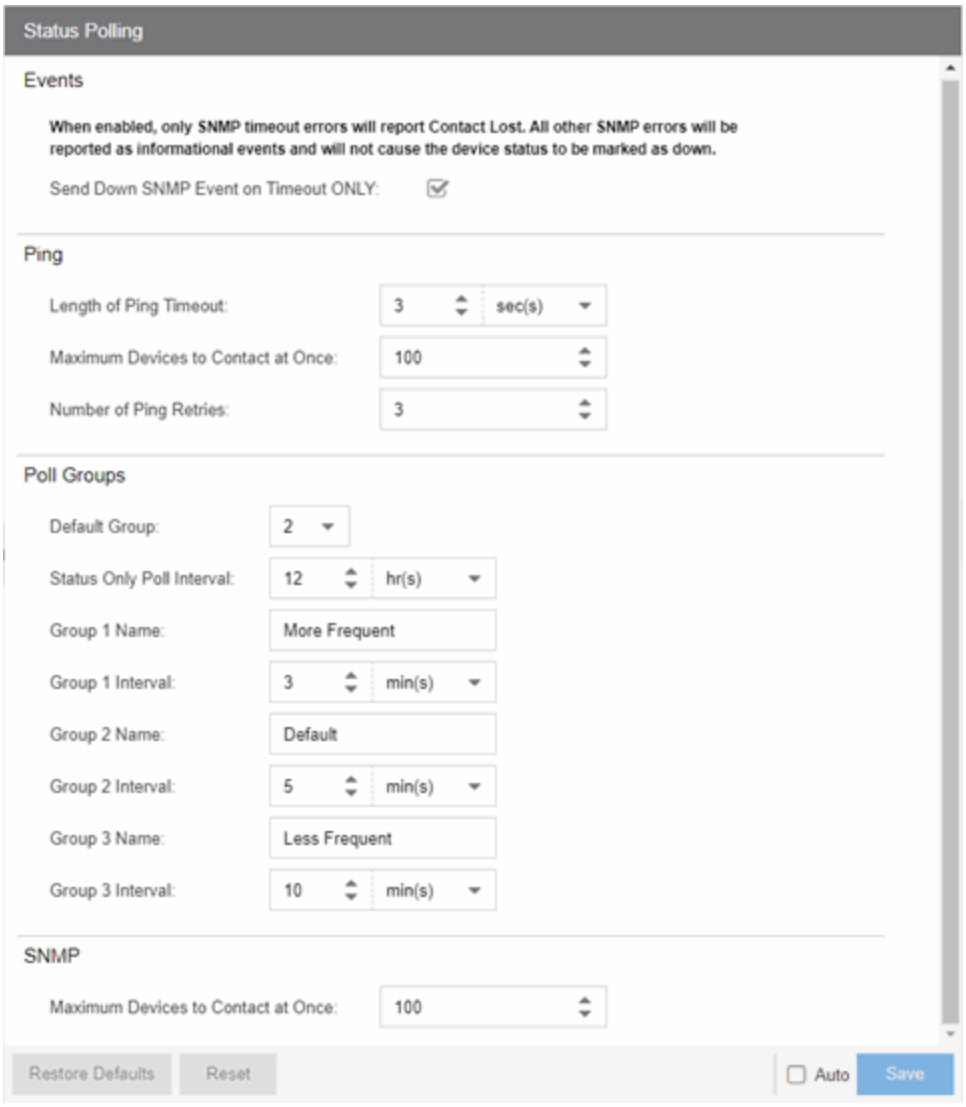
For information on related topics:

- Administration

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.

Related Information

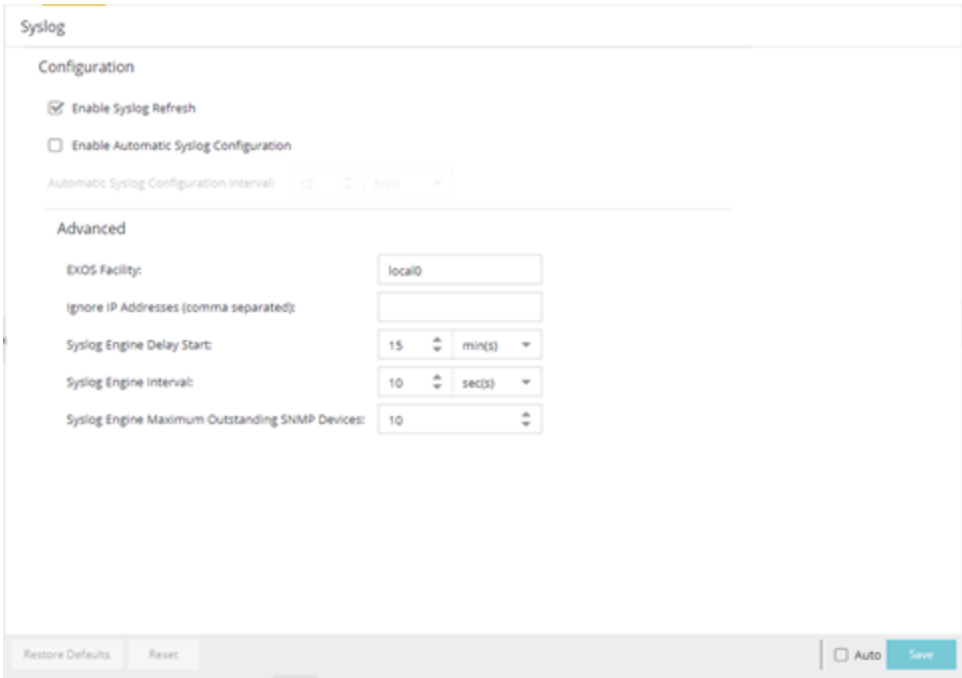
For information on related topics:

- Administration

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 configure ExtremeCloud IQ - Site Engine to automatically refresh syslog information. Deselecting this option disables the **Enable Automatic Syslog Configuration** field.

Enable Automatic Syslog Configuration

Select the checkbox to configure ExtremeCloud IQ - Site Engine to automatically gather information and post it to the syslog. Deselecting this option disables the **Automatic Syslog Configuration Interval** field.

Automatic Syslog Configuration Interval
Enter the frequency with which ExtremeCloud IQ - Site Engine automatically gathers information and posts it to the syslog.

Advanced

EXOS Facility
The Syslog facility to be used by the script when registering/ unregistering syslog for EXOS 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.

Related Information

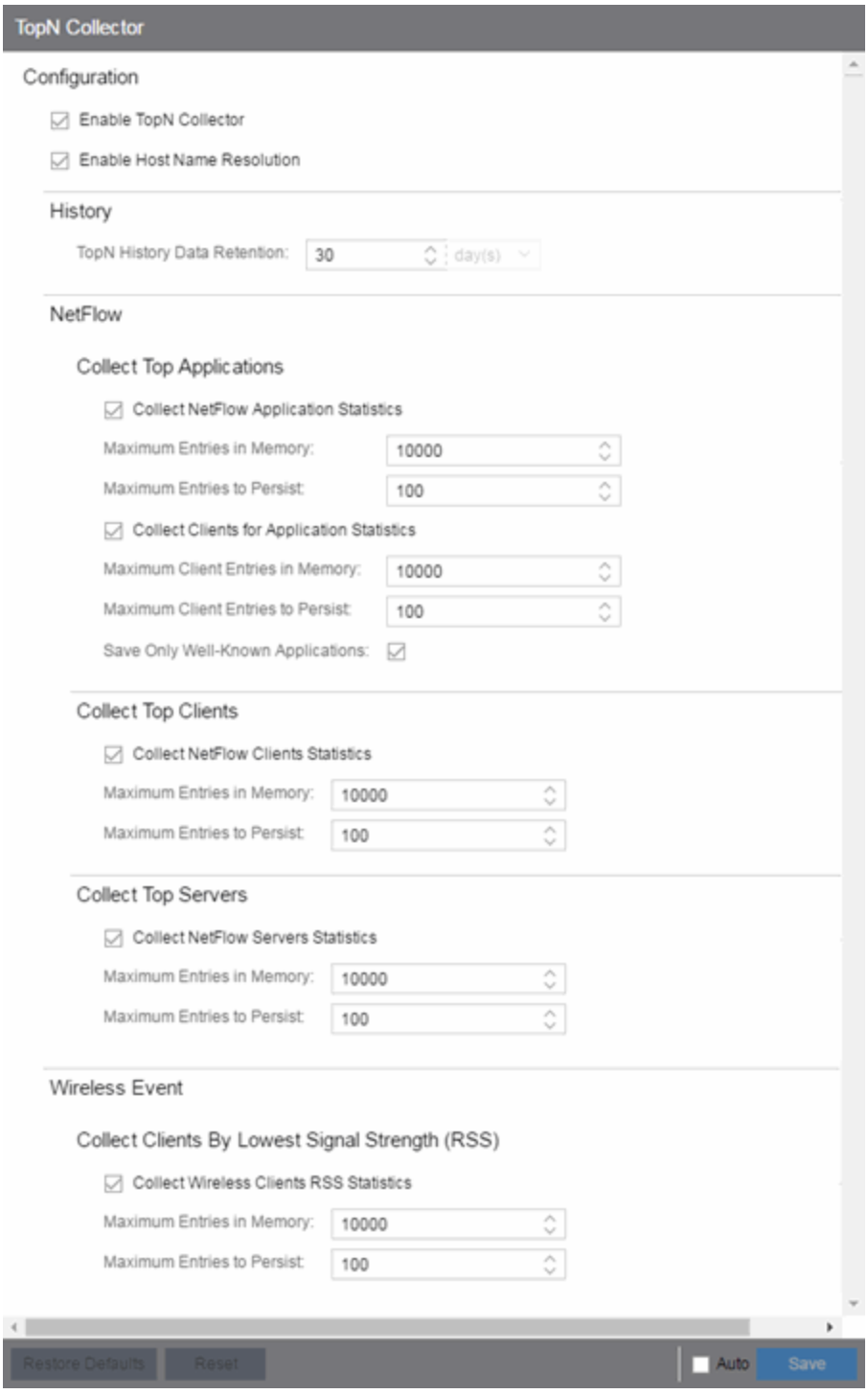
For information on related topics:

- Administration

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 1day 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.

Related Information

For information on related topics:

- Administration

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 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 refresh information on the devices when the trap is received.

SNMPv1Credential Name
Select the SNMPv1credentials 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 VOSS devices for SNMPv3 informs.

NOTE: Do not change the **Server Engine ID**.

Enable Automatic Trap Configuration
Select this option to configure the ExtremeXOS switches on your network to send ExtremeCloud IQ - Site Engine traps using the SNMP credentials specified in the **SNMP Credential Name** fields. Devices on which **Automatic Trap Configuration** is enabled are polled at the interval specified in **Automatic Trap Configuration Interval**.

Automatic Trap Configuration Interval
Select the frequency with which your devices send SNMP traps to ExtremeCloud IQ - Site Engine.

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.

Related Information

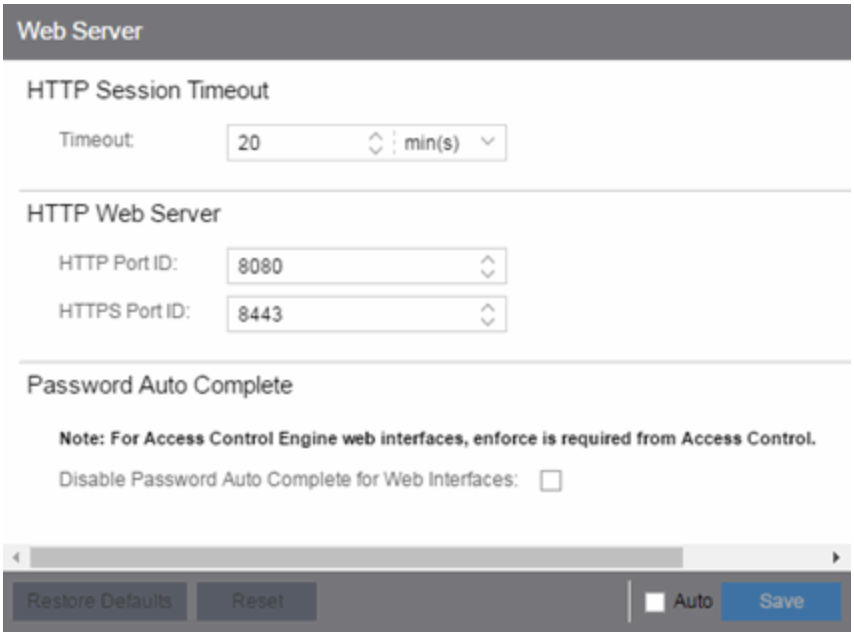
For information on related topics:

- Administration

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.

IMPORTANT: Enforce your ExtremeControl engines via the **Control** > **ExtremeControl** tab immediately after changing the **HTTP Port ID**. Do not change the **HTTPS Port ID** until after you enforce.

When adding a new ExtremeControl engine, the **HTTP Port ID** must be **8080**.

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: Do not change the HTTP Port ID for at least one minute after changing the HTTPS Port ID to ensure ExtremeCloud IQ - Site Engine polls the ExtremeControl engine.

When adding a new ExtremeControl engine, 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 ExtremeControl web interfaces, you must enforce from the **Control** > **ExtremeControl** 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.

Related Information

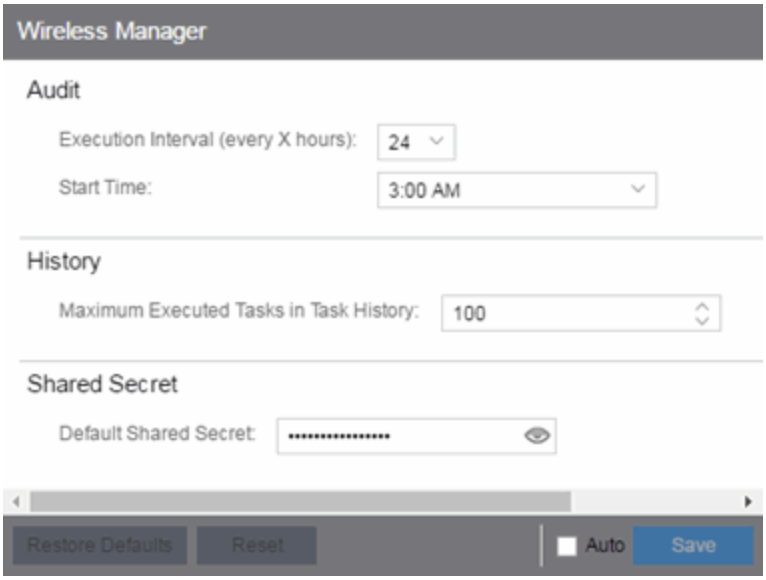
For information on related topics:

- Administration

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.

Related Information

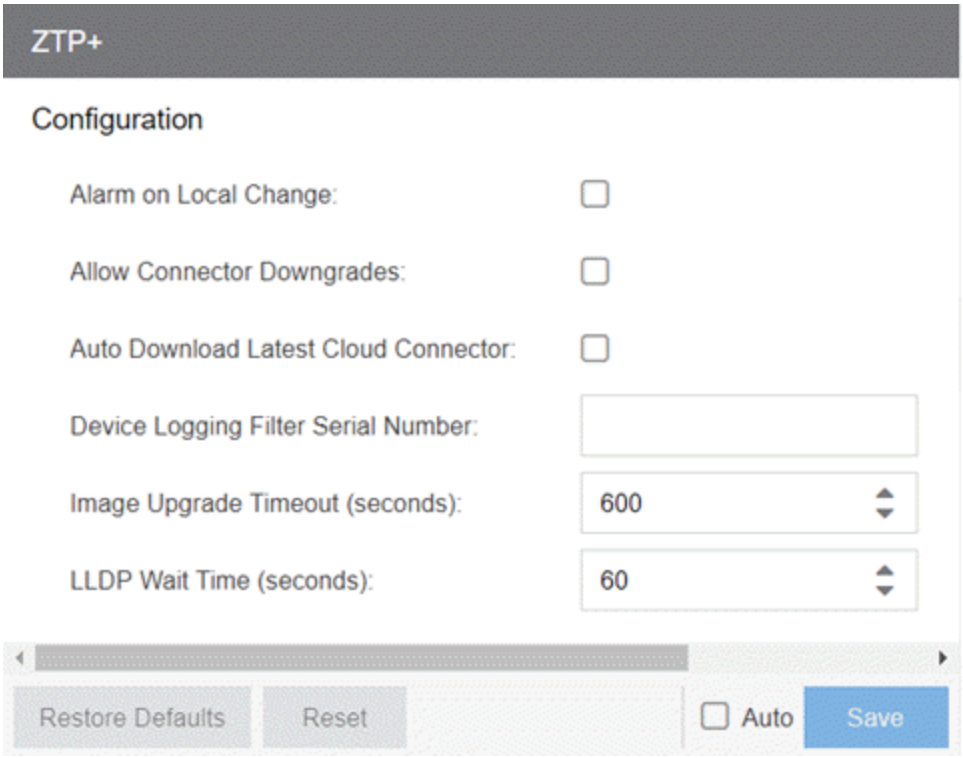
For information on related topics:

- Administration

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.



Alarm on Local Change

Select the checkbox 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 checkbox to allow ExtremeCloud IQ - Site Engine to downgrade to a previous version of the cloud connector.

Auto Download Latest Cloud Connector
Select the checkbox to allow ExtremeCloud IQ - Site Engine to automatically download the latest 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.

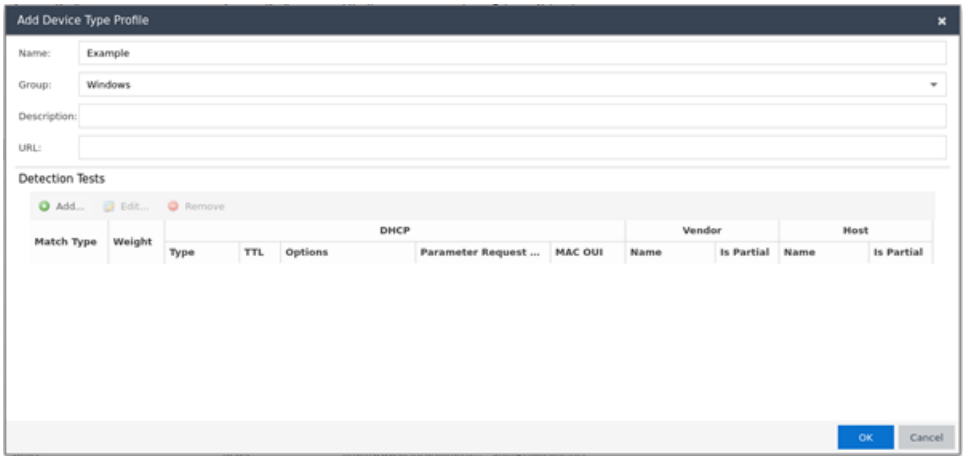
Related Information

For information on related topics:

- Administration

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.

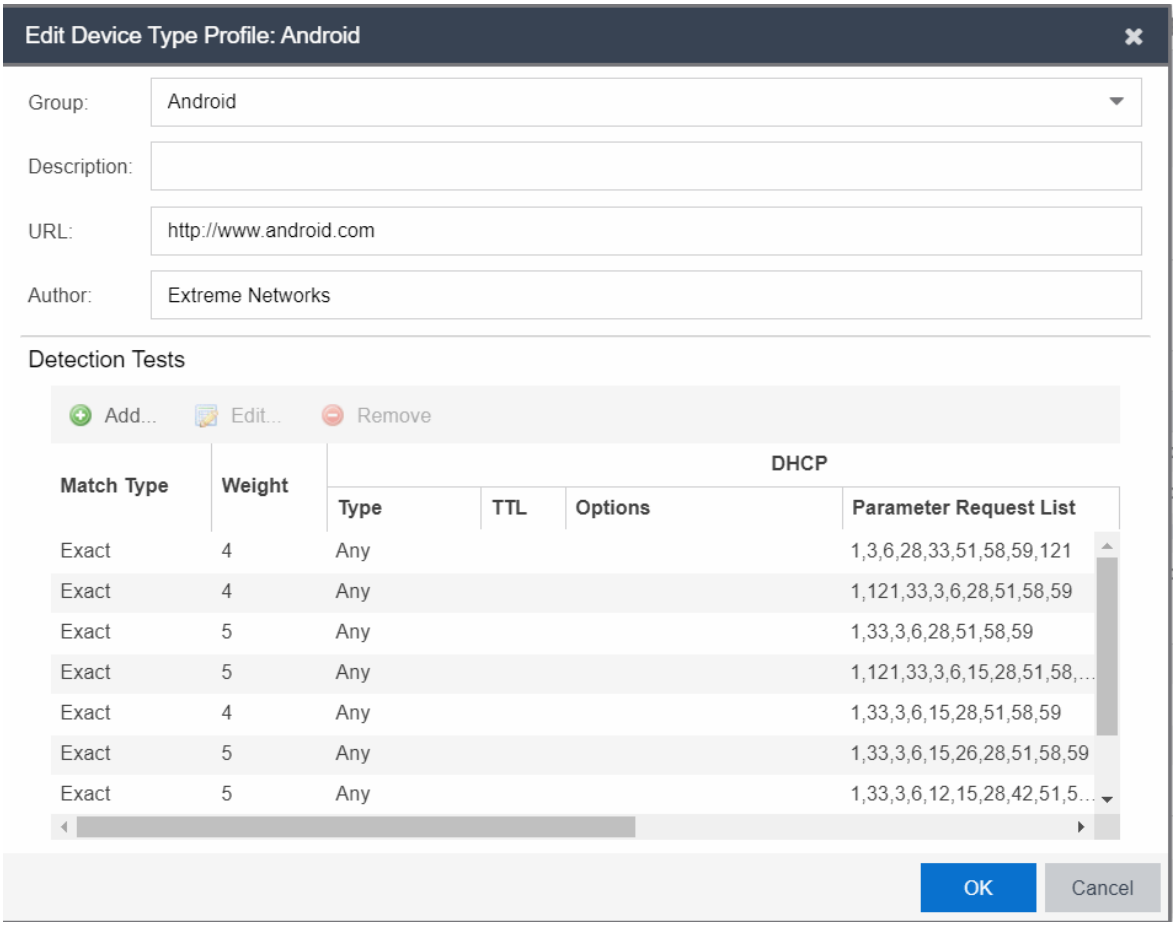
Related Information

For information on related topics:

- 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.

Related Information

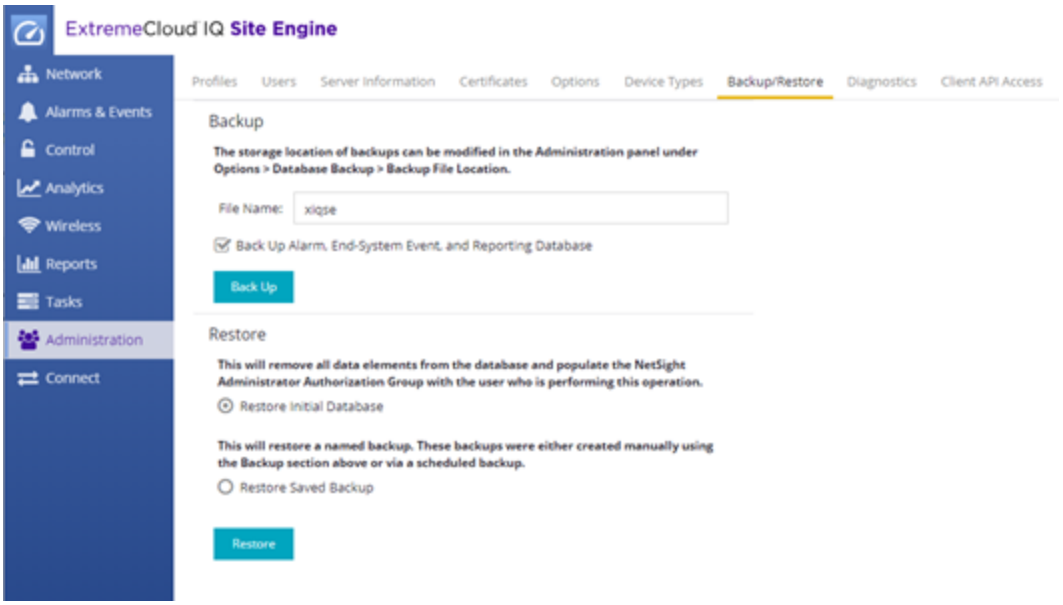
For information on related topics:

- 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.

IMPORTANT: By default, version 21.1.1.0 of ExtremeCloud IQ - Site Engine creates a binary database backup, which provides a more efficient method of backing up the database and uses less resources. The backup process functions identically to previous versions of ExtremeCloud IQ - Site Engine.



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**.

File 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 ExtremeControl 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 there are no database backups saved (backups saved in version 8.0), this field does not display.

Restore Legacy Backup

Select this option to remove all data elements from the database and then re-populate the database using a saved backup file created before version 8.0. Use the drop-down list to select the file from which you want to populate the database.

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.

Related Information

For information on related topics:

- 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.

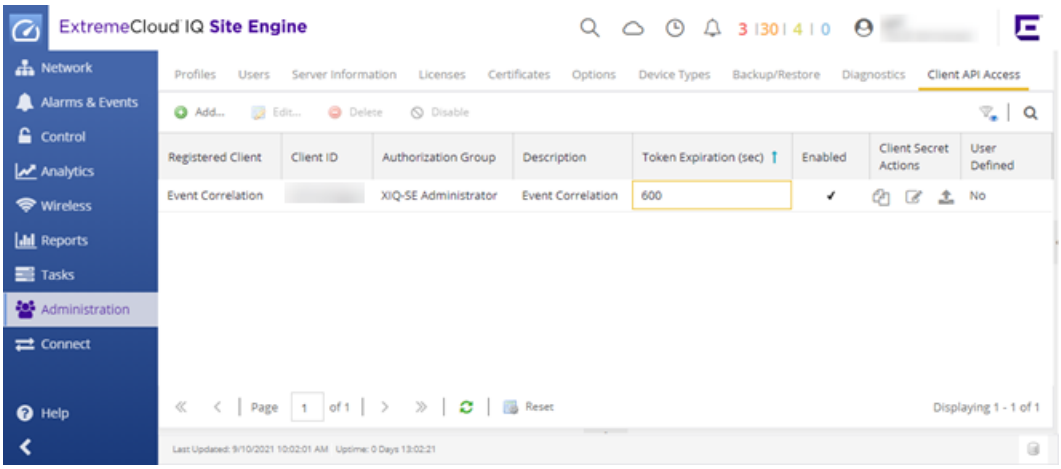
Via this tab, ExtremeCloud IQ - Site Engine provides a client ID and secret that can be used by the client to generate a token to use for accessing ExtremeCloud IQ - Site Engine. When the external application uses the token to access ExtremeCloud IQ - Site Engine, access is granted according the capabilities 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.

Related Information

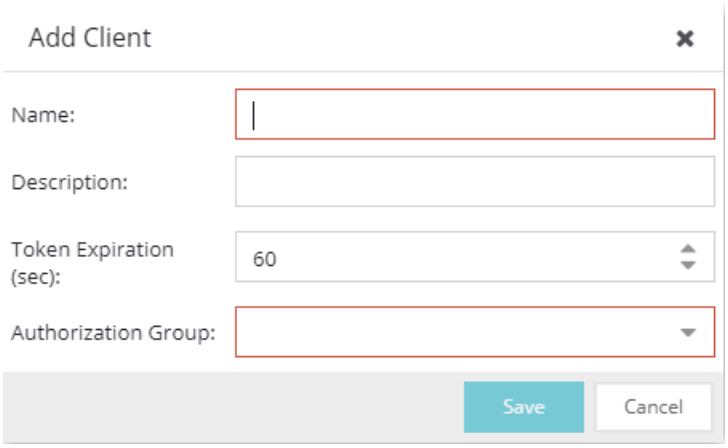
For information on related windows:

- Add/ Edit Client
- Northbound Interface
- Users/ Groups Tab
- Site Tab

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.

Related Information

For information on related windows:

- Client API Access
- Northbound Interface
- Event Correlation
- Northbound API

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.

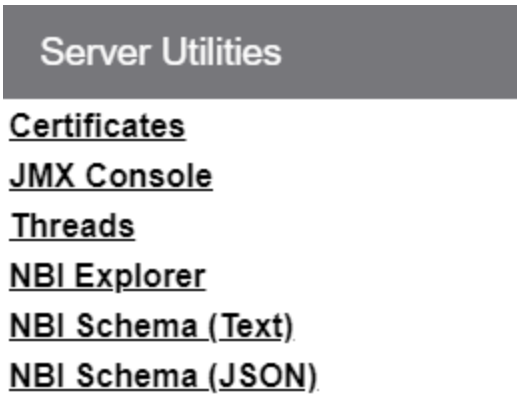
This topic contains the following sections:

Accessing NBI Tools in ExtremeCloud IQ - Site Engine

Using the NBI 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.

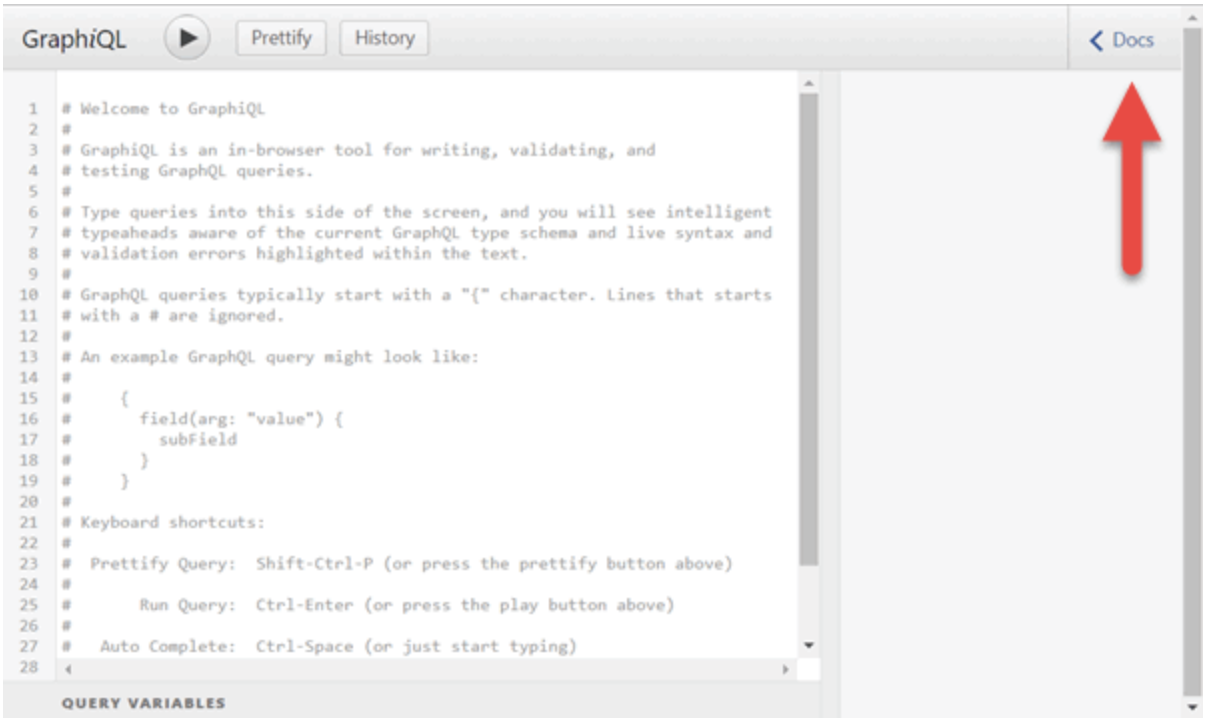
For example, to retrieve the IP address and policy domain for a device, enter:

```
#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']
```

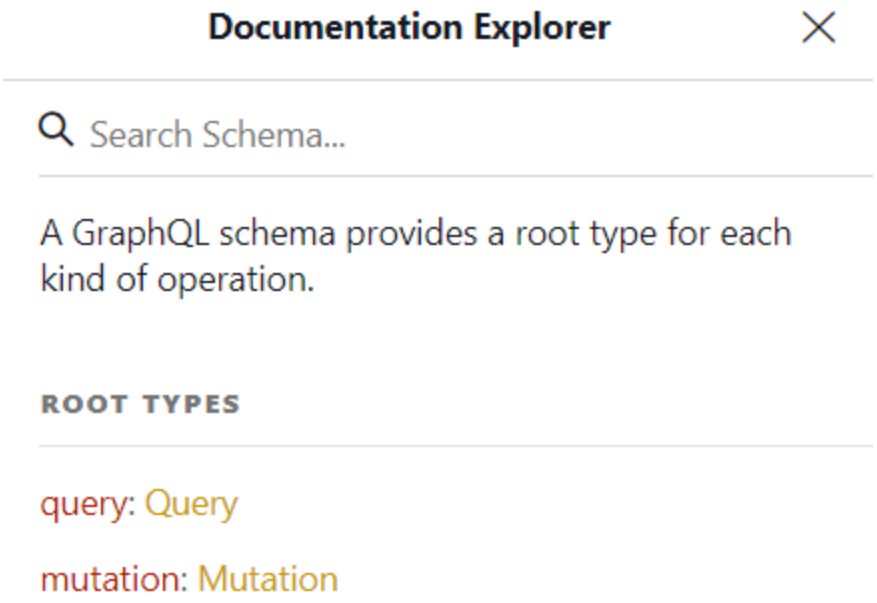
```
print " Policy Domain: ", device['policyDomain']
```

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.

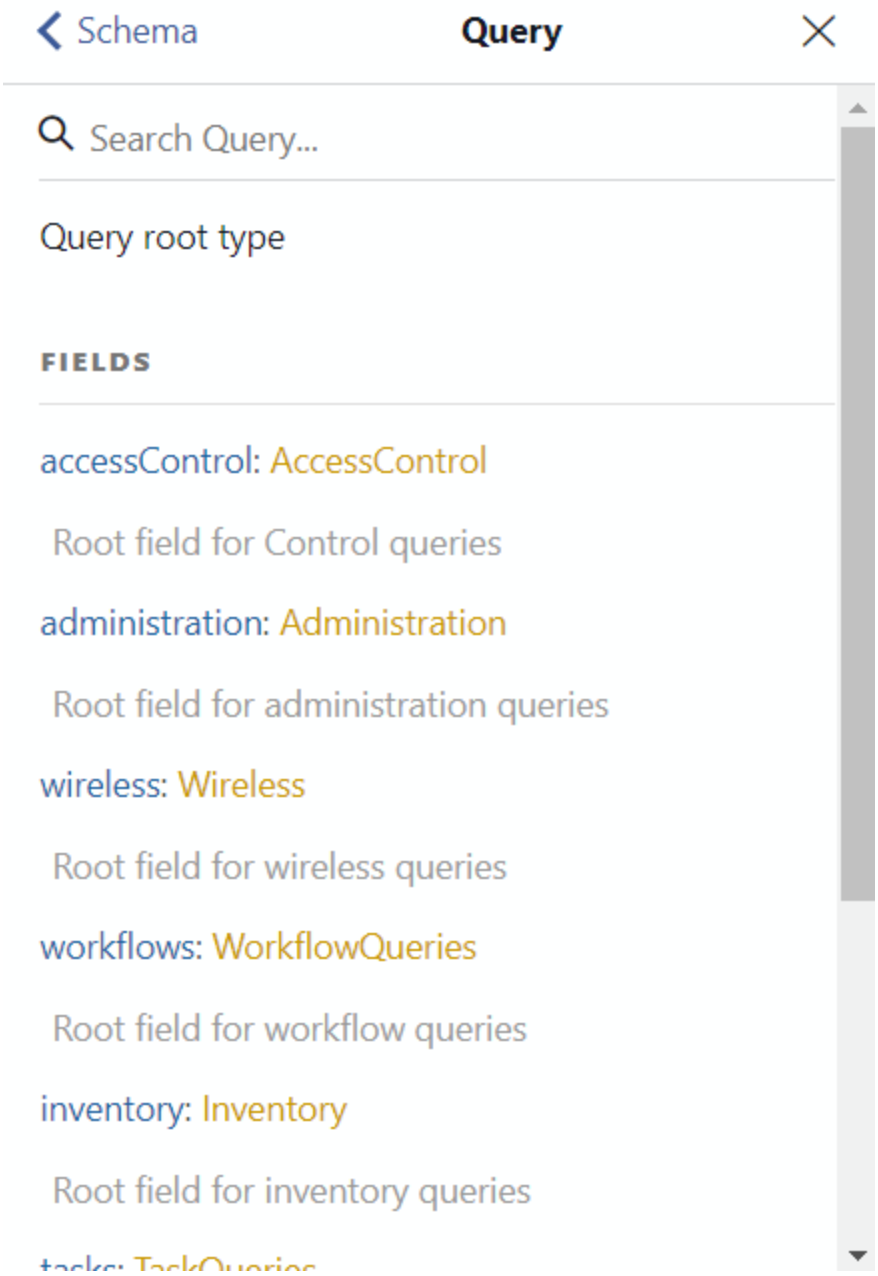


The Documentation Explorer opens.



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.

Related Information

- NBI API Site
- Administration
- Client API

Tasks Overview

The **Tasks** tab in ExtremeCloud IQ - Site Engine 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 you define.

The **Tasks** tab contains the following sub-tabs:

- Workflow Dashboard
- Scheduled Tasks
- Saved Tasks
- Scripts
- Workflows

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

Workflow Dashboard

The **Workflow Dashboard** tab 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

The **Scheduled Tasks** tab 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** tab 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

The **Scripts** tab 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

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 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 you configure on the **Scheduled Tasks** tab. Other action and task/workflow function sources can also trigger a workflow to run.

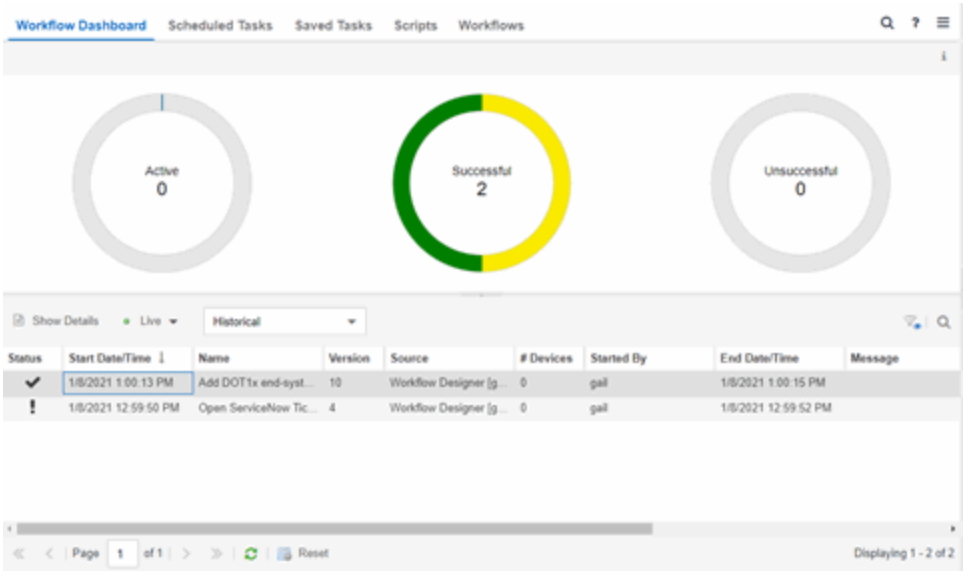
Related Information

For information on related tabs:

- Scheduled Tasks
- Saved Tasks
- Scripts
- Workflows
- Workflow Dashboard

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**.

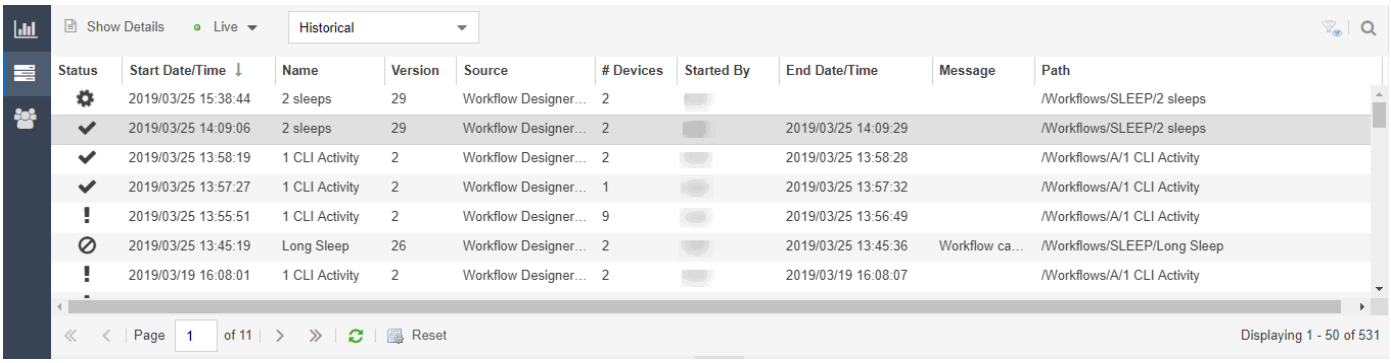
Unsuccessful

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.

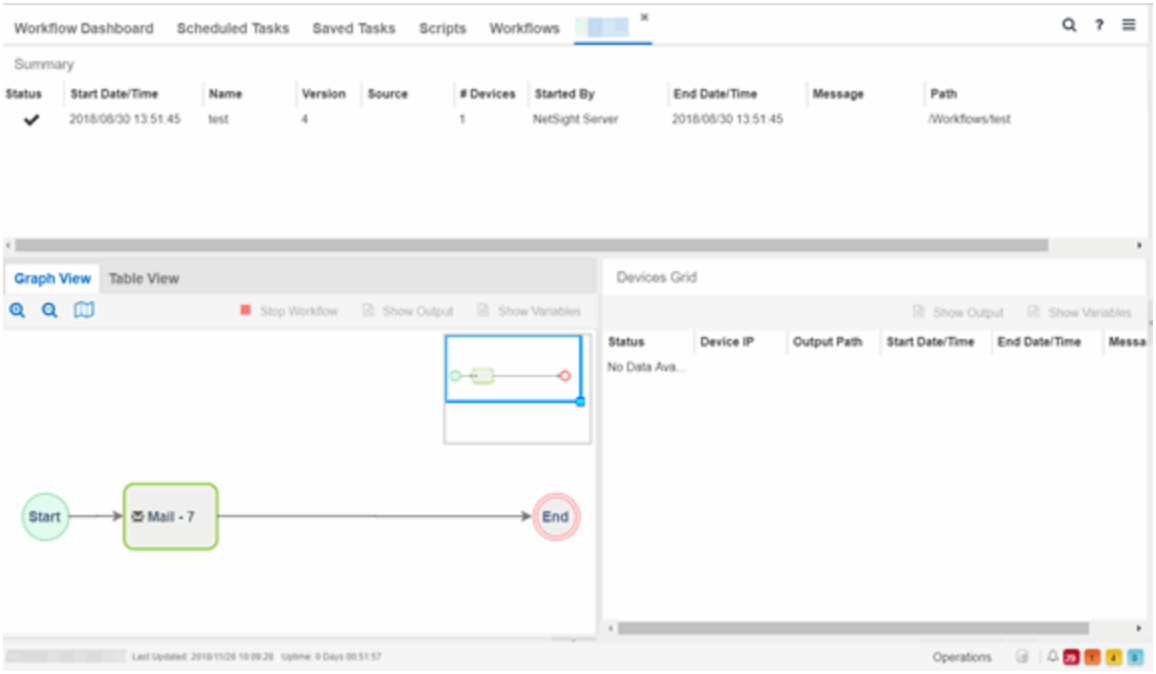
Message
Displays information regarding the reason for the Status (for example, Exceeded default time out).

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.

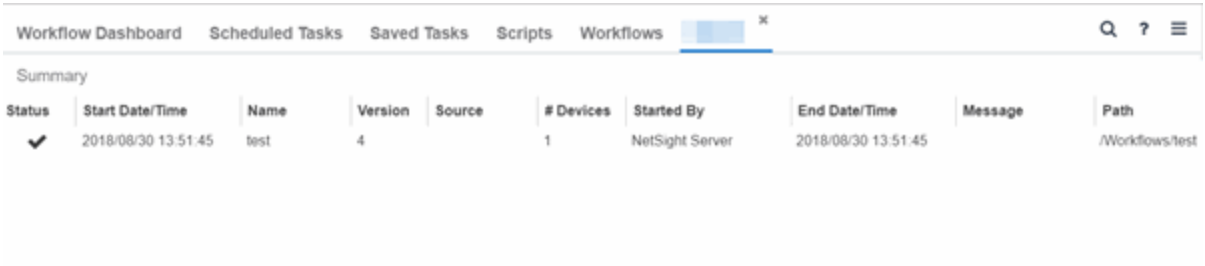


The **Workflow Details** view contains three sections:

- 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:

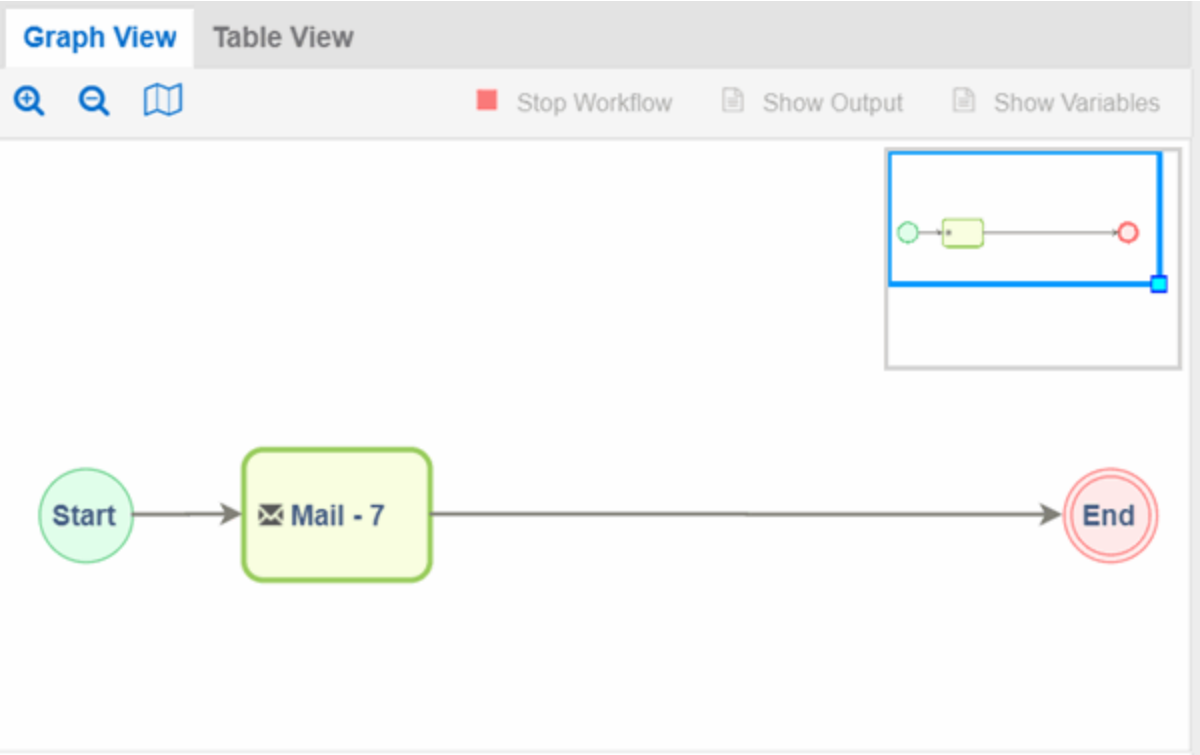
- Graph View
- Table View

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

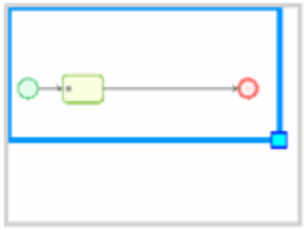
Use the buttons at the top of the **Graph View** tab to perform the following functions:

- **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

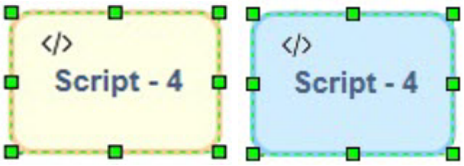
The mini map view displays the workflow run and the surrounding space in the graph view area.



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.

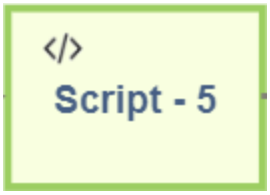
Workflow Run

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.

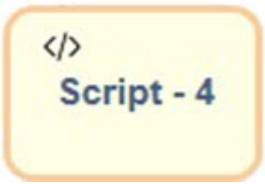
	Orange	A user canceled the activity.
	Blue	The activity is active.
	Red	The activity failed to complete.
	Grey	The workflow skipped the activity.

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).

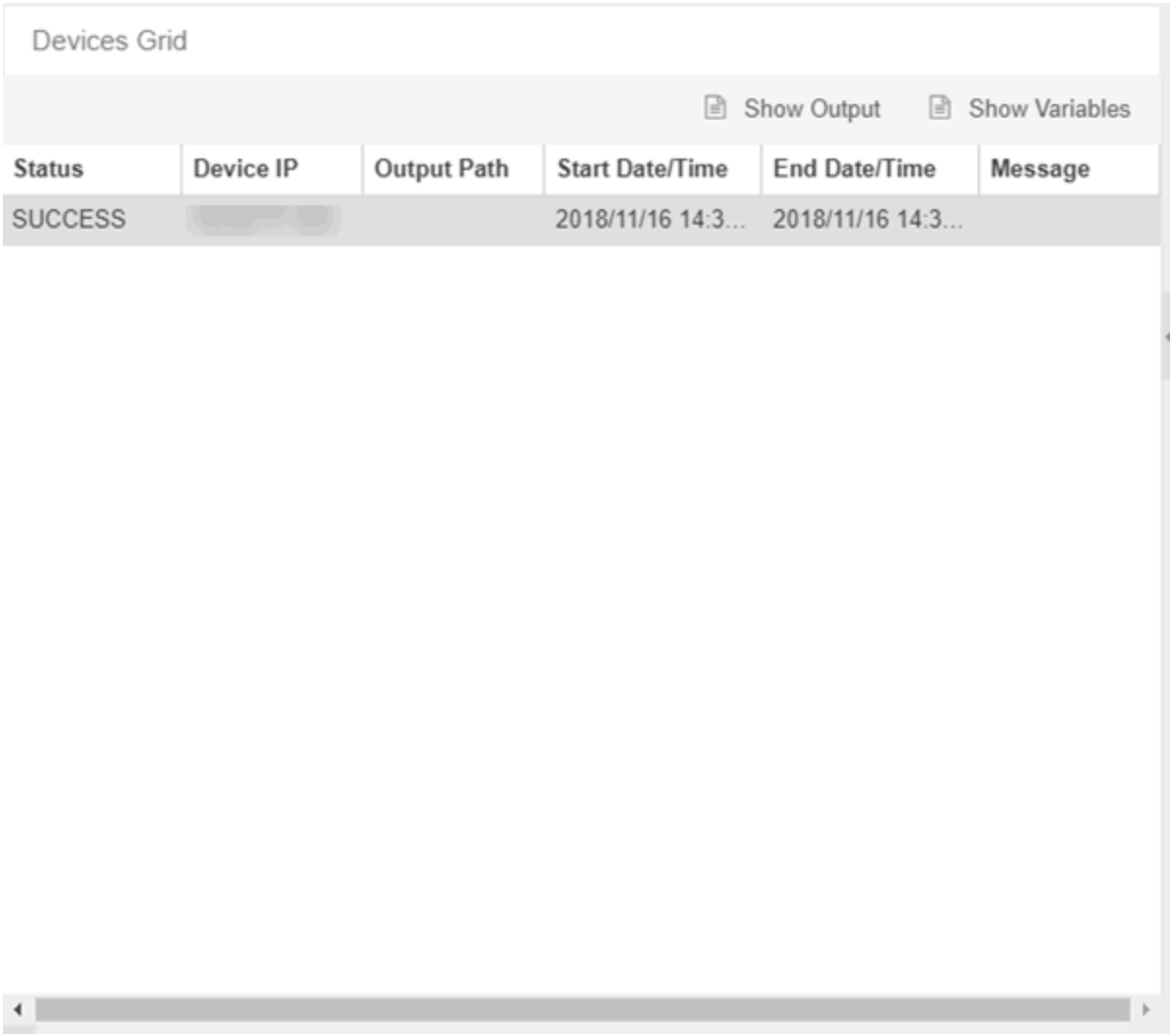
Start Date/ Time
Displays the date and time the activity started.

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.

Related Information

For information on related topics:

- Workflows
- Scripts
- How to Create Scripts in ExtremeCloud IQ - Site Engine
- Saved Tasks
- Scheduled Tasks

Scheduled Tasks Overview

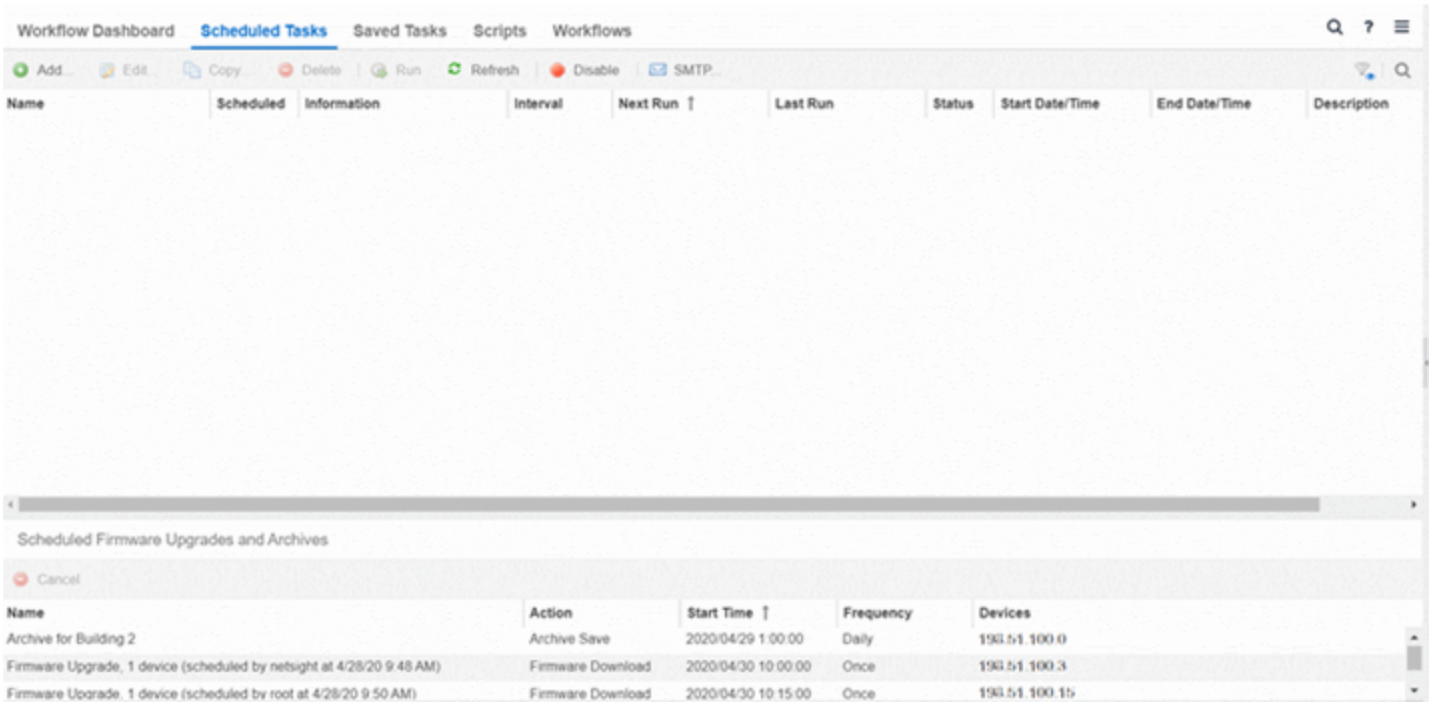
The **Scheduled Tasks** tab allows you to configure ExtremeCloud IQ - Site Engine to automatically perform the following tasks:

- 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 the SMTP Email Server window, 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)



The 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.

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 & 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.

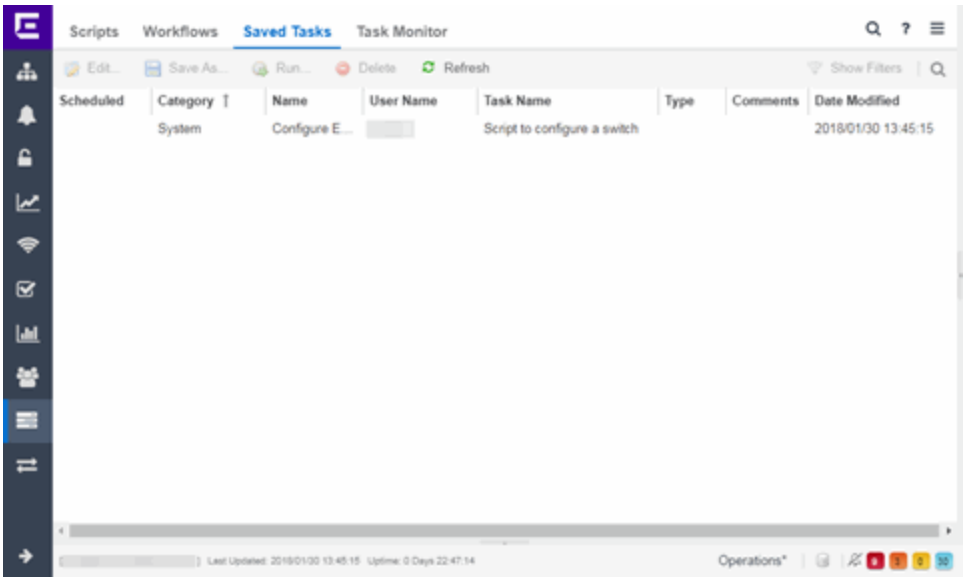
Related Information

For information on related tabs:

- How to Schedule Tasks
- Saved Tasks
- Scripts
- Workflows
- Workflow Dashboard
- Upgrade Firmware

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 checkmark 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.

Task Name
: The name assigned to the saved task. The **Task 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.

Date Modified
: The date the task was last modified.

Related Information

For information on related tabs:

- How to Create Scripts in ExtremeCloud IQ - Site Engine
- Workflows
- Scheduled Tasks

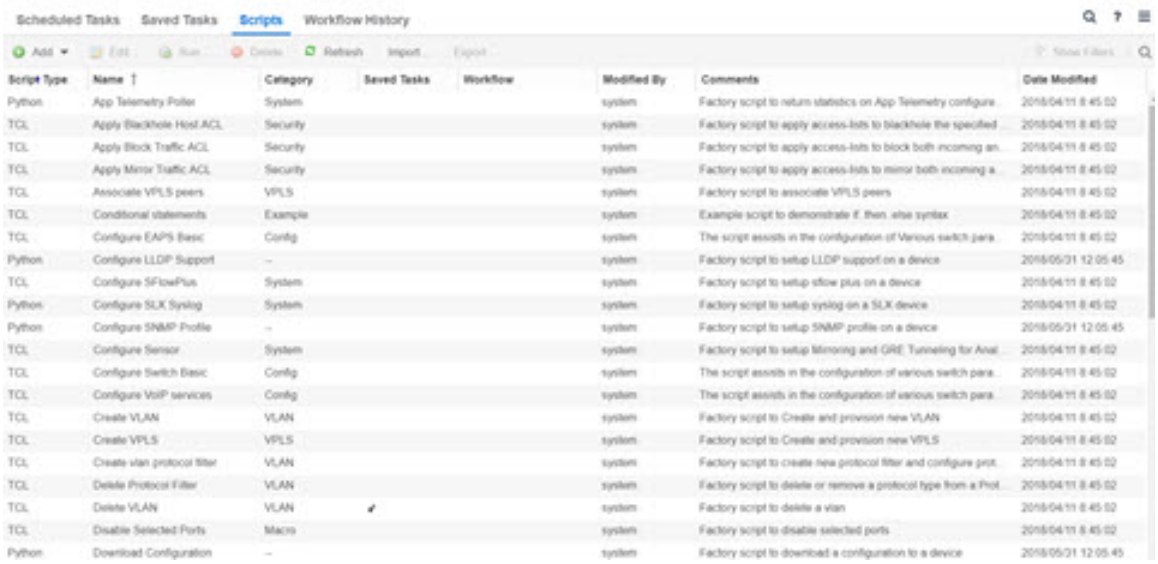
Scripts Overview

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 checkmark in this column indicates the script is configured as a saved task and is available on the **Saved Tasks** tab.

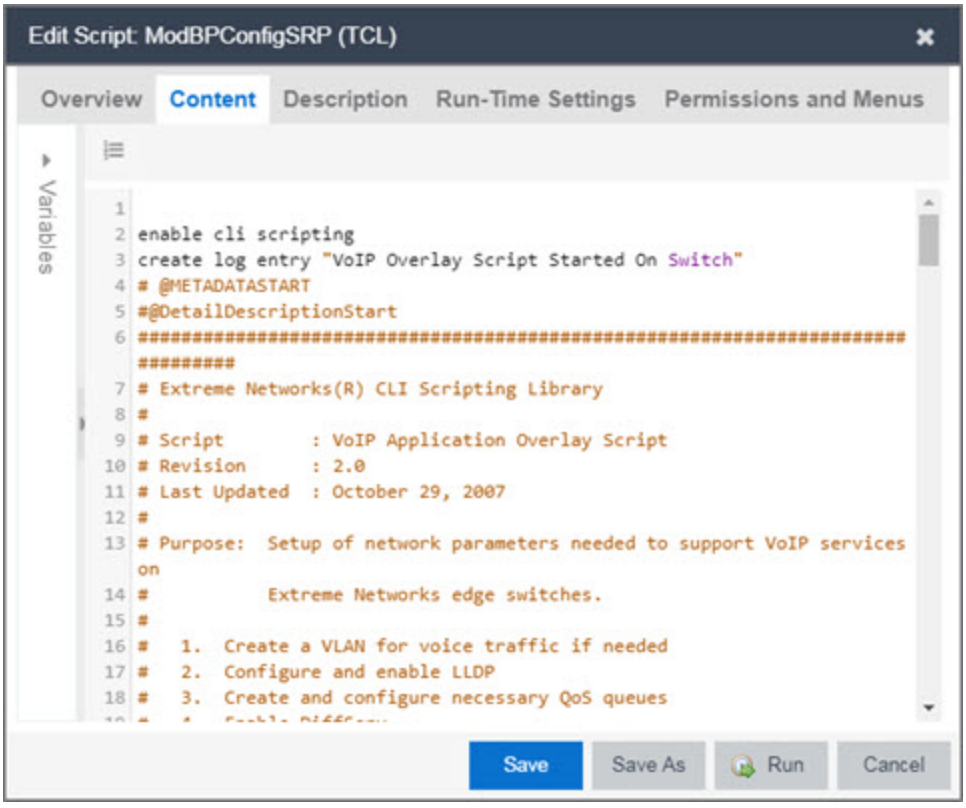
Workflow
: A checkmark in this column indicates the task is included in a workflow.

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.



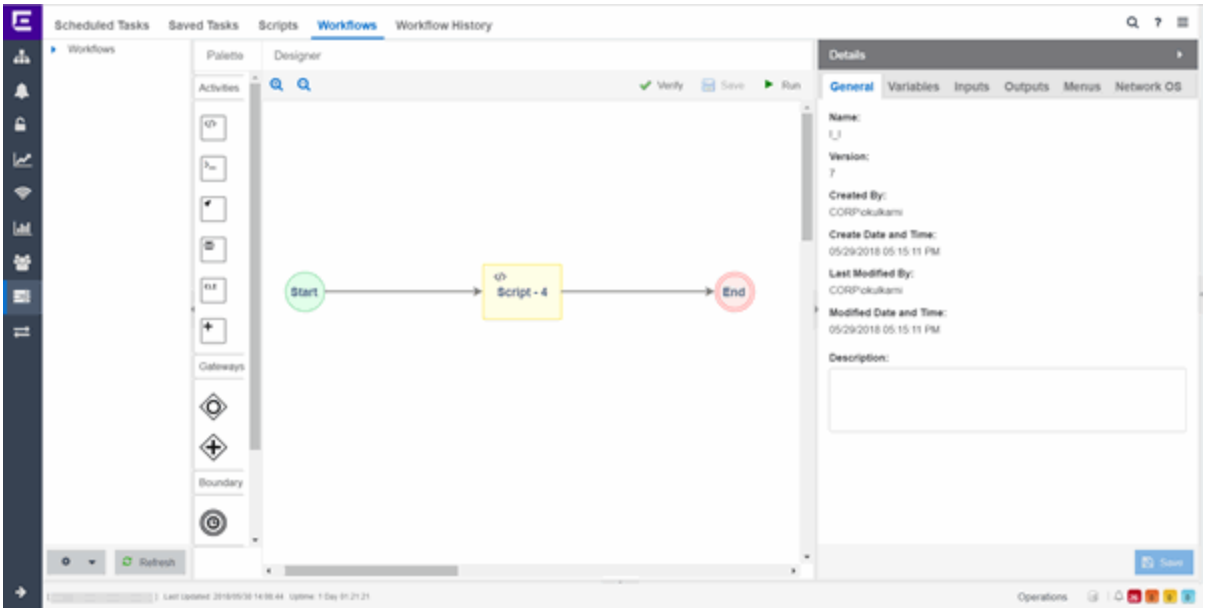
Related Information

For information on related tabs:

- How to Create Scripts in ExtremeCloud IQ - Site Engine
- Workflows
- Saved Tasks
- Scheduled Tasks

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.

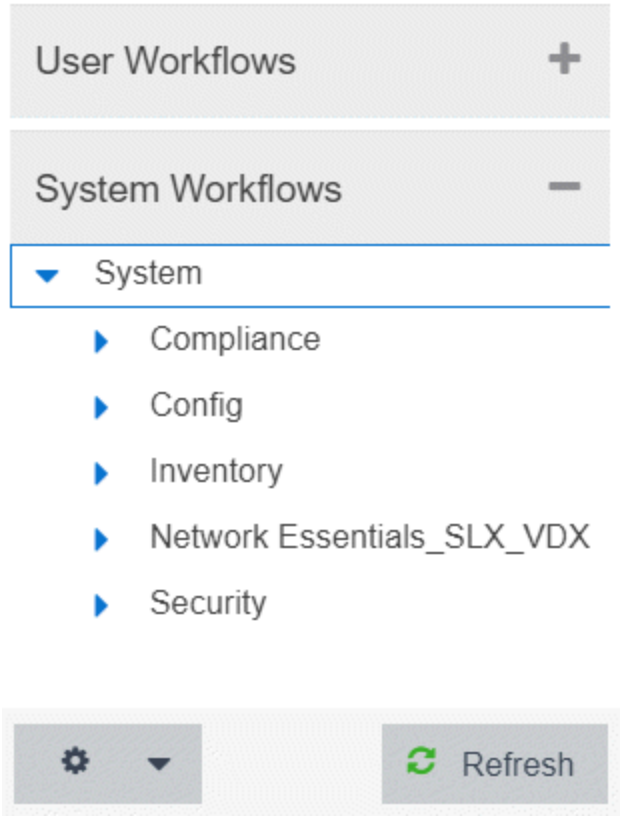
The **Workflows** tab contains four sections:

- 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

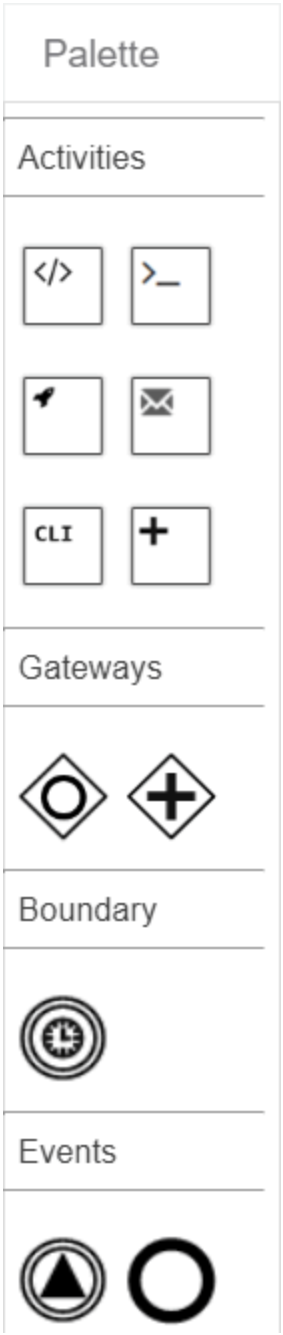
Select the **Gear** icon () to open a menu from which you can create a new workflow or workflow group, rename or delete the selected workflow or workflow group, or import or export a workflow as an encrypted file.

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

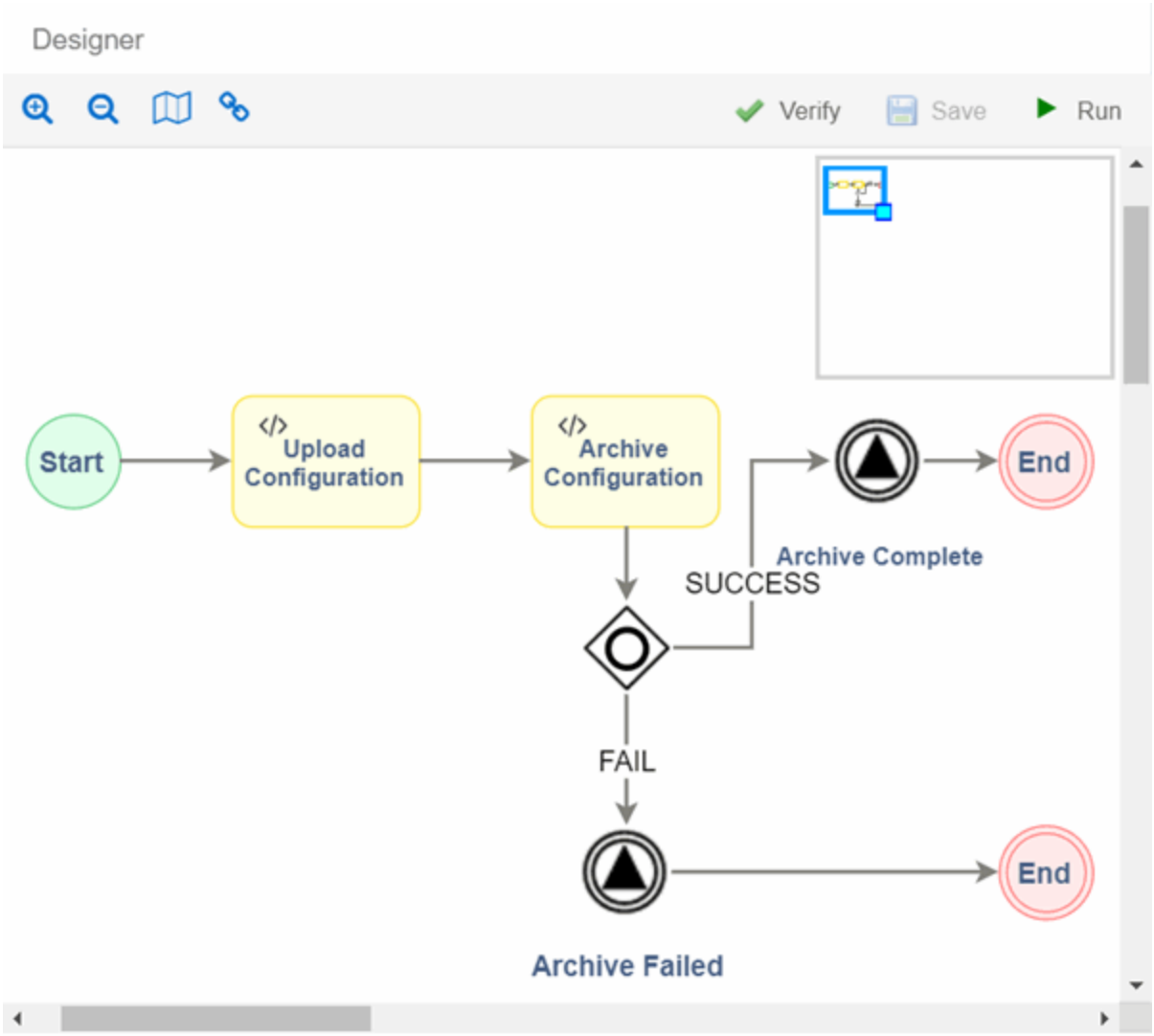
Activities	 Script Activity	Use the **Script Activity** icon to add a script to your workflow. Drag the **Script Activity** icon into the Designer at the location in the workflow where you want the script to execute. Select the script and use the **Details** section to configure the script for the workflow.
	 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.
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.
- **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.

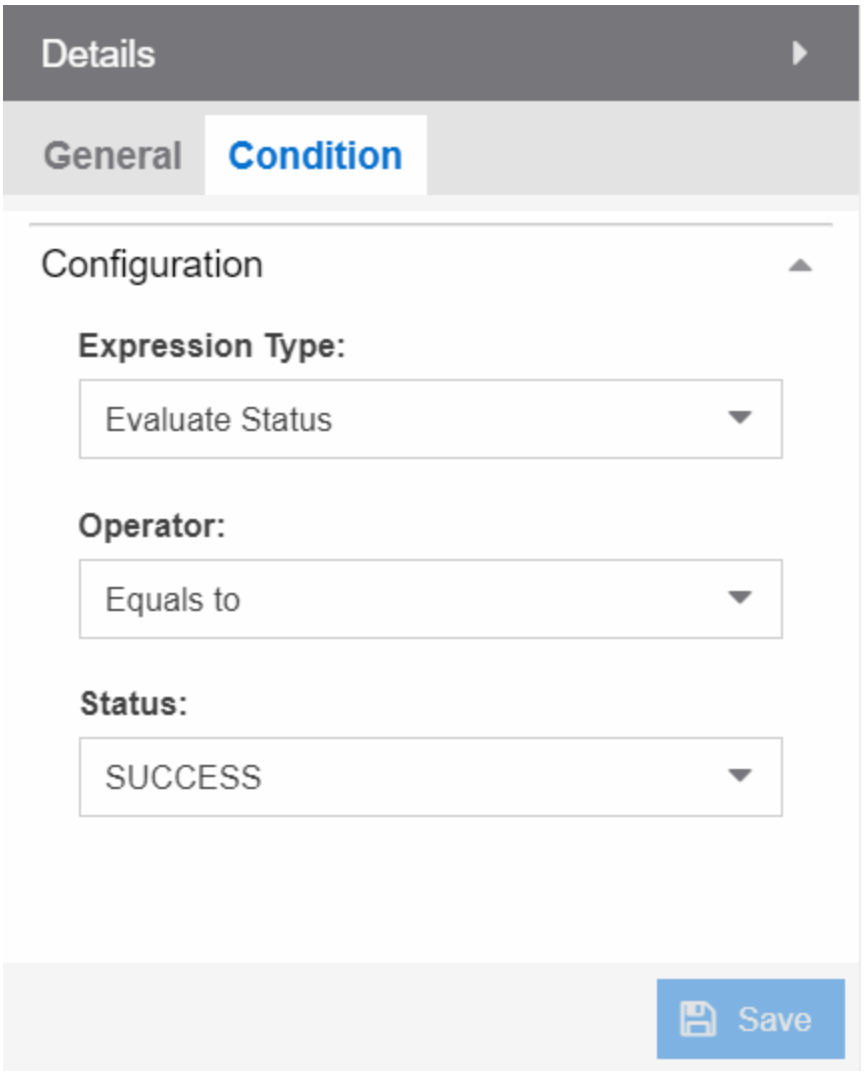
  NOTE: The '**-**' and '_' characters are also valid.

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.

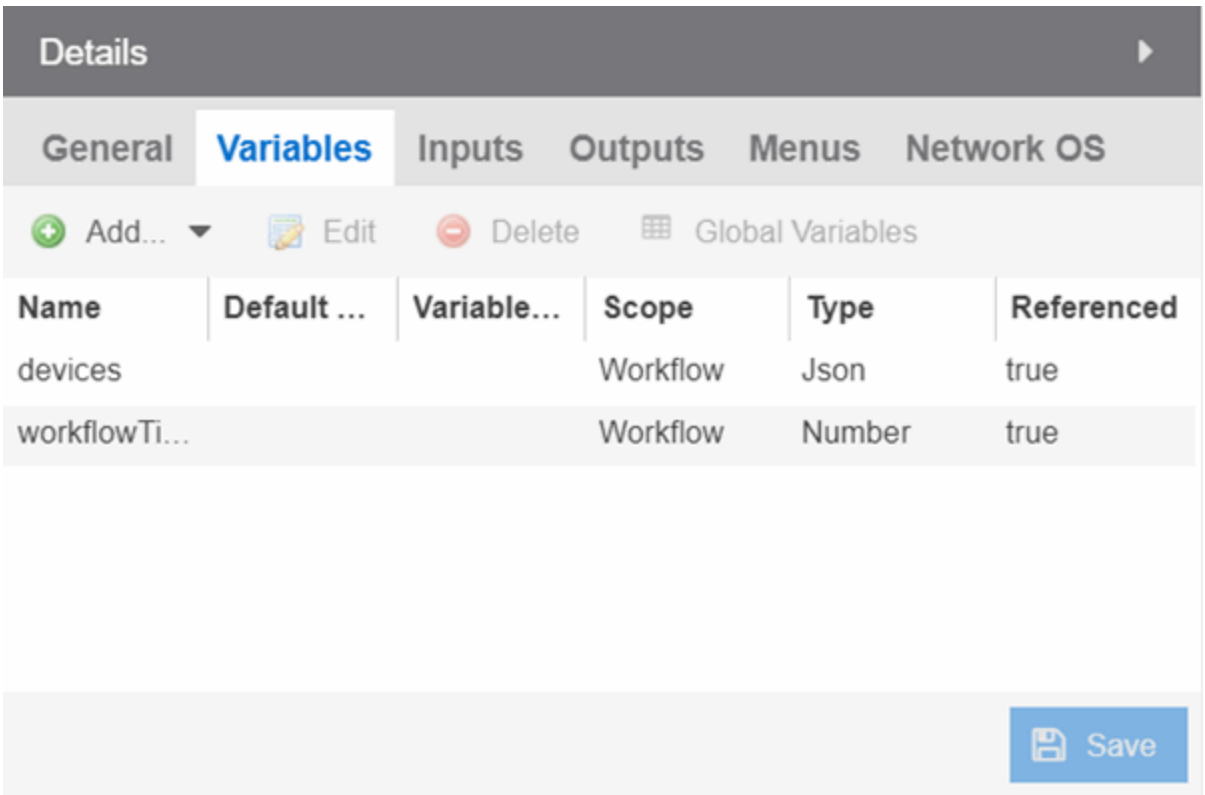
Value
: **Value** indicates the value against which ExtremeCloud IQ - Site Engine compares the **Variable** using the relationship defined as the **Operator** to determine if the workflow continues after the link.

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

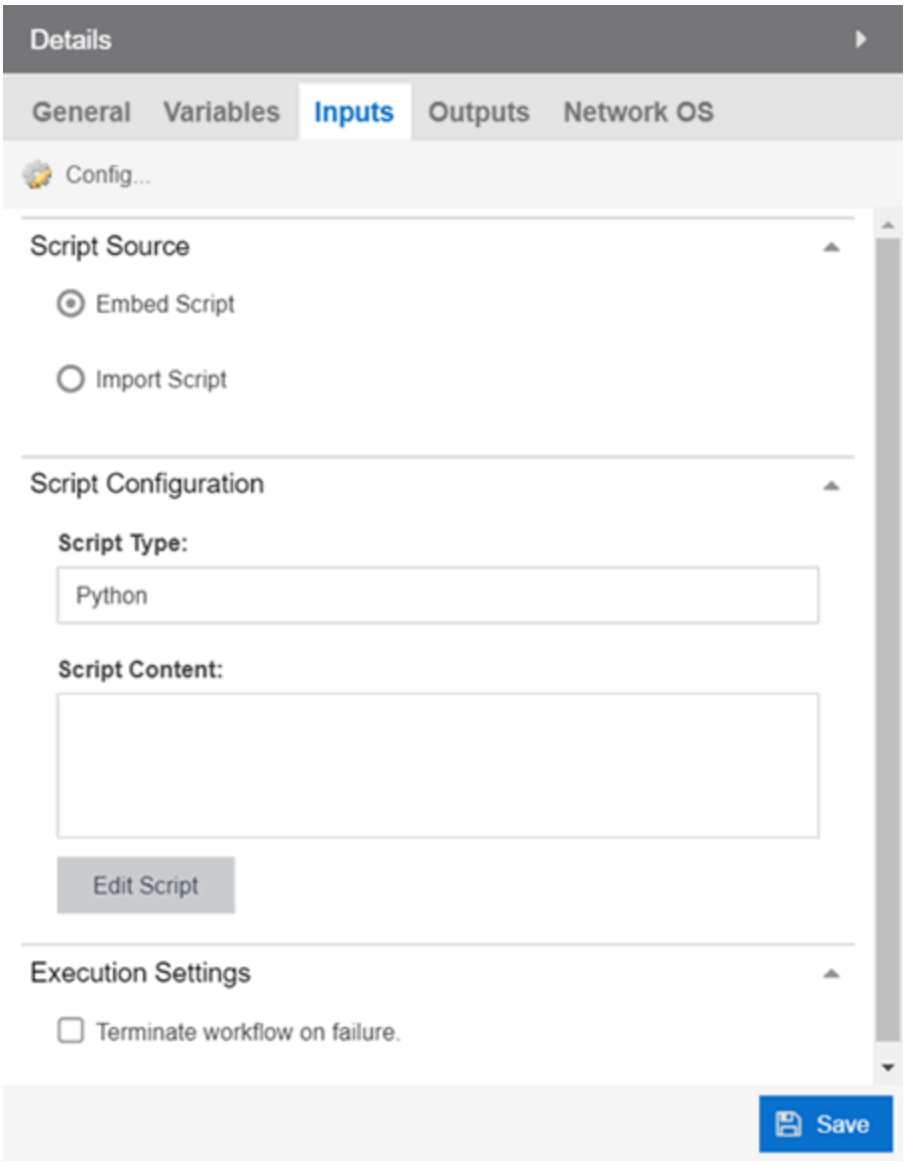
Select the button to open a new window, where you can select custom variables to include in your activity. Custom variables include system-defined variables and those user-defined variables you create on the Site > **Custom Variables** tab.

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.



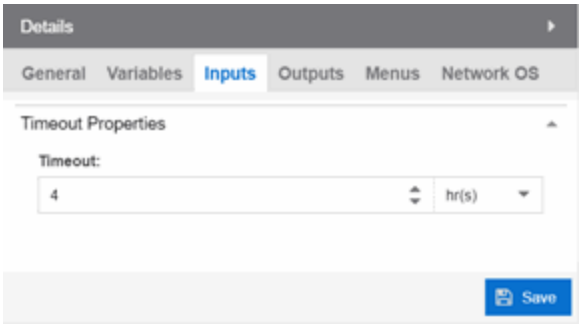
The fields on this tab change depending on the type of activity you select:

- 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.

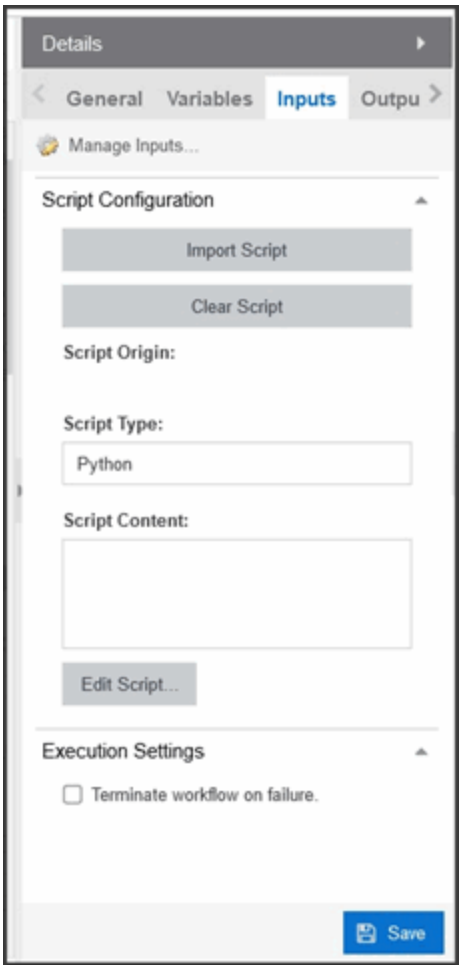


Timeout

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.



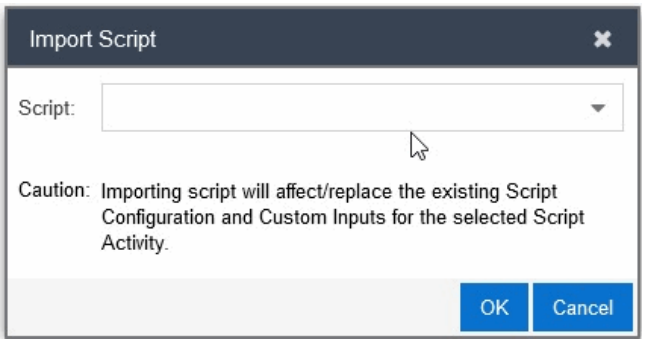
Manage Inputs

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.

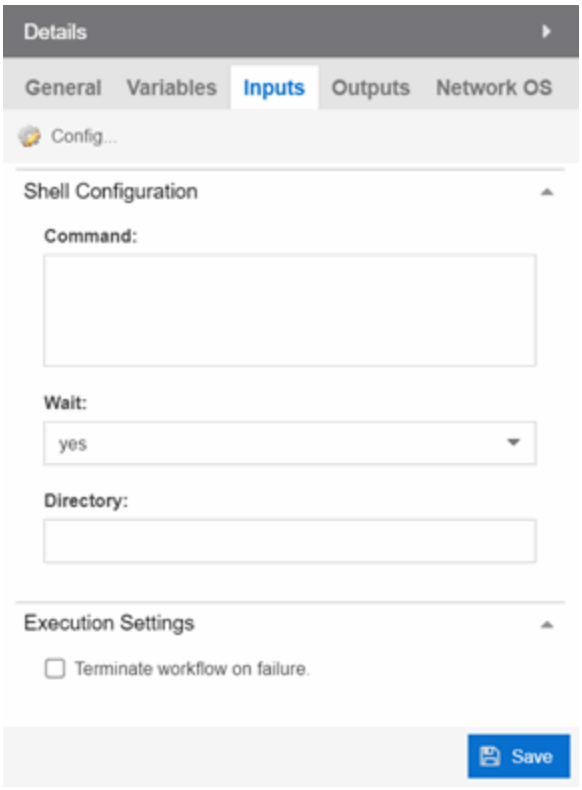
Edit Script
: Select the **Edit Button** to change the **Script Content**.

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.

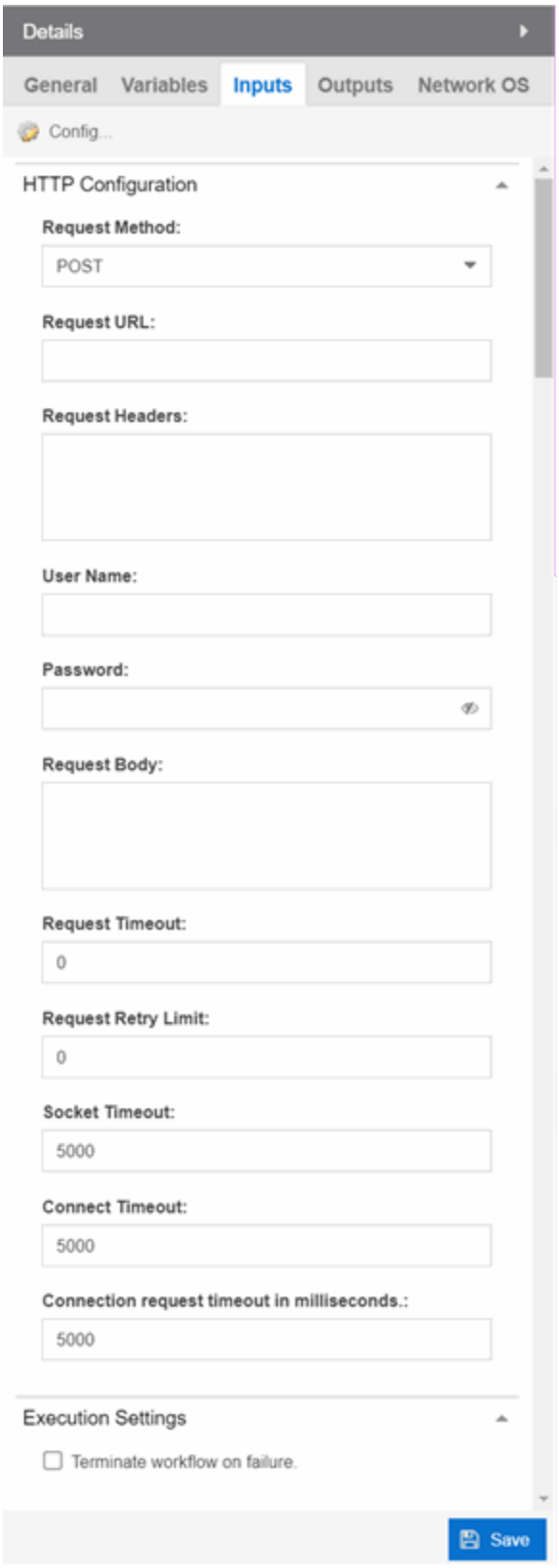
Terminate workflow on failure
: Select the checkbox to stop the workflow if the workflow does not complete the activity successfully.

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.

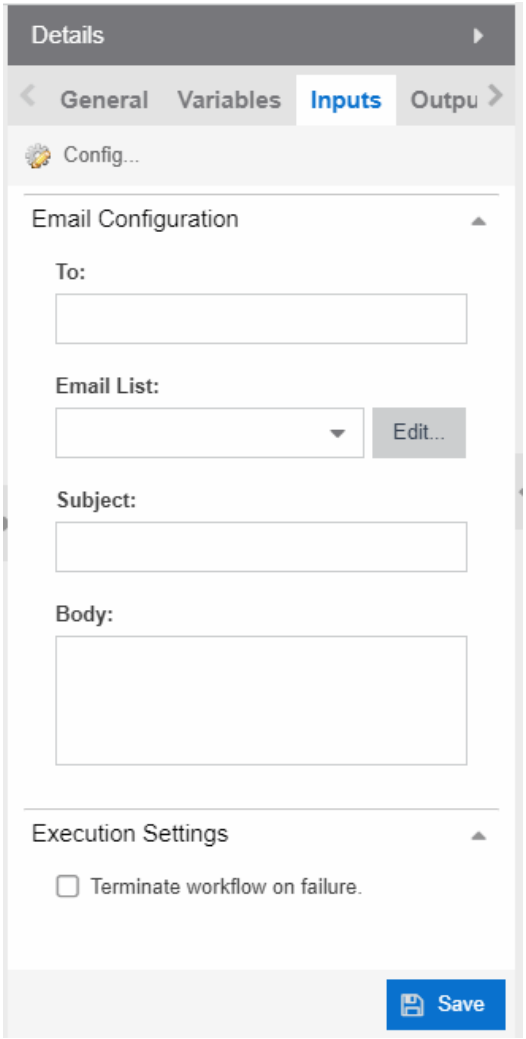
Connection request timeout in milliseconds
: The amount of time (in milliseconds) ExtremeCloud IQ - Site Engine waits when requesting a connection from the connection manager. ExtremeCloud IQ - Site Engine performs a check every 10 seconds, so if the timeout is set to 10 seconds for an activity, then 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.

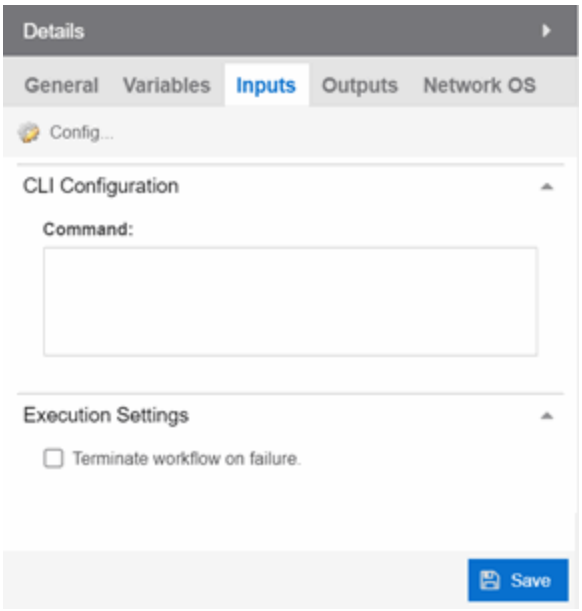
Save

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.

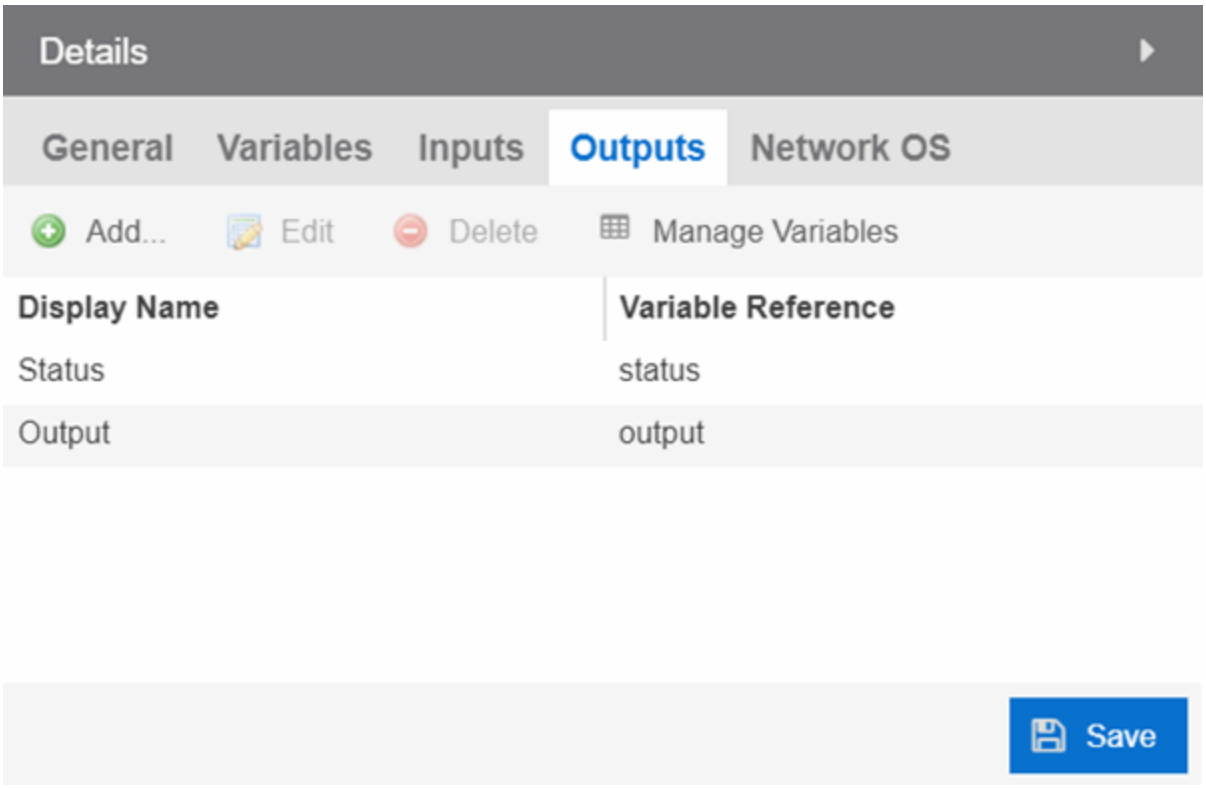
Command
: The CLI command or commands run as part of your workflow.

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.



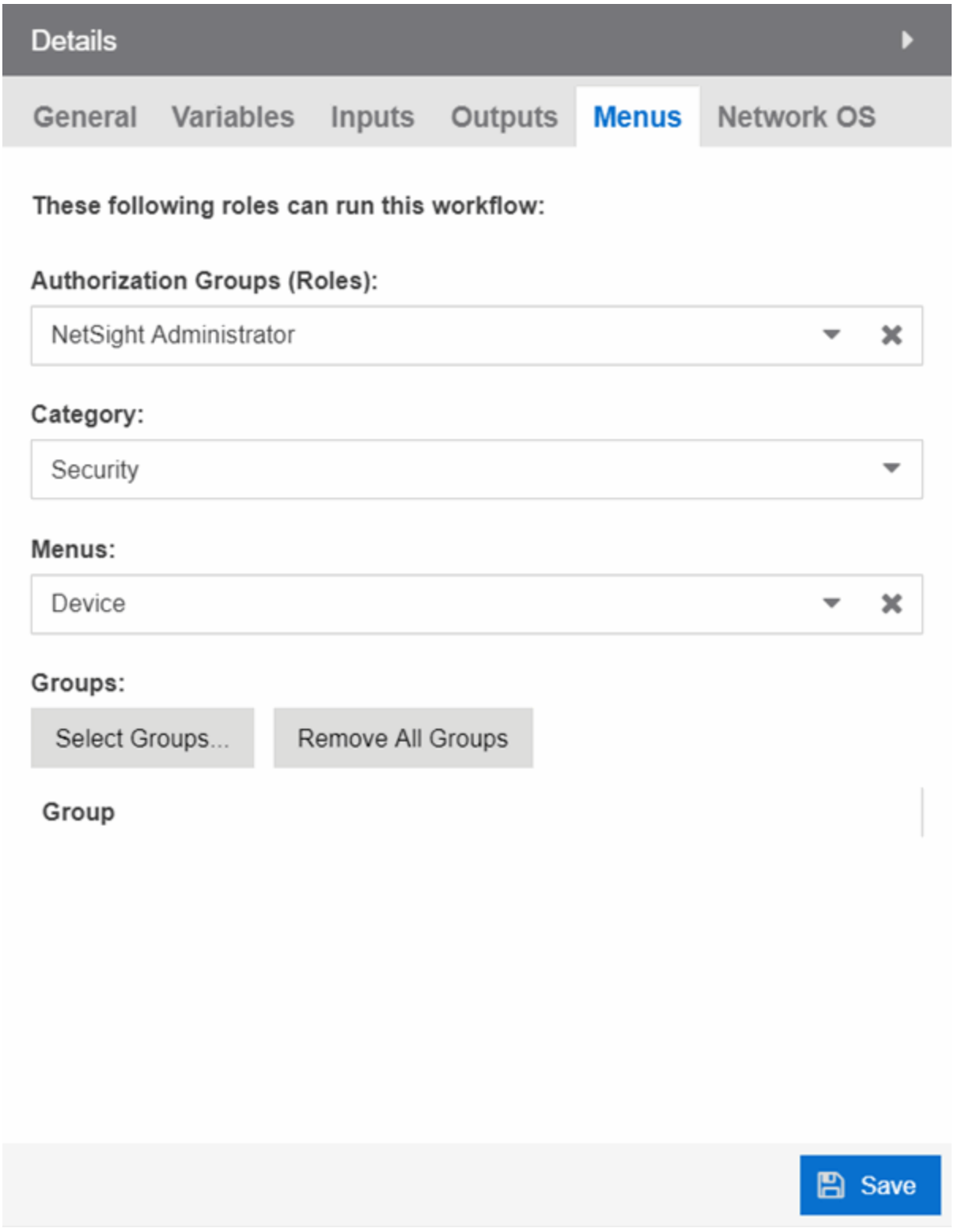
The **Outputs** tab allows you to specify the output variable you use to determine the result of the activity. You can then use this variable as the input variable for the next activity in the workflow, or as the final output in the workflow.

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

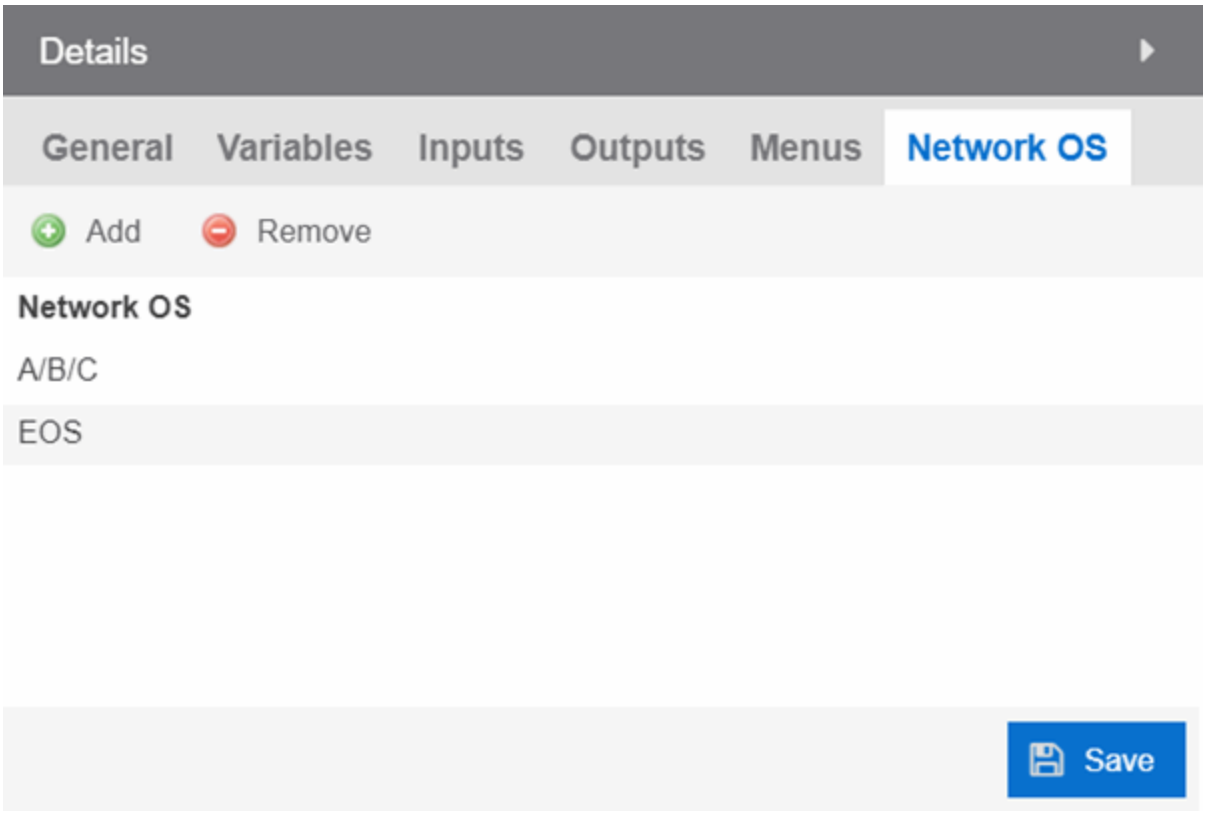
Select the button to open the **Select Device Groups** window, from which you can select the device groups for which the workflow displays in the Tasks submenu.

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.

Related Information

For information on related tabs:

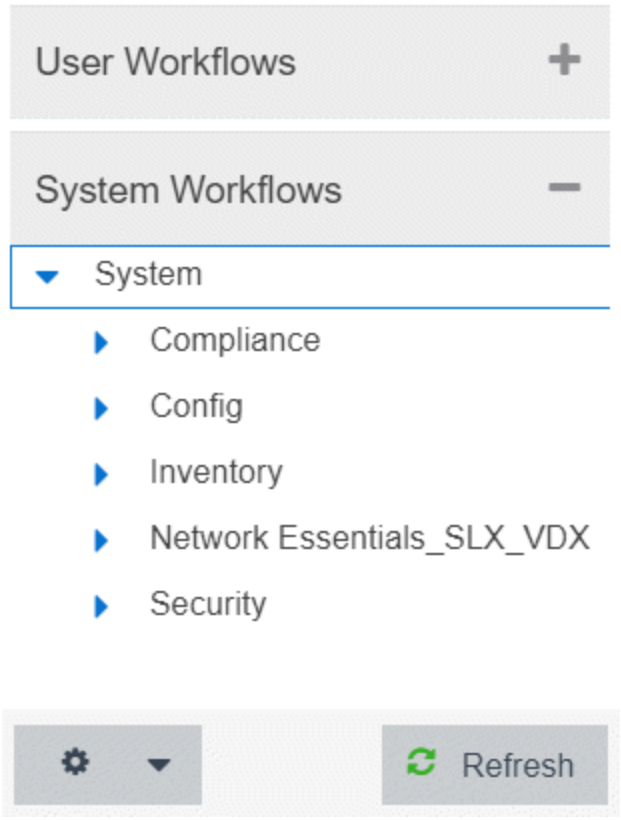
- How to Create Scripts in ExtremeCloud IQ - Site Engine
- Saved Tasks
- Scheduled Tasks
- Workflow Dashboard

System Workflows

The **Workflows** tab contains system-defined workflows as well as workflows you create.

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 VOSS, 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 VOSS, 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 VOSS, 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 VOSS 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 VOSS devices.

NOTE: This forces the device to reset.

Enable SPBM boot config mode

Enables the SPBM boot config flag for VOSS 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 the EXOS-VPEX folder configure devices so you can onboard or remove VPEX Bridge Port Extenders on EXOS 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 from EXOS

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 VOSS vIST cluster devices and ExtremeXOS devices.

MLAG port on CBs and LAG on remote EXOS
Configures MLAG between VOSS vIST cluster devices and ExtremeXOS devices.

MLAG with VOSS Cluster
Configures MLAG between VOSS vIST cluster devices and ExtremeXOS 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.

Related Information

For information on related topics:

- Workflows
- Scripts
- How to Create Scripts in ExtremeCloud IQ - Site Engine
- Saved Tasks
- Scheduled Tasks

Importing Workflows

The **Workflows** tab allows you to define a complex series of activities that run in the order in which you configure them.

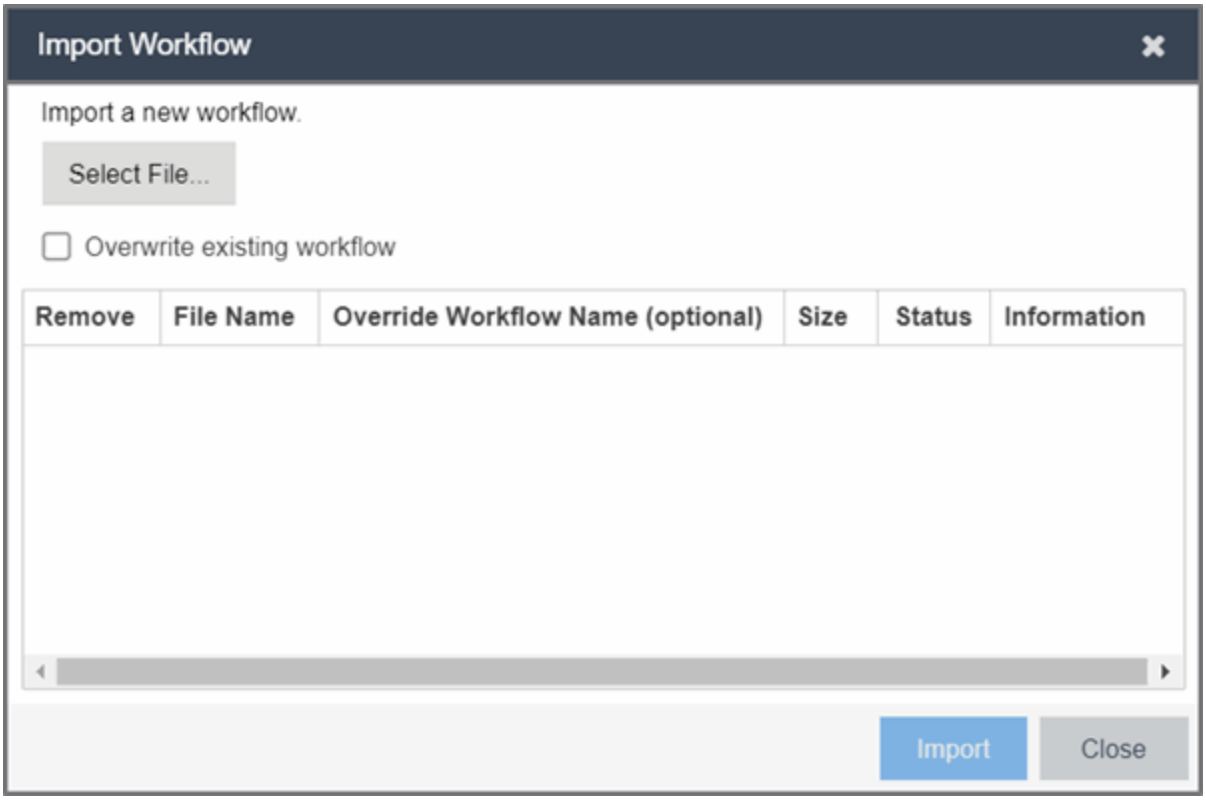
You can import saved User Workflows[1] to ExtremeCloud IQ - Site Engine using the following steps:

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.

[1]Only User Workflows can be imported or exported. System Workflows cannot be imported or exported.

3. Select **Import**.

   The **Import Workflow** window displays.



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

Related Information

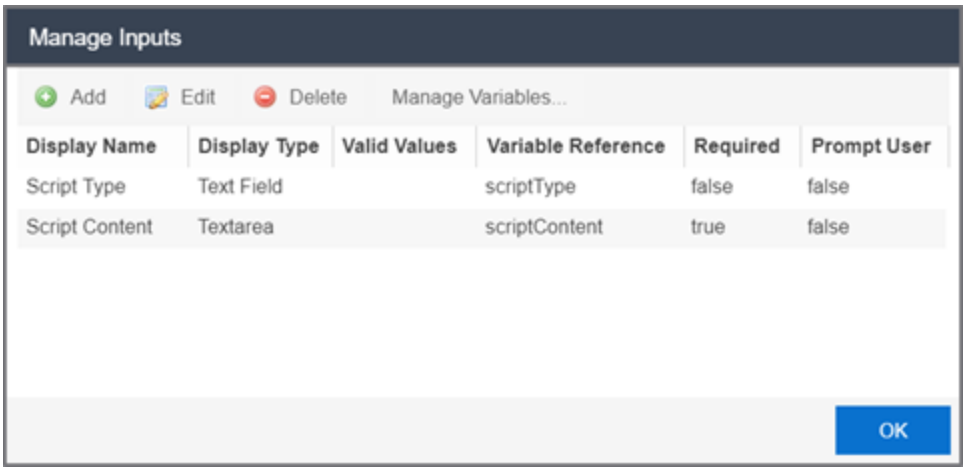
For information on related tabs:

- How to Create Scripts in ExtremeCloud IQ - Site Engine
- Saved Tasks
- Scheduled Tasks
- Workflow Dashboard

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.

Related Information

For information on related topics:

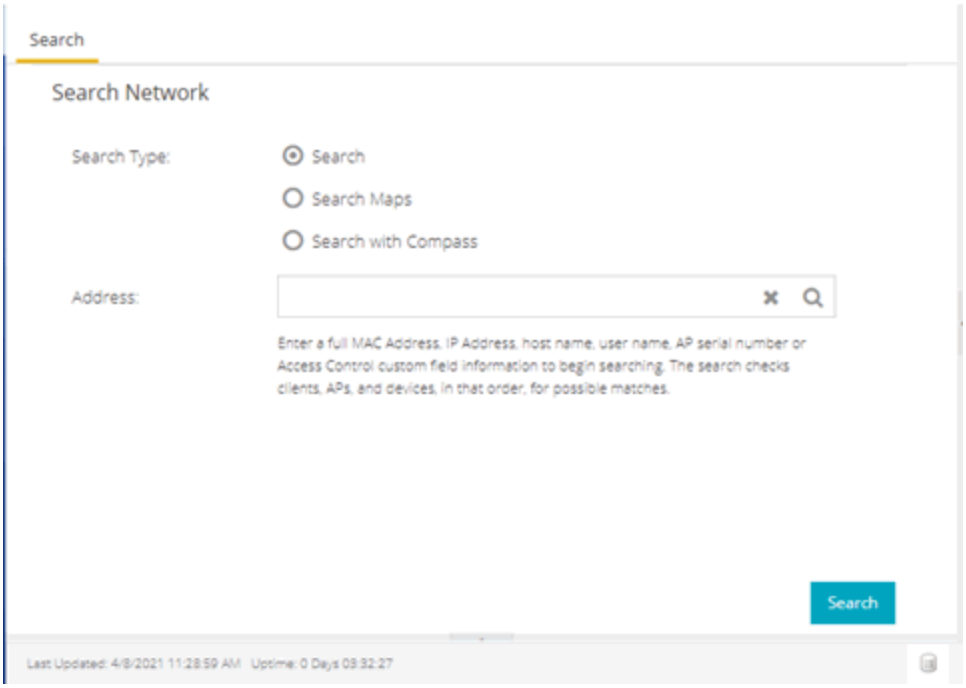
- Inputs

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 ExtremeControl authenticated client.

To view ExtremeCloud IQ - Site Engine Search Network, you must be a member of an authorization group assigned the NetSight OneView > Access OneView Search capability. To perform a Search with Compass, you must also have the NetSight Console > Launch a NetSight 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

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 ExtremeControl 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 ExtremeControl 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 ExtremeControl 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, ExtremeControl Gateway, or switch, one device is returned.

Related Information

For information on related tabs:

- Administration
- Alarms and Events
- Network
- Reports
- Wireless

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.

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 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.

Related Information

For information on related topics:

- Sites
- Discovered
- How to Create and Edit Maps
- Device Operations

How to 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 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.

Related Information

For information on related topics:

- Users
- Authorization Group Capabilities

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.

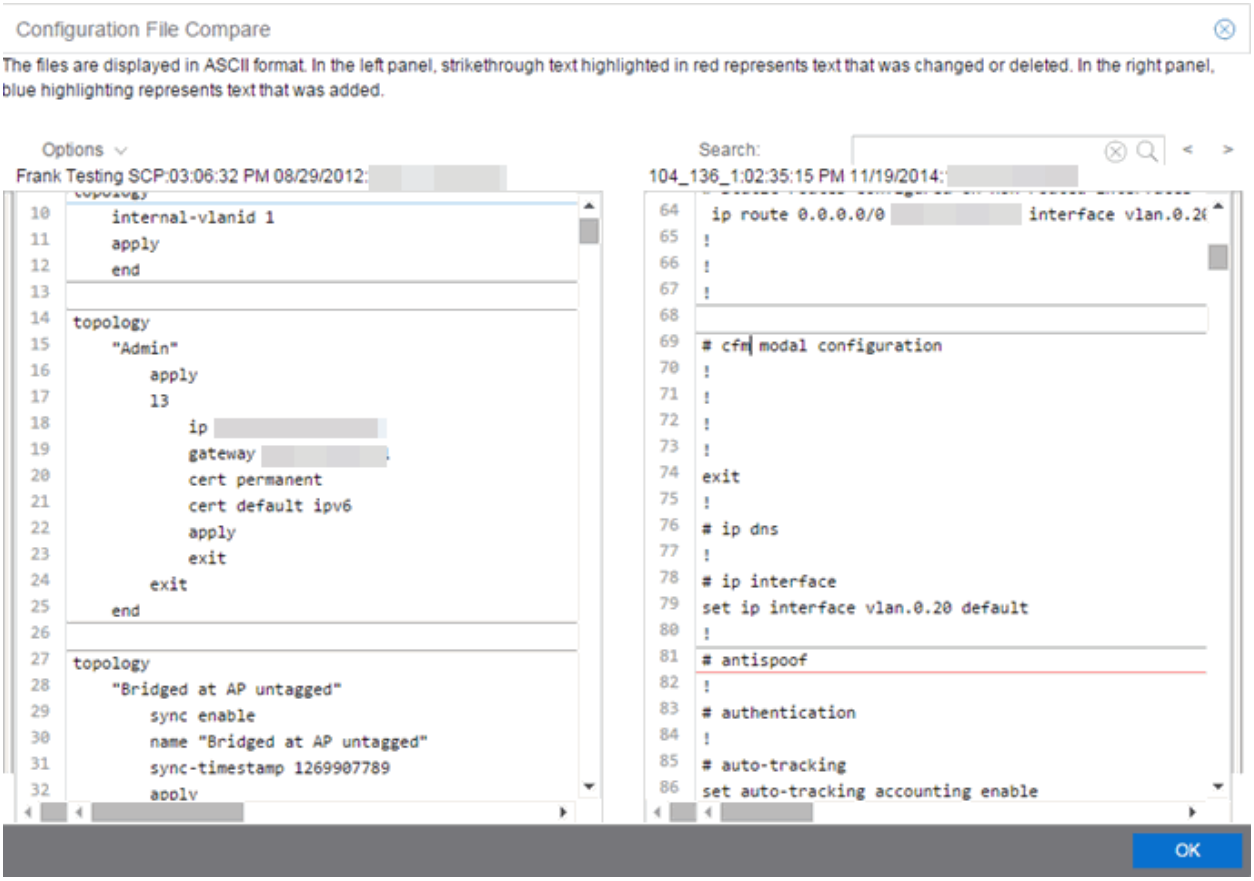
Select the Device > Device Archives report. Select the **Archive Details** tab in the right panel and then select the **Archives by Device** sub-tab.

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.

Related Information

For information on related topics:

- Network
- Reports

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

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.

- NetSight OneView > Access OneView
- NetSight OneView > Access OneView Reports

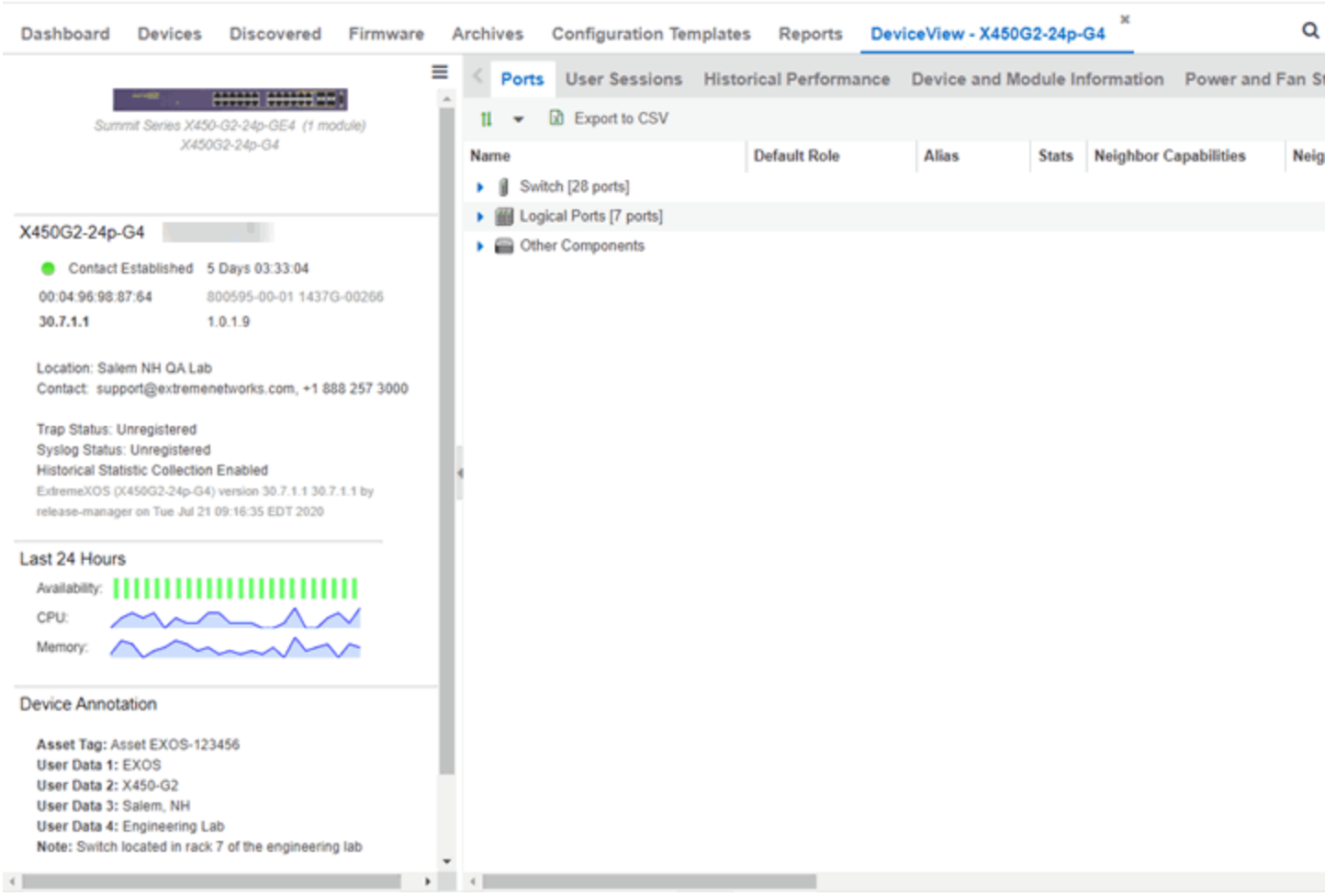
- NetSight OneView > Events and Alarms > OneView Event Log Access
- NetSight OneView > FlexView > OneView FlexView Read Access

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.

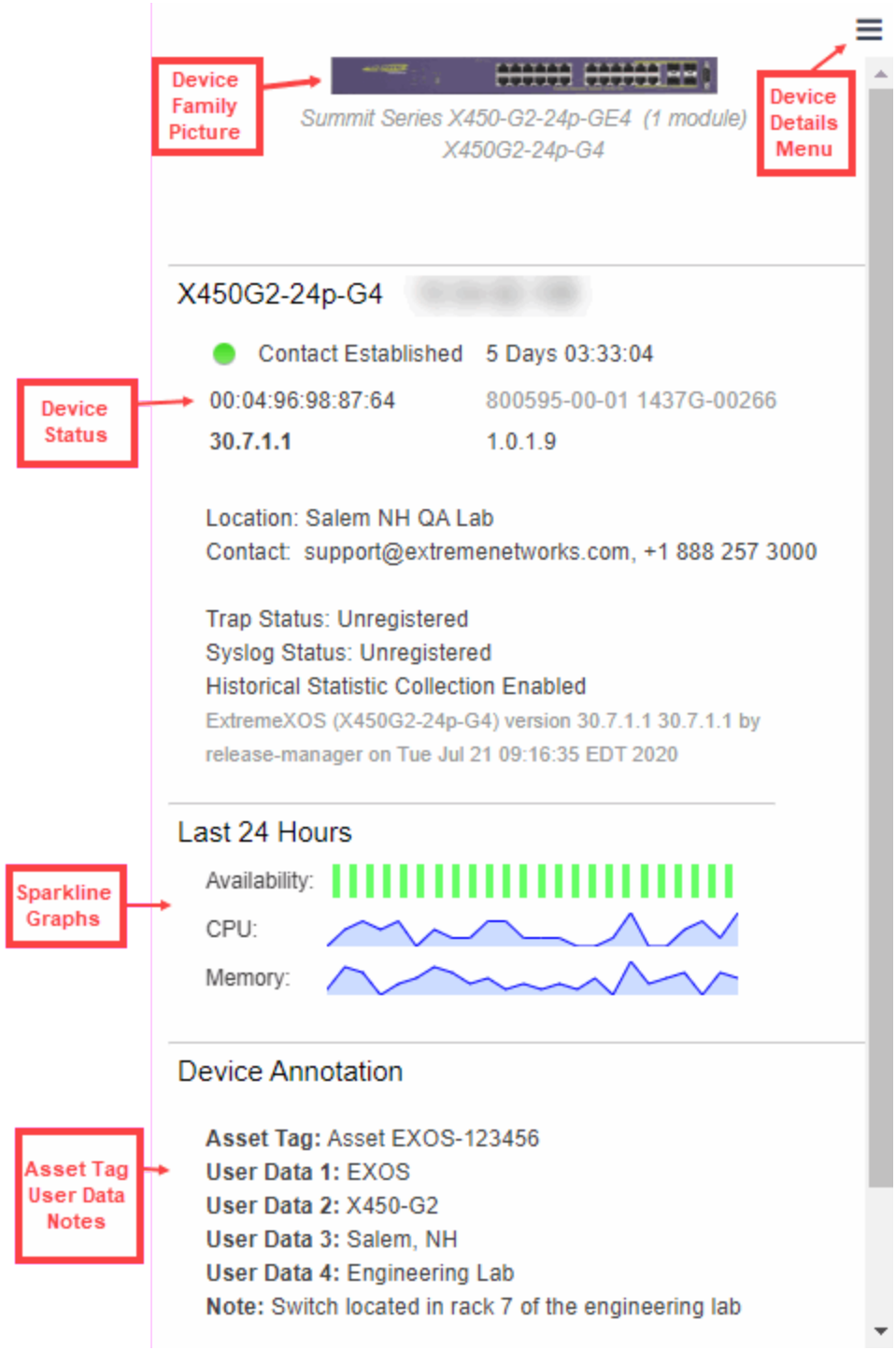
Device View Panels

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.
- **Firmware Updates Available** —If there are new firmware releases available for the device (based on the results from the latest Check for Firmware Updates operation), the Firmware Update icon displays. Right-click on the icon to open a window listing the current available firmware releases with links to download the firmware.
- **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.

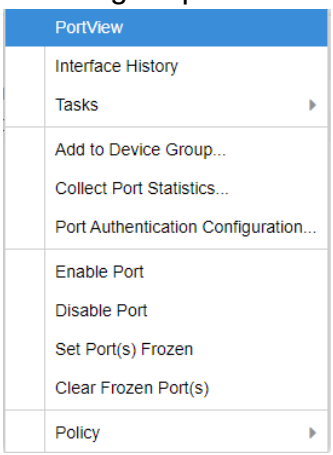
Ports

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.
- 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 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.

Related Information

For information on related topics:

- Network Tab

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

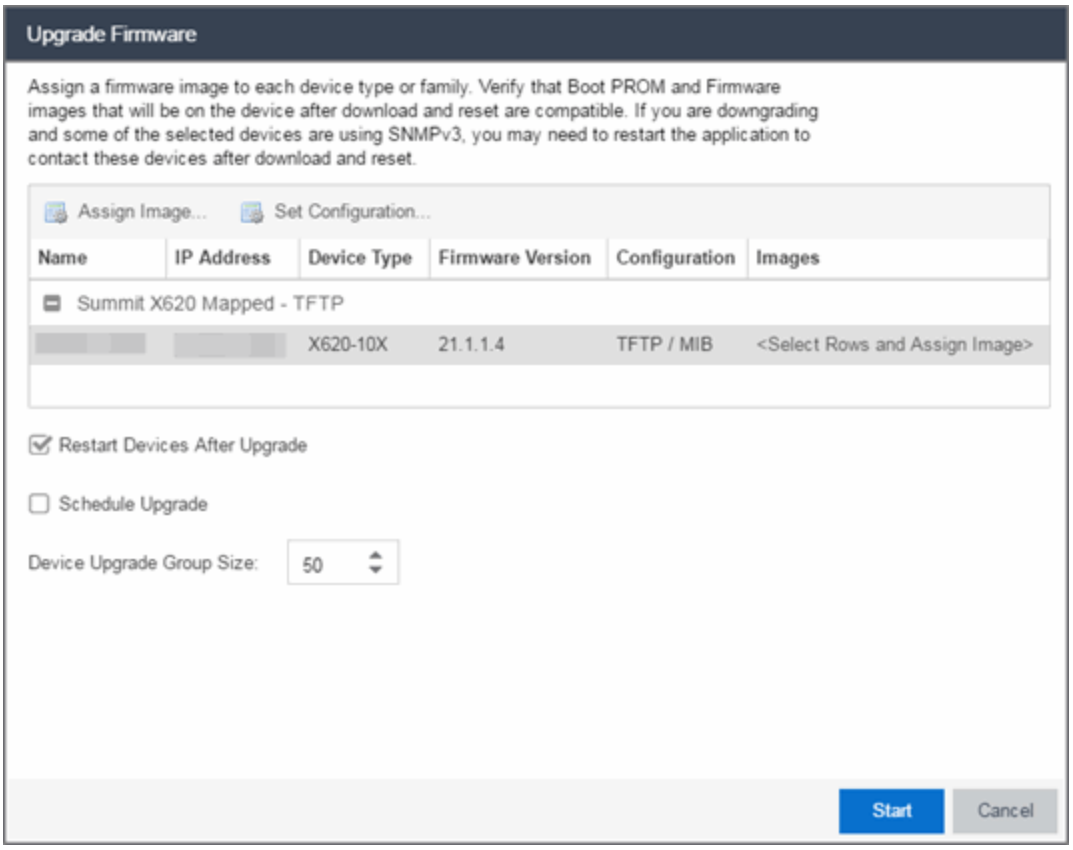
To upgrade firmware for a particular device:

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**.

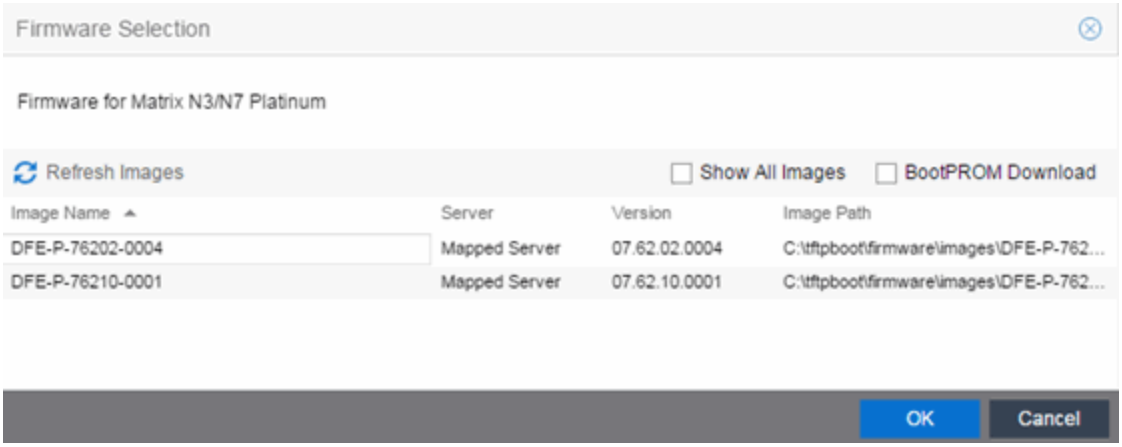
   The Upgrade Firmware window opens, displaying the devices you selected grouped

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.

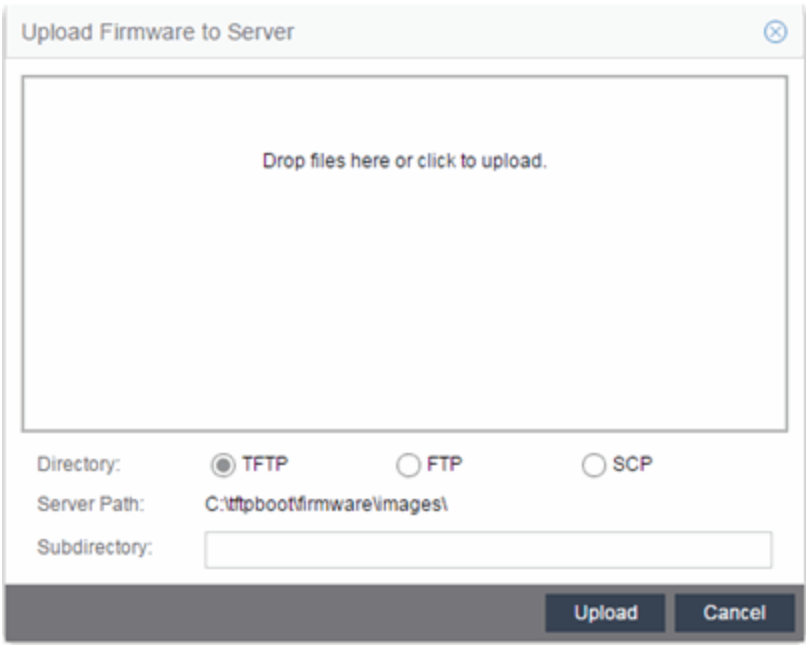
- **Name** —The name for the scheduled upgrade. The default name automatically populates with the creation date and time of the firmware upgrade.
- **Select Date** —The date and time the upgrade automatically runs. Enter a date in the mm-dd-yyyy format or select the **Calendar** icon to open a monthly 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.



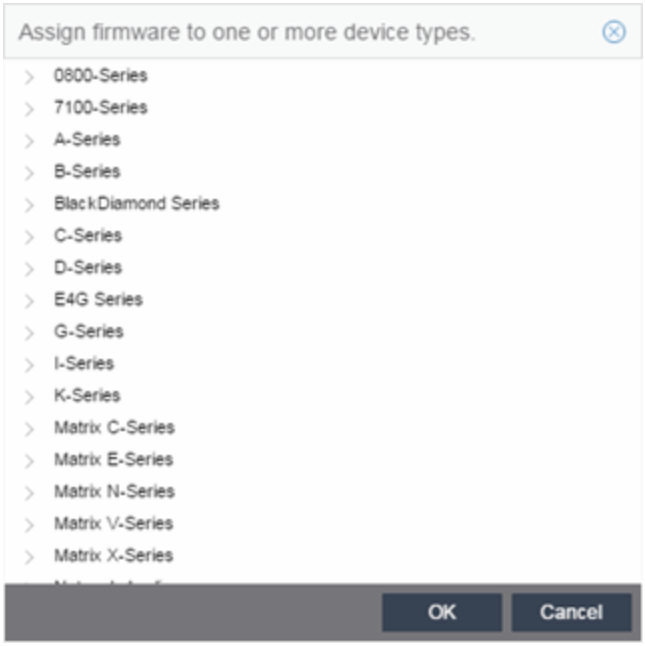
b. Drag the file or files into the box in the main part of the window or select the box to open a window from which you can navigate to the appropriate directory.

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 checkmark 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.

Related Information

For information on related windows:

- Network Tab
- Devices Tab
- Firmware Tab
- Scheduled Tasks Tab

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.

Related Information

For information on related topics:

- How to Upgrade Firmware
- Restart Device Window

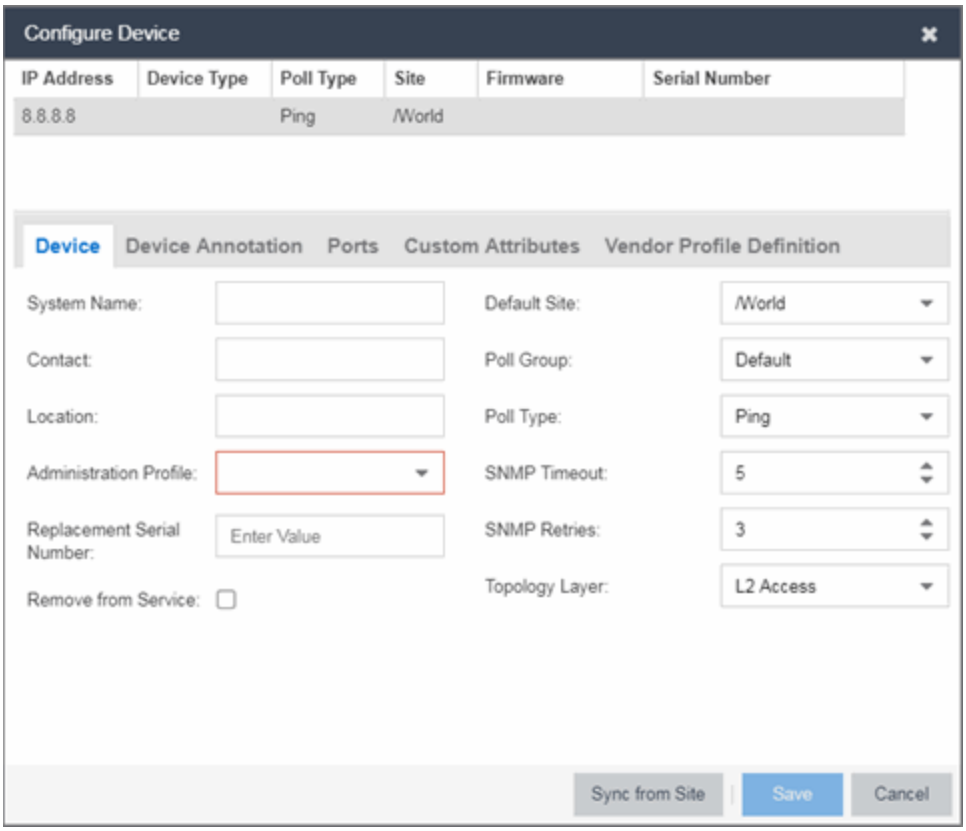
Create and Edit a VLAN on a Device

This section outlines how to create and edit a VLAN. From the **Network** tab, you can:

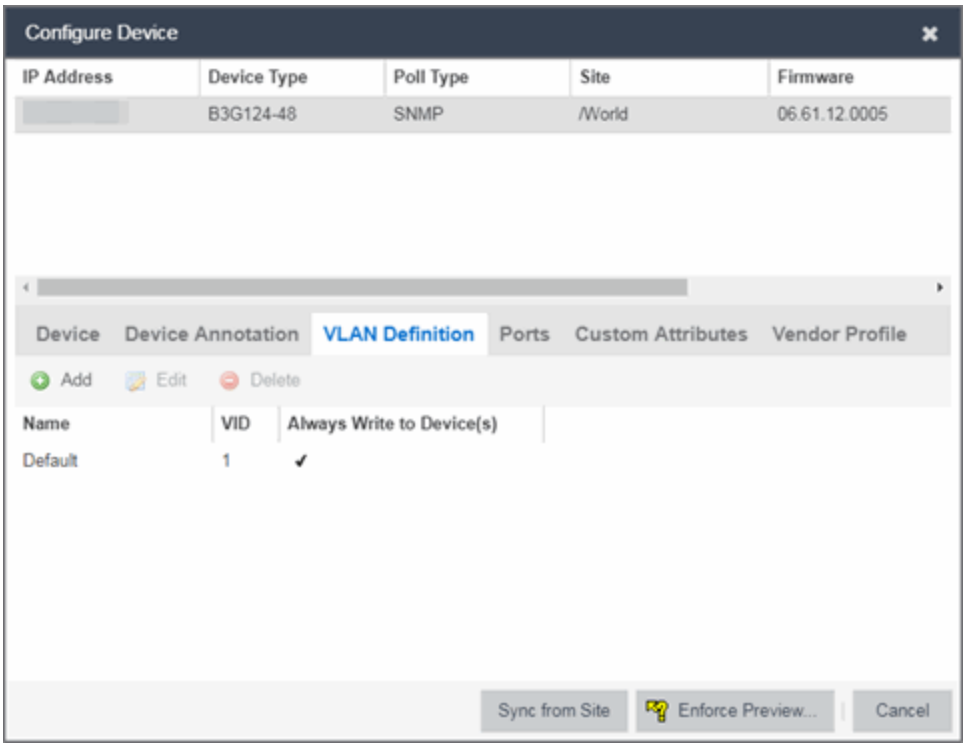
- Create a new VLAN
- Edit the ports of an existing VLAN
- Edit the name of an existing VLAN
- Remove devices from an existing VLAN

To create a new VLAN:

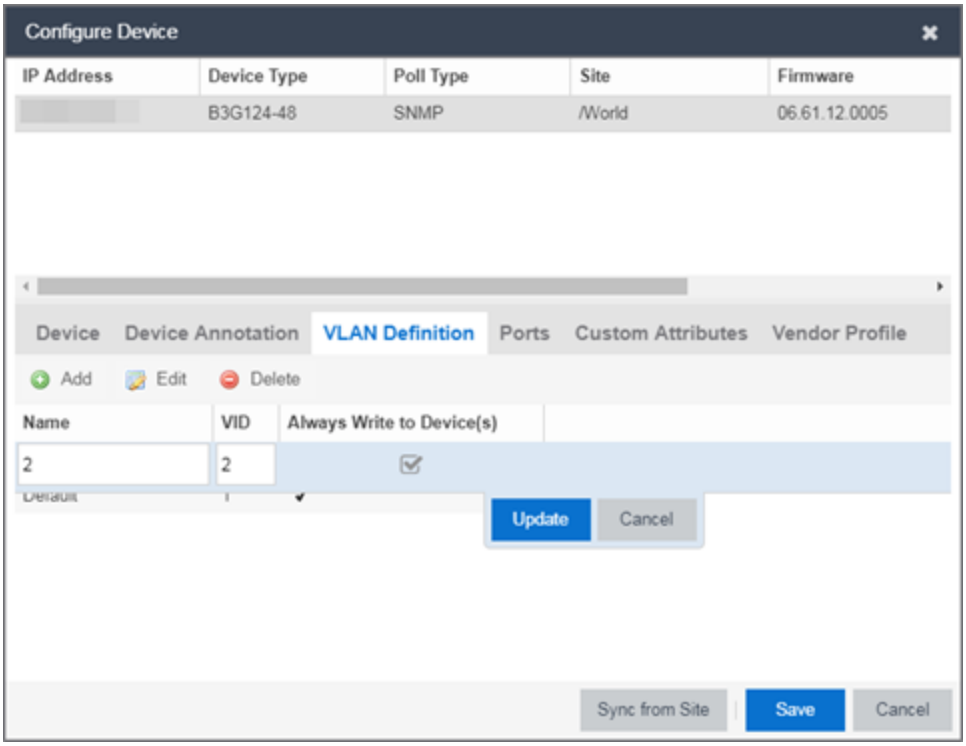
1. Launch ExtremeCloud IQ - Site Engine.
2. Open the **Network > Devices** tab.
3. Select the device from the devices list. Right-click the device and select **Device > Configure Device**.
   The **Configure Device** window opens.



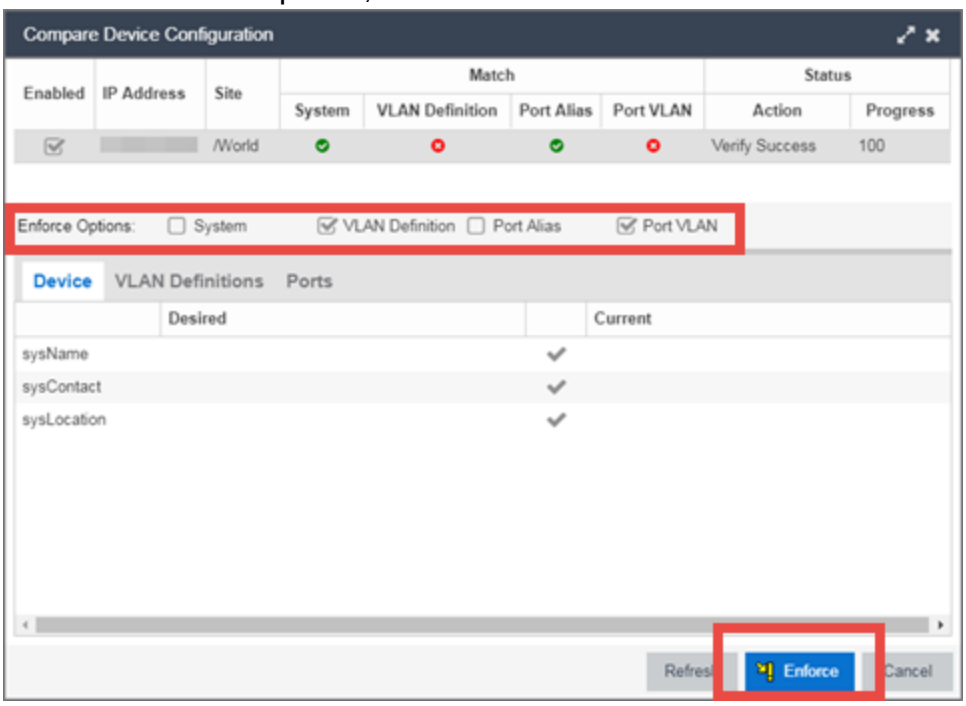
4. Select the **VLAN Definition** tab.



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:

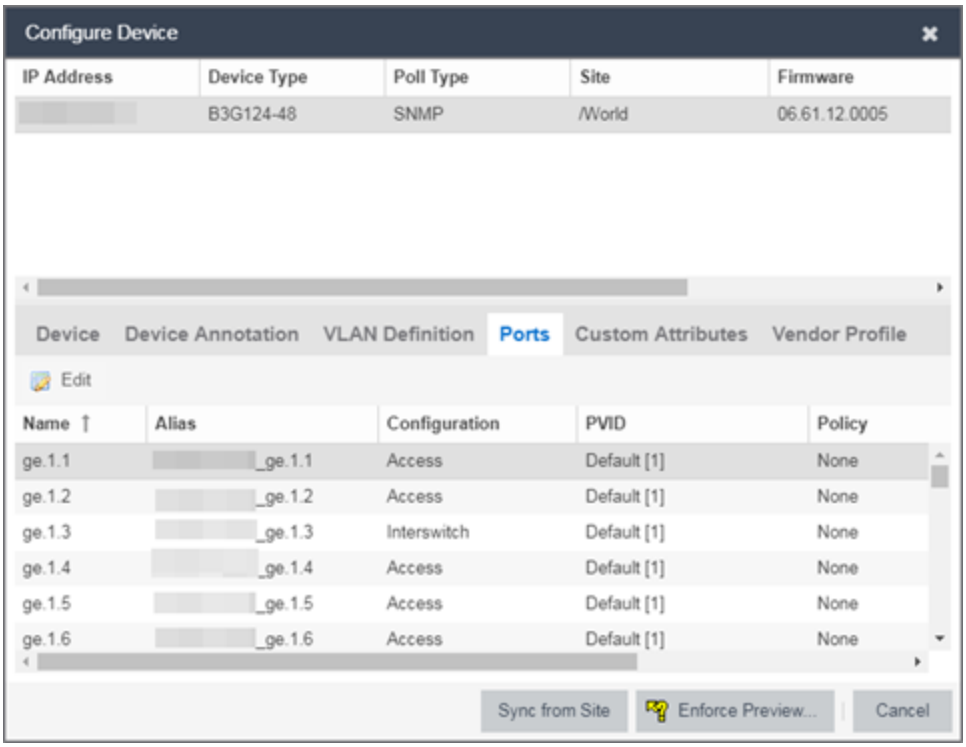
- `site.enforceOption.autoEnable.system=false`
- `site.enforceOption.autoEnable.vlanDefinition=false`
- `site.enforceOption.autoEnable.portAlias=false`
- `site.enforceOption.autoEnable.portVlan=false`

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**.

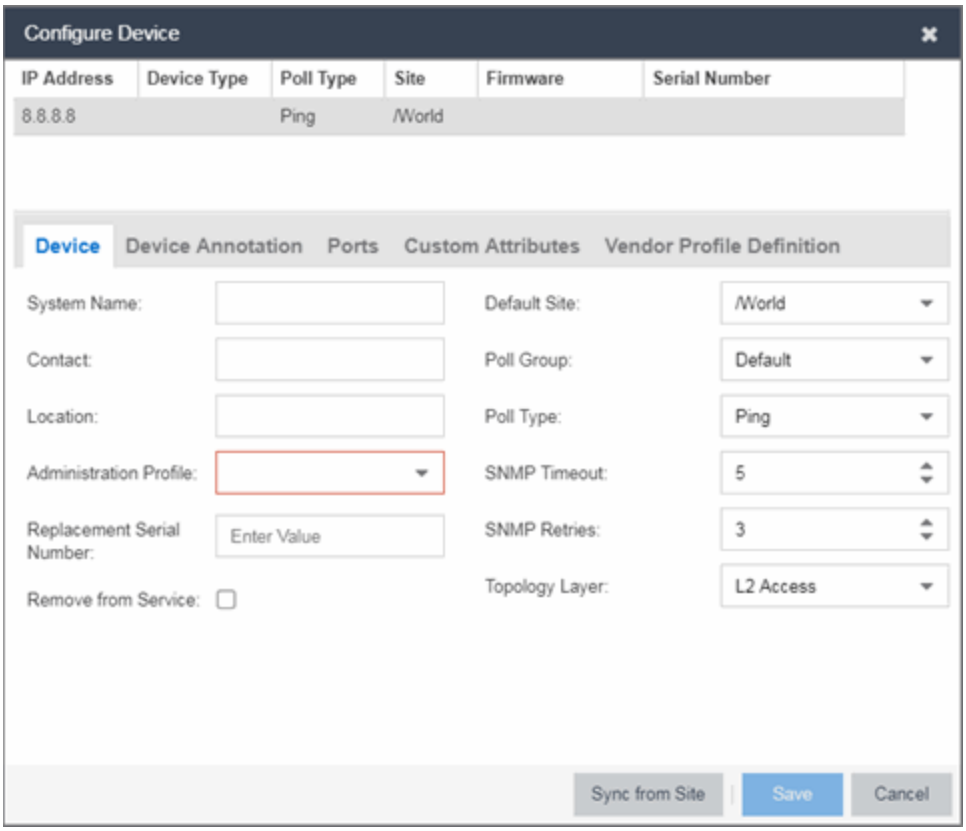
NOTE: By default, the checkboxes in the Enforce Options section of the window are not selected. To configure ExtremeCloud IQ - Site Engine to select the checkboxes by default, open the `NSJBoss.properties` file and change **false** to **true** in the following lines:

- `site.enforceOption.autoEnable.system=false`
- `site.enforceOption.autoEnable.vlanDefinition=false`
- `site.enforceOption.autoEnable.portAlias=false`
- `site.enforceOption.autoEnable.portVlan=false`

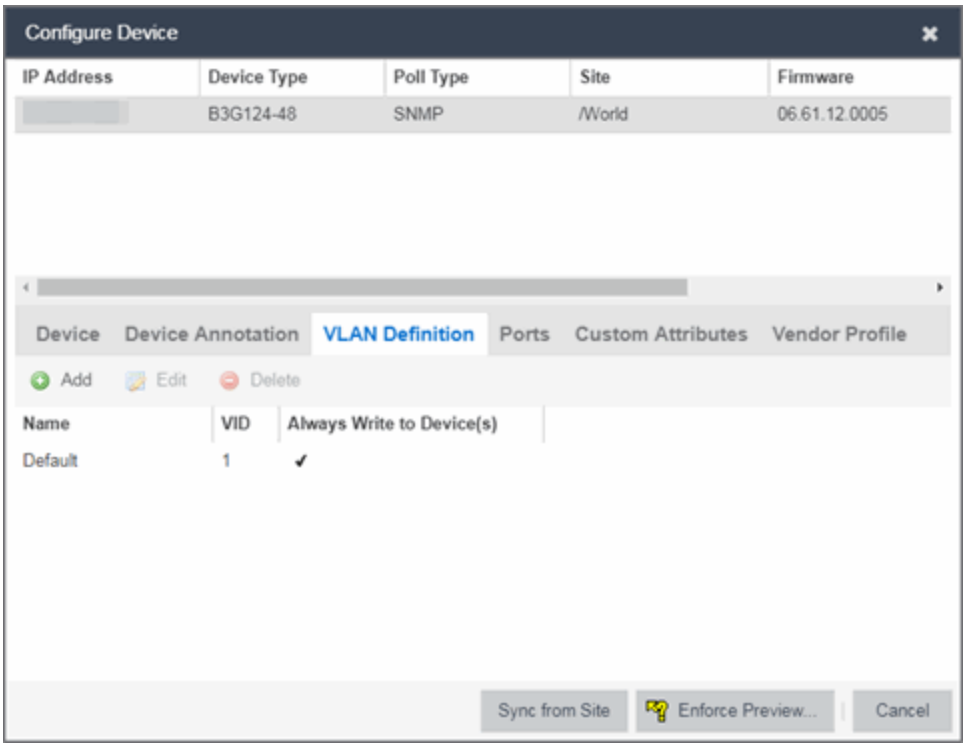
The VLAN is now configured to the Ports.

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.



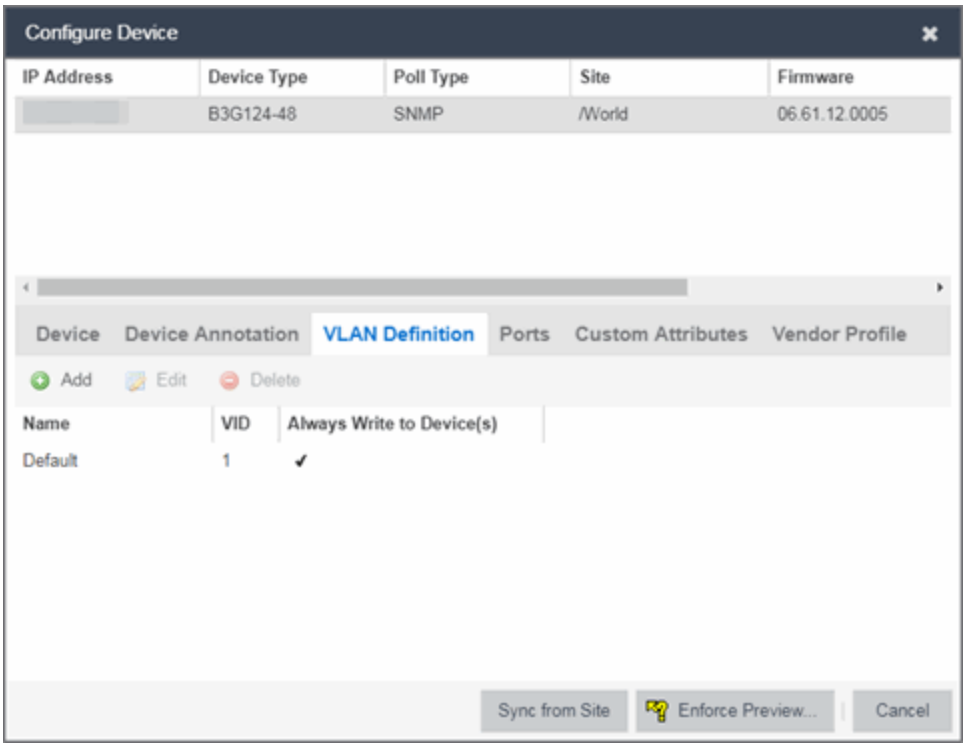
5. Select the **VLAN Definition** tab.



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**.

Related Information

For information on related topics:

- Maps
- Devices tab

How to Add a New Regime

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.

Related Information

For information on related tabs:

- ExtremeCompliance Overview
- Diagnostics

How to Obtain and Apply an ExtremeCompliance License

To use the **Compliance** tab in ExtremeCloud IQ - Site Engine, an additional license is required.

To obtain and apply the license in ExtremeCloud IQ - Site Engine:

1. Contact your sales representative to purchase an ExtremeCompliance license.

   An email voucher is generated and sent to you with instructions.
2. Create an Extreme Networks Support Portal account, if necessary.
   a. Open a browser and go to https://secure.extremenetworks.com/.
   b. Enter your information and select **Create An Account**.

      An email is sent to you with instructions to activate your account.
   c. Select the link in your email.

      The Portal - Account Activation web page displays.
   d. Enter your **Email Address** and the **Activation Code** included in your activation email, if they do not automatically populate.
   e. Select **Activate**.
3. Access the Extreme Networks Support Portal at https://extremeportal.force.com/ExtrLicenseLanding.
4. Enter your **Email** and **Password** and select **Log In**.
5. Select **Generate License**.

   The Generate License window displays.
6. Enter your **Voucher ID** from the email voucher sent to you and select **Next**.
7. Select the **Terms and Conditions** checkbox and select **Submit**.

   A window displays with your software license key.

8. Copy the license key from the window.
9. Open ExtremeCloud IQ - Site Engine.
10. Access the **Administration** > **Licenses** tab.
11. Select **Add**.

    The **Add License** window displays.
12. Paste the license key you copied in Step 8 and select **OK**.
13. Restart ExtremeCloud IQ - Site Engine.
14. The **Compliance** tab is now available in the menu, allowing you to use ExtremeCompliance audit functionality.

Related Information

For information on related tabs:

- ExtremeCompliance Overview
- Administration

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 systems must be running ExtremeXOS 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
- Download XMODs (ExtremeXOS devices only)
- Default Device Configuration in ExtremeCloud IQ - Site Engine
- General Network Configuration

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**.

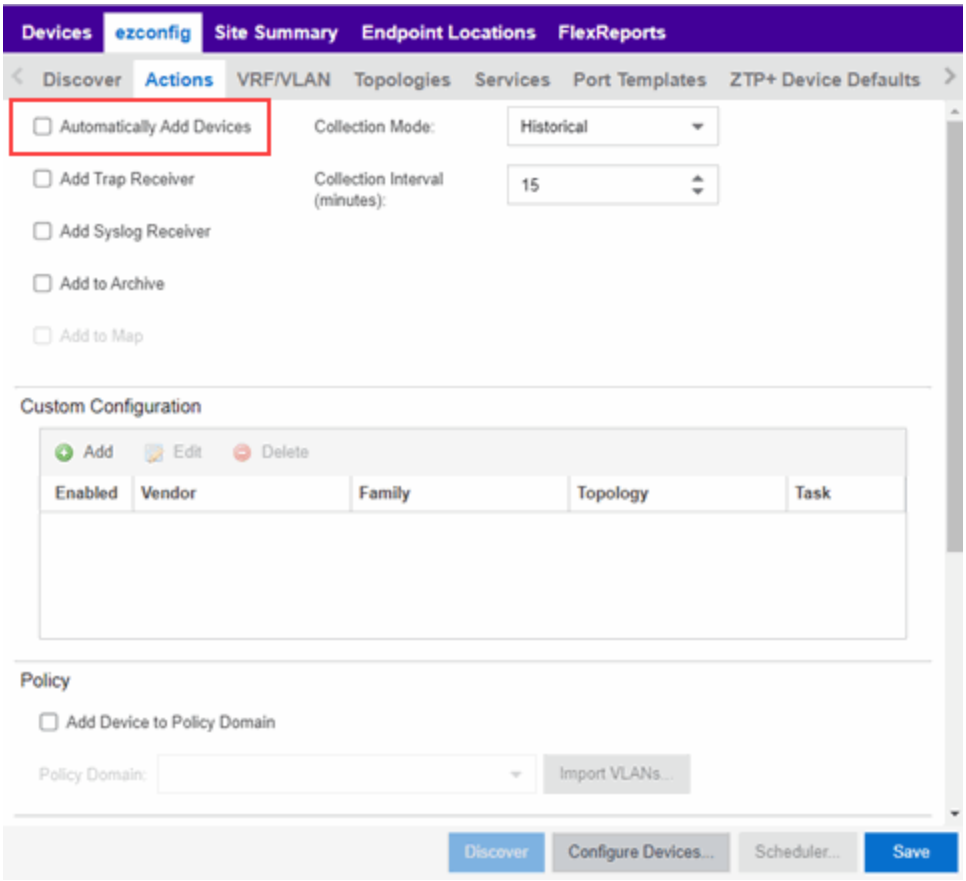
   Your device automatically updates with this firmware image when it restarts and is logged in the Event log with a **Category** of **Inventory**.

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 ExtremeControl Engine Group** to automatically add devices being added to the site to a Policy Domain or ExtremeControl 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 devices only)

XMODs are files that work in conjunction with firmware image upgrades to enhance ZTP+ functionality on ExtremeXOS 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 on which version 21114 is running require an update to the CloudConnector XMOD for ZTP+ functionality to work properly. Saving the most recent XMOD in the directory specified above updates the device and allows ZTP+ to function as intended.

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.

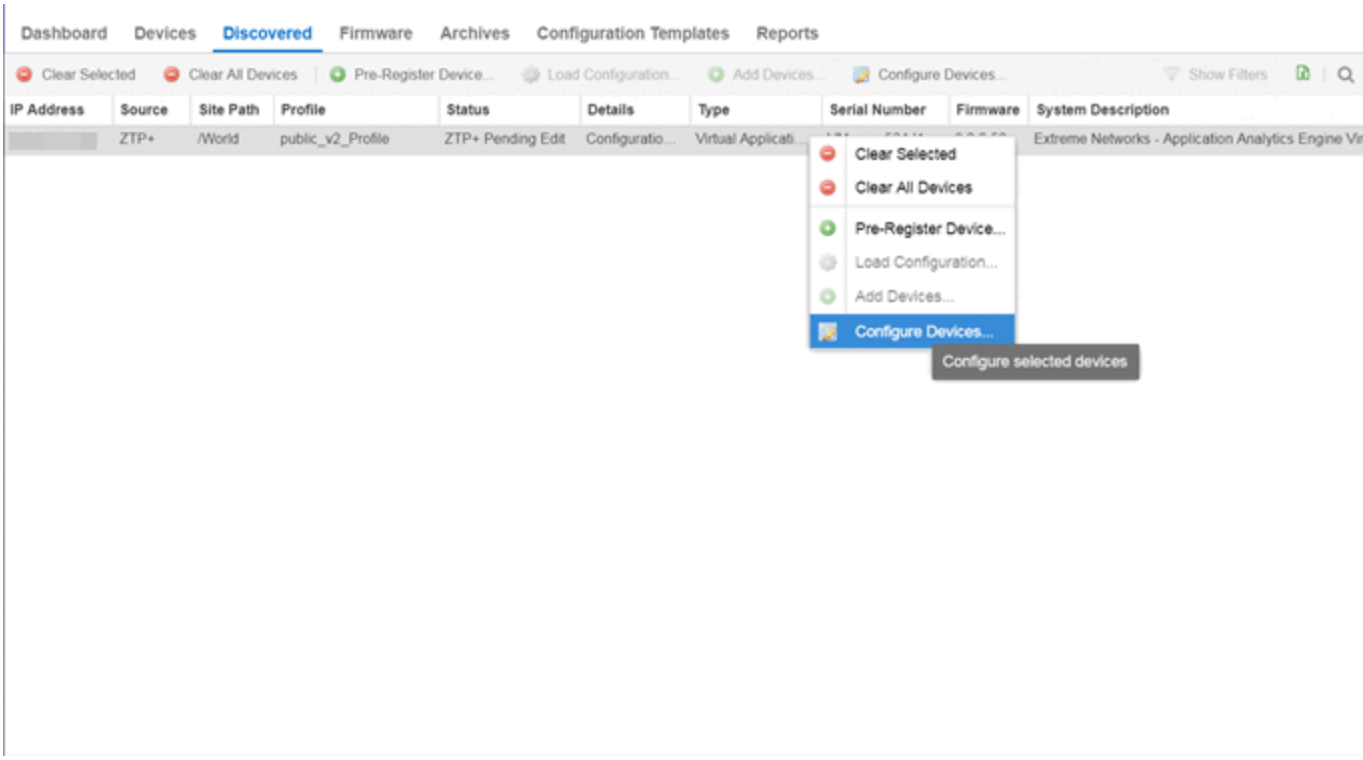
Adding the Device to the ExtremeCloud IQ - Site Engine Database

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.

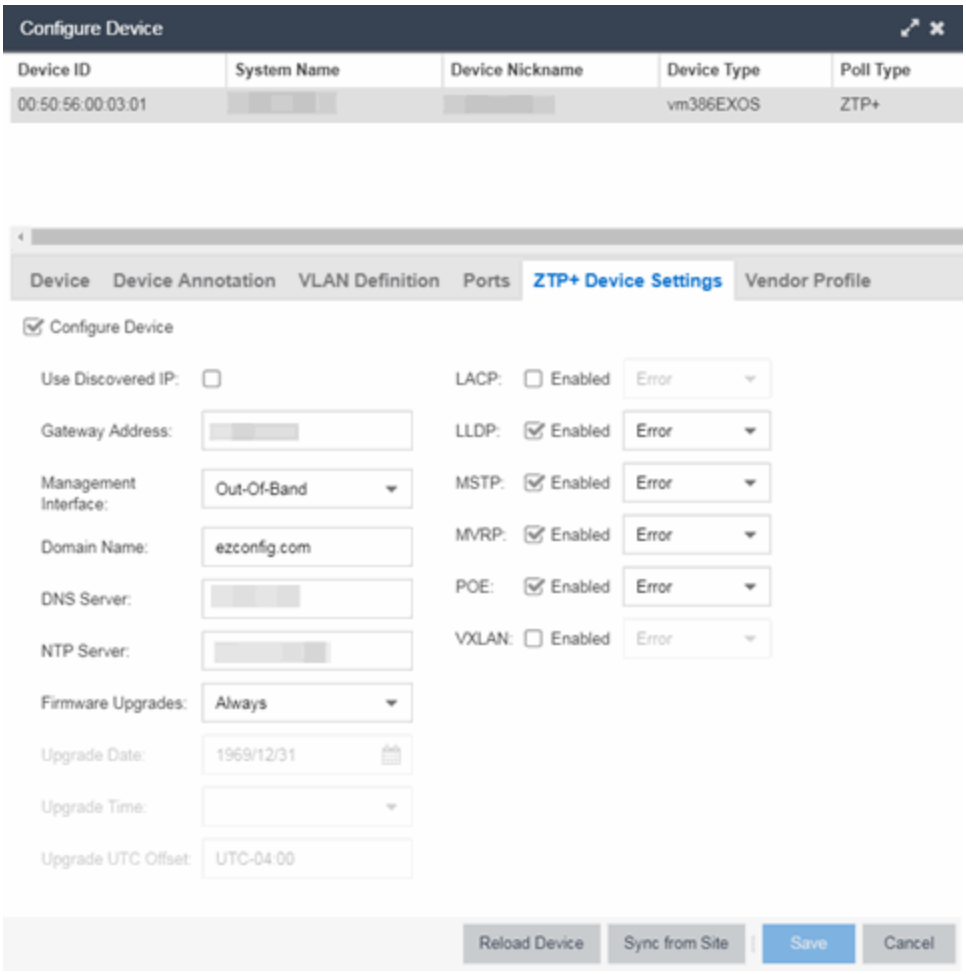
   ZTP+ enabled devices communicate with ExtremeCloud IQ - Site Engine securely via an HTTPS connection and transmit information to ExtremeCloud IQ - Site Engine, including the serial number, firmware version, MAC address, operating system, and port information. ExtremeCloud IQ - Site Engine determines 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.

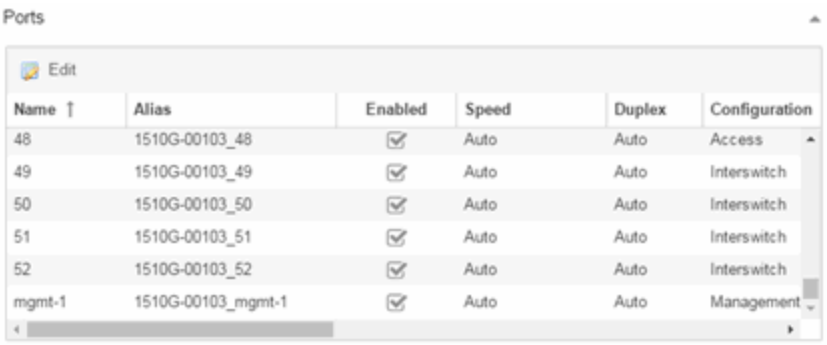
   The **Configure Device** window opens.



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.

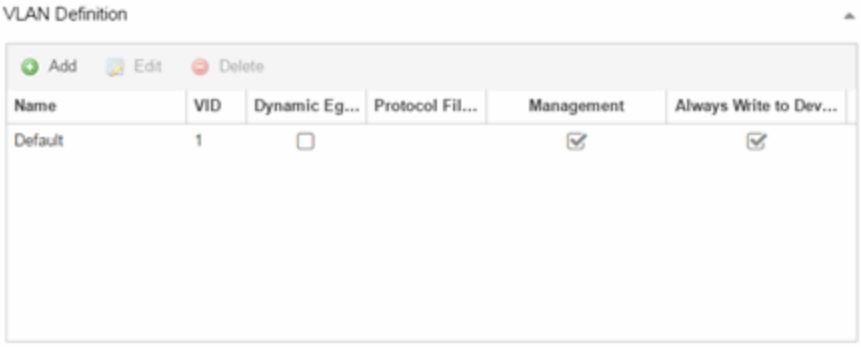
    - **Access**—The port provides access to end-systems.
    - **Interswitch**—The port connects the switch to another switch.
    - **Management**—The port is used to manage the network via ExtremeCloud IQ - Site Engine.

    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.

Related Information

For information on related topics:

- Sites
- Profiles
- Add Device
- Configure Device
- Devices

ExtremeAnalytics Engine ZTP+ Configuration

Using Extreme Networks' ZTP+ (Zero Touch Provisioning Plus) functionality, you can quickly add new ExtremeAnalytics engines 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.

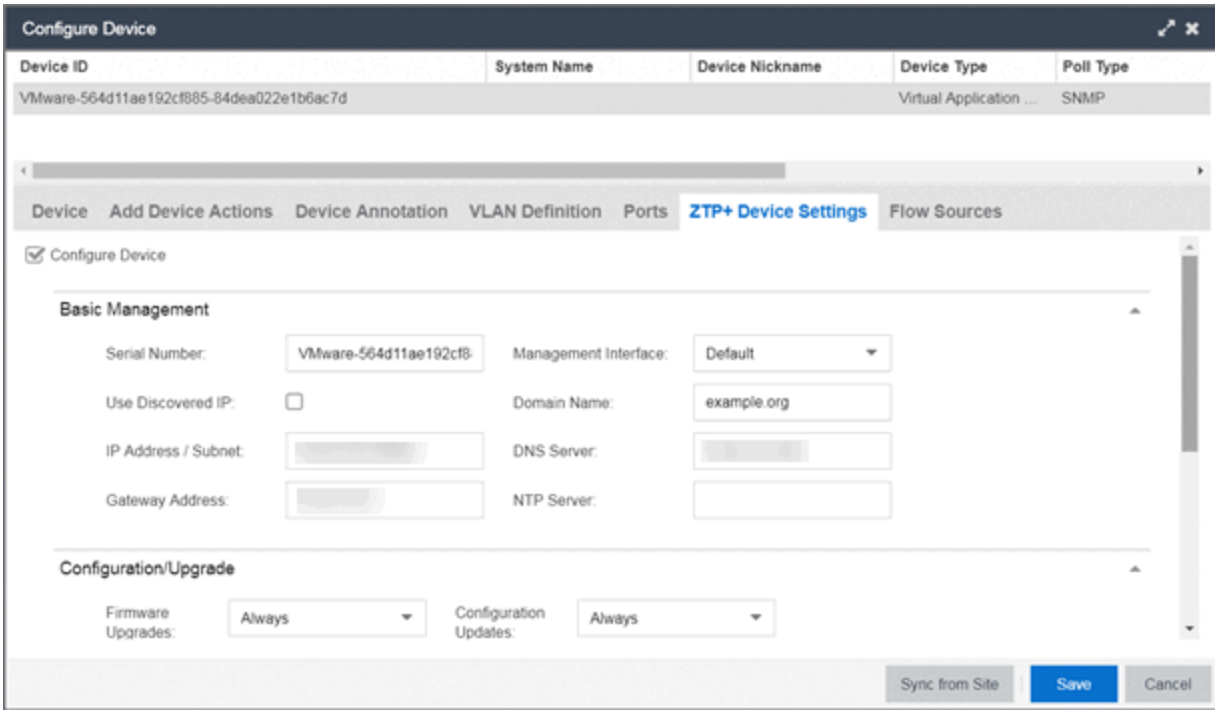
1 Open the **Discovered** tab in ExtremeCloud IQ - Site Engine.

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.

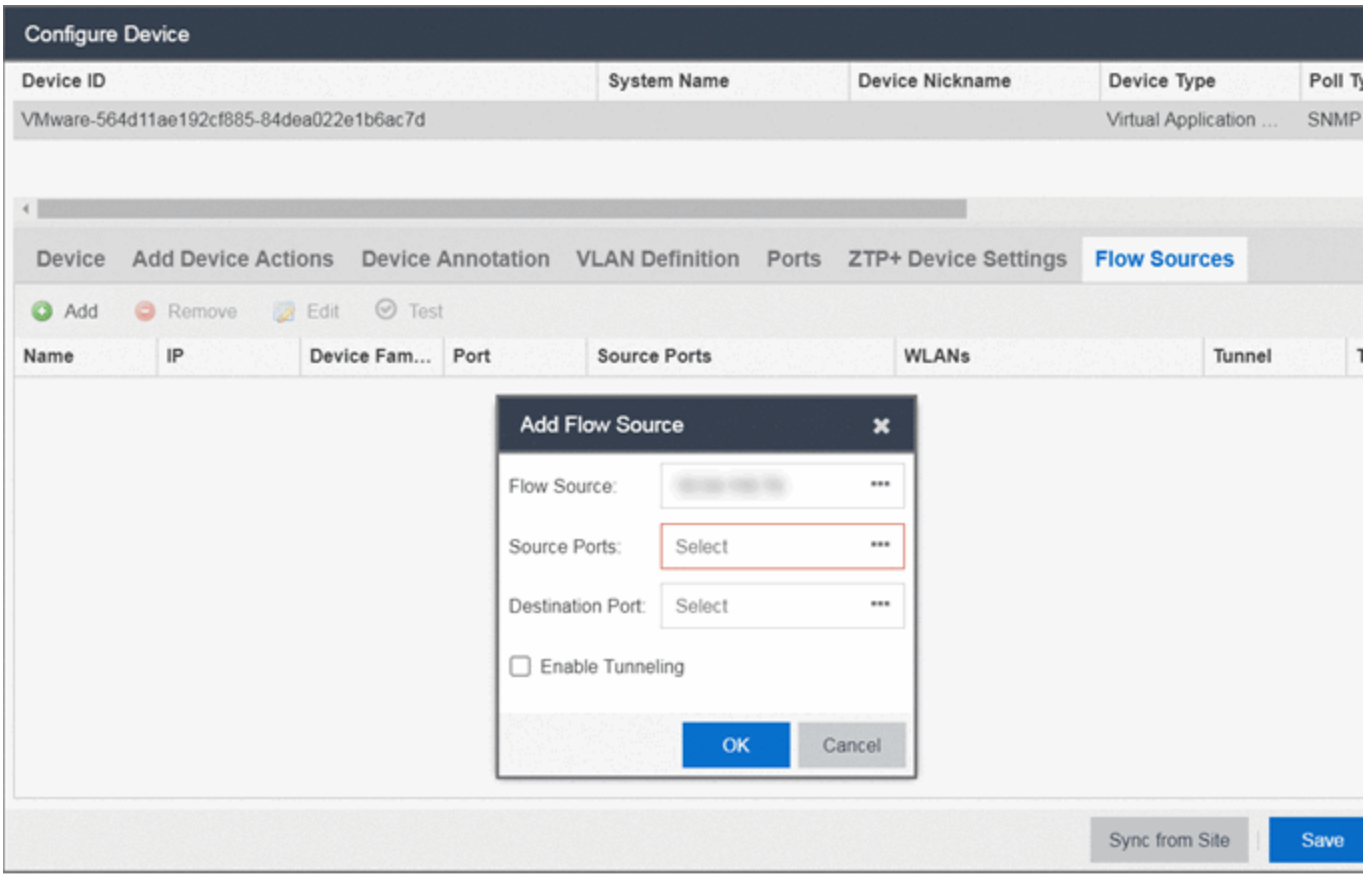
The **Configure Device** window opens.

3. Select the **ZTP+ Device Settings** tab.



4. Configure the fields on the **ZTP+ Device Settings** tab to determine how the ExtremeAnalytics engine is managed by ExtremeCloud IQ - Site Engine using ZTP+ functionality.

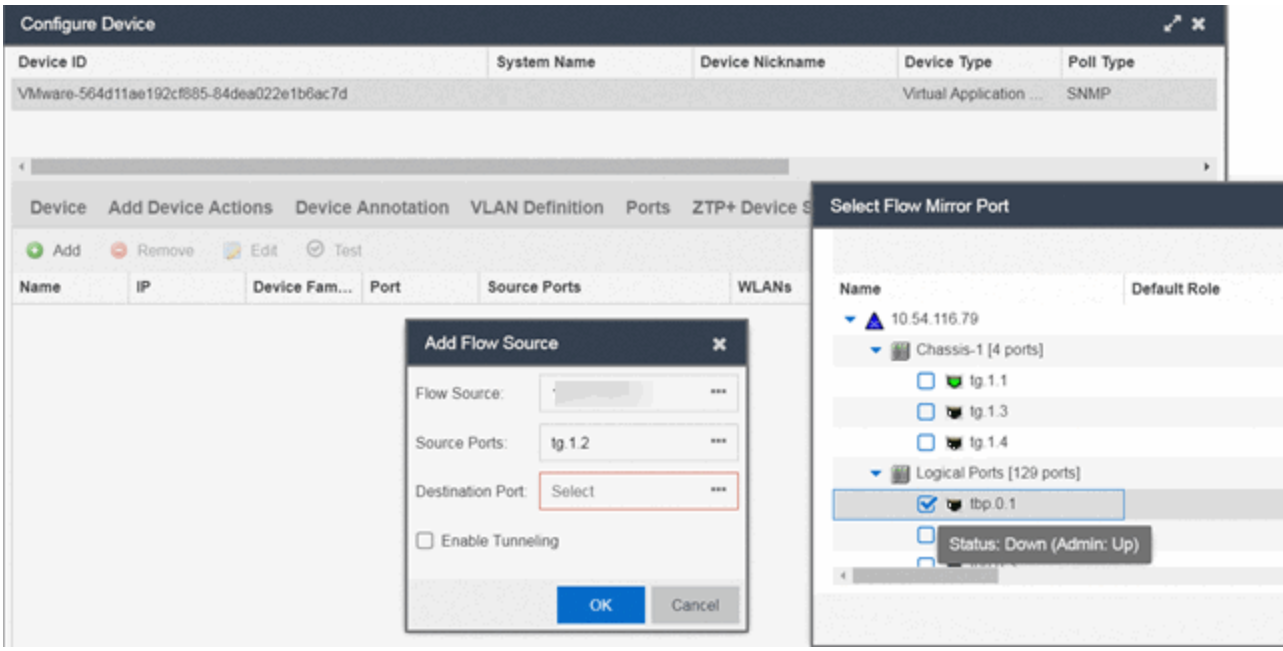
5. Select the **Flow Sources** tab in the **Configure Device** window.



6. Select the ExtremeAnalytics engine 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 ExtremeAnalytics engine 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.

Related Information

For information on related topics:

- Sites
- Profiles
- Add Device
- Configure Device
- Devices

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, as well as in the legacy java applications Console and NAC Manager.

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

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 ExtremeControl 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 ExtremeControl 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 ExtremeControl 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 ExtremeControl 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	NetSight OneView > Access OneView or NetSight OneView > Access OneView and Access OneView Administration
Sessions > NetFlow	NetSight OneView > NetFlow Read Access
Modify Flow Collection	NetSight OneView > NetFlow Read/Write Access
Map	NetSight OneView > Maps > Maps Read Access or Maps Read/Write Access
Details Sessions > End-System Events	NetSight OneView > ExtremeControl > OneView End-Systems Read Access or NetSight OneView > ExtremeControl > OneView End-Systems Read/Write Access

Launching PortView

You can launch PortView from a variety of locations in ExtremeCloud IQ - Site Engine, as well as the legacy java applications Console and NAC Manager. 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 ExtremeControl 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 ExtremeControl 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.

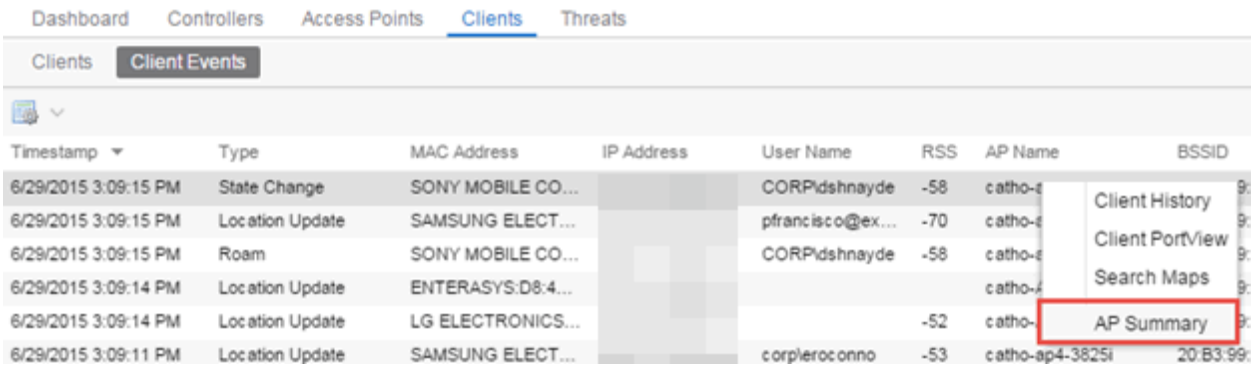
In addition to capturing network traffic for analysis in Wireshark, the AP also collects RF information. The RADIOTAP header format delivers RF information. You must use Wireshark 1.6 or later to read the full RADIOTAP header information. For troubleshooting features like TxBF/STBC, you can enable capturing 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.

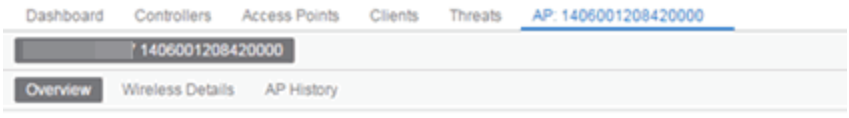
Configure and Use Real Capture

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.

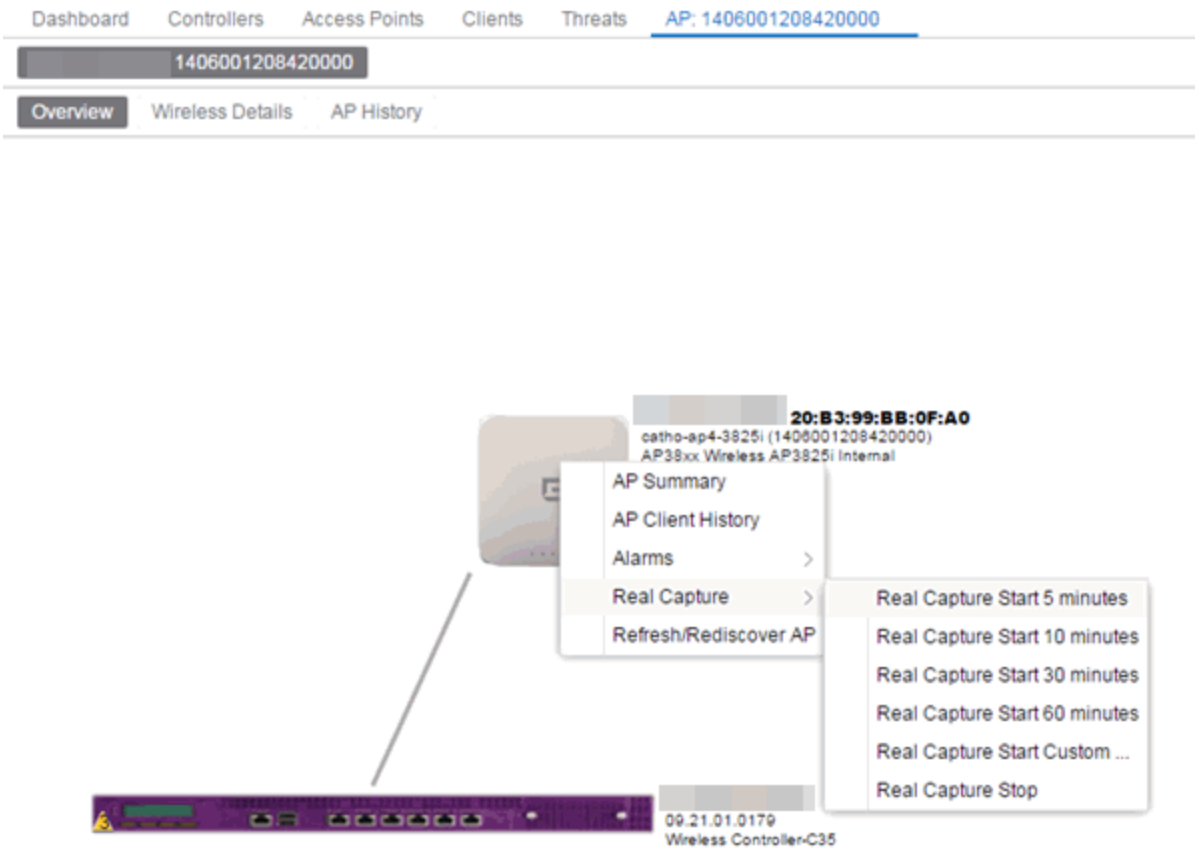


   b. The AP PortView opens.

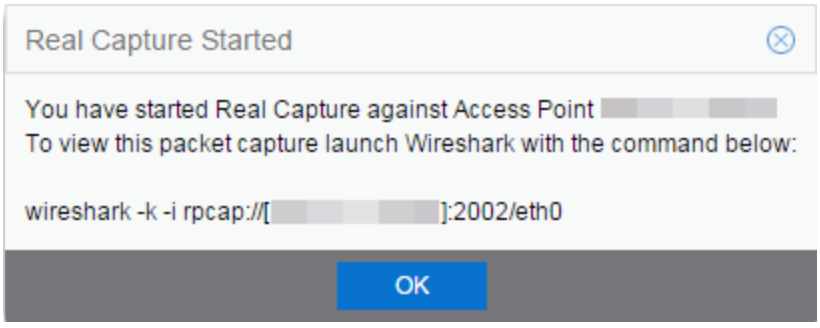


NOTE: You can also launch PortView for the AP using the **Search** tab. Open the **Search** tab, enter the search criteria (MAC, IP, hostname, or AP serial number) and press **Enter** to display the AP PortView.

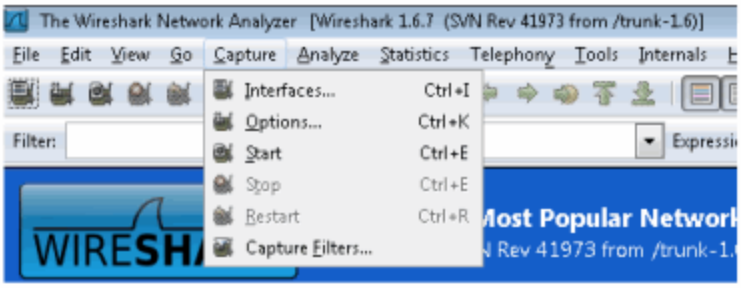
3. Right-click on the AP in the PortView topology display and select **Real Capture** > **Real Capture Start xx minutes**. Select the desired amount of time to run the capture or create a custom capture duration value. If you need to, you can stop the Real Capture by selecting **Real Capture Stop**.



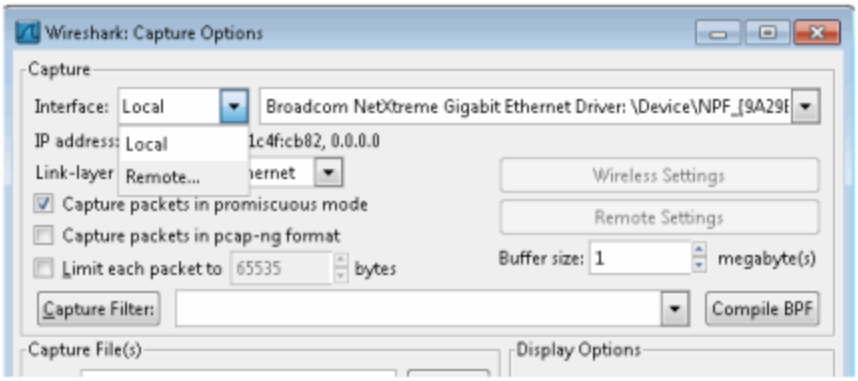
4. A message appears to inform you Real Capture has started, and provides a CLI command you can use on a client on which Wireshark is installed, to launch Wireshark against the AP and view the captured traffic.



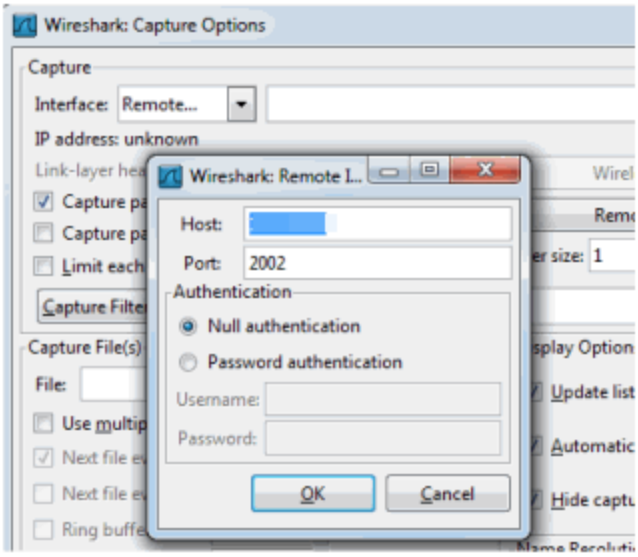
5. You can also access the captured traffic in Wireshark using the following steps:
   a. In Wireshark, select **Capture** > **Options** from the menu bar.



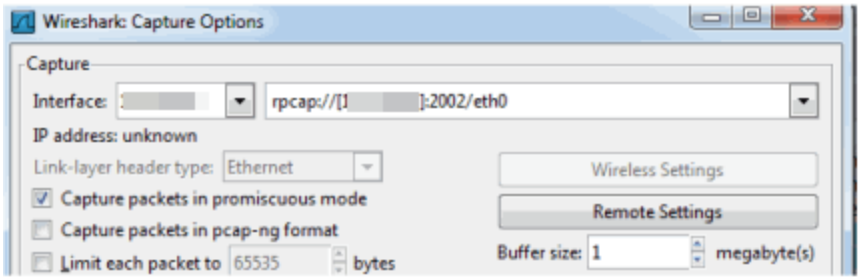
   b. In the Capture Options window, set the **Interface** value to **Remote**.



   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.

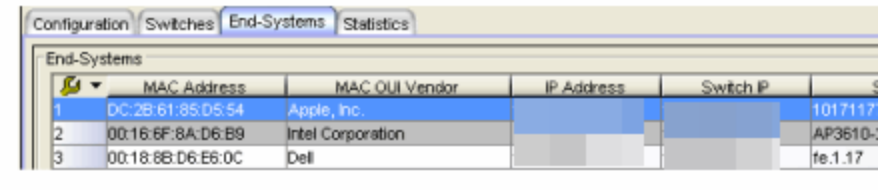


e. Select **OK** in the Capture Options window to begin viewing the captured traffic in Wireshark. When you have the data you need, you can stop the capture and save it to a file for further diagnosis and troubleshooting.

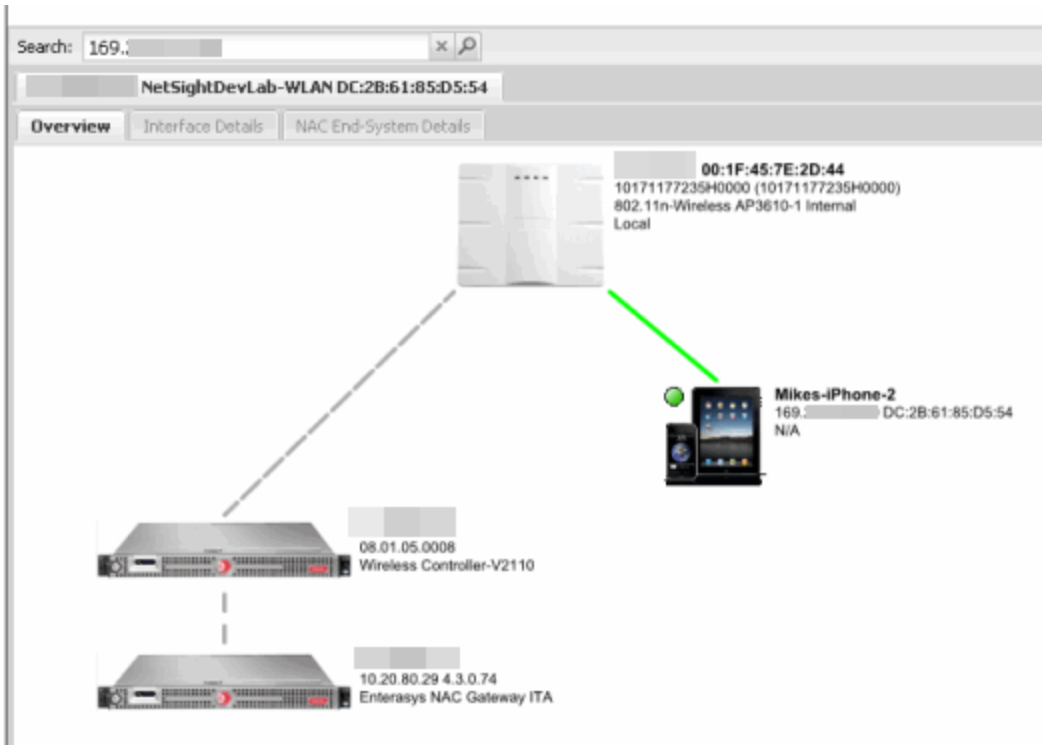
Real Capture Example

The following example shows how to use Real Capture to diagnose an end-system connection problem in NAC Manager.

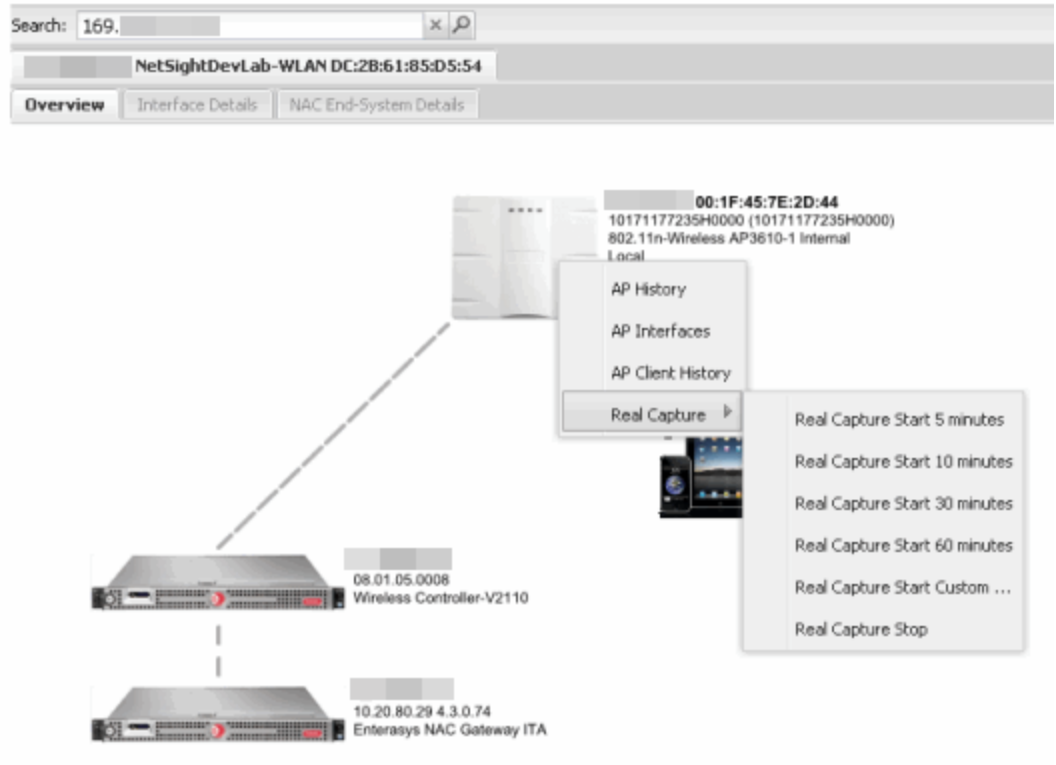
The problem starts when an end-system in NAC Manager is not able to obtain an IP address.



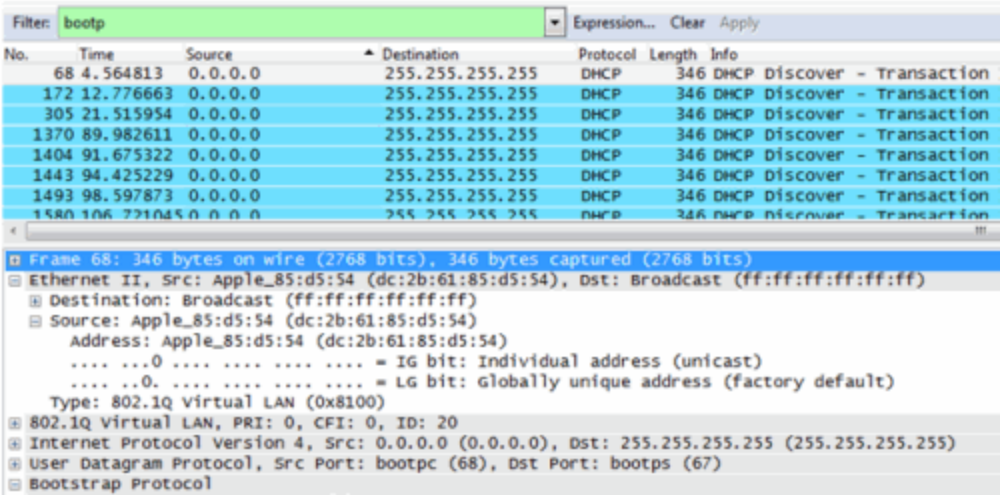
A search is performed on the 169.x.x.x IP address.



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 an ExtremeCloud IQ - Site Engine 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: This topic assumes you previously created a database backup via the **Backup/ Restore** tab.

The restore runs using the `mysqlbackup_restore` script in the `<install directory>\scripts` directory.

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 mysqlback_restore script:
   - Enter `./mysqlbackup_restore.sh <full backup directory structure configured on **Backup/Restore** tab, including path>`

     (for example, `./mysqlbackup_restore.sh /usr/local/Extreme_Networks/NetSight/backup/xiqse_03302021.sql/`).

The database backup is restored.

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

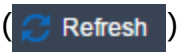
In order to perform the restore configuration operation, you must be a member of an authorization group with the following capabilities.

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
NetSight 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.

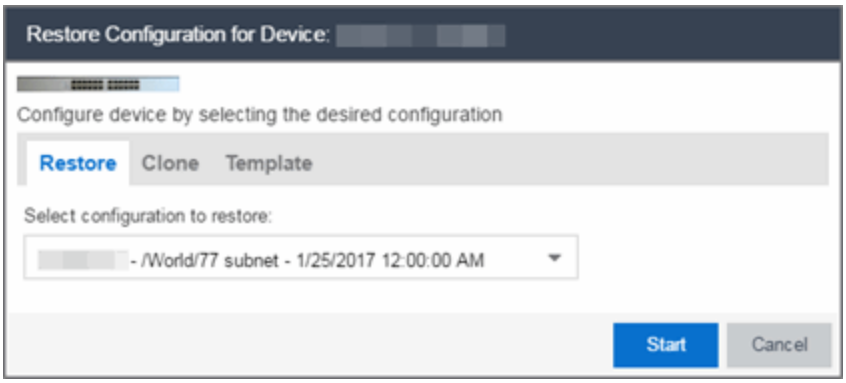
Cloning a device configuration is useful when you want to use the exact same configuration on another device. If you are cloning a device configuration, you must have an existing configuration for that device archived.

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.

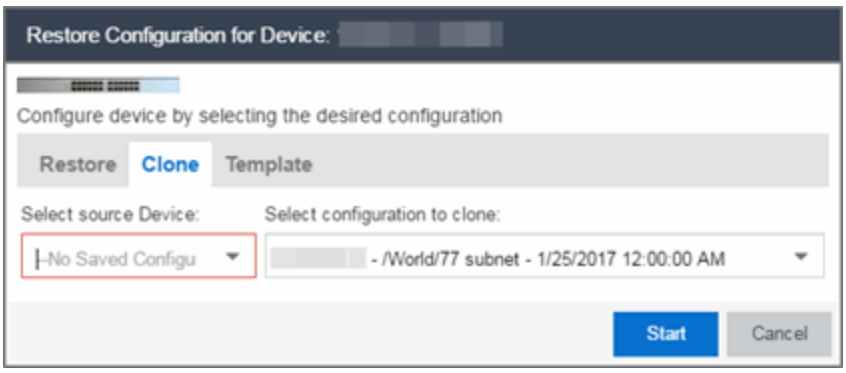
Cloning a Device Configuration

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.

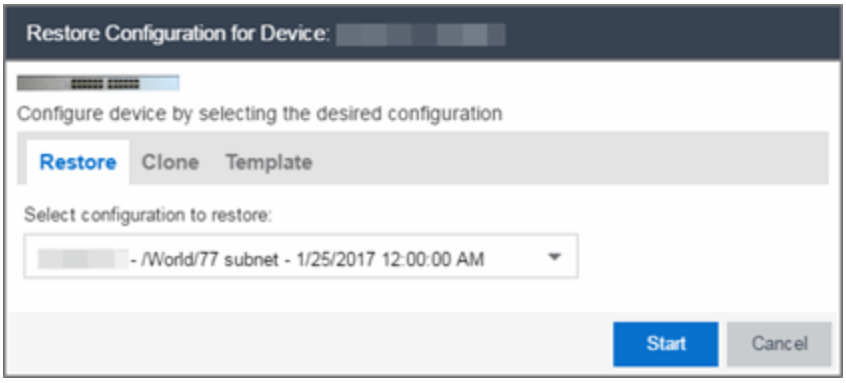


3. If desired, select a new version of firmware to download to the device. (You must add the new firmware version to ExtremeCloud IQ - Site Engine. For more information; see "Device Firmware".)
4. Select the Device option as the Configuration Source.
5. Select the source device for the configuration. 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.

Related Information

For information on related topics:

- Network Tab
- New Device Configuration in ExtremeCloud IQ - Site Engine

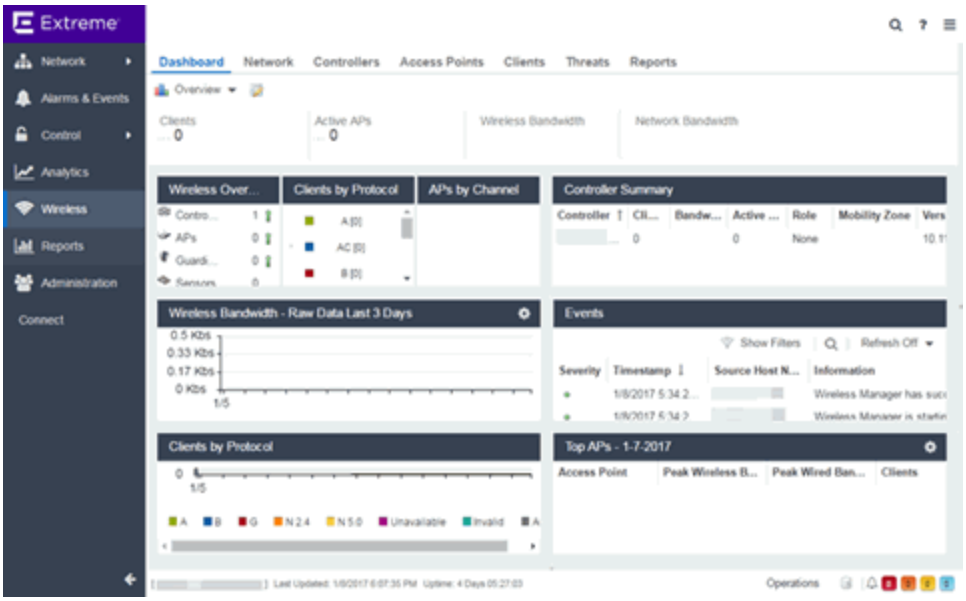
Configuring Enhanced Netflow for Extreme Analytics and Extreme Wireless Controller Version 10.21 in ExtremeCloud IQ - Site Engine

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.

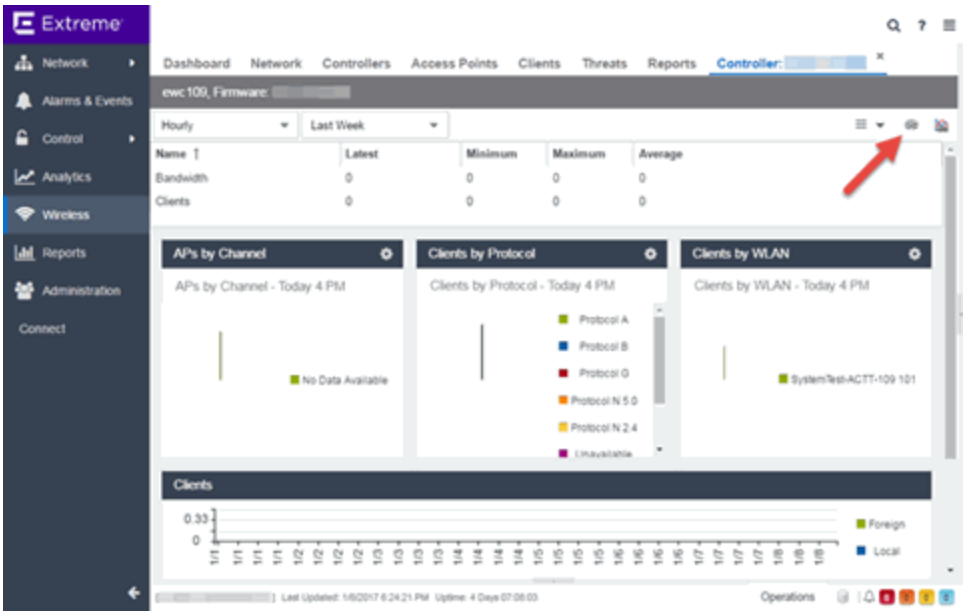
To remove a mirror port on a Wireless Controller running version 10.21:

1. Access the **Wireless** tab in ExtremeCloud IQ - Site Engine.
   The **Wireless** tab opens.



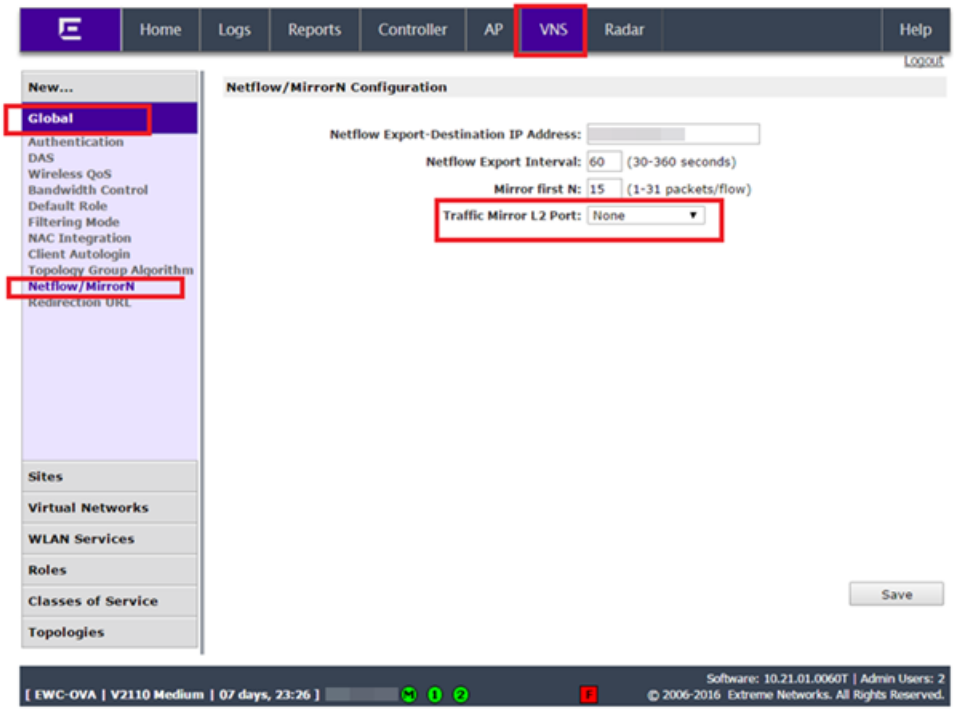
2. Select the **Controllers** tab.
   The **Controllers** tab opens.

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.

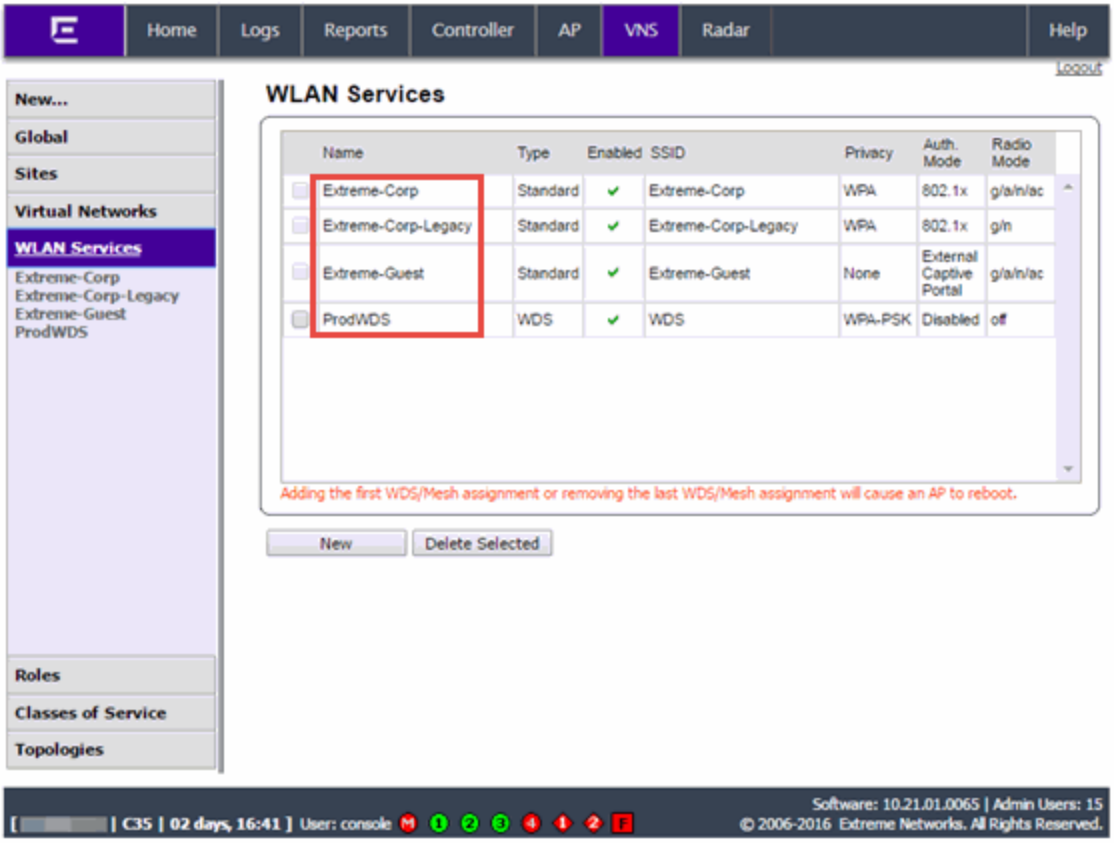
5. Select the **VNS** tab.
   The **VNS** tab opens.



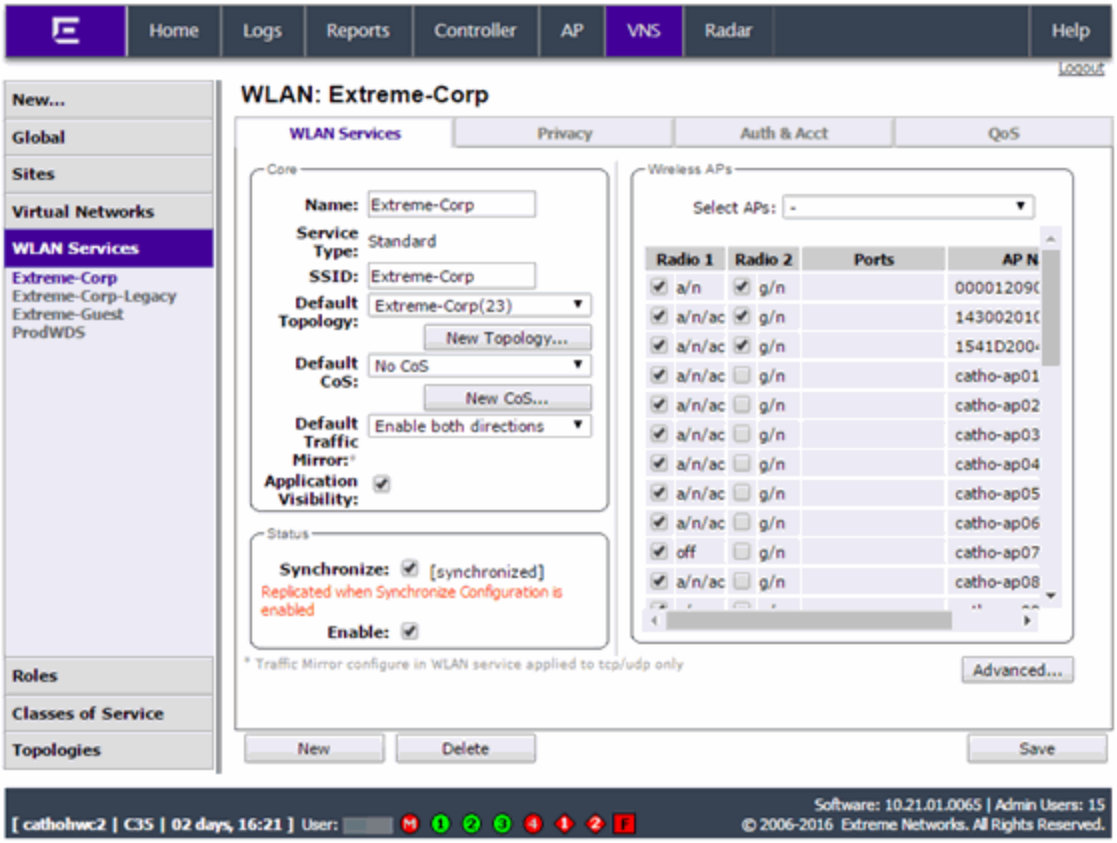
6. Select **Netflow/ MirrorN** from the left-panel.
   The Netflow/ MirrorN Configuration page opens.
7. Select **None** from the **Traffic Mirror L2 Port** drop-down list.
8. Select the **Save** button.

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.

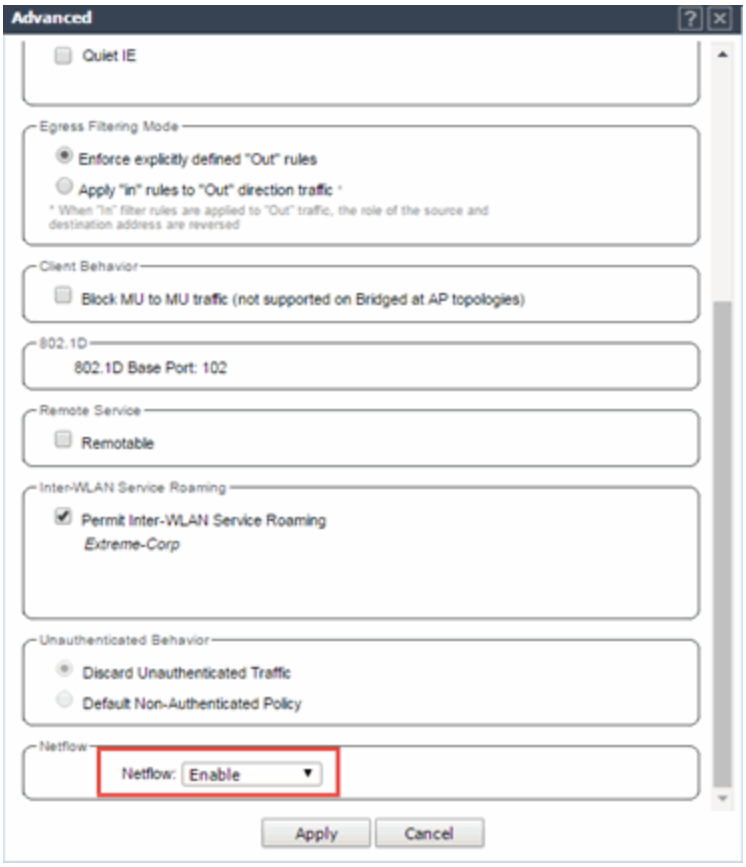

Home
Logs
Reports
Controller
AP
VNS
Radar
Help
Logout
New...
Global
Sites
Virtual Networks
WLAN Services
Extreme-Corp
Extreme-Corp-Legacy
Extreme-Guest
ProdWDS
Roles
Classes of Service
Topologies
WLAN Services
Name
Type
Enabled
SSID
Privacy
Auth. Mode
Radio Mode
Extreme-Corp
Standard
Extreme-Corp
WPA
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.

Related Information

For information on related topics:

- Wireless

How to Configure ExtremeXOS 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 > ExtremeControl 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 ExtremeControl 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**.

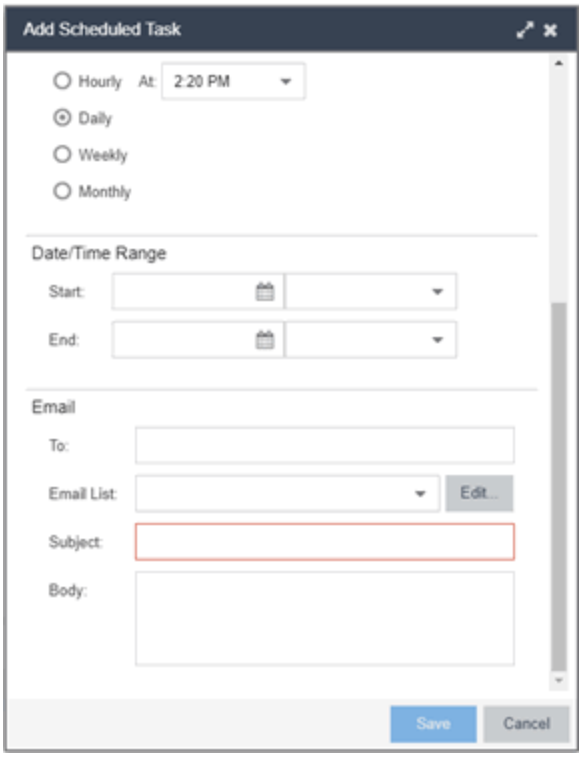
Schedule Tasks

The **Scheduled Task** tab allows you to configure ExtremeCloud IQ - Site Engine to automatically perform the following tasks:

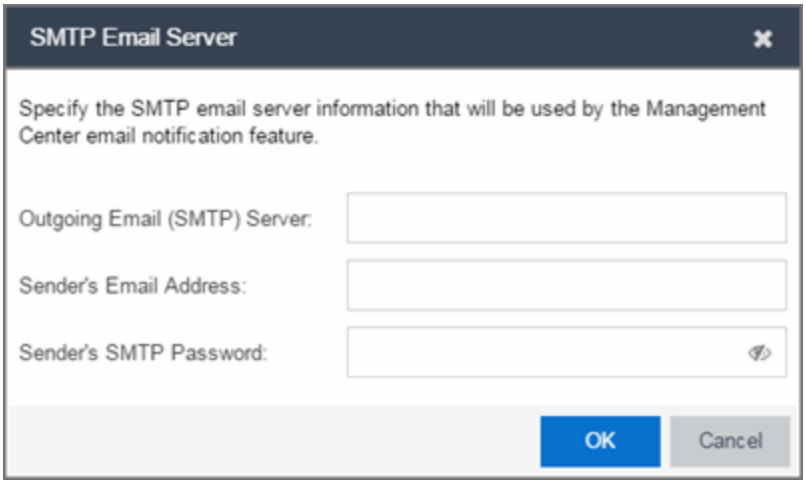
- Generate a subset of available reports in PDF format
- Run a script or workflow
- Set SMTP Email Server Options to use when the scheduled task sends an email notification.
- Discover newly added devices

Create a New Scheduled Task

1. Launch ExtremeCloud IQ - Site Engine.
2. Select 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 by Extreme Networks Support.***
- **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.

Related Information

For information on related topics:

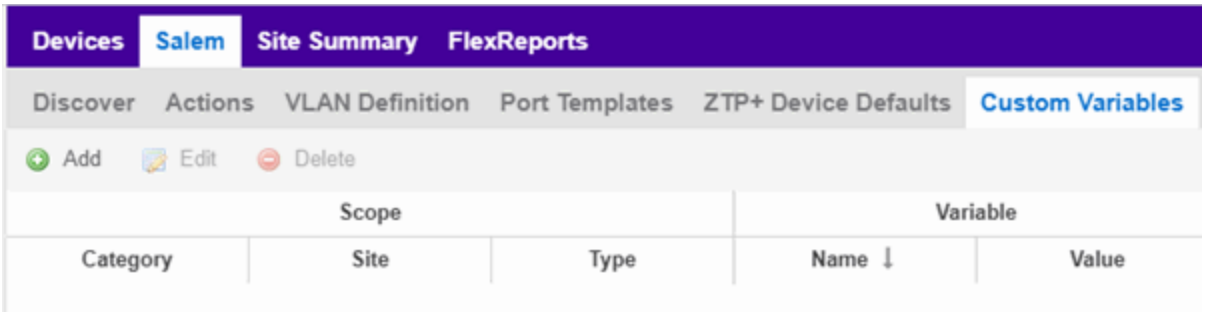
- Tasks
- SMTP Email Options

How to 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.

Related Information

For information on related topics:

- Sites
- Scripts

- Workflows
- Northbound Interface

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 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 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 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 User Guide*.

- **ExtremeXOS CLI commands**—ExtremeXOS 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 commands do not work unless you prefix the shortened command with CLI. For example, to abbreviate `show vlan`, type `CLI sh vlan`.

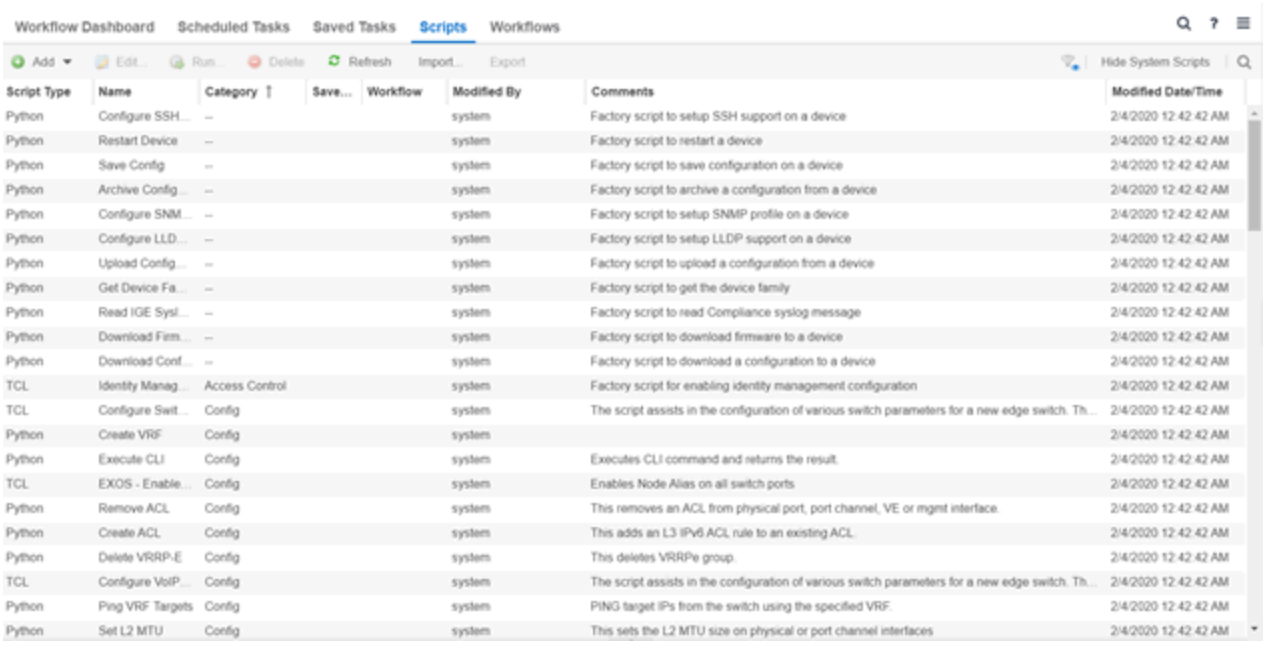
Bundled ExtremeCloud IQ - Site Engine Scripts

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

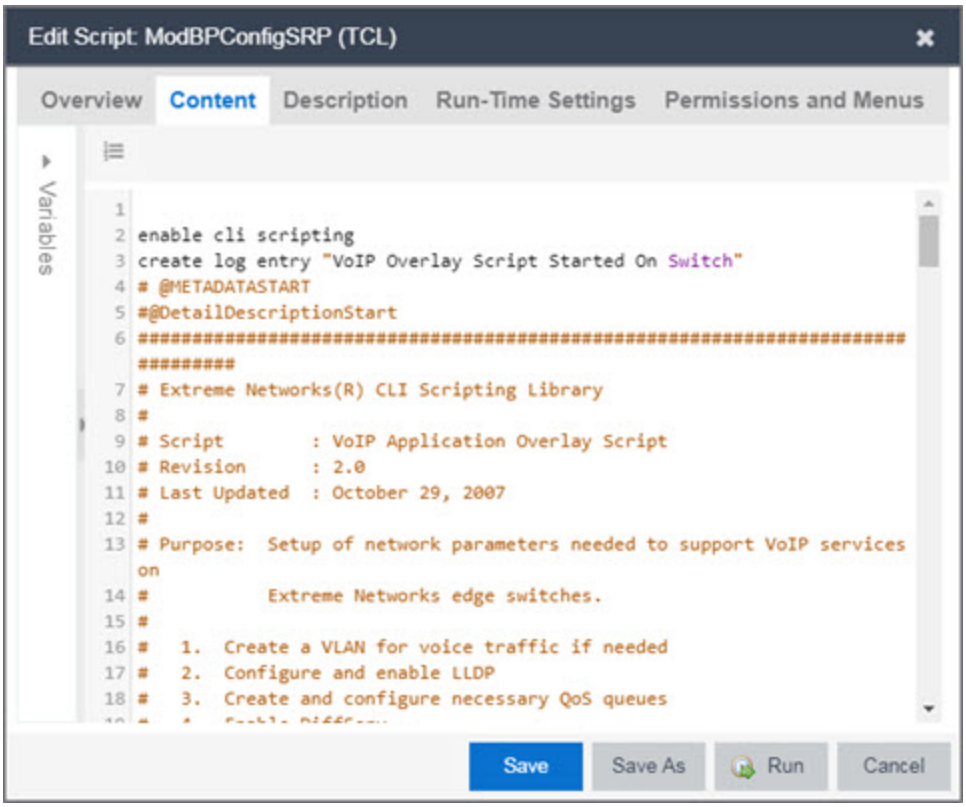
To display the scripts configured in ExtremeCloud IQ - Site Engine, select the **Tasks** tab, then select the **Scripts** tab.



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

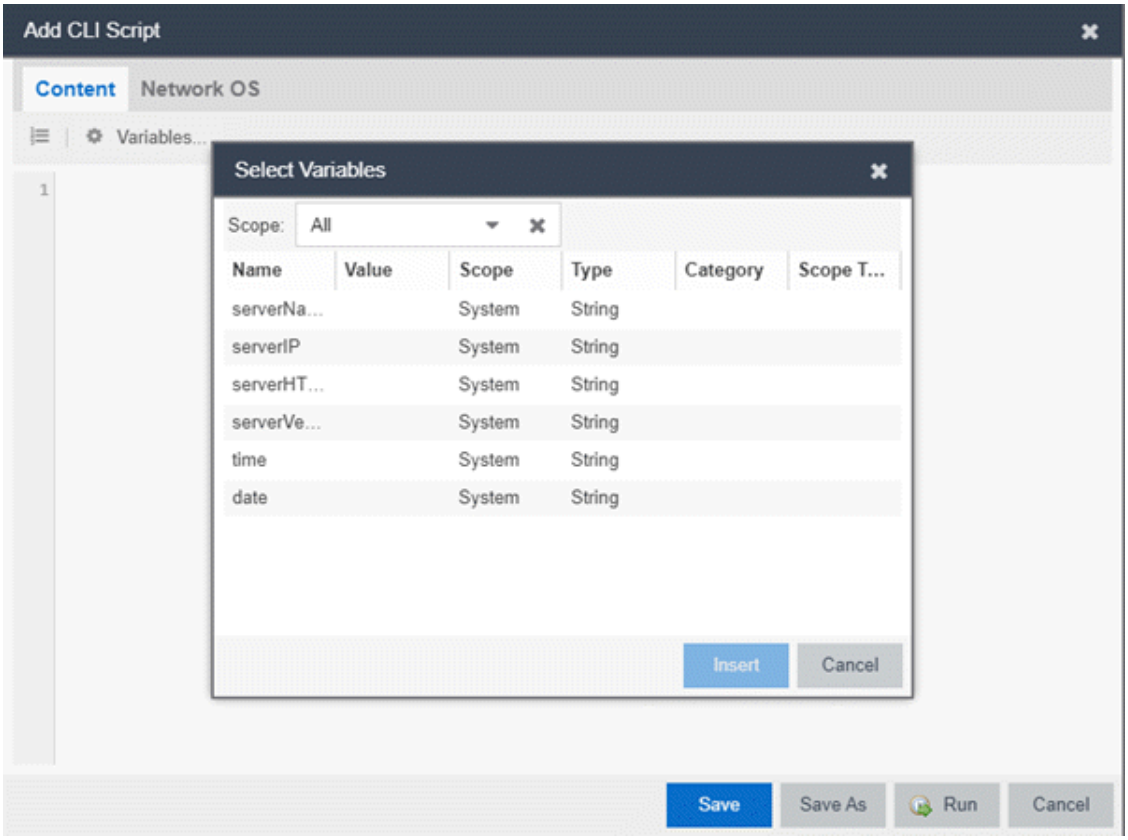
With scripting, you can:

- 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 device). Proceed to step 5.
   - **JSON-RPC-CLI**—Machine to Machine Interface (used to send CLI commands to an ExtremeXOS 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.

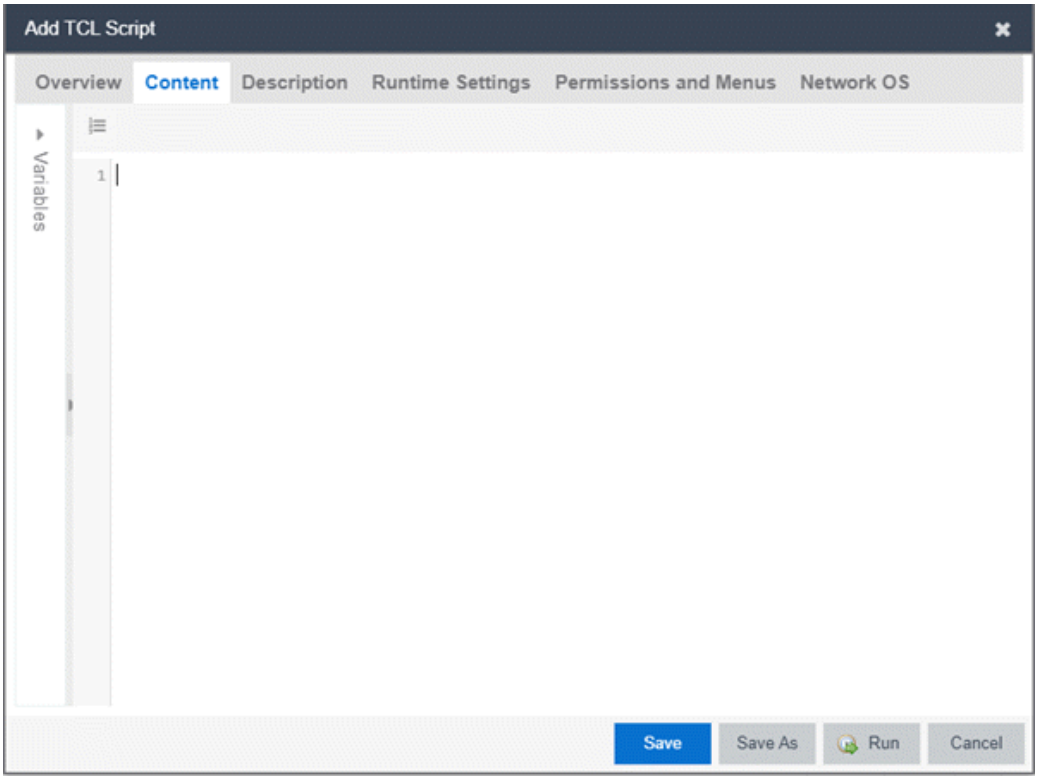
Select **Run** to run the CLI script immediately.

5. When selecting the **TCL**, **Python**, **JSON-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.

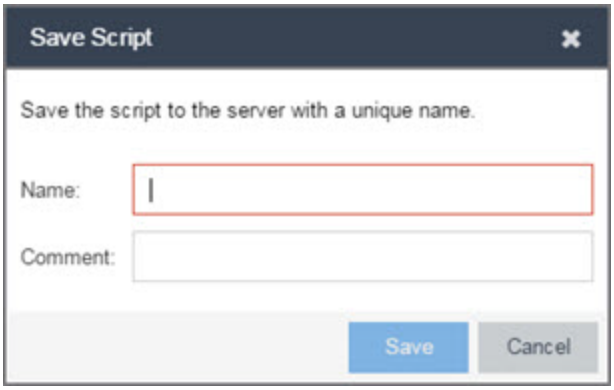
   The following are examples of types of script commands supported in ExtremeCloud IQ - Site Engine:

   - ExtremeXOS 12.1and 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.

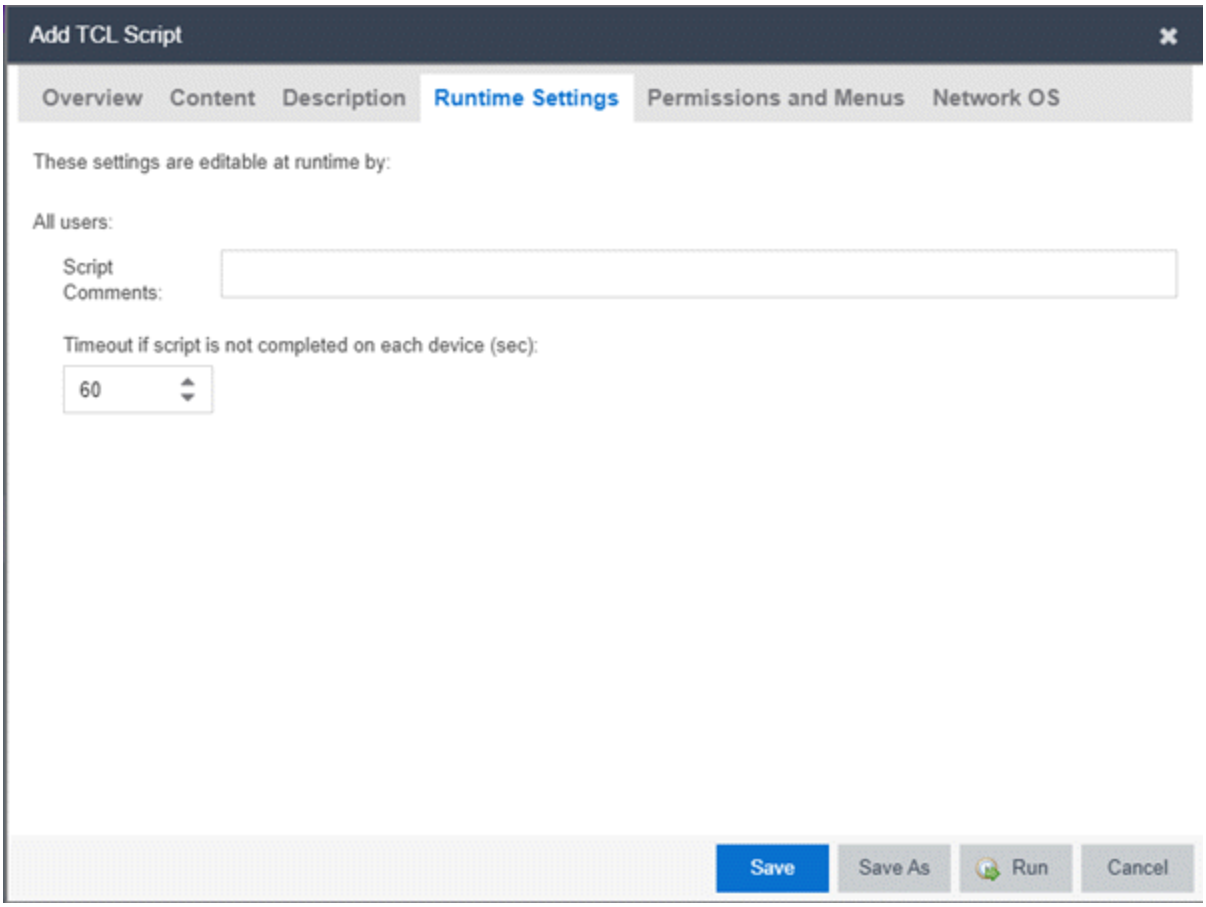


13. Type a name for the script file in the **Name** field and a comment about the script in the **Comment** field, if necessary.

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:

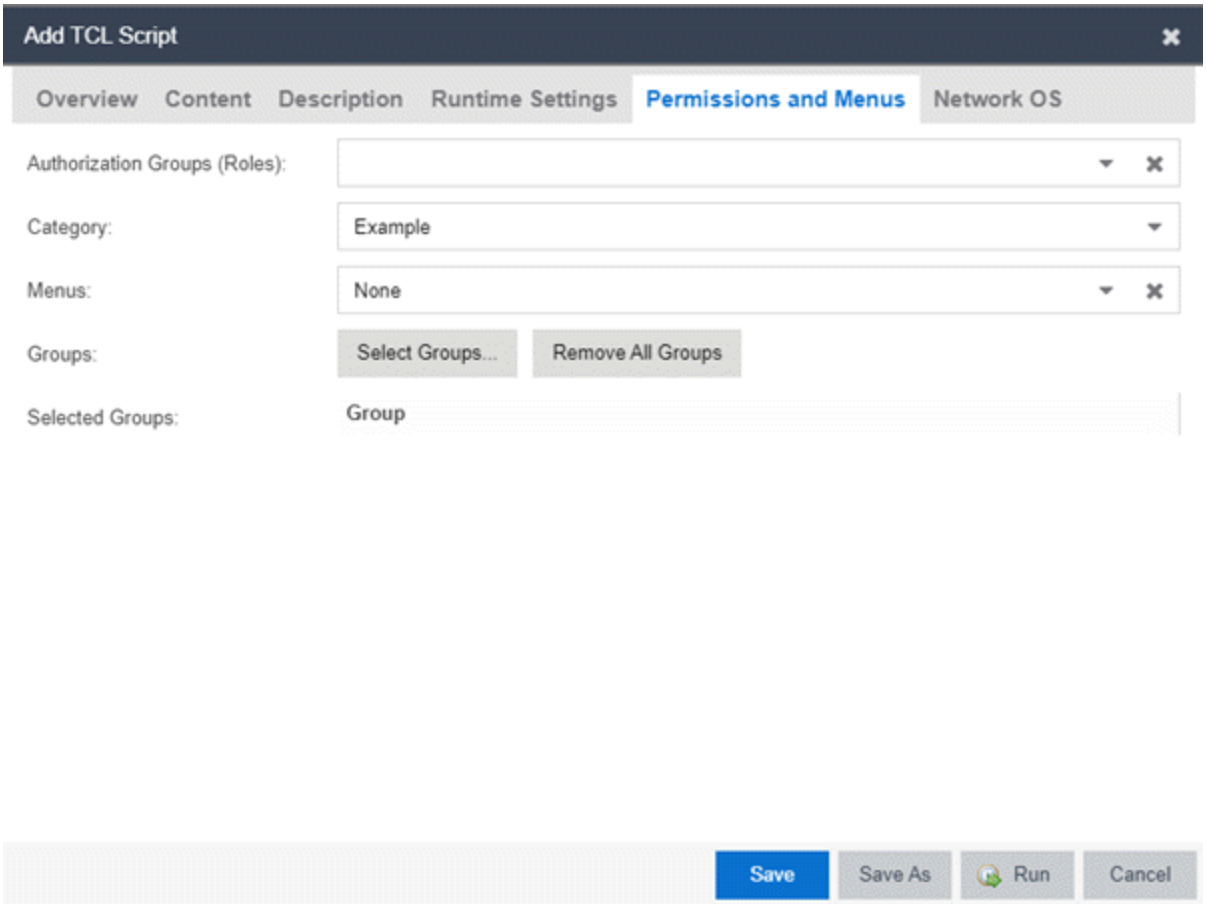
- **Script Comments**—Use this field to enter comments or a description of the script.
- **Timeout if script is not completed on each device (in seconds)** —Select the maximum length of time the script runs on each device or port (in seconds) before the process ends. This timeout value applies to each 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.

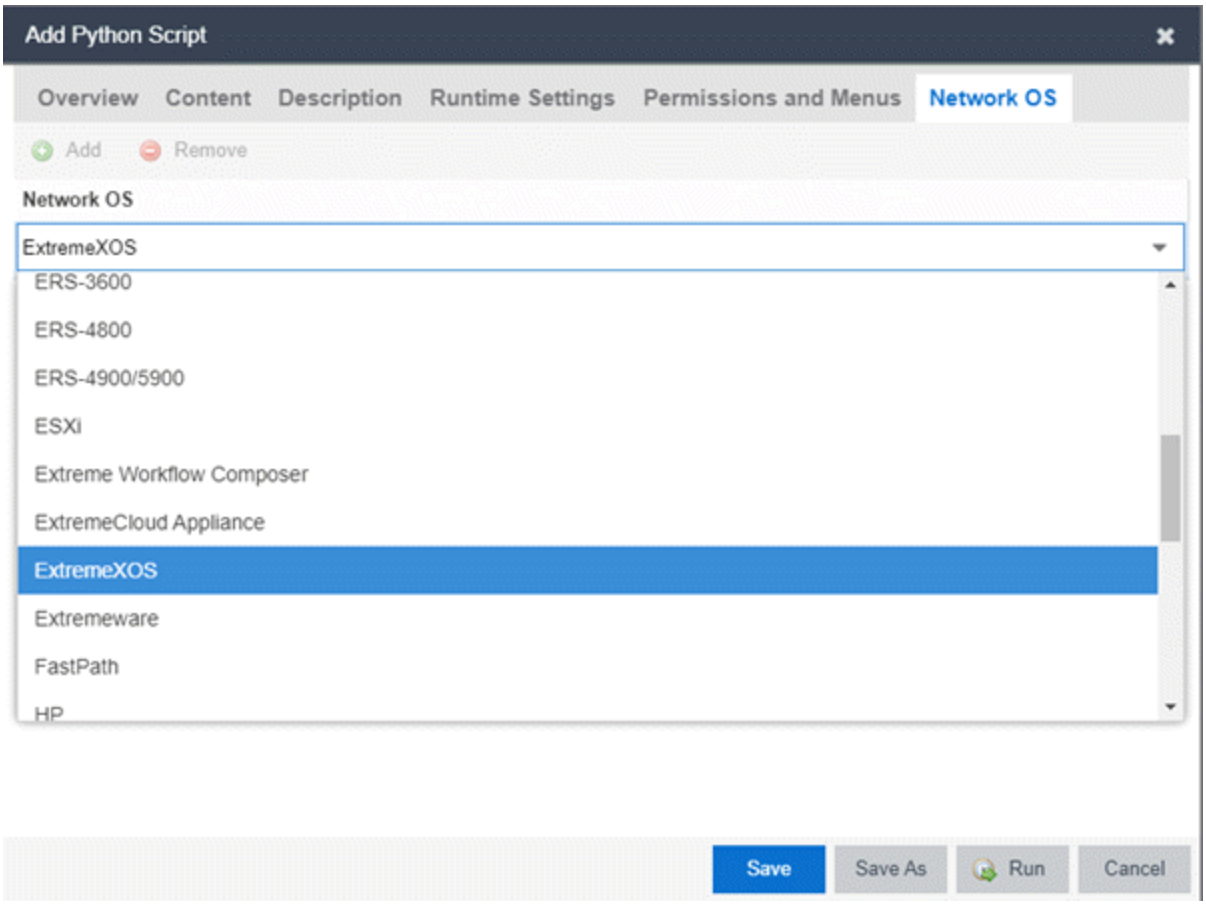
Groups
: Select the **Select Groups** to select the device groups on which the script displays.

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**.

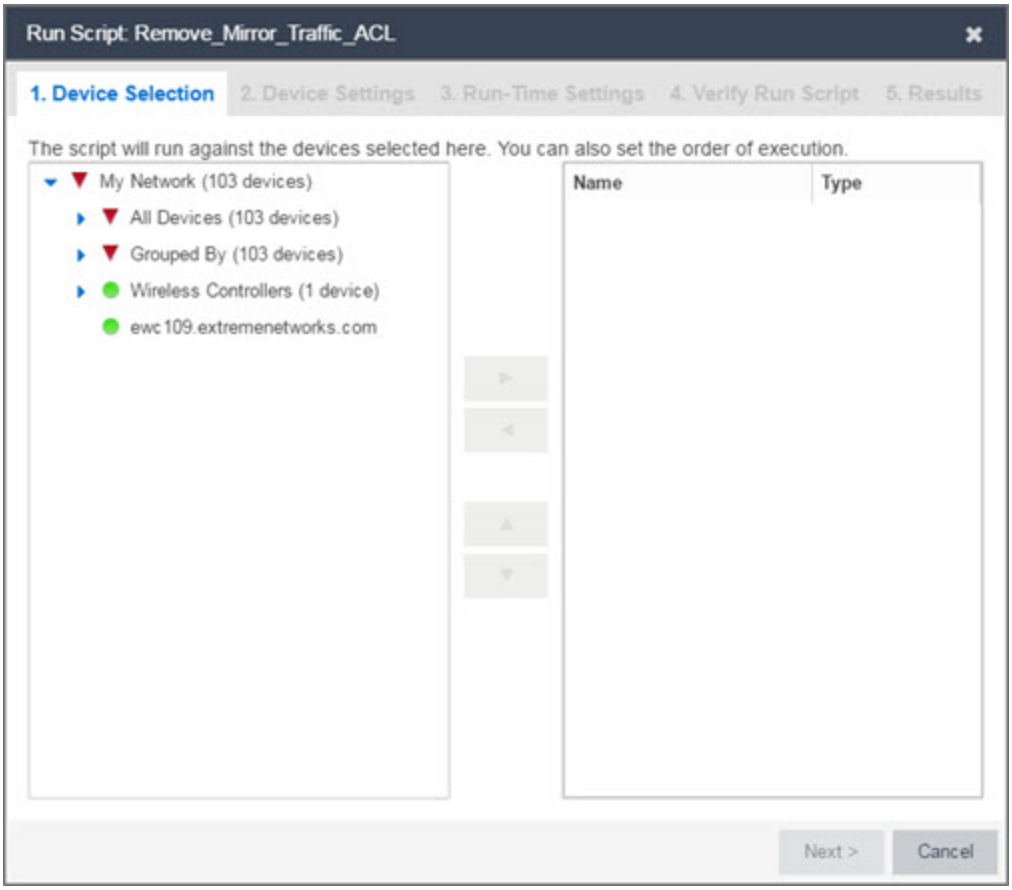
From the Tasks tab

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.

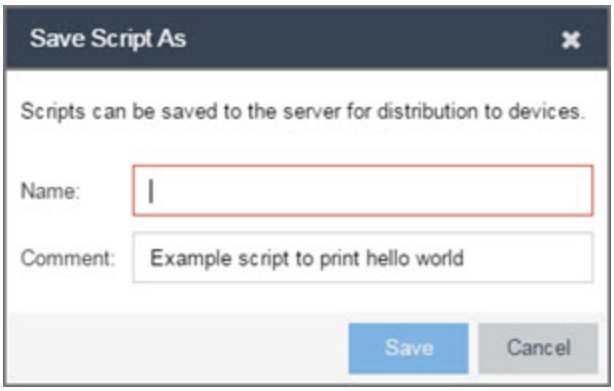
An event is stored in the console.log file in the `<install directory>/appdata/logs` folder each time a script is executed. The event in the log contains the location of the audit file. These audit logs reside in the tmp directory and remain for two weeks (per user), or until the next server restart, 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:

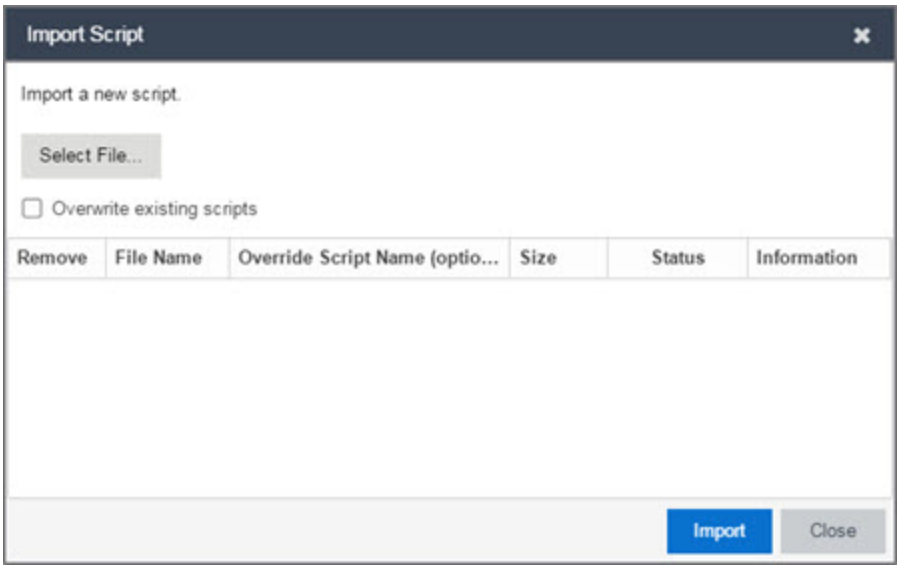
1. In the **Tasks** tab, select **Scripts**.
2. In the scripts table, select one or more scripts you want to delete.
3. Select the **Delete** button.
4. Select **Yes** to confirm the script deletion.

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 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 CLI commands
- Names of TCL functions

Also, do not use a period (.) within a variable name, use an underscore (_).

ExtremeXOS 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 12.1and 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 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 11.6 and higher support this command.

NOTE: The $UPPERCASE command is deprecated in ExtremeXOS 12.1CLI 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 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 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 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 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 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 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.

Related Information

For information on related topics:

- Scripts
- Workflows
- Saved Tasks
- Scheduled Tasks

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

The following web browsers are supported:

- Microsoft Edge and Internet Explorer version 11
- 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.

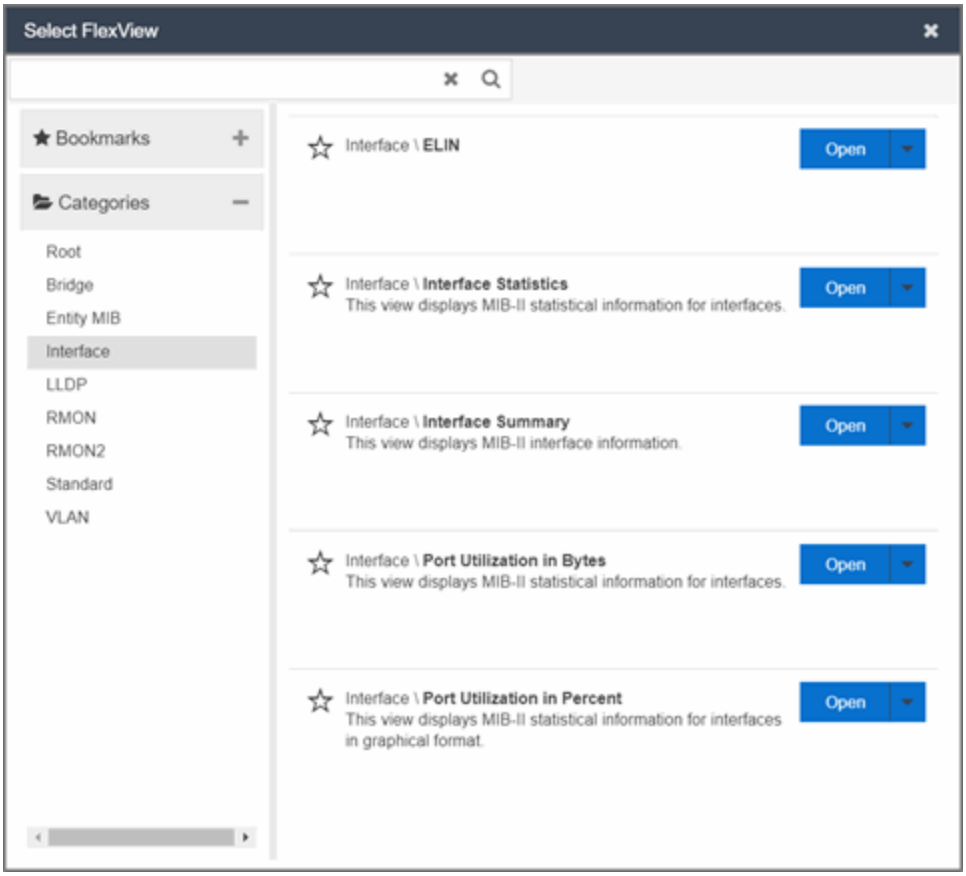
1. Launch ExtremeCloud IQ - Site Engine and select **Network** > **Devices**.
2. Select one or more devices in the **Devices** tab left panel or from within the Devices list.

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.

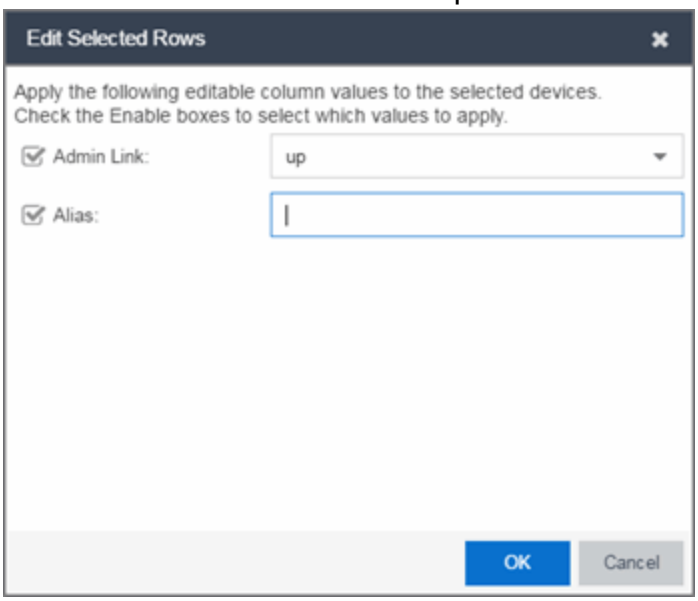
NOTE: Row creation and data exports are not currently supported in FlexViews.

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.

Related Information

For information on related topics:

- Adding Custom FlexViews and MIBs
- Network

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)

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.)

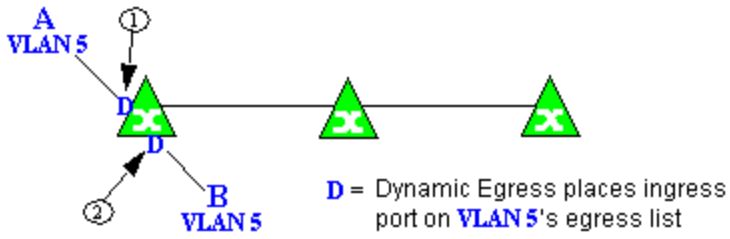
When you disable Dynamic Egress for a VLAN, the VLAN effectively becomes a discard VLAN. Since the destination port is not added to the egress list of the VLAN, the device discards the traffic. If you want a VLAN to act as a discard VLAN, disable Dynamic Egress for that VLAN. (See Example 3, below.)

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 NetSight 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.

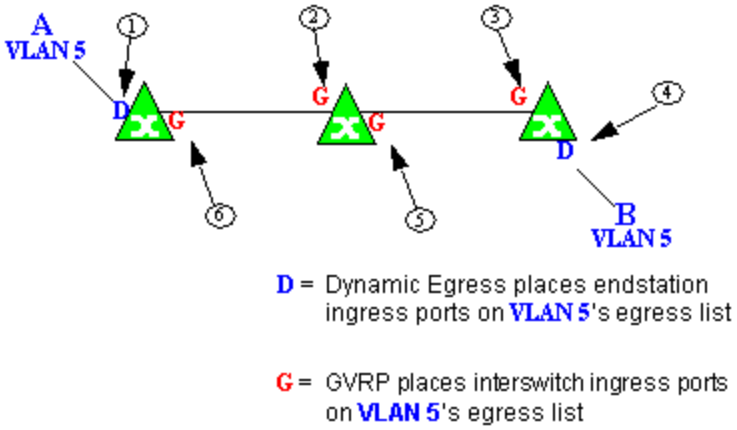
Example 1: Dynamic Egress Enabled

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

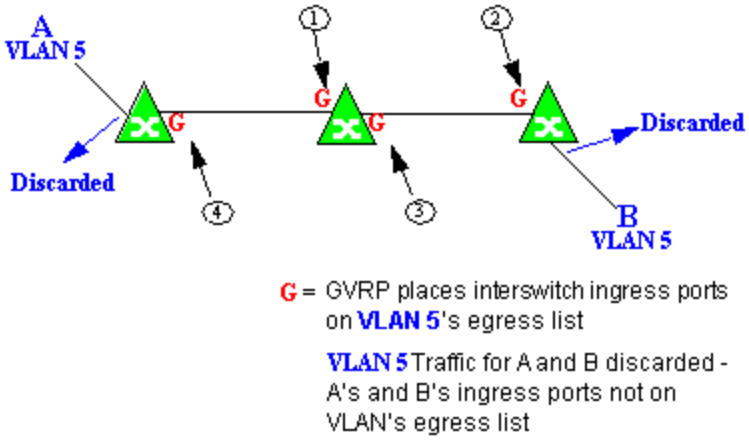
In this example, Dynamic Egress is enabled for VLAN 5, and the destination endstation, B, is on a different device from the source endstation, A. When A is tagged with VLAN 5, Dynamic Egress places A's ingress port (1) on VLAN 5's egress list. GVRP then places interswitch ingress ports (2) and (3) on 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 1through 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 1through 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 1through 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: 1through 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 1and 4094 that identifies a particular VLAN. VID 1is 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.

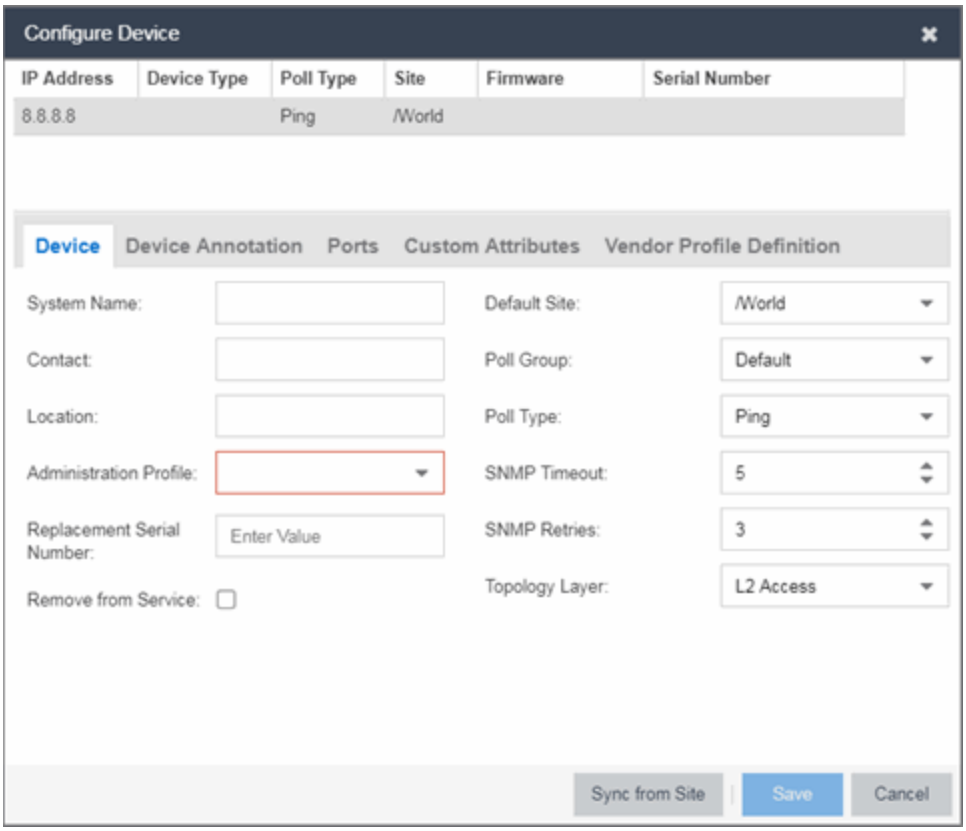
Create and Edit a VLAN on a Device

This section outlines how to create and edit a VLAN. From the **Network** tab, you can:

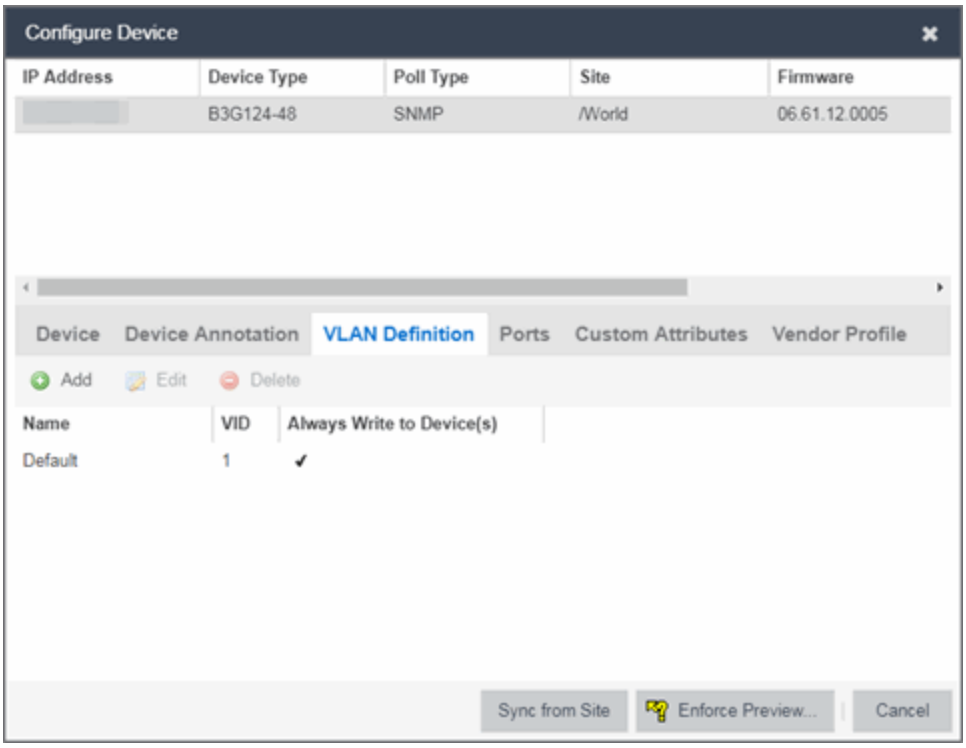
- Create a new VLAN
- Edit the ports of an existing VLAN
- Edit the name of an existing VLAN
- Remove devices from an existing VLAN

To create a new VLAN:

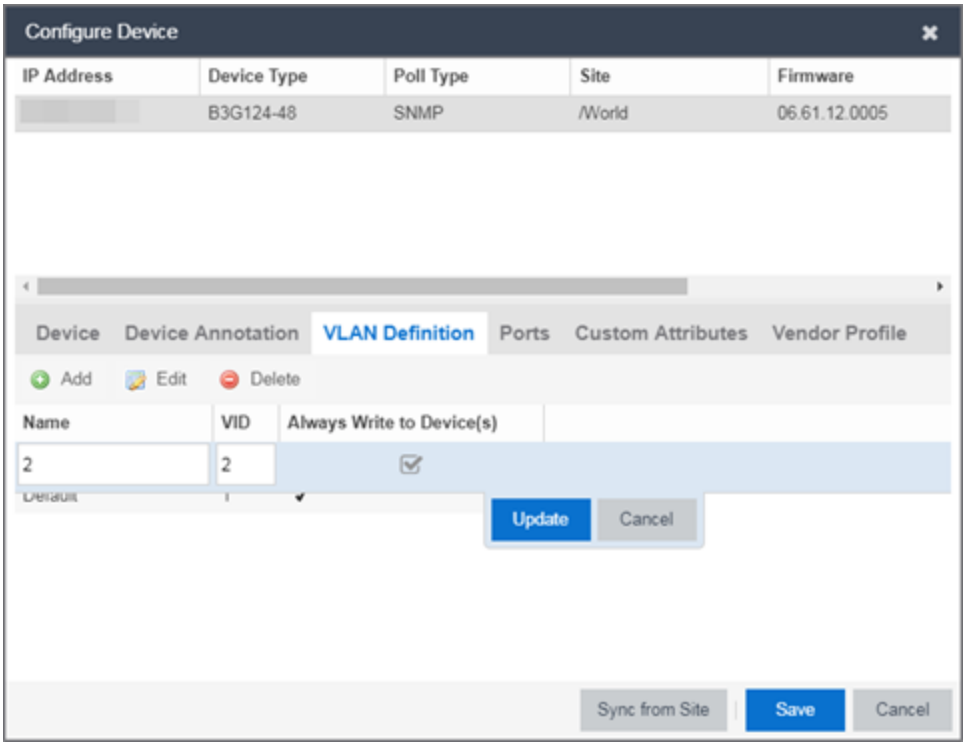
1. Launch ExtremeCloud IQ - Site Engine.
2. Open the **Network > Devices** tab.
3. Select the device from the devices list. Right-click the device and select **Device > Configure Device**.
   The **Configure Device** window opens.



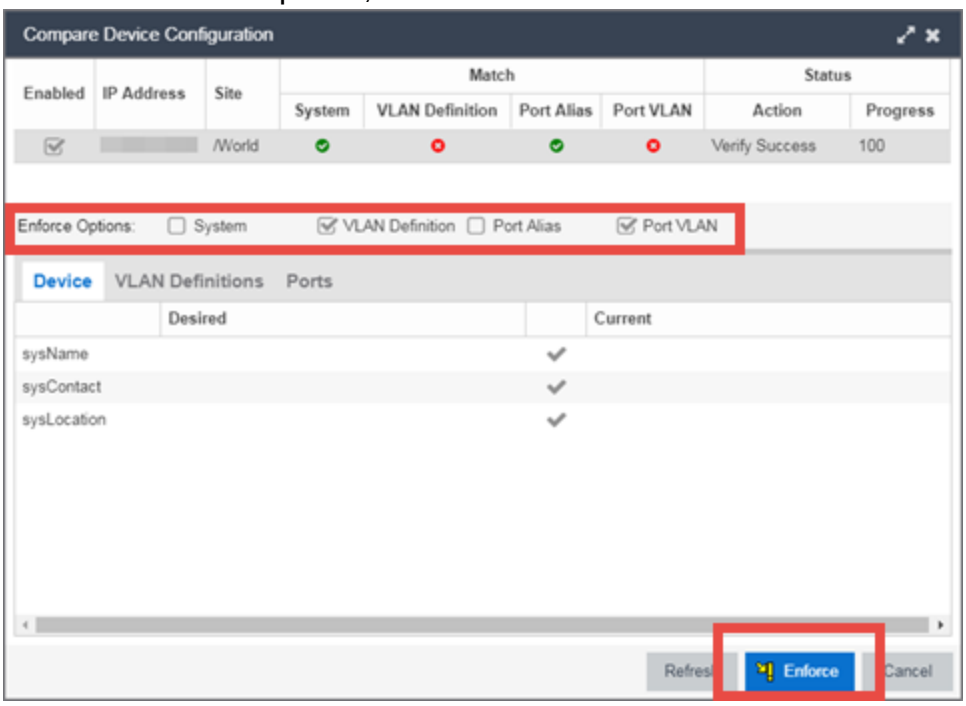
4. Select the **VLAN Definition** tab.



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:

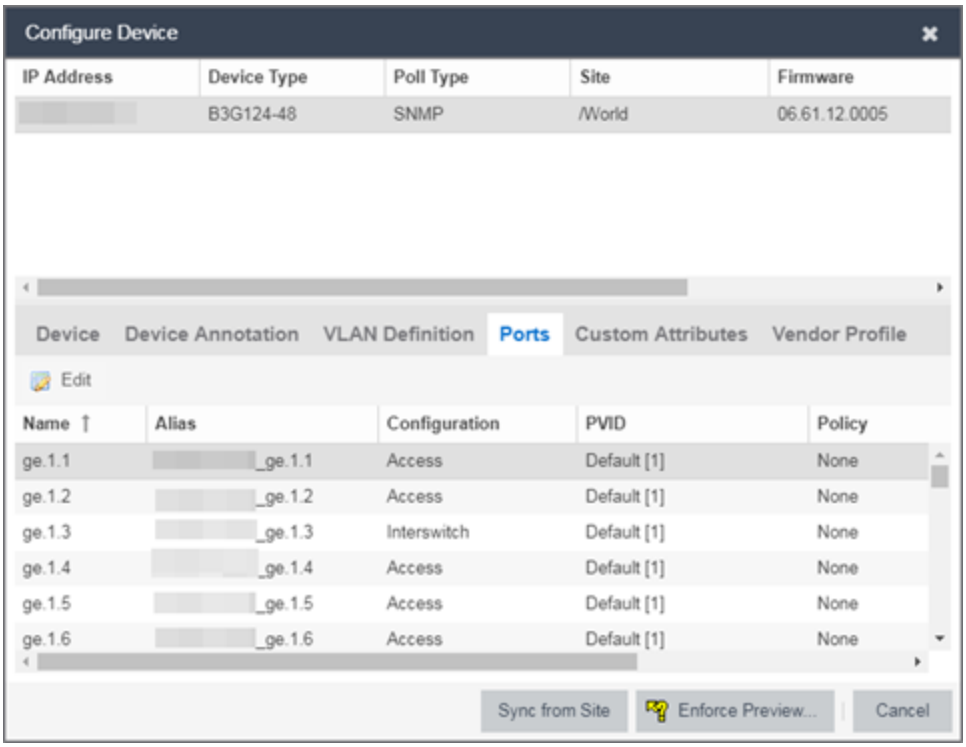
- `site.enforceOption.autoEnable.system=false`
- `site.enforceOption.autoEnable.vlanDefinition=false`
- `site.enforceOption.autoEnable.portAlias=false`
- `site.enforceOption.autoEnable.portVlan=false`

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**.

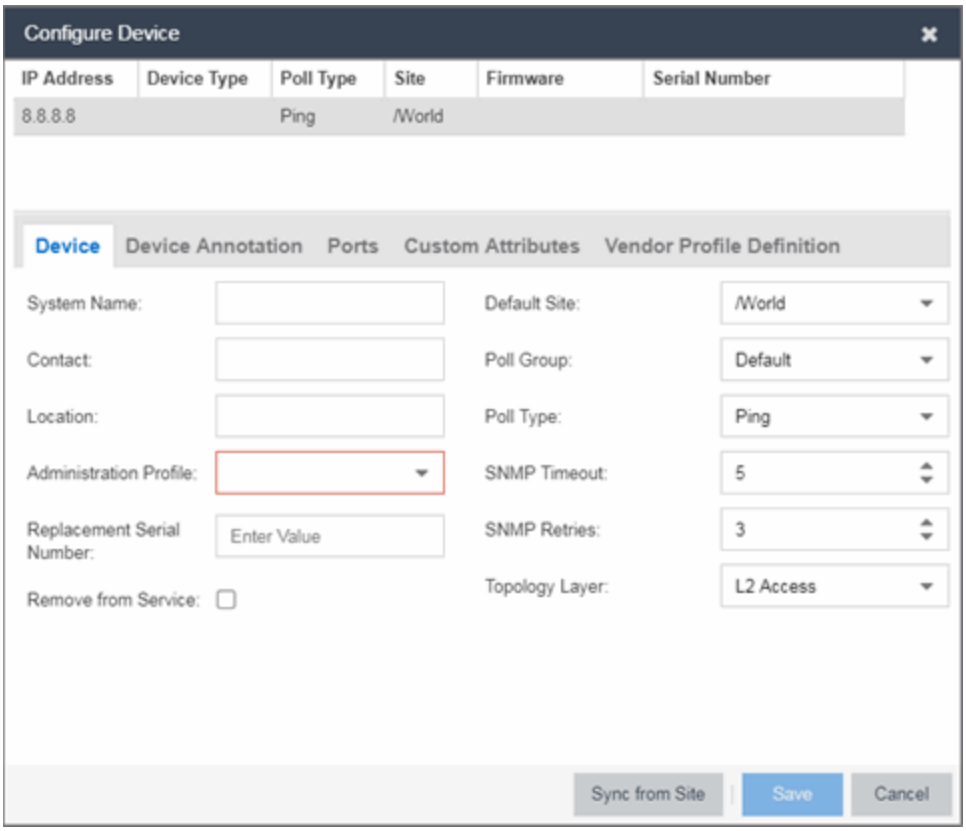
NOTE: By default, the checkboxes in the Enforce Options section of the window are not selected. To configure ExtremeCloud IQ - Site Engine to select the checkboxes by default, open the `NSJBoss.properties` file and change **false** to **true** in the following lines:

- `site.enforceOption.autoEnable.system=false`
- `site.enforceOption.autoEnable.vlanDefinition=false`
- `site.enforceOption.autoEnable.portAlias=false`
- `site.enforceOption.autoEnable.portVlan=false`

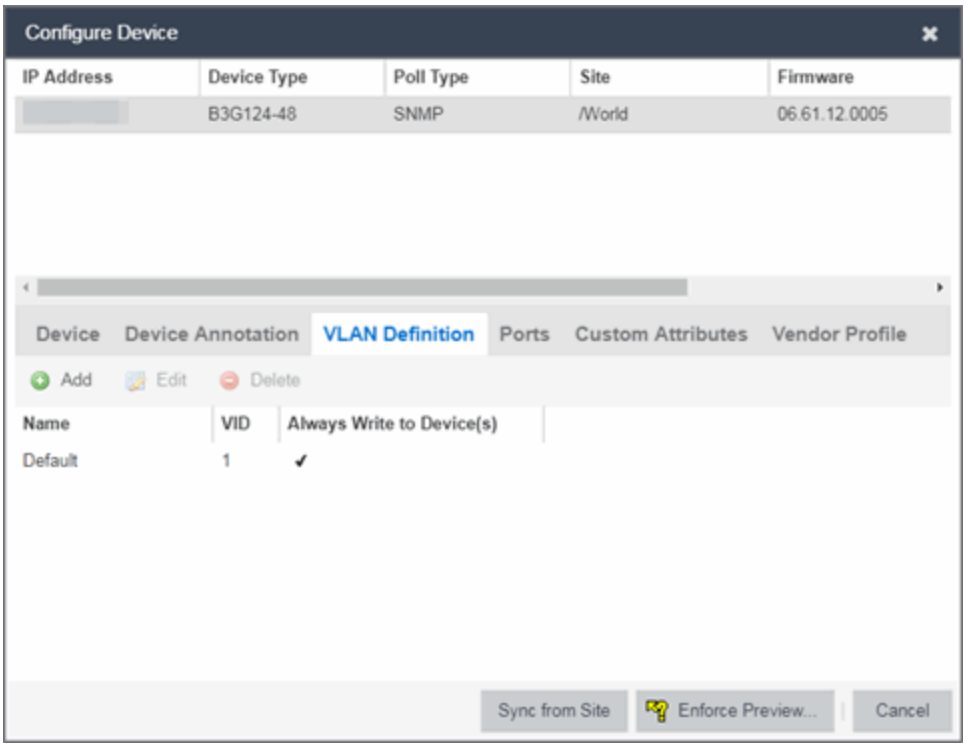
The VLAN is now configured to the Ports.

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.



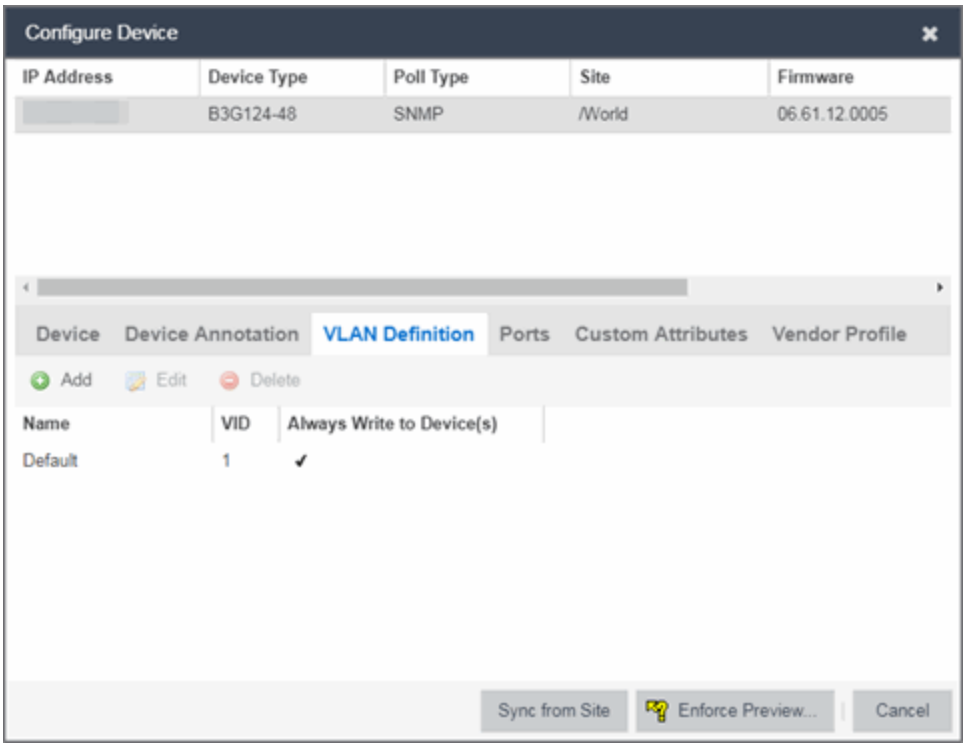
5. Select the **VLAN Definition** tab.



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**.

Related Information

For information on related topics:

- Maps
- Devices tab

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`.

Related Information

For information on related topics:

- FlexViews
- Network

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