Extreme Networks®

Extreme Management Center User Guide

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

Extreme Management Center Help

Extreme Management Center provides access to web-based reporting, network analysis, troubleshooting, and helpdesk tools. Extreme Management Center 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 Extreme Management Center license.

For a list of instructions outlining the initial setup of your network in Extreme Management Center, see Extreme Management Center Initial Configuration Checklist.

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

Extreme Management Center Features

Extreme Management Center provides the following features:

- 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. If you have a NetSight Advanced License (NMS-ADV), 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 — Extreme Management Center administration tools to monitor and maintain the Extreme Management Center application and its components.
- Connect — Provides configuration to allow you to integrate third-party software with Extreme Management Center's Extreme Access Control 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.

Document Version

The following table displays the revision history for the Extreme Management Center Help documentation.

Date	Revision Number	Description
6-18	8.1 Revision -00	Extreme Management Center 8.1 release

Date	Revision Number	Description
06-17	8.0 Revision -00	Extreme Management Center 8.0 release
04-16	7.0 Revision -00	Extreme Management Center 7.0 release

PN: 9035223-03

Getting Started with Extreme Management Center

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

Requirements

This section provides information on license requirements for the different Extreme Management Center features, as well as access requirements, browser requirements, and screen resolution requirements.

Extreme Management Center License Requirements

The following table shows license requirements for the different Extreme Management Center features. Contact your sales representative for information on obtaining the appropriate Extreme Management Center license.

Extreme Management Center Feature	License Required
Network Alarms and Events Administration Search Control (End Systems tab)	NetSight Base (NMS-BASE)
All the above features and: Reports Maps Control (Dashboard, System, Health, Data Center, and Configuration tabs) Analytics Wireless PortView Web FlexViews Check for Firmware Updates Policy	NetSight (NMS)
All the above features and: Advanced Wireless Map features	NetSight Advanced (NMS-ADV)

Extreme Management Center Access Requirements

Access to the Extreme Management Center application and its features is determined by the user's membership in an Extreme Management Center authorization group and the group's assigned capabilities. The following table

lists the different Extreme Management Center access options and features, and their corresponding capabilities. For more information on how to configure capabilities and authorization group membership, see the Extreme Management Center Help topic "How to Configure User Access to Extreme Management Center Applications," located in the Extreme Management Center Suite-Wide Tools user guide in the "Authorization Device Access" section.

To have full read/write access to all Extreme Management Center 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 Extreme Management Center functionality by selecting a combination of capabilities.

Extreme Management Center Access Options and Features	Required Capabilities
Launch Extreme Management Center. Allows the ability to launch the Extreme Management Center application.	NetSight OneView > Access OneView
View Extreme Management Center Reports. Adds the ability to view reporting data.	NetSight OneView > Access OneView Reports
View Extreme Management Center Maps. Adds the ability to view maps.	NetSight OneView > Maps > Maps Read Access
View and Configure Extreme Management Center Maps. Adds the ability to view and configure maps.	NetSight OneView > Maps > Maps Read/Write Access
View Extreme Management Center Wireless. Adds the ability to view wireless data.	NetSight Console > Wireless Manager > Launch
View Extreme Management Center Administration. Adds access to the Extreme Management Center administration tools and the ability to enable data collection.	NetSight OneView > Access OneView Administration
View Extreme Management Center Search. Adds the ability to use the Extreme Management Center Search functionality.	NetSight OneView > Access OneView Search
View Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center 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
View and modify Extreme Management Center 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 Extreme Management Center 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

Extreme Management Center Access Options and Features	Required Capabilities
View and Edit Extreme Management Center 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 Extreme Management Center Flows. Adds the ability to view NetFlow data for devices in the network.	NetSight OneView > NetFlow Read Access
View Extreme Management Center 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 Extreme Management Center **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 Extreme Management Center **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 Extreme Management Center **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 Extreme Management Center **Network** tab.	NetSight Suite > Devices > Add, Discover and Import
Delete Devices. Adds the ability to delete devices in the Extreme Management Center **Network** tab.	NetSight Suite > Devices > Delete
Compare Configurations. Adds the ability to compare archived device configurations in either the Extreme Management Center **Network** tab or the Archive Details Report available in the Extreme Management Center **Reports** tab.	Inventory Manager > Configuration Archive Management > View/Compare Configurations

Here are several scenarios that show how different Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center 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 and Internet Explorer version 11
- 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, Extreme Management Center is best viewed on a system with a minimum screen resolution of 1280x1024.

Enable Report Data Collection

To view Extreme Management Center 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 Extreme Management Center device reports, you must enable statistics collection for your network devices from either Extreme Management Center Devices, or the Console device tree or Device Properties tab. Statistics can be collected in a historical collection mode or a monitor collection mode.

- Historical Mode — Device and physical port statistics are saved to the database and aggregated over time, and are then used in Extreme Management Center 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.

- Monitor Mode — Device statistics are saved to a Monitor cache for one hour and then dropped. These statistics are used for active threshold alarms, configured in the Console Alarms Manager, but not for Extreme Management Center reporting.

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

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

- Extreme Access Control Engine
  When collecting statistics on an Extreme Access Control engine, the engine must be added to Extreme Management Center to collect all engine statistics. In addition, Monitor mode is not supported on Extreme Access Control engines.
- Application Detection Engine
  When collecting statistics on an Application Detection engine, the engine must be added to the Analytics > Configuration > Application Analytics Engines table in order for Extreme Management Center to collect all Application Detection statistics. In addition, Monitor mode is not supported on Application Detection engines.
- ExtremeWireless Controller
  Wireless Controller statistics collection is configured separately from other devices.

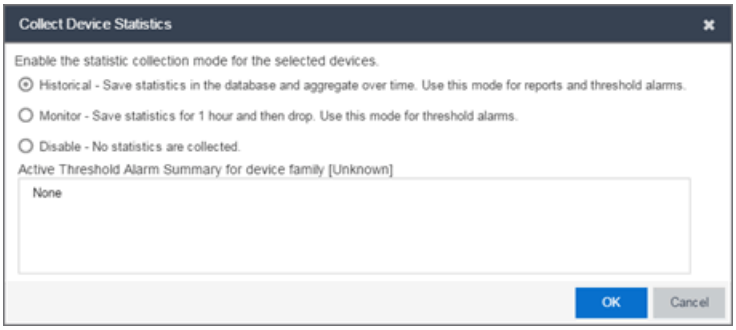
Steps for Enabling Collection

Use the following steps to enable device statistics collection.

1. You can enable statistics collection from either Extreme Management Center 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 click 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 or Monitor.



All active threshold alarms configured in the Extreme Management Center 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 Monitor 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. Click OK. Extreme Management Center begins collecting statistics for the selected devices.

Enable Interface Statistics Collection

To view Extreme Management Center interface reports, you must enable statistics collection for your device interfaces from either the Extreme Management Center Network tab, or the Console Port Properties tab or Interface Summary FlexView. Statistics can be collected in a historical collection mode or a monitored collection mode.

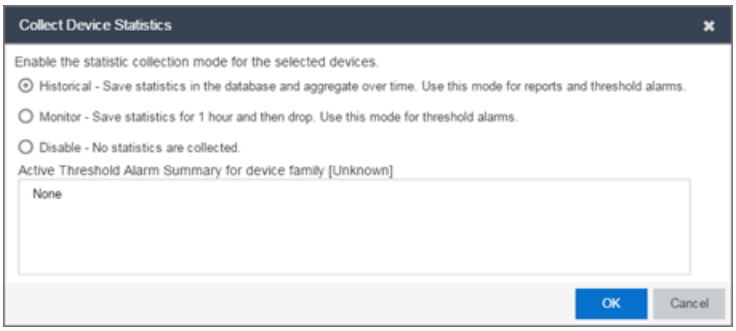
- Historical Mode — Interface statistics are saved to the database and aggregated over time, used in Extreme Management Center reports. The interface statistics are also used for active threshold alarms configured in the Alarms and Events tab.
- Monitor Mode — Interface statistics are saved to a Monitor cache for one hour and then dropped. These statistics are used for active threshold alarms configured in the Console Alarms Manager, but not for Extreme Management Center reporting. (Note that the Monitor mode option is not available if you have disabled Monitor Collection

in the OneView Collector Advanced Settings window in the **Administration** > **Options** tab.)

Steps for Enabling Collection

Use the following steps to enable interface statistics collection.

1. You can enable statistics collection from either Extreme Management Center or Console:
   - On the **Network** tab, click on 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** or **Monitor**.



   All active threshold alarms configured in the Extreme Management Center **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 Monitor 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. Click **OK**. Extreme Management Center begins collecting statistics for the selected interfaces.

Enable Wireless Controller Statistics Collection

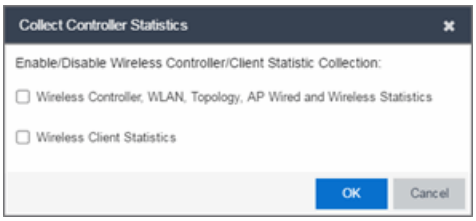
Wireless Controller statistics collection is configured separately from other devices. When you enable Wireless Controller statistics collection, it includes Wireless Controller, WLAN, Topology, and AP wired and wireless statistics, and you also have the option to collect wireless client statistics.

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.

Steps for Enabling Collection

Use the following steps to enable wireless controller statistics collection.

1. You can enable statistics collection from either Extreme Management Center or Console:
   - On the **Network** tab, right-click one or more wireless controllers and select **Device** > **Collect Device Statistics**. You can also click 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. Click **OK**. Extreme Management Center begins collecting statistics for the selected controllers.

Enable Flow Collection

To view Extreme Management Center 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 Extreme Management Center. Flow collection is only available with the NMS-ADV license.

Enable Flow Collection on a Device

In Extreme Management Center, open the Advanced Configuration panel. Select an Application Analytics 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.

Extreme Management Center Scalability

Extreme Management Center 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

Extreme Management Center Timeout

Extreme Management Center 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 Extreme Management Center web page. For additional information, see the Web Server Options Help topic.

Network

Selecting the **Network** tab displays details for the managed devices in Extreme Management Center, with sorting and filtering of relevant information for network troubleshooting.

Additionally, the Legacy menu in the **Network** tab menu provides access to the following Java-based applications:

- Console
- MIB Tools

Navigating the Network Tab

Clicking **Network** in the Menu Bar to the left of Extreme Management Center opens the **Network** tab. The **Network** tab provides access to the following sub-tabs:

- Dashboard — Displays summary Extreme Management Center data including switch, network and interface statistics, the five most recent alarms, important wireless data, as well as archive, backup, database, and scheduled event information.
- 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 Extreme Management Center.

Dashboard

Select the Dashboard tab to view graphical data about devices on your network. Click Info (ℹ) at the top-right of the page to access detailed information about each of the reports. Some of the charts and tables can be selected to provide additional information.

The Dashboard contains three options, the Impact Analysis, Overview, 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

This shows twelve panes containing statistical information about devices on your network. The information presents a sampling of the performance of individual devices.

Inventory

The Inventory dashboard contains three tabs, presenting network inventory and change management information.

- Summary — Displays a pie chart of the percentage of archived devices, archived devices with changed configurations, and devices not archived; a pie chart of the percentage of firmware with a reference image; number of devices backed up, a listing of database properties, and upcoming scheduled events.

  NOTE: Click a section of a pie chart to view a list of devices filtered to meet the selected criteria.

- Asset Tracking — Provides a list of devices based on their asset tag. An asset tag is a unique asset number assigned to a device for inventory tracking purposes.

- Device Tracking — Allows you to view a history of device attributes and monitor changes made to devices.
- Capacity Planning — Provides a pie chart indicating the number of ports in use, the number of ports not in use, and the number of ports for which port information is not collected. Click a section in the chart to display a list of ports that match the selected criteria.

Devices

Select the Devices tab to display information about devices in your network and the maps and sites in which they are added. The left-panel of the Devices tab contains a drop-down menu, allowing 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 the item you selected 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.

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.
- 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 — The Site tab allows you to create a default configuration for devices being added to the selected site.
- Site Summary — The Site Summary tab contains a table of information about the sites on your network, including the path, addresses, and configuration.
- FlexReports — The FlexReports tab contains reports available for the device, controller, map, or site selected in the left-panel.

Discovered

When a new device is added to the network, it is automatically detected and displayed in the Discovered tab.

Select the Discovered tab to quickly configure a new device using a configuration template created on the Site tab or a cloned configuration from an existing network device.

Extreme Management Center can discover and configure new devices automatically using ZTP+ device configuration.

NOTE: You can also add a new device directly to Extreme Management Center in a specific site using the Site tab.

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 menu at the top of the tab and are grouped into the following three reporting areas:

- Device
- Interface
- Network

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

Click **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:

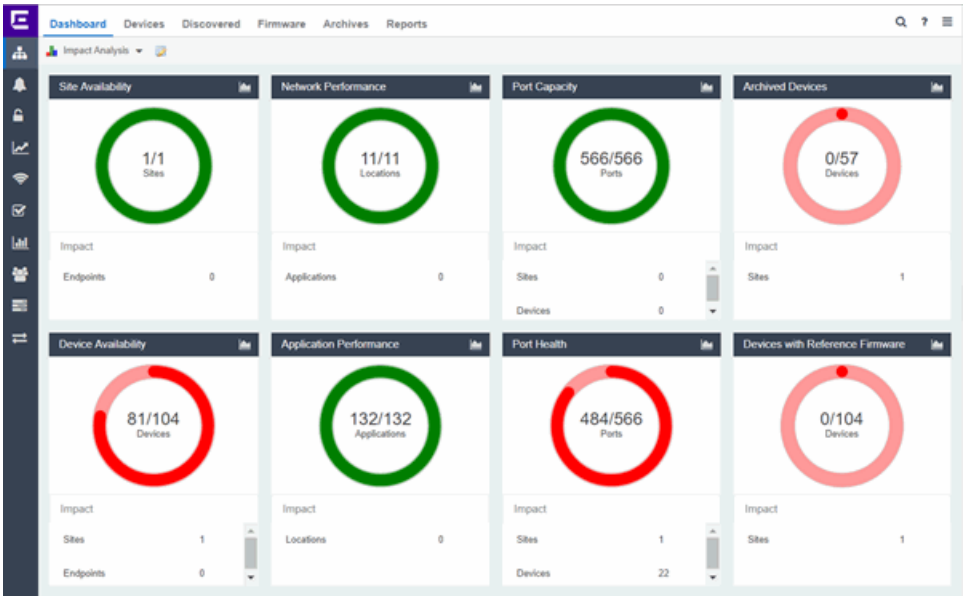
- Device Operations
- Search

For information on related tasks:

- Create Device Group
- Add Devices to Maps
- New Device Configuration in Extreme Management Center

Impact Analysis Dashboard Overview

Accessible from the **Network** tab, the **Impact Analysis Dashboard** displays a real-time summary of Availability, Performance, Capacity/Health, and Configuration data for your network.



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

- 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.

Charts

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

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. Extreme Management Center 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 Extreme Management Center can communicate to the total number of sites with at least one device. The number of end-points impacted by sites Extreme Management Center can not reach is listed in the Impact Summary beneath the ring chart.

- Click the ring chart to open the Unavailable Sites report that displays sites Extreme Management Center can not reach.
- Click **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.
- Click 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 Extreme Management Center can communicate to the total number of devices. The number of sites and endpoints that contain devices with which Extreme

Management Center can not communicate are listed in the Impact Summary beneath the ring chart.

- Click the ring chart to open the Unavailable Devices report that provides detailed data for all unavailable devices.
- Click **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.
- Click **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.
- Click 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 network locations with a network response time in the expected or better-than-expected range to the total number of network locations. 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 locations are counted separately.

NOTE: Enable Dynamic Thresholding to allow Extreme Management Center to automatically determine the expected response times based on previously observed response times. If you do not use Application Analytics or do not want to enable Dynamic Thresholding, you can remove this chart from the Impact Analysis dashboard in the Report Designer.

Use the **Locations** tab to configure the location at which an Application Analytics engine is located.

- Click the ring chart to open the Slow Locations report that displays locations with slower-than-expected network response times.
- Click **Applications** in the Impact Summary beneath the ring chart to open the Applications Impacted by Slow Locations 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 Extreme Management Center to report specific end-points impacted by slower-than-expected response times.

- Click **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.
- Click 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 locations 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 locations are counted separately.

NOTE: Enable Dynamic Thresholding to allow Extreme Management Center to automatically determine the expected response times based on previously observed response times. If you do not use Application Analytics or do not want to enable Dynamic Thresholding, you can remove this chart from the Impact Analysis dashboard in the Report Designer.

Use the Locations tab to configure the location at which an Application Analytics engine is located.

- Click 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.
- Click **Locations** in the Impact Summary beneath the ring chart to open the Locations Impacted by Slow Applications report that provides more details about the locations impacted by tracked applications and network services with slower-than-expected response times.
- Click **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 Extreme Management Center to report specific end-points impacted by slower-than-expected response times.

- Click 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.

- Click 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.
- Click 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.
- Click 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.
- Click 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.

- Click the ring chart to open the High Error Ports report that lists the ports with an excessive error rate.
- Click 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.

- Click **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.
- Click 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.

- Click the ring chart to open the Unarchived Devices report that provides a list of the devices not archived in the last 30 days.
- Click **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.
- Click 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.

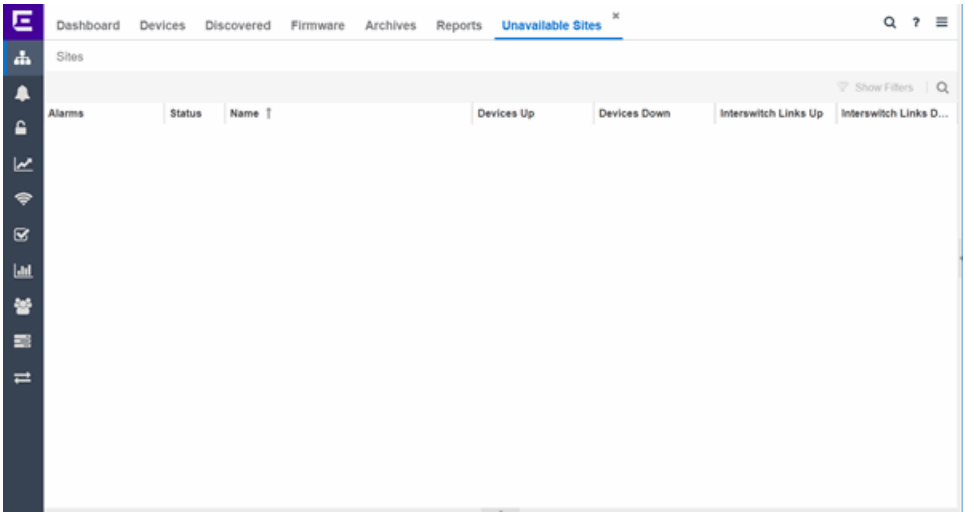
- Click the ring chart to open the Devices Without Reference Firmware report that displays a list of affected devices not running reference firmware.
- Click **Sites** in the Impact Summary beneath the ring chart to open the Sites Impacted by Devices Without Reference Firmware report that provides a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

Related Information

- Impact Analysis Options
- Extreme Management Center Network Tab Overview

Unavailable Sites Report

The Unavailable Sites report provides a list of sites Extreme Management Center considers to be down. Use the **Devices Up for Site Up (percent)** field on the Impact Status Options tab to configure the threshold Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center 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.

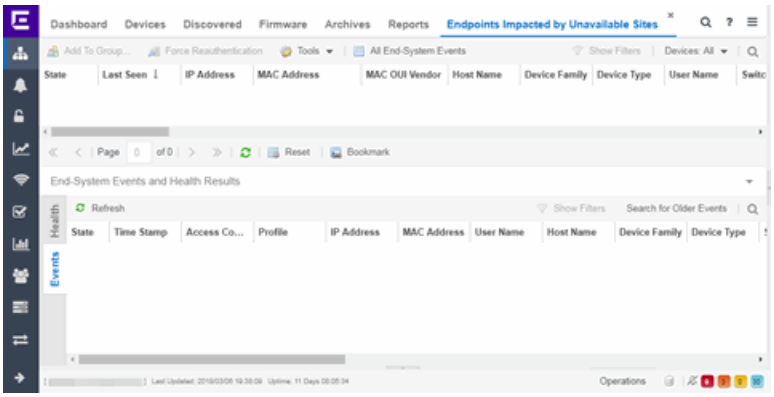
Interswitch Links Down
This column indicates the number of Interswitch Links with a Status of Down in the site.

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 Extreme Management Center unable to communicate with a site (Status of Down). The report also shows any events that pertain to the end-systems selected in the top table. Additionally, the report lists the risks and vulnerabilities for the device and assigns a score based on the severity of the risk.



The report contains three tables:

- End-System Information
- Events
- Health

End-System Information

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

ID

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

State

The end-system's connection state:

- Scan - The end-system is currently being scanned.
- Accept - The end-system is granted access with either the Accept policy or the policy returned from the RADIUS server in the filter-ID.
- Quarantine -The end-system is quarantined because the scanning test failed.
- Reject - The end-system was rejected because the assigned NAC 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 Extreme Management Center
- 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 on 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 NAC appliance 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 NAC appliance.

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 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 NAC 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.

Access Control engine / Source IP
The NAC appliance to which the end-system is connecting.

Profile
The Profile assigned to the end-system in the Extreme Management Center 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

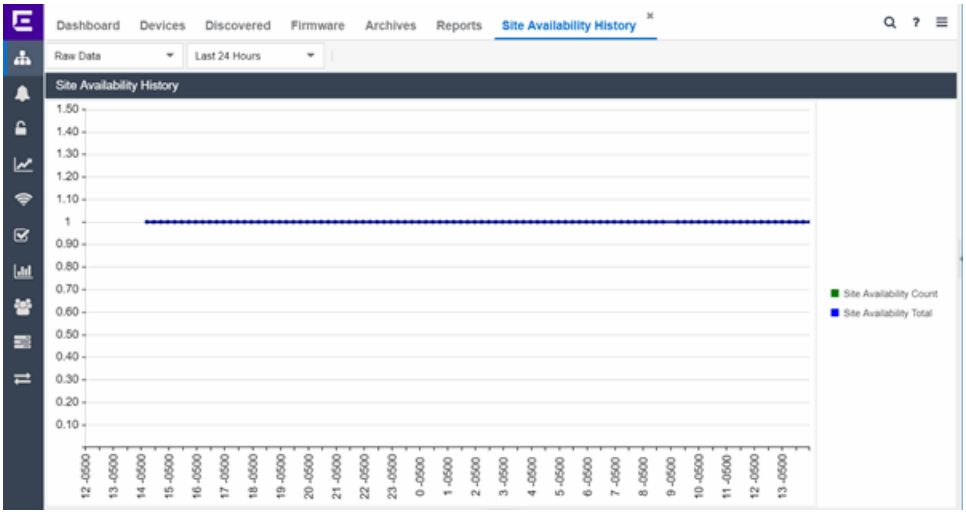
Site Availability History Report

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 Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center analyzes sites from the data drop-down menu. Available options are **Raw**, **Hourly**, or **Daily** data.

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

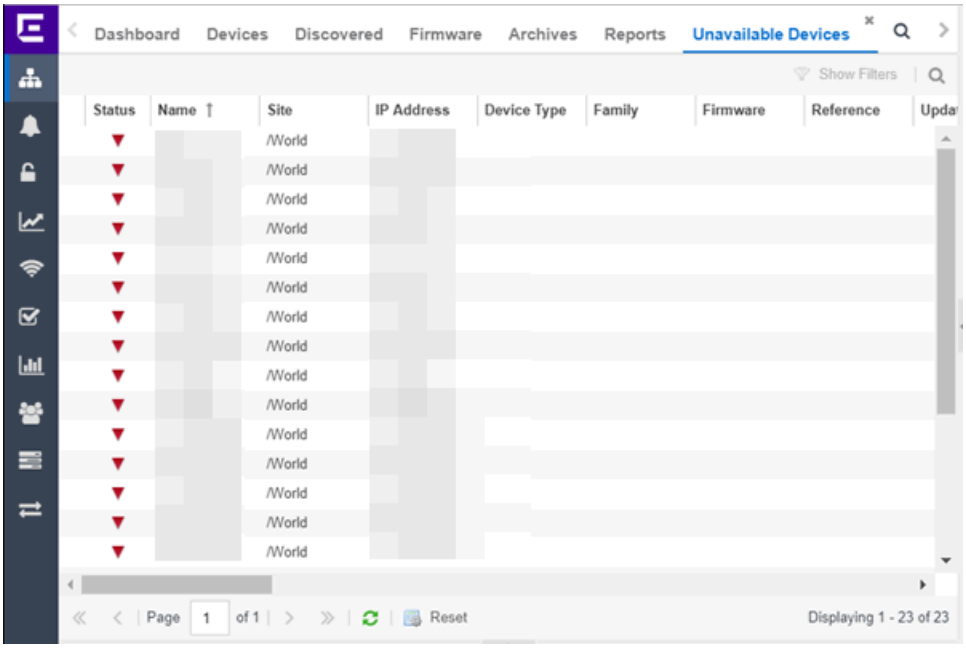


Related Information

- Impact Analysis Dashboard Overview

Unavailable Devices Report

The Unavailable Devices report provides detailed information for devices with which Extreme Management Center 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 Extreme Management Center is in contact with the device.
- Yellow icon (●) — Indicates Extreme Management Center has issues contacting the device.
- Red icon (●) — Indicates Extreme Management Center 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 (●) — Extreme Management Center can contact the device.

Hover over the status icon to view the number of alarms. Click 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 Extreme Management Center 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 Extreme Management Center administrative access to the device.

Client Profile

This column, hidden by default, indicates the access Profile that gives Extreme Management Center 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 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.

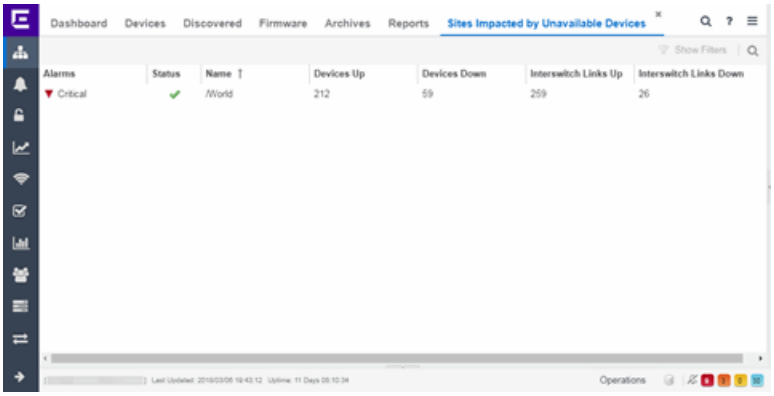
User Data 1-4, Notes
These columns can provide additional information about the device.

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 Extreme Management Center 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 Extreme Management Center 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

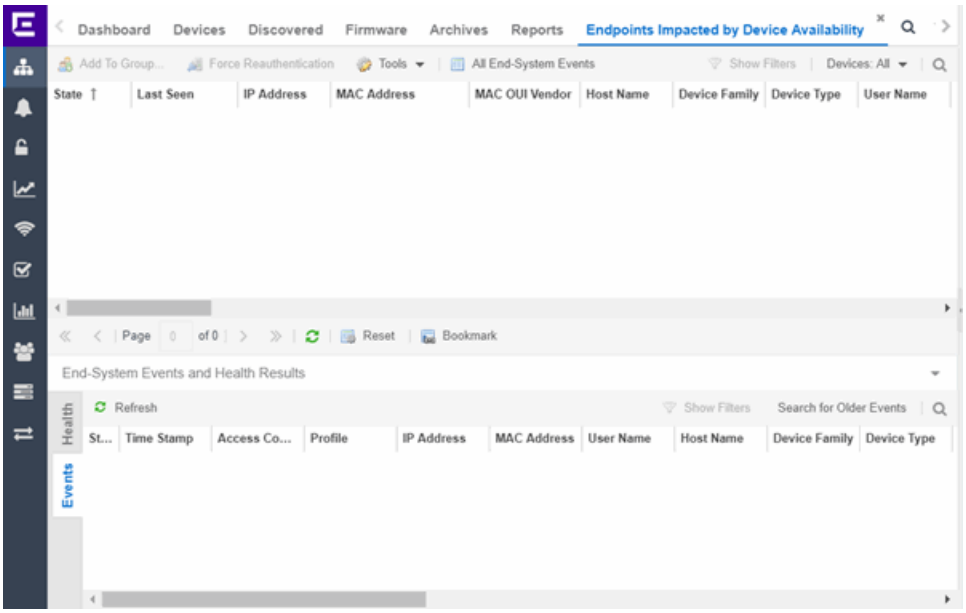
- Impact Analysis Dashboard Overview

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 Extreme Management Center uses to determine if a site is up. The threshold is based on the percentage of devices in a site with which Extreme Management Center 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 NAC 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 Extreme Management Center
  - 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 on the Access ControlOptions 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 NAC appliance 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 NAC appliance.

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 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 NAC 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.

Access Control engine / Source IP
The NAC appliance to which the end-system is connecting.

Profile
The Profile assigned to the end-system in the Extreme Management Center 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

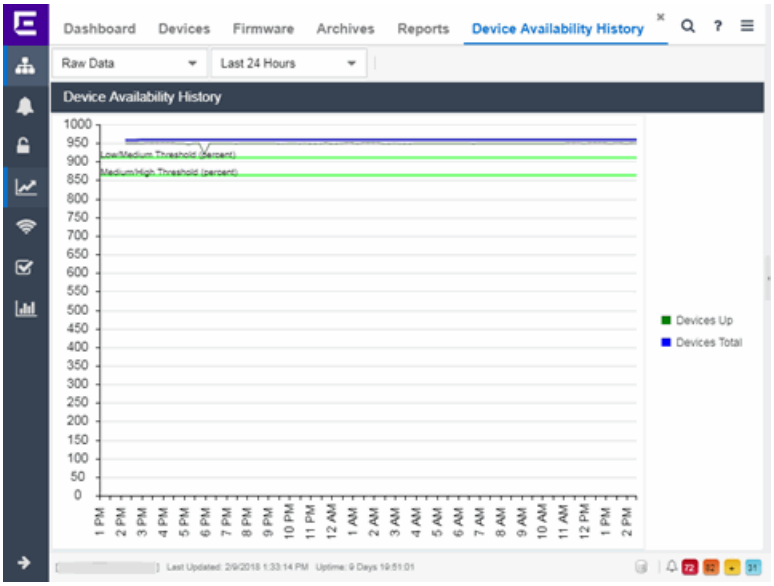
- Impact Analysis Dashboard Overview

Device Availability History Report

The Device Availability History report contains a graph that displays the number of devices with which Extreme Management Center 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 Extreme Management Center analyzes devices from the data drop-down menu. Available options are Raw, Hourly, or Daily data.

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



Related Information

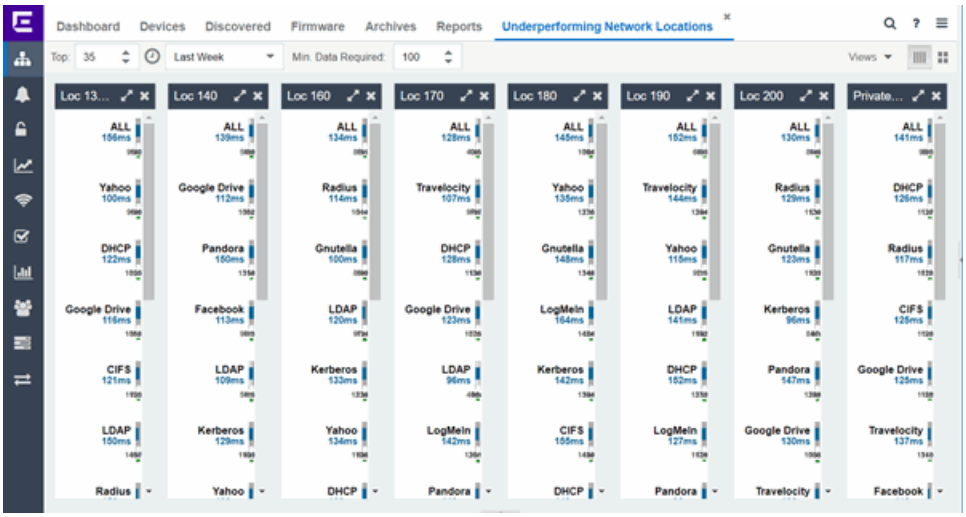
- Impact Analysis Dashboard Overview

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, once for each location. 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 Application Analytics 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 menu. 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: Click (IIII) to display the data in columns or (⊞) to display the data in rows.

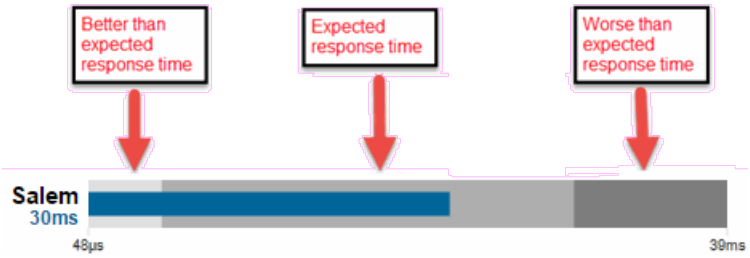
The report contains two types of graphs:

- 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 location (or all locations) during the date range you configure in the Time Span drop-down menu. 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 location as well as the date and time the measurement occurred.

Extreme Management Center 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 Extreme Management Center 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

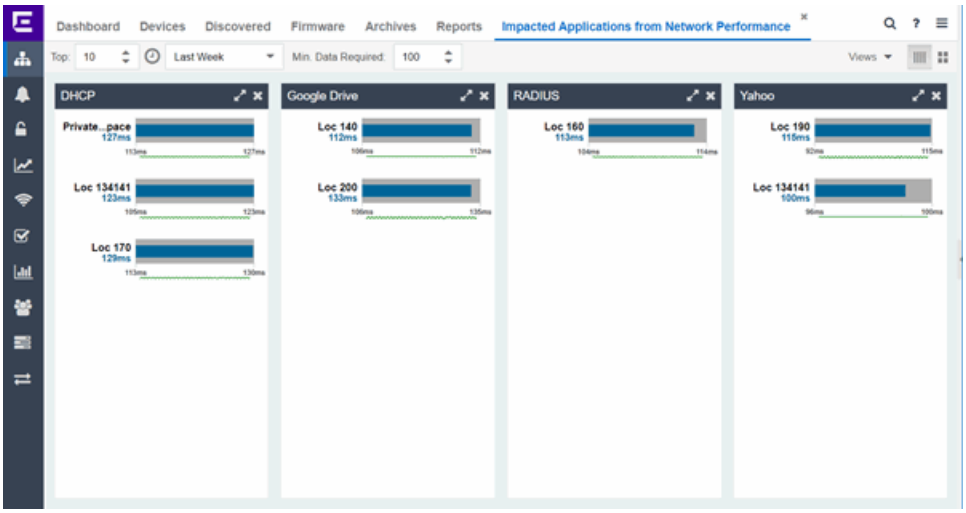
- Impact Analysis Dashboard Overview

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 locations, a tracked application accessed at each location appears twice, once for each location. 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 Application Analytics engines.



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 network response times.

Time Span

Select the span of time for which network response times for locations are displayed from the drop-down menu. 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: Click (IIII) to display the data in columns or (⊞) to display the data in rows.

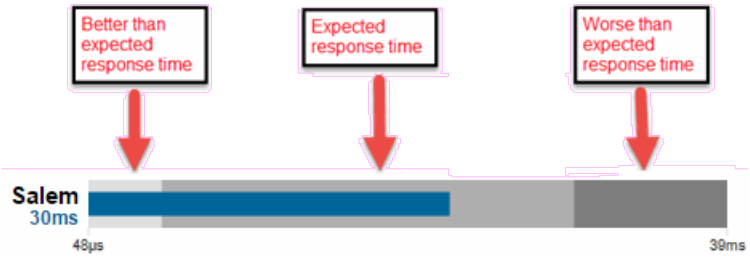
The report contains two graphs:

- 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 location (or all locations) during the date range you configure in the Time Span drop-down menu. 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.

Extreme Management Center 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 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 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 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 Extreme Management Center 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

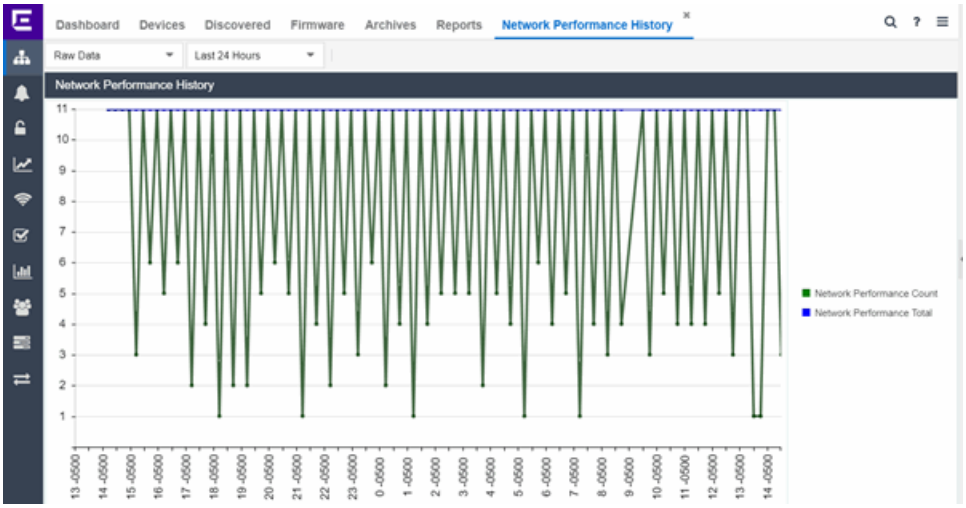
Network Performance History Report

The Network Performance History report contains a graph that displays the number of network locations 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 Application Analytics engines.

Select the increment between which Extreme Management Center analyzes network locations from the data drop-down menu. Available options are Raw, Hourly, or Daily data.

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

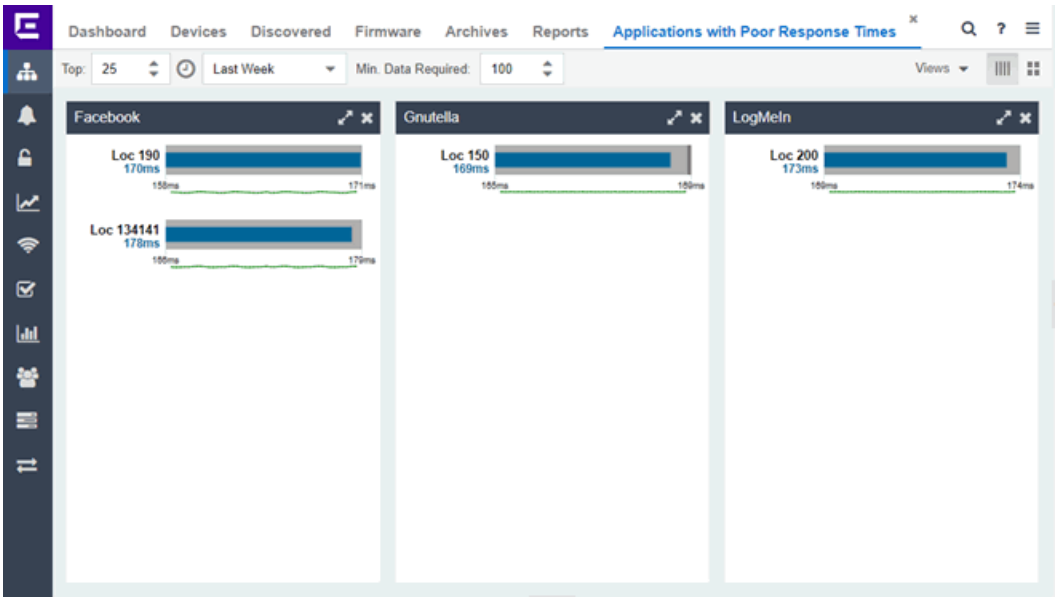


Related Information

- Impact Analysis Dashboard Overview

Slow Applications Report

The Slow Applications report displays the tracked applications and network services at locations with slower-than-expected application response times. In a network with two locations, a tracked application accessed at each location appears twice, once for each location. Only affected applications for each location 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 menu. 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: Click (IIII) to display the data in columns or (▪▪) to display the data in rows.

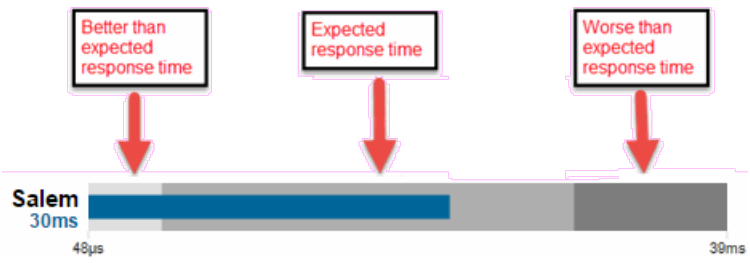
The report contains two types of graphs:

- 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 location (or all locations) during the date range you configure in the Time Span drop-down menu. 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.

Extreme Management Center uses the standard deviation of the values gathered as application response times to determine the expected application response time for an application at a location. 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 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 an application response time appears for that point.

This is the data set from which Extreme Management Center 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.

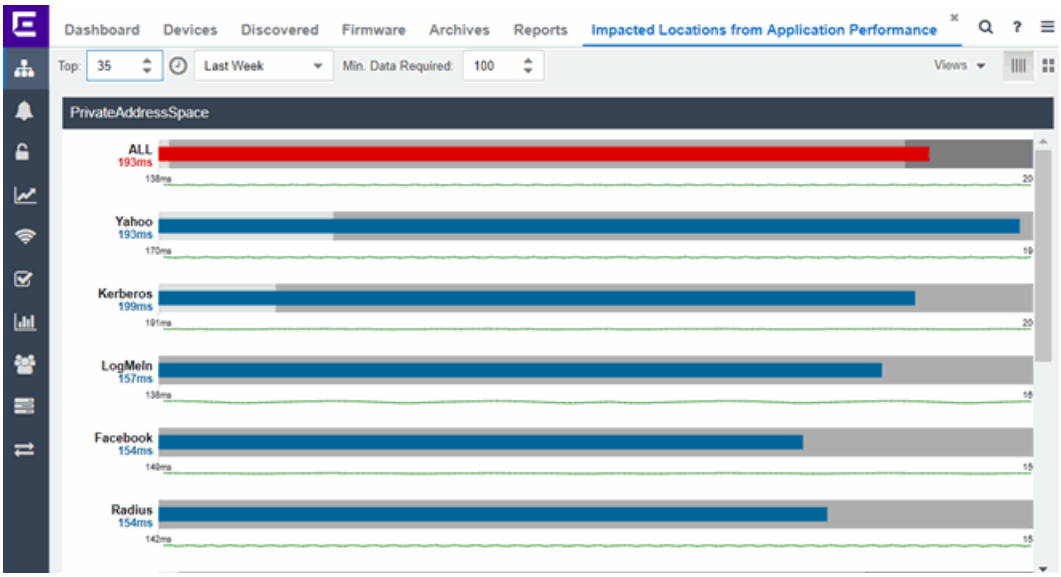
Related Information

- Impact Analysis Dashboard Overview

Locations Impacted by Slow Applications

The Locations Impacted by Slow Applications report provides detailed information about locations that have 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 Application Analytics 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 menu. 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: Click (IIII) to display the data in columns or (⊞) to display the data in rows.

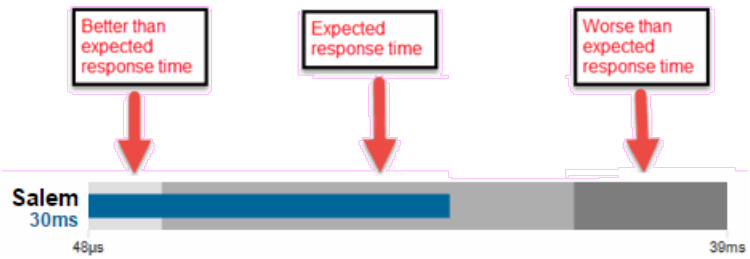
The report contains two types of graphs:

- 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 menu. 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.

Extreme Management Center 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 Extreme Management Center 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

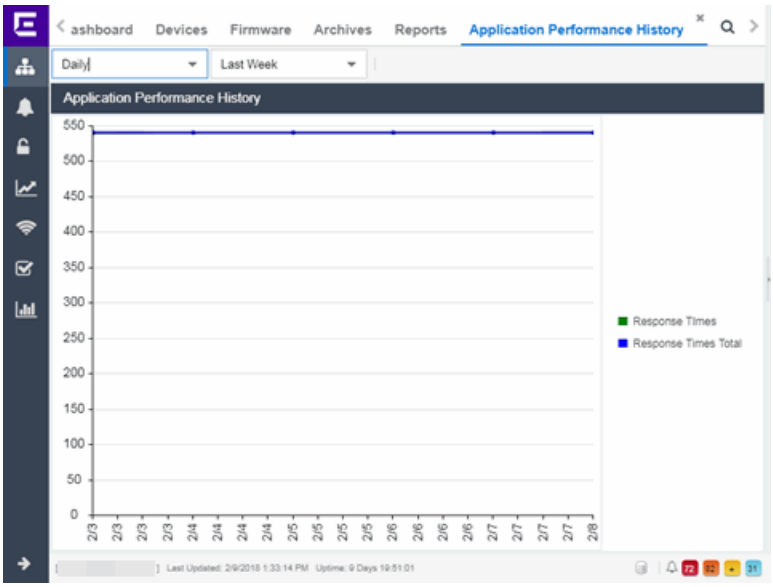
Application Performance History Report

The Application Performance History report contains a graph that provides the number of tracked applications and network services at all of your locations with an application response time within the expected range (green) and the total number of tracked applications and network services at all locations (blue) for the duration you define. If no locations have application response times within the expected range, the chart may not display data (green). In a network with two locations, a tracked application accessed at each location appears twice, once for each location. 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 Application Analytics engines.

Select the increment between which Extreme Management Center analyzes applications from the data drop-down menu. Available options are Raw, Hourly, or Daily data.

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



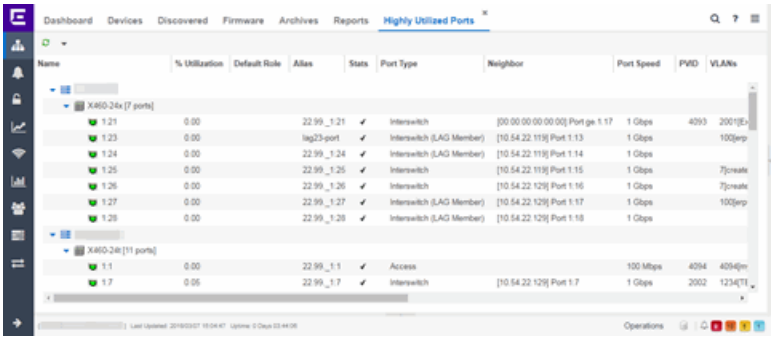
Related Information

- 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 Extreme Management Center uses to determine port utilization.



The following columns are included in the report:

Name
The interface name for the port.

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

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

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

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

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

Neighbor
The port to which the port is connected.

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

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

VLANs
The VLANs to which the port is associated.

Description
A description of the port and the device.

Port Type Details
Additional information about the type of port.

Serial Number
The serial number of the device.

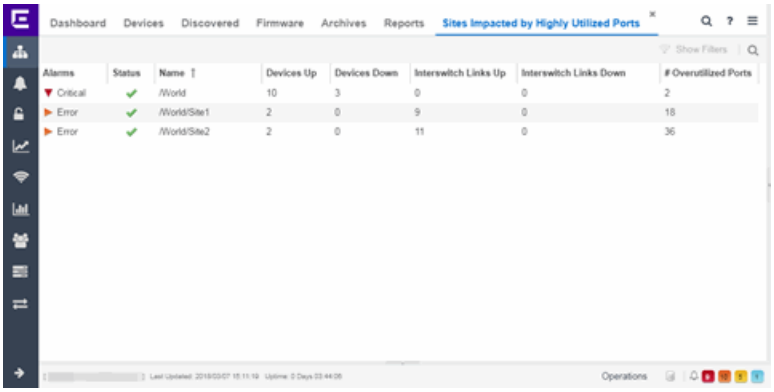
Related Information

- 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 Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center 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

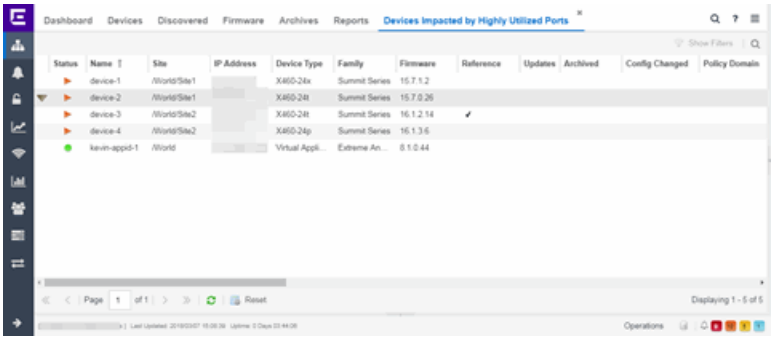
- Impact Analysis Dashboard Overview

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 Extreme Management Center 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 Extreme Management Center is in contact with the device.
- Yellow icon (●) — Indicates Extreme Management Center has issues contacting the device.
- Red icon (●) — Indicates Extreme Management Center 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 (●) — Extreme Management Center can contact the device.

Hover over the status icon to view the number of alarms. Click 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 Extreme Management Center 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 Extreme Management Center administrative access to the device.

Client Profile

This column, hidden by default, indicates the access Profile that gives Extreme Management Center 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 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.

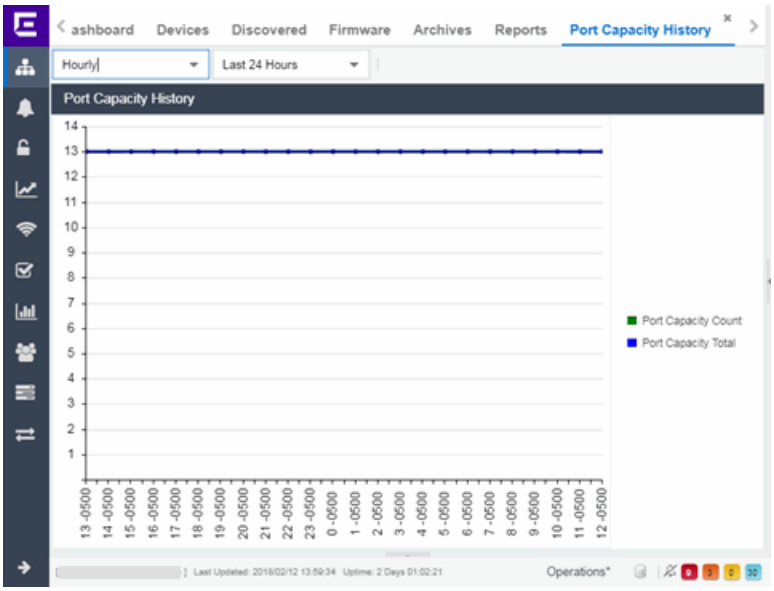
Related Information

- 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 Extreme Management Center uses to determine port utilization.



Select the increment between which Extreme Management Center analyzes ports from the data drop-down menu. Available options are Raw, Hourly, or Daily data.

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

{img placeholder}

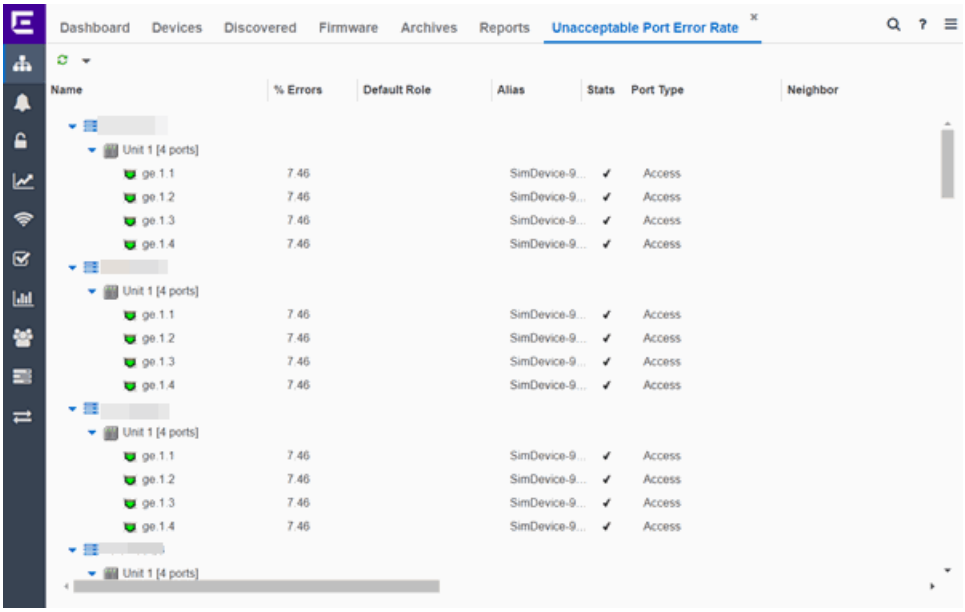
Related Information

- 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 Extreme Management Center uses to determine port error rates.



The following columns are included in the report:

Name

The device or port interface name.

% Errors

The percentage of errors (which is based on the Port Error Packets % statistic) as of the last report, in relation to the total number of ports indicated. The total errors indicated may include measurements of ifInDiscards, ifOutDiscards, IfInErrors,

ifOutErrors, and ifInUnknownProtos. Other errors counters may be included if they are available on the device.

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

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

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

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

Neighbor
The port to which the port is connected.

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

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

VLANs
The VLANs to which the port is associated.

Description
A description of the port and the device.

Port Type Details
Additional information about the type of port.

Serial Number
The serial number of the device.

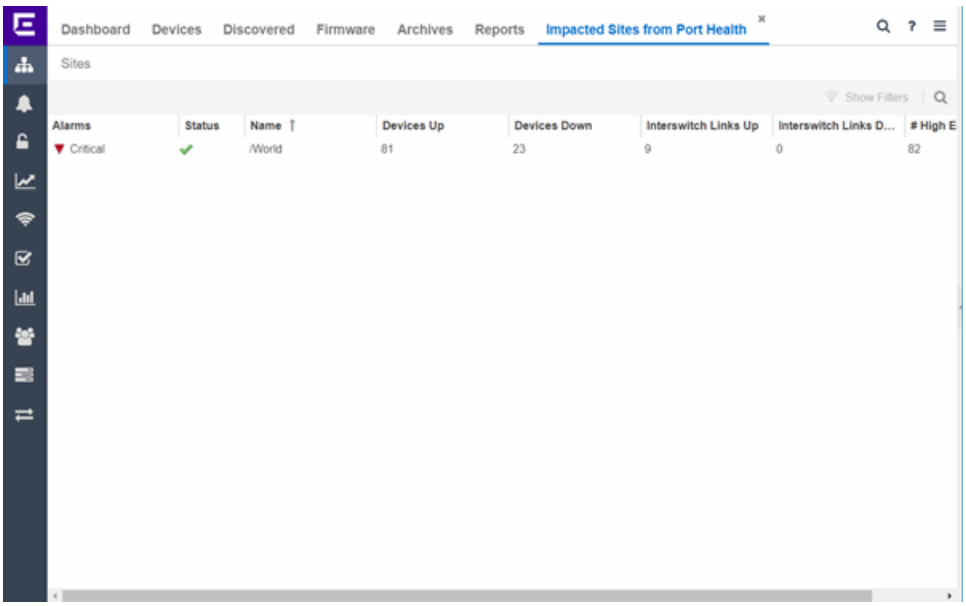
Related Information

- 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 Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center 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.

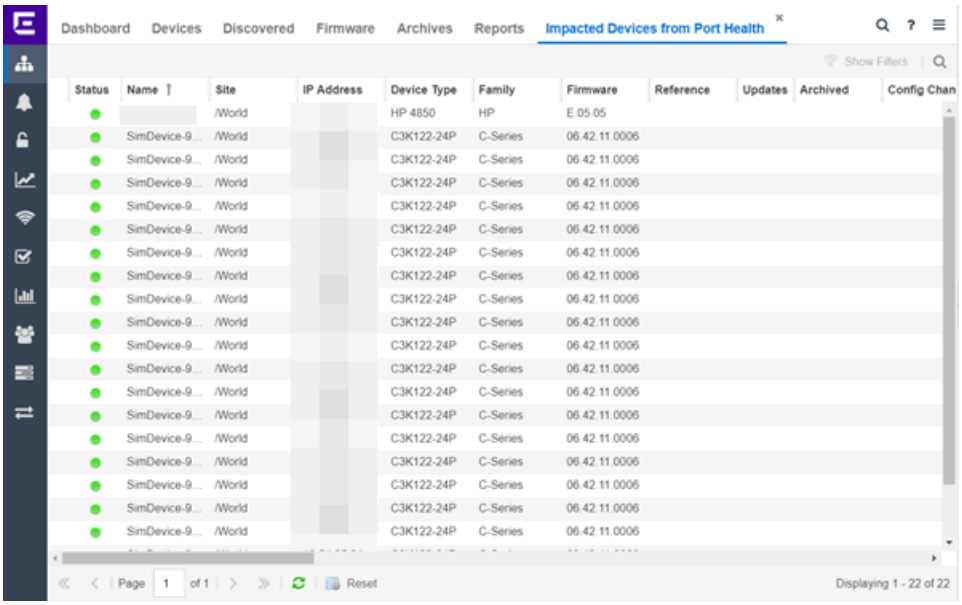
Related Information

- 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 Extreme Management Center 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 Extreme Management Center is in contact with the device.
- Yellow icon (●) — Indicates Extreme Management Center has issues contacting the device.
- Red icon (●) — Indicates Extreme Management Center 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 (●) — Extreme Management Center can contact the device.

Hover over the status icon to view the number of alarms. Click 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 Extreme Management Center 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 Extreme Management Center administrative access to the device.

Client Profile

This column, hidden by default, indicates the access Profile that gives Extreme Management Center 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 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

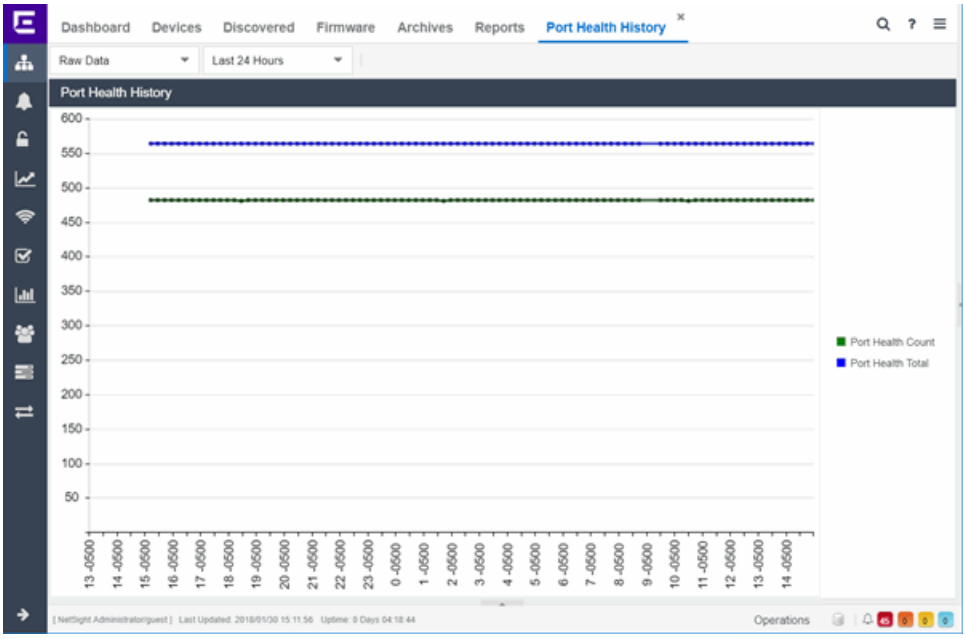
Port Health History Report

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 Extreme Management Center uses to determine port error rates.

Select the increment between which Extreme Management Center analyzes ports from the data drop-down menu. Available options are **Raw**, **Hourly**, or **Daily** data.

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

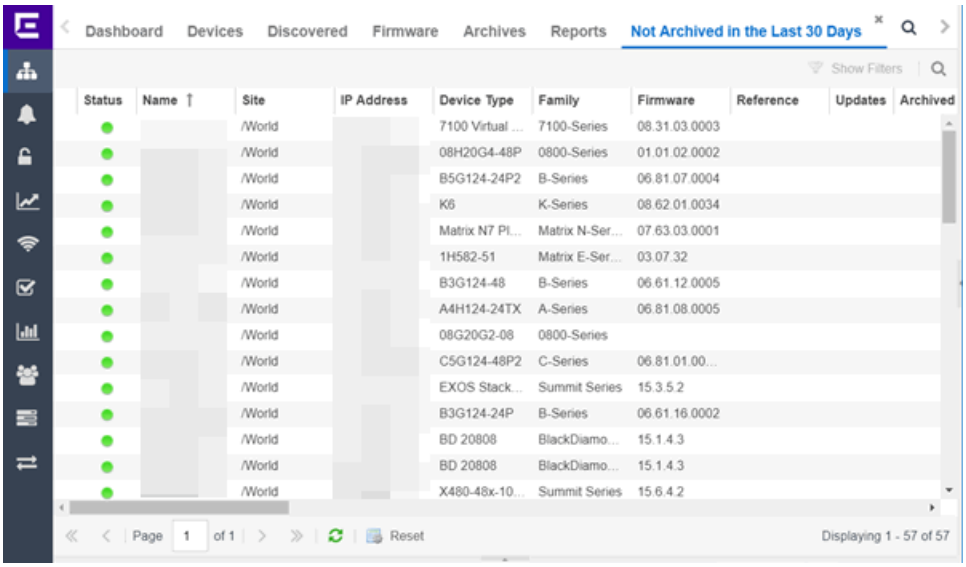


Related Information

- 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 Extreme Management Center archive by right-clicking a device and selecting Configuration/Firmware > 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 Extreme Management Center is in contact with the device.
- Yellow icon (●) — Indicates Extreme Management Center has issues contacting the device.
- Red icon (●) — Indicates Extreme Management Center 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 (●) — Extreme Management Center can contact the device.

Hover over the status icon to view the number of alarms. Click 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 Extreme Management Center 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 Extreme Management Center administrative access to the device.

Client Profile
This column, hidden by default, indicates the access Profile that gives Extreme Management Center 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 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.

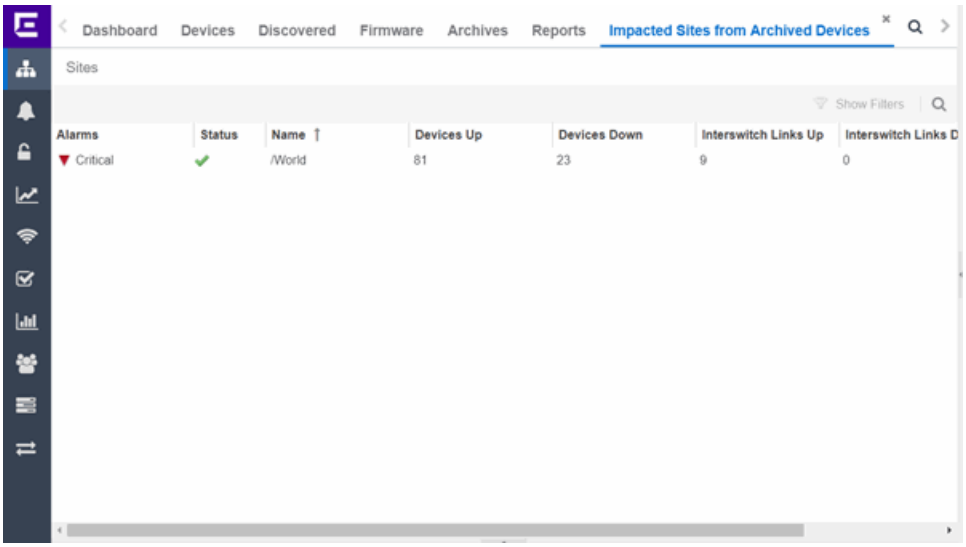
Asset Tag
A unique asset number assigned to the module or component for inventory tracking purposes.

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 Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center analyzes device archives from the data drop-down menu. Available options are **Raw**, **Hourly**, or **Daily** data.

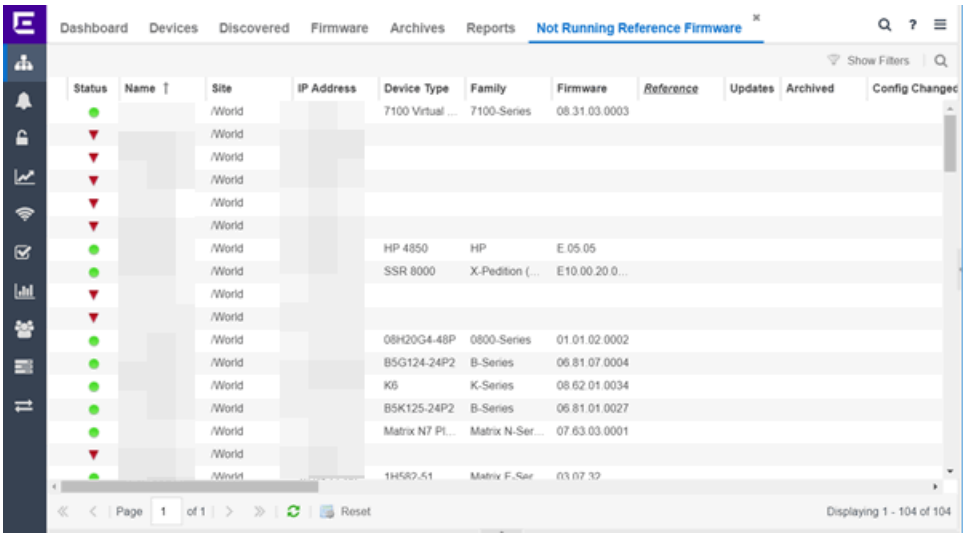
Select the time span for which the report displays from the time span drop-down menu. Available options are **Last 24 Hours**, **Yesterday**, **Last 3 Days**, **Last Week**, **Last 2 Weeks**, **Last Month**.

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 Extreme Management Center is in contact with the device.
- Yellow icon (●) — Indicates Extreme Management Center has issues contacting the device.
- Red icon (●) — Indicates Extreme Management Center 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 (●) — Extreme Management Center can contact the device.

Hover over the status icon to view the number of alarms. Click 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 Extreme Management Center 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 Extreme Management Center administrative access to the device.

Client Profile

This column, hidden by default, indicates the access Profile that gives Extreme Management Center 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 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

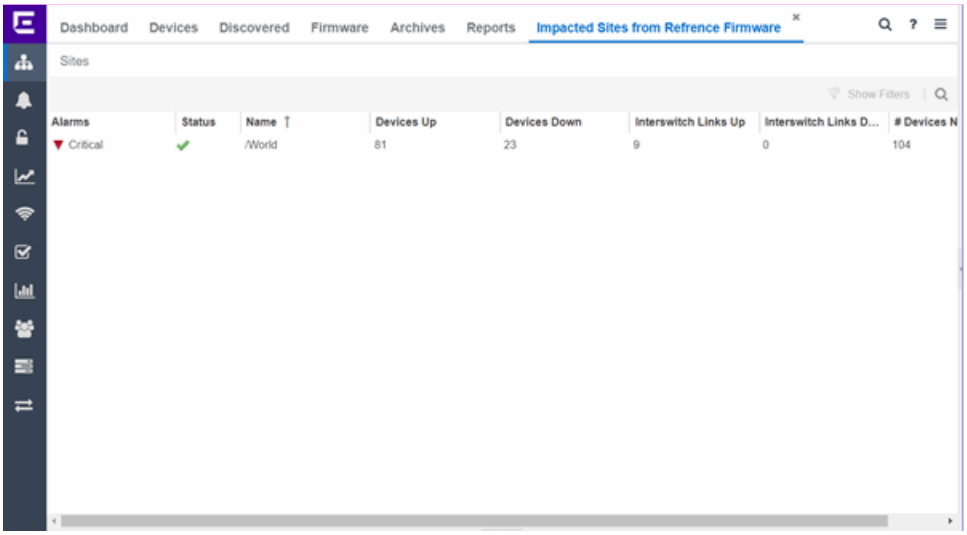
A unique asset number assigned to the module or component for inventory tracking purposes.

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 Extreme Management Center 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 Extreme Management Center 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

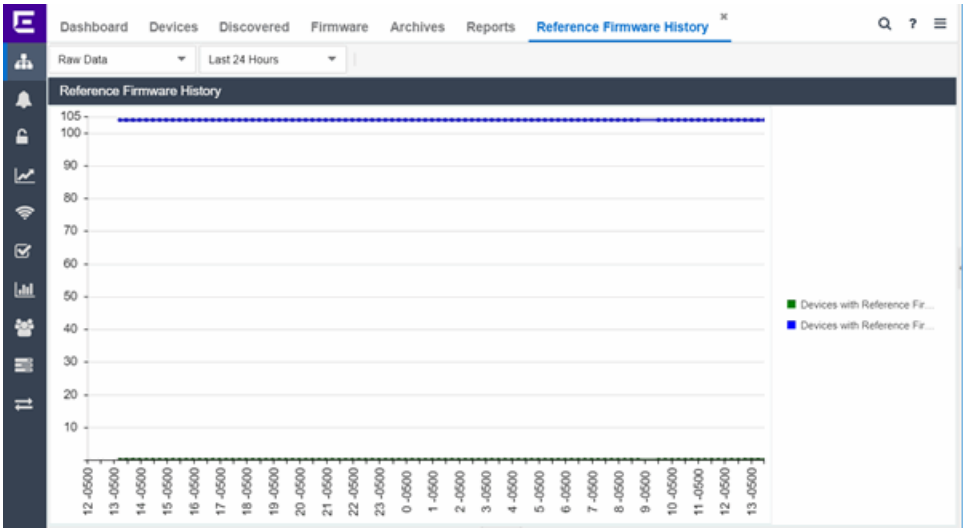
Reference Firmware History Report

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 Extreme Management Center analyzes devices from the data drop-down menu. Available options are **Raw**, **Hourly**, or **Daily** data.

Select the time span for which the report displays from the time span drop-down menu. 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:

- Add Device
- Configure Device
- Execute CLI Commands
- Delete Device

- Set Device Profile
- Create Device Group
- Add Devices to a Device Group
- Backup, Restore, and Compare Device Configurations
- View Port Tree
- View Interface Summary
- View FlexViews
- View User Sessions
- Authentication Configuration
- Launch WebView
- View Network Details
- Collect Device Statistics
- Upgrade Firmware
- Contact Device Using Group's Profile
- Register Trap Receiver
- Unregister Trap Receiver
- Register SysLog Receiver
- Unregister SysLog Receiver
- View Device Details
- Create and Edit Maps
- Add Devices to Maps
- View and Set Policy
- Manage Device Serial Numbers
- Run Tasks on Devices, Ports, and Groups
- Working in the Devices Table
    - Set Device Values
    - 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:

1. Click the **Menu** icon (≡) or right-click in the Devices list.
2. Select **Device** > **Add Device**.

   Once the device is added to the Devices list, it can be used in Extreme Management Center.

Configure Device

To configure device information for an existing device:

1. Click the **Menu** icon (≡) or right-click in the Devices list.
2. Select **Device** > **Configure Device**.

   The Configure Device window opens, which allows you to configure the device properties.

Execute CLI Commands

To run commands against multiple devices, use the Execute CLI Commands option:

1. Click the **Menu** icon (≡) or right-click in the Devices list.
2. Select **Device** > **Execute CLI Commands**.

The **Execute CLI Commands** window opens, from which you can enter the commands and execute on the devices you select. Click the **Launch** link at the top of the window in the **Termial 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.

Delete Device

To delete a device or multiple devices from the Devices list:

1. Select the device or devices in the Devices list.
2. Click the **Menu** icon (≡) or right-click in the Devices list.
3. Select **Device** > **Delete Device**.

   A Delete Confirmation window appears.
4. Click **Yes** to remove the device from Extreme Management Center and to remove the device from any maps to which the device is added.
5. Select the **Delete Extreme Management Center Data** checkbox to remove all data associated with the device from Extreme Management Center.

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. Click the **Menu** icon (≡) or right-click in the Devices list.
3. Select **Device** > **Set Device Profile**.

   The Set Profile window appears.
4. Select a profile from the drop-down menu to change the profile for the selected device or devices.
5. Click **OK**.

   A message appears confirming the device profile change.

Create Device Group

Devices can be grouped by type, geographic location, or any other criteria you choose in order to make the list of devices easier to navigate. Device groups are located in the left-hand panel of the **Network** tab in the My Network navigation tree.

To add a new device group:

1. Right-click on My Network in the Groups/Maps left-panel and select **Device Groups** > **Create Device Group**.

   The Add Device Group window appears.
2. Enter a name for the device group.
3. Click **OK**.

   The new device group appears within the My Network navigation tree.

Add Devices 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. Click the **Menu** icon (≡) or right-click in the Devices list.
3. Select **Device** > **Add Devices to Group**.

   The Add Devices to Group window appears, which allows you to select the device group to which the device or devices are added.
4. Click **OK** to add the devices to the group.

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 Extreme Management Center.

View Port Tree

The Port Tree displays interface information for a device.

To open the Port Tree:

1. Open the **Network** tab.
2. Select a device in the Device list.
3. Click the **Menu** icon (≡) or right-click in the Devices list.
4. Select **View** > **Port Tree**.

   The Port Tree opens in a new tab.

5. 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, a blue check indicates that 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.

View Interface Summary

From the Interface Summary, 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. Open the **Network** tab.
2. Select a device in the Device list.
3. Click the **Menu** icon (≡) or right-click in the Devices list.
4. Select **View** > **Interfaces**.

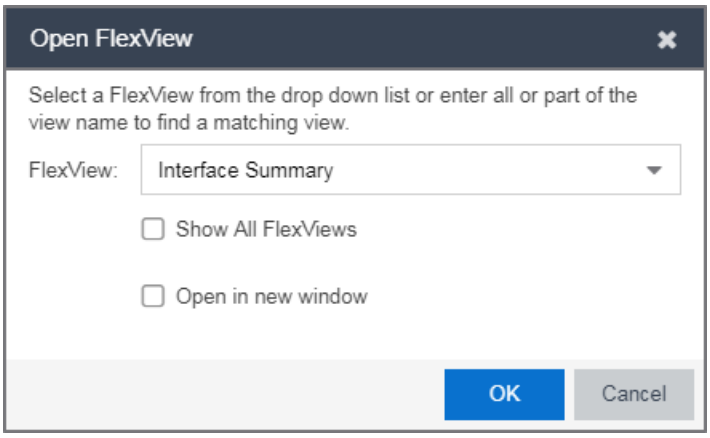
    An Interface Summary FlexView opens for the device in a new tab.

View FlexViews

You can use the **Network** tab to access web-based FlexViews that provide a convenient way for Operations people to view FlexView data without requiring access to Console.

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, click the **Menu** icon (≡) or right-click in the Devices list and select **View** > **FlexView** from the menu. You can also right-click on a device and select **View** > **FlexView** from the menu.



In the Open FlexView window, select a FlexView from the drop-down menu, or enter all or part of the FlexView name to find a matching view. Any FlexView configured in Console is listed for selection, including standard FlexViews or any custom FlexViews that are created. Select Open in new window to open the FlexView in a new browser window, otherwise the FlexView opens in a new tab in the current window. Select **Show All FlexViews** to display all available FlexViews in the **FlexView** drop-down menu. When **Show All FlexViews** is not selected, the **FlexView** drop-down menu 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.

View User Sessions

You can use the **Network** tab 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, select a device in the Device list, click the **Menu** icon (≡) or right-click in the Devices list to select **View** > **User Session** from the menu. You can also right-click on a device and select **View** > **User Session** from the menu. 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.

Authentication Configuration

Opens the Authentication Configuration wizard, which allows you to configure the authentication used on a device or on the individual ports of a device.

Launch 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, click the **Menu** icon (≡) or right-click in the Devices list to select **View** > **Device Details** > **Launch 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 Extreme Access Control engines and wireless controllers.

WebView is only available with certain Extreme Networks and Enterasys devices.

View Network Details

The **Network** tab allows you to view information about all of your network connections.

To open the Network Details:

1. Click the **Menu** icon (≡) or right-click in the Devices list.
2. Select **Network Details**.
3. From this submenu, select **EAPS**, **Link**, **MLAG**, or **VPLS**, which opens the Summary window for EAPS, Linked, MLAG, or VPLS connections, respectively.

   The tabs at the bottom of the window populate with information about the connection you select. All connections managed by Extreme Management Center 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.

Collect Device Statistics

The **Network** 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. Click the **Menu** icon (≡) or right-click in the Devices list.
3. Select one of the following menu options from within the Device submenu:
   - **Collect Device Statistics** — Opens a window that allows you to enable or disable Historical or Monitor statistics collection mode.
     - In **Historical mode**, device and physical port 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 **Monitor mode**, device statistics are saved to a Monitor cache for one hour and then dropped. You can use these statistics for threshold alarms, but not for Extreme Management Center 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 Monitor mode option if you have disabled Monitor Collection in the OneView Collector Advanced Settings in **Administration** > **Options**.)

- **Refresh Devices** — Select this option to perform an SNMP refresh of the selected device's active collection targets. No action is taken on devices with statistics collection disabled.

4. If you are enabling statistics collection on an Extreme Access Control engine, Application Analytics engine, or ExtremeWireless Controller, read through the following notes:
   - **Extreme Access Control Engine** — When collecting statistics on an Extreme Access Control engine, the active engine must be added to Extreme Management Center to collect all appliance statistics. In addition, Monitor mode is not supported on Extreme Access Control engines.
   - **Application Analytics Engine** — When collecting statistics on an Application Analytics engine, the engine must be added to the **Analytics** > **Configuration** > Application Analytics Engines table in order for Extreme Management Center to collect all Application Detection statistics. In addition, Monitor mode is not supported on Application Analytics 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.

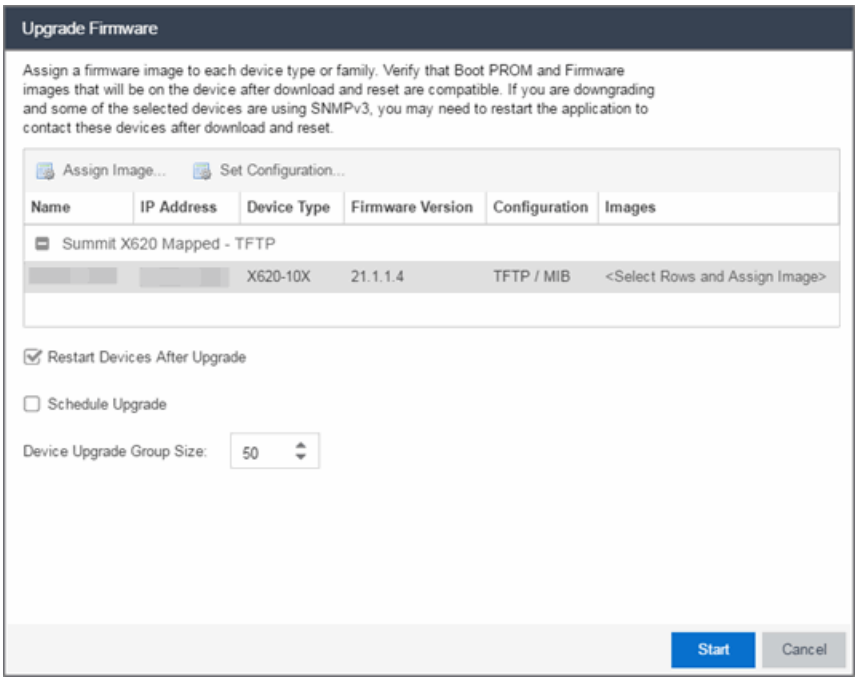
For additional information about collecting statistics, see Enable Report Data Collection.

Open Device Terminal

To open a terminal session to a device, click the **Menu** icon (≡) or right-click in the Devices list and select **Device** > **Open Device Terminal**. The Extreme WebShell window opens a terminal session or the selected device.

Upgrade Firmware

To update devices in the Extreme Management Center database with the latest firmware releases, click the **Menu** icon (≡) or right-click in the Devices list and select **Configuration/Firmware** > **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 once the firmware is upgraded via the Restart Devices window by selecting **Configuration/Firmware** > **Restart Device**.



Contact Device Using Group's Profile

To attempt to contact the selected devices with the currently configured profile, click the **Menu** icon (≡) or right-click in the Devices list and select **Device** > **Contact Device Using Group's Profile** from the menu.

Register Trap Receiver

To receive trap information from the devices on your network, click the **Menu** icon (≡) or right-click in the Devices list and select **Device** > **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, Extreme Management Center creates the trap configuration via SNMP or a script.

Unregister Trap Receiver

To stop receiving trap information from the devices on your network, click the **Menu** icon (≡) or right-click in the Devices list and select **Device** > **Unregister Trap Receiver** from the menu.

Register SysLog Receiver

To receive syslog information from the devices on your network, click the **Menu** icon (≡) or right-click in the Devices list and select **Device** > **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, Extreme Management Center creates the syslog configuration via SNMP or a script.

Unregister SysLog Receiver

To stop receiving syslog information from the devices on your network, click the **Menu** icon (≡) or right-click in the Devices list and select **Device** > **Unregister SysLog Receiver** from the menu.

View Device Details

Select a device in the list, click the **Menu** icon (≡) or right-click in the Devices list to select **View > Device Details** to access various device information including:

- Launch WebView — Access WebView web-based management for certain Extreme Networks and Enterasys devices.
- System — View a physical entity summary.
- Interface — View Ethernet statistics and Ethernet error statistics as well as interface statistics and summary information for the selected device.
- VLAN — View current, port, and static VLAN information.

- Switch — View learned MAC addresses and port spanning tree information.
- Node Alias — View node alias and multi auth, node alias control, and node alias summary information.
- Troubleshooting — View CDP neighbor, CDP port control, and SpanGuard blocking status information.
- DeviceView — Opens a DeviceView for the device in a separate tab.

Create and Edit Maps

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 clicking the **Menu** icon (≡) or right-click in the World map navigation tree and selecting **Maps** > **Create New 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.

Additionally, you can create sites, which allow you to set a default configuration for devices added to your network. For additional information about sites, see Sites.

Add Devices to Maps

To add a device to an existing map:

1. Select one or more devices in the Device list.
2. Click 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. Click 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.

View and Set Policy

You can use the Network tab to access a Policy menu, which lets you 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. Click the Menu icon (≡) or right-click in the Devices list.
3. Open the Policy 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. Click the Menu icon (≡) or right-click in the Devices list.
2. Select View > 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.

Manage Device Serial Numbers

Use the Network tab to register your network device serial number or export the serial numbers to a .csv file.

To register or export your network device serial number:

1. Select one or more devices in the Device list.
2. Click the Menu icon (≡) or right-click in the Devices list.
3. Select Configuration/Firmware > Register/Export Serial Numbers.

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.

Run Tasks on Devices, Ports, and Groups

If you configure tasks to appear on devices, ports, or groups, you can use the Network tab to run a task on a device, port, or group.

To run a task, right-click a device, port, or group in the Device Groups left-hand panel and select a task from the Tasks menu. Additionally, you can select a device in the Devices table, click the Menu icon (≡), and select an option from the Tasks menu.

NOTE: The Tasks menu is not available when right-clicking My Network, All Devices, and All Port Elements in the Device Groups section of the Network tab.

Working in the Devices List

You can manipulate the Devices list data in several ways to customize the view for your own needs:

- Click on the column headings to perform an ascending or descending sort on the column data.

- Hide or display different columns by clicking on a column heading drop-down arrow and selecting the column options from the menu.
- Filter and search the data in each column in the table.

Set Device Values

Set device values for the following columns in the Devices list: Location, Contact, System Name, Nickname, User Data 1-4, and Notes.

Select one or more rows in the table, right-click in the column you want to change and select the Set option off the Device submenu.

NOTE: You cannot set multiple rows for the System Name or Nickname column.

Devices List Column Definitions

- DeviceView — Hover your mouse over the first column and click on the icon to open a DeviceView that provides analysis and troubleshooting information for the selected device, including device summary, FlexView, and Extreme Management Center 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. 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. Hover over the status icon to view the number of alarms. Click 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 or nickname, or IP address. Click on the link to open an Interface Summary FlexView for the device.

- Poll Type — This column, hidden by default, indicates the poll type Extreme Management Center 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 Extreme Management Center administrative access to the device.
- Client Profile — This column, hidden by default, indicates the access Profile that gives Extreme Management Center 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.
- 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. Click the Menu icon (≡) or right-click the icon and select Configuration/Firmware > View Available Releases to open a window listing the current firmware releases available with links to download the firmware.
    - Run 'Check for Updates' to find new firmware releases — A Check for Firmware Updates needs to be performed to get updates for this device. Click the Menu icon (≡) or right-click the device and select Configuration/Firmware > Check for Updates from the menu.

    - 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 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 — An administratively-assigned hostname for the device taken from the *sysName* MIB object. You can set the system name for a device by selecting the device in the table, right-clicking, and selecting Set System Name from the menu
- 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 Use User Defined Nickname option is selected in Console > Options > Console > How to display devices in the device tree. You can set the nickname for a device by selecting the device in the table, right-clicking in the Nickname column, and selecting Device > Set Nickname from the menu.
- Description — A description of the device.
- User Data 1-4, Notes — These columns can provide additional information about the device. You can set the user data and notes for one or more devices by selecting the devices in the table, right-clicking, and selecting Device > Set Selected User Data/Notes from the menu.

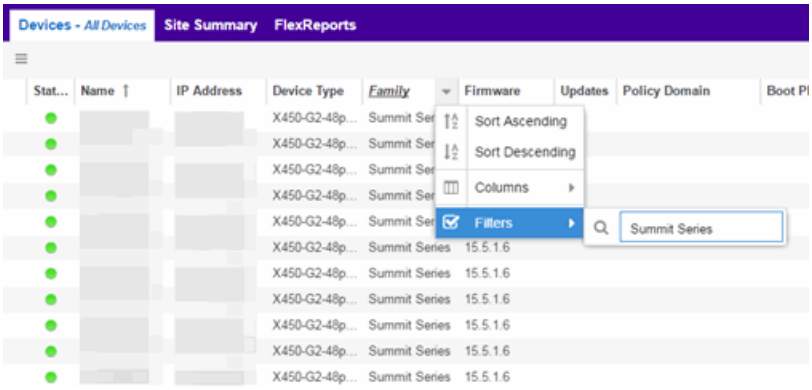
Filtering

The Network tab provides two types of filters that help you narrow the data shown in the table. You can filter multiple columns and data displayed is specific to the type of data presented in the column. When a column has a filter applied, the column heading is displayed in italic with a filter icon . To apply a filter, click on the down arrow in a column heading and use the Filters menu option to specify the filter. The type of filter available depends on the data displayed in the column.

Filter by String

Allows you to filter by an exact match of a full or partial string in the column. For example, you can filter for a specific device family.

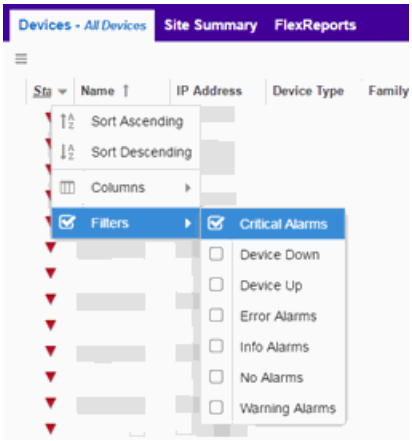
Sample Filter by Family



Filter by List Choices

Allows you to filter according to items selected on a list. For example, you can filter for a specific status.

Sample Filter by Status Level



Buttons, Search Field, and Paging Toolbar

Show Filters

The Show Filters button becomes active when any filters are applied. It opens a window that shows all active filters.

Click the Magnifying Glass icon (🔍) to display the Search field. The Search function allows you to search for full or partial matches on all fields. Enter the full or partial value you are searching for and click the Search button. Matching items are displayed in the table. Press the Reset button to clear the Search results and refresh the table.

The paging toolbar provides four buttons that let you easily page through the table: first, previous, next, and last page. It also displays an indicator of the current and total number of pages. Enter a page number in the Page field and press Enter to quickly move to that page.

Refreshes the page.

Reset

Clears the search field and search results, clears all filters, and refreshes the table.

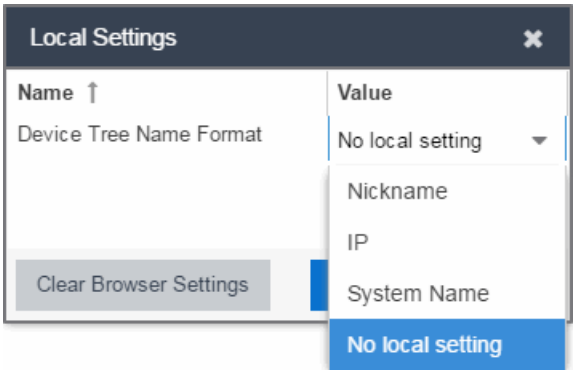
Bookmark

Use the bookmark button to save the search, sort, and filtering options you have currently set. It opens a new window for the current report with a link that can be

bookmarked in your browser. You can then use the bookmark whenever you want the same search, sort, and filtering options.

Local Settings

Clicking 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 menu.



- 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, clicking the Clear Browser Settings button changes the Extreme Management Center 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 Extreme Management Center

Devices Navigation

The Extreme Management Center **Network** > **Devices** tab contains a left-panel drop-down menu 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 menu 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 (e.g. Summit Series).

by IP

Select **by IP** to organize devices based on the IP address of your devices (e.g. 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.

Sites

Select Sites to display all of your sites in the left-panel. A site is a group of devices that share a configuration. When a device is added to a site, Extreme Management Center 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 organize devices into device groups you create.

Wireless Controllers

Select Wireless Controllers to filter the left-panel to display wireless controllers in your network.

Once you select the device, device group, or site in the left-panel, use the right-panel to perform a variety of device operations.

Related Information

For information on related topics:

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

DeviceView

DeviceView is an Extreme Management Center component that provides a wide range of analysis and troubleshooting information for your network wired and wireless devices, including a device summary, FlexViews, and Extreme Management Center reports.

The primary launch point for DeviceView is from the Network tab. DeviceView can also be launched from other locations in Extreme Management Center and Console.

This Help topic provides the following DeviceView information:

Requirements

Access Requirements

Access to DeviceView reports is determined by the user's membership in an Extreme Management Center authorization group and the group's assigned capabilities. The following list shows the capabilities required for full access to all the DeviceView 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

DeviceView 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 Extreme Management Center User Guide.

DeviceView Reports

The DeviceView is comprised of a left-panel device summary, and a selection of tabbed panels that display FlexViews and reports based on the device family.

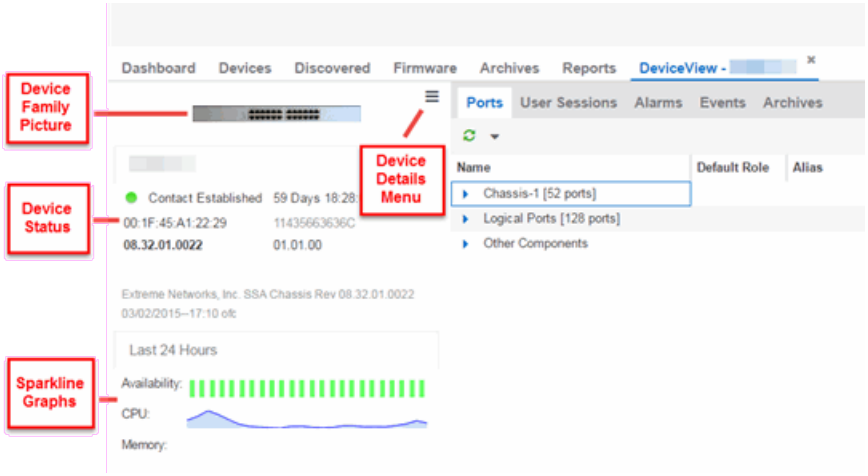
The following table shows the reports available for EOS devices, ExtremeXOS devices, and wireless controllers. The reports displayed in a DeviceView vary according to the selected device.

EOS Devices*	ExtremeXOS devices**	Wireless Controllers
Ports***	Ports***	Ports***
User Sessions	User Sessions	User Sessions
Switch Resources	Device and Module Information	Controller History
Power and Fan Status	Power and Fan Status	Active Access Points
Storage Utilization	Process Utilization	WLAN Services
CPU and Process Utilization	Port Utilization	Active Clients
IP Traffic Summary	VLAN****	Alarms
Alarms	MLAG	Events
Events	VPLS	Device Logs
Device Logs	Alarms	Archives
Archives	Events	
	Device Logs	
	Archives	

*Includes N-Series, S-Series, and K-Series devices.
**Includes BlackDiamond, E4G, and Summit Series devices.
***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.
****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.

Left-Panel Device Summary

The left-panel device summary view (shown below) is displayed in each DeviceView 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 Extreme Management Center User Guide.
- 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 — Click the Menu icon (☰) in the upper right corner to access additional device reports.

Launching DeviceView

DeviceView can be launched from a variety of locations in Extreme Management Center.

Network Tab

The primary launch point for DeviceView is from the Network tab.

1. Open the Network > Devices tab.
2. Hover your mouse over the first column and click on the DeviceView icon .
3. The DeviceView opens as a separate tab.

NOTE: You can also launch a DeviceView from any Device Details menu throughout Extreme Management Center.

Control Tab

Use the following steps to launch DeviceView from the Control tab.

1. Open the **Control** > Dashboard tab.
2. Click on the System view.
3. In the Engine Information report, click on an engine IP address to open a DeviceView for the engine.

Extreme Management Center Maps

Use the following steps to launch DeviceView from a map.

1. Open Extreme Management Center Maps and click on a map.
2. In the map, right-click on a device icon and select DeviceView.

Search

Use the following steps to launch DeviceView from the **Search** tab.

1. Open Search and search for a device.
2. In the Overview, right-click on the device icon and select DeviceView.

Related Information

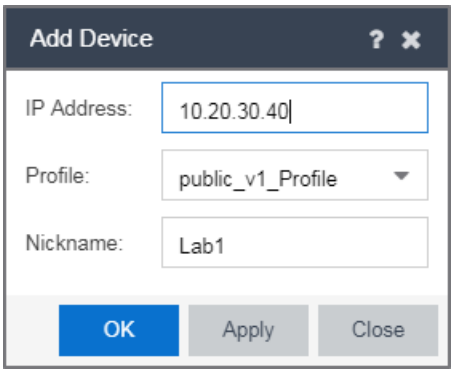
For information on related topics:

- Network Tab

Add Device

Use this window to add a device to the Extreme Management Center database. From this window you can enter the device IP address, the device profile, and the device nickname.

This window is accessible by clicking 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.

OK
Click **OK** to add the device to Extreme Management Center and close the **Add Device** window.

Apply
Click **Apply** to add the device to Extreme Management Center and keep the **Add Device** window open to add additional devices.

Close
Click **Close** to close the **Add Device** window.

Related Information

For information on related windows:

- Discovered

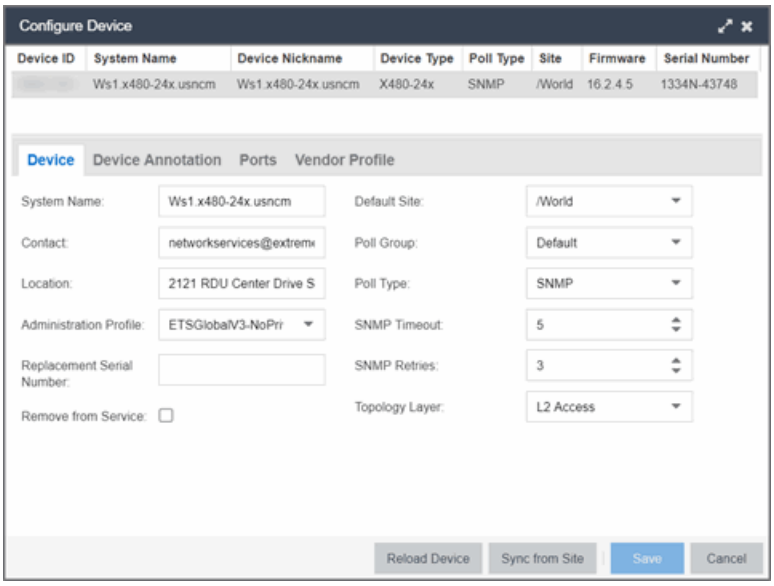
Configure Device

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. Click the **Menu** icon (≡) or right-click on a device.
4. Select **Device** > **Configure Device**.

This window is also accessible by clicking the **Configure Device** button on the Discovered and Site tabs.



When you first open the window, the **Device** tab opens.

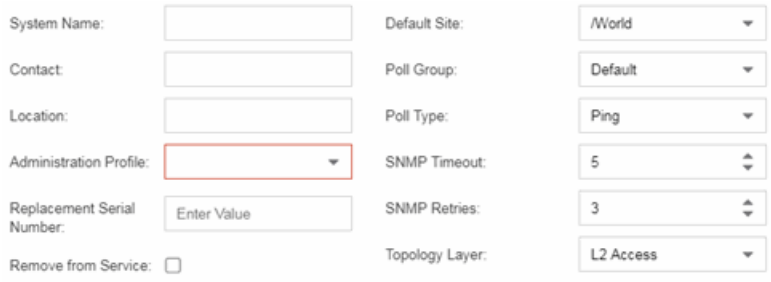
The **Configure Device** window contains the following tabs:

- Device
- Device Annotation
- VLAN Definition
- 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 menu 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, Extreme Management Center restores the most recent archive of the device removed from service.

Remove from Service

Select this checkbox if the device is being removed from the network. When Remove from Service is selected, the device is not polled and alarms are not triggered for the device.

Default Site

Use the drop-down menu to select the map to which the device is associated. For additional information, see the Maps Overview topic.

Poll Group

Use the drop-down menu to select a Poll Group for the discovered devices. Extreme Management Center 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: If Poll Type is Not Polled is specified, the Poll Group is only used if/when the Poll Type is changed to SNMP or Ping.

Poll Type

Use the drop-down menu to select the Poll Type used to discover devices:

- Select Not Polled if you do not want to poll the devices.
- 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 once maintenance on the device is complete.

- Select SNMP to poll the device using SNMP. The SNMP version (SNMPv1 or SNMPv3) is determined by the Profile specified for the IP Range.
- Select 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 Extreme Management Center as a user with Administrative privileges.

SNMP Timeout

The amount of time that Extreme Management Center 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 Retries

The number of attempts Extreme Management Center makes to contact a device after an attempt at contact fails. The value for this setting must be between 1 and 60 tries.

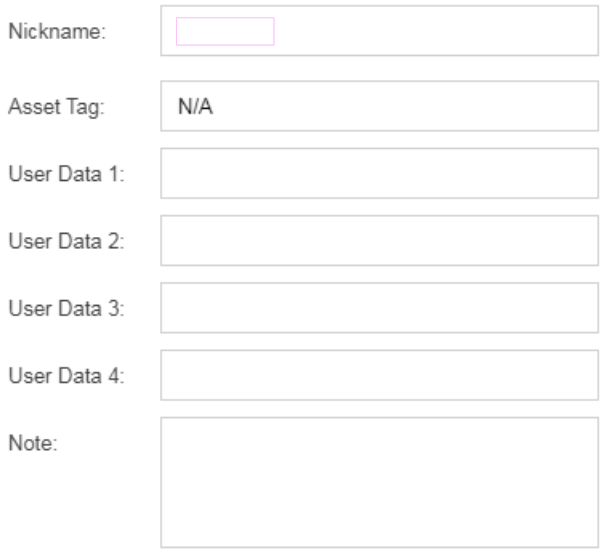
The value entered in this field overrides the default entered in the SNMP Advanced view in the Administration > Options tab.

Topology Layer

The layer and networking attributes for the device.

Device Annotation

The Device Annotation tab 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 Extreme Management Center options menu in the 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.

VLAN Definition

The VLAN Definition tab allows you to configure VLANs on the device. To add a VLAN, click the Add button. You can remove a VLAN by clicking the Delete button.

Name

Displays the name of the VLAN.

VID

Indicates the VLAN ID for the VLAN. A unique number between 1 and 4094 that identifies a particular VLAN. VID 1 is reserved for the Default VLAN.

Dynamic Egress

Indicates if the associated dynamic egress setting for the VLAN (Enable or Disable) is written to the device(s) when you enforce.

Protocol Filter

Indicates the VLAN uses an X-Pedition Protocol Filter.

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.

Ports

The Ports tab allows you to enter information about the ports on a device. Click the Add button to add a new port to the list. Click the Delete button to remove a device from the list.

Name ↑	Alias	Enabled	Speed	Duplex	Configuration	PVID	Policy	Tagged
tg.1.1		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
ge.1.1	Uplink to Core Router	✓	1 Gbps	Full	Interswitch	Default VLAN [1]	None	180,200-2...
tg.1.2		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
ge.1.2		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
tg.1.3		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
ge.1.3	R6C3G-LW-201-21	✓	1 Gbps	Full	Access	RH_Sw_Mgmt_201_...	None	180,200,2...
tg.1.4		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
ge.1.4	R6C3G-SHARED-201-20	✓	1 Gbps	Full	Interswitch	RH_Sw_Mgmt_201_...	None	180,200-208
ge.1.5	R6N1-RH-201-2	✓	1 Gbps	Full	Access	RH_Sw_Mgmt_201_...	None	180,200-208
ge.1.6	R6C3G-201.101	✓	1 Gbps	Full	Interswitch	RH_Sw_Mgmt_201_...	None	180,200-208
ge.1.7		✓	1 Gbps	Full	Access	RH_Sw_Mgmt_201_...	None	180,200-208

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.

Configuration

Use the drop-down menu 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 are configurable.
- Management — Select this option if the port is used to manage network traffic with Extreme Management Center.
- 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).

Authentication

Use the drop-down menu 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.

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 Extreme Management Center 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 checkbox to enable ZTP+ devices being discovered to broadcast MVRP (Multiple VLAN Registration Protocol) information. Select the appropriate logging level from the drop-down menu.

Update

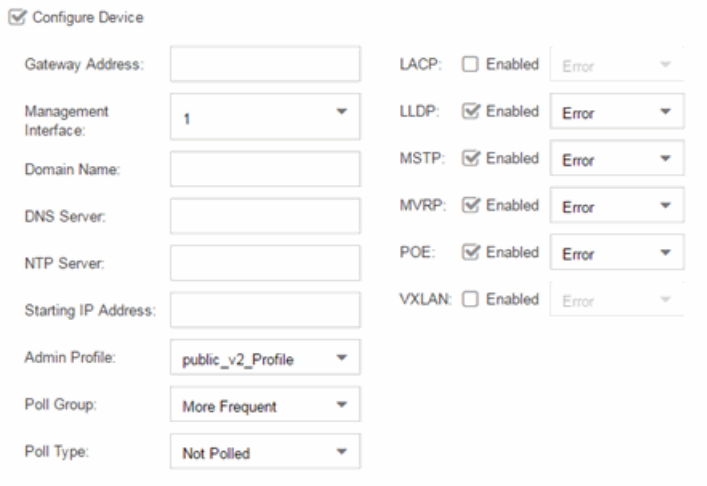
Click Update to save any changes made to the device configuration.

Cancel

Click Cancel to close the window and discard any changes.

ZTP+ Device Settings

The ZTP+ Device Settings tab contains basic information about the device being discovered.



Configure Device

Select this checkbox to enable ZTP+ (Zero Touch Provisioning Plus) functionality device being discovered. ZTP+ allows you to quickly add a supported device to your network with minimal configuration.

Gateway Address

Enter the Gateway Address for the ZTP+ devices being discovered.

Management Interface

Select the interface the ExtremeXOS device uses for Management and assigns the device IP to that interface.

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 being discovered

NTP Server

The NTP Server field allows you to set the NTP server address on the ZTP+ devices being discovered.

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 being discovered.

Admin Profile

Use the drop-down menu to select the access Profile that gives Extreme Management Center administrative access to the ZTP+ devices you wish to discover. 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, saving the device overwrites the profile currently being used in the database.

Poll Group

Use the drop-down menu to select a Poll Group for the discovered ZTP+ devices. Extreme Management Center 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 will overwrite 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 menu to select the Poll Type used to discover devices. Valid options are SNMP, Ping, and Not Polled. When SNMP is specified, the SNMP version (SNMPv1 or SNMPv3) is determined by the Profile specified for the IP range. If the Profile is set to Ping Only, the Poll Type must be set to Ping. If you discover an existing device using a different poll type than the device is already using in the database, saving the device overwrites the Poll Type currently being used in the database.

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 Console as a user with Administrative privileges.

LACP

Select the checkbox to enable ZTP+ devices being discovered to broadcast LACP (Link Aggregation Control Protocol) information. Select the appropriate logging level from the drop-down menu.

LLDP

Select the checkbox to enable ZTP+ devices being discovered to broadcast LLDP (Link Layer Discovery Protocol) information. Select the appropriate logging level from the drop-down menu.

MSTP

Select the checkbox to enable ZTP+ devices being discovered to broadcast MSTP (Multiple Spanning Tree Protocol) information. Select the appropriate logging level from the drop-down menu.

MVRP

Select the checkbox to enable ZTP+ devices being discovered to broadcast MVRP (Multiple VLAN Registration Protocol) information. Select the appropriate logging level from the drop-down menu.

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.

Flow Sources

The Flow Sources tab allows you to configure devices to act as flow sources for an Application Analytics 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 Application Analytics engine or used to create the GRE tunnel.

Source Ports
Displays the ports on which flow collection is enabled.

NOTE: Policy mirrors the first 15 packets of each flow received on the Source Ports to the Application Analytics engine.

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 Application Analytics 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
Click Add to open a window from which you can select a device in Extreme Management Center to add as a flow source.

Remove
Select a flow source device in the table and click Remove to remove the device as a flow source.

Edit

Click **Edit** to open a window from which you can change the configuration of a flow source device.

Test

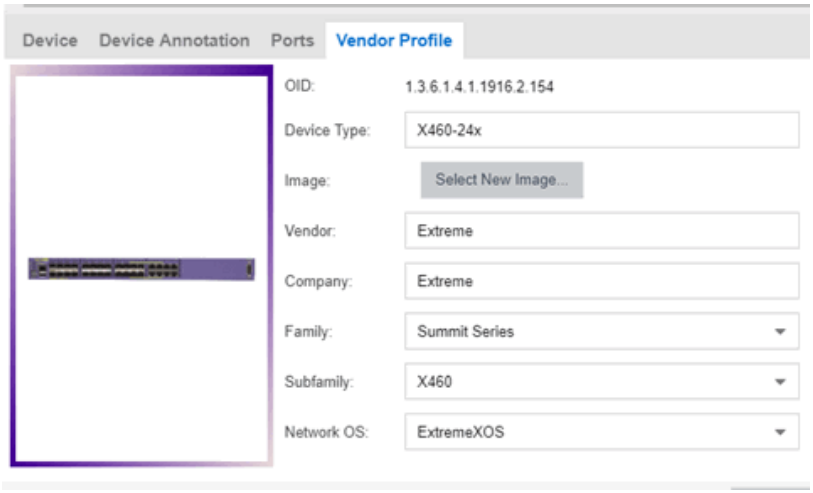
Click **Test** to verify the GRE tunnel end-points can communicate.

NOTE: **Test** is only available if **Tunnel** is enabled.

Vendor Profile

The **Vendor Profile** tab allows you to edit configurations for devices. The configuration you select allows you to enter information about the device to help identify it in Extreme Management Center.

NOTE: To remove all user-defined Vendor Profile configurations and restore the default system configurations, click the **Restore to Defaults** button on the **Administration** > **Diagnostics** > **System** > **Vendor Profile Cache** tab.



OID

Displays the Object Identifier for the device.

Device Type

Displays the specific type of device.

NOTE: When **Device Type** is blank:

- The tab is named **New Vendor Profile**.
- If a device's Vendor is recognized, but Extreme Management Center does not have a profile for the device's unique **OID**, the **Device Type**, **Family** and **Subfamily** values are empty, but Extreme Management Center supplies the **Vendor** and **Company** values.
- 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 DeviceView and Maps. Click 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 Extreme Management Center.

Subfamily
Displays a smaller grouping to which the device belongs, if applicable.

Network OS
The operating system that the device type uses.

Buttons

Reload Device
Click to read configuration information from the device to populate Extreme Management Center. **Reload Device** reads the configuration (e.g. VLAN Definition, Ports, Port VLANs) from the device and reloads it in Extreme Management Center.

NOTE: Clicking **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
Click 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
Click to copy the default configurations from the site to Extreme Management Center's representation of the devices. The Enforce Preview button displays, which you can use to decide whether to save the settings to the device.

Save
Click to save any changes you make to a device in Extreme Management Center.

Cancel
Click to discard any unsaved changes and close the window.

Related Information

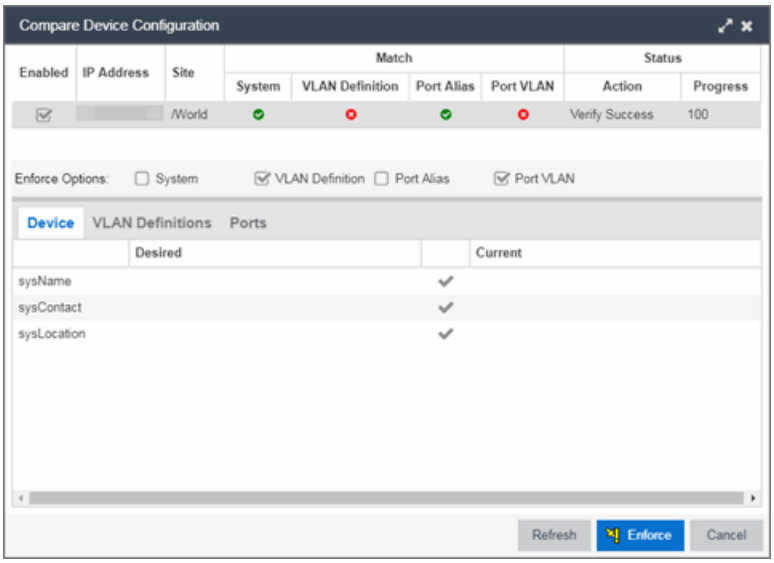
For information on related windows:

- 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 click Enforce Preview in the Configure Device window.



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 bottom of the window.

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 (✖). The System column indicates the whether the information on the **Device** tab matches, the VLAN Definition column indicates whether the information on the **VLAN Definitions** tab matches, and the Port Alias and Port VLAN columns indicate whether the information on the **Ports** tab matches.

The Enforce Options section of the window allows you to select the changes you want to make on the device. Select **System** to push changes you make on the **Device** tab to the device, select **VLAN Definition** to push changes you make on the **VLAN Definitions** tab, select **Port Alias** to push changes you make to the top table on the Ports tab, and select **Port VLAN** to push changes you make to the Port VLAN Details table on the **Ports** tab.

NOTE: By default, the checkboxes in the Enforce Options section of the window are not selected. To configure Extreme Management Center 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`

In each tab, the configurations are separated into two columns:

- 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.

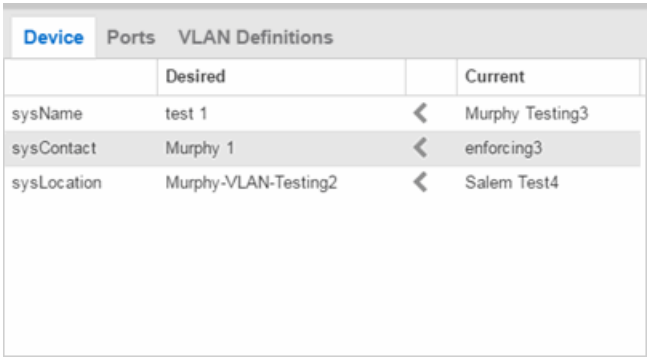
A check mark between the columns (✔) indicates the Current configuration matches the Desired configuration.

A left arrow icon (<) indicates the configurations do not match. Clicking it copies the Current configuration to the Desired configuration so no configuration change is made when enforcing the device.

Click Enforce to save your changes to the device.

Device

The Device tab displays any changes to basic information about the device.



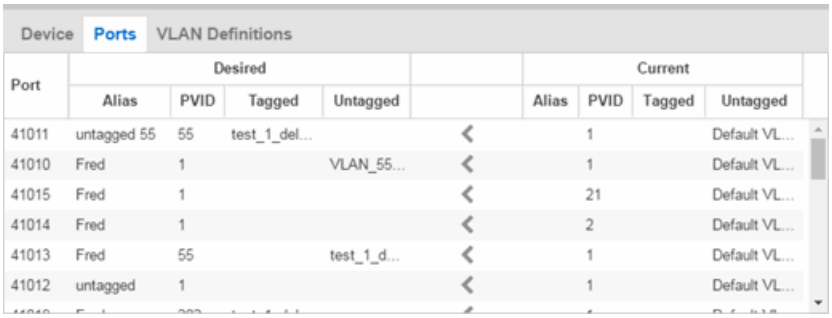
sysName
The name by which the device is known.

sysContact
Allows you to specify contact information for the person maintaining the device.

sysLocation
The physical location of the device.

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

Shows the alias for the port, if one is assigned.

PVID

The port's VLAN assignment. Possible values are 1 through 4094.

Tagged

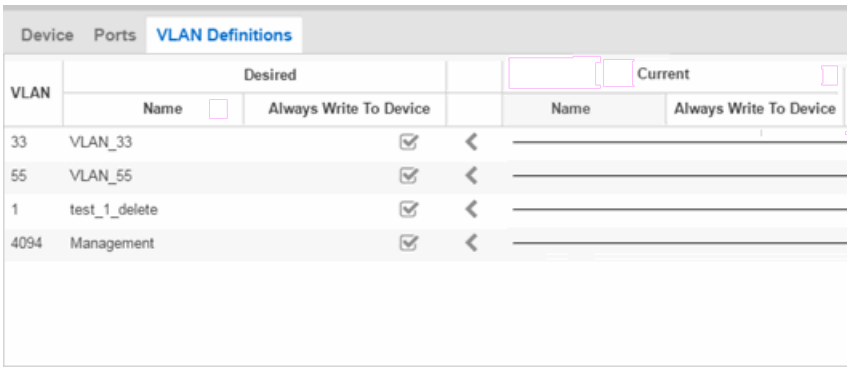
The port is added to the list with the egress state set to Tagged (frames are forwarded as tagged).

Untagged

The port is added to the list with the egress state set to Untagged (frames are forwarded as untagged).

VLAN Definitions

The VLAN Definitions tab displays any changes to the VLANs defined for the device selected at the top of the window.



VLAN
A unique numerical identifier of the VLAN.

Name
The name of the VLAN.

Always Write to Device(s)
Indicates whether or not the VLAN is written to the device(s) when you enforce, or compared to the actual VLANs on the device(s) when you verify.

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 menu.
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 click Save.

Related Information

For information on related topics:

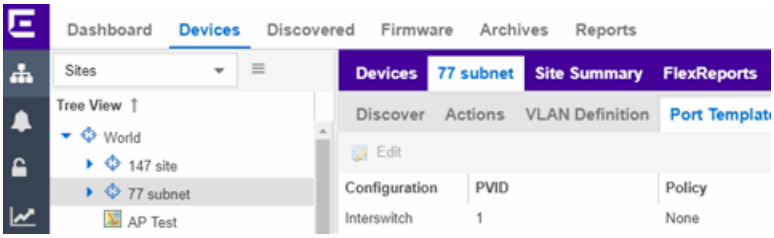
- Sites
- How to Discover Devices in Extreme Management Center
- Devices

Site

Sites allow you to select the default configuration for devices you add to your network via a device discover or by using ZTP+ functionality. The **Sites** tab allows you to configure devices included in the site when they are discovered. It also allows you to discover new devices at the site. The tab is divided into multiple sections, which you can expand by clicking the down arrow (▾) at the right of each section.

NOTE: To save the changes to the devices included in the site, right-click on a device to open the Configure Device window and click **Sync from Site**. Clicking **Save** saves any changes you make in Extreme Management Center.

Access **Network** > Devices and select **Sites** from the left-panel drop-down menu. Select the site from the left-panel. 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** tab contains the following tabs:

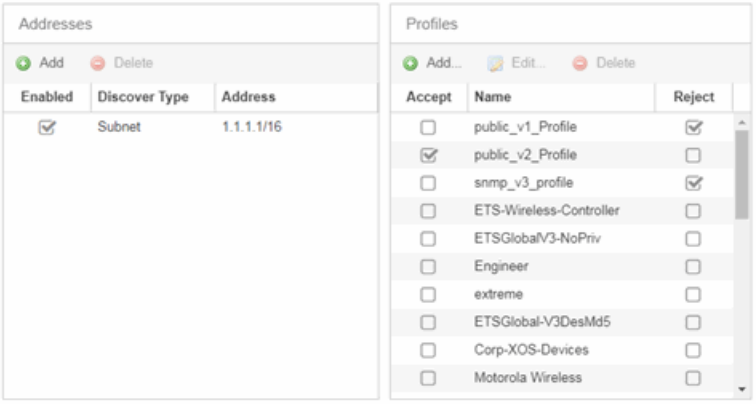
- Discover
- Actions
- VLAN Definition

- Port Templates
- ZTP+ Device Defaults
- Custom Variables
- Buttons

Discover

The Discover tab allows you to enter address information for new devices on your network, which adds them to the Extreme Management Center 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.

NOTE: Extreme Management Center only allows a subnet search of a 16-bit mask or higher when discovering devices.



Addresses

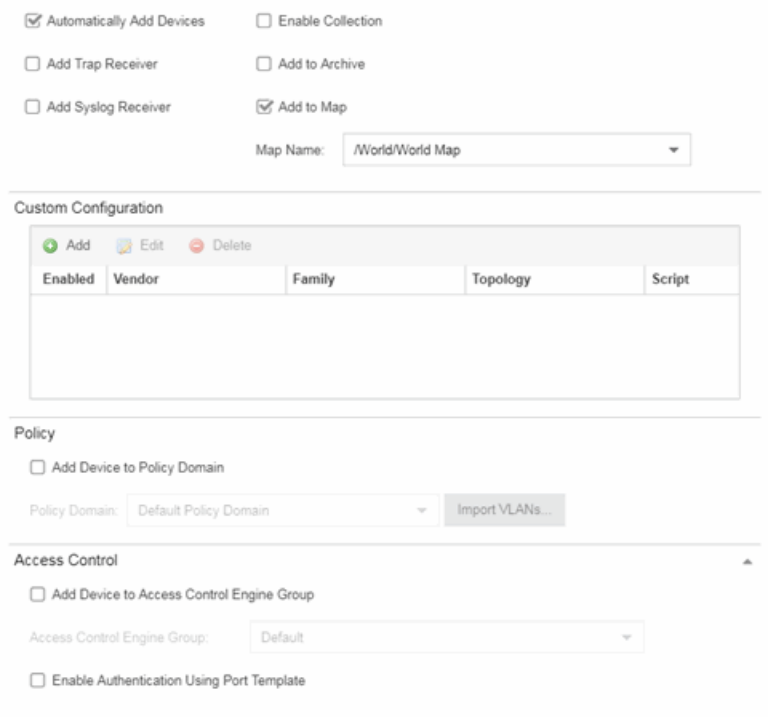
Click the Add button in the Addresses list to allow you to add devices by seed address, subnet, or address range. Selecting Seed Address allows you to perform a discover for CDP, LLDP, or EDP-compliant devices. Click the Discover button at the bottom of the tab to begin the device discover. The results of the Discover process are displayed in the left-panel tree when added to the Extreme Management Center database.

Profiles

Select the access Profiles that gives the Discover tool read access 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 clicking 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 Extreme Management Center to automatically add devices to the database that match the address information you entered in the Discover section of the tab. 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 Extreme Management Center. You can define the trap configuration details on the Options > Trap tab. Depending on the device, Extreme Management Center 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 Extreme Management Center. You can define the syslog configuration details on the Options > Syslog tab. Depending on the device, Extreme Management Center creates the syslog configuration via SNMP or a script.

Enable Collection

Select this checkbox to collect device and physical port statistics on devices being discovered. Extreme Management Center uses the device and physical port statistics in reports.

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 menu and then manually add it via the Maps > Add to Map on the Devices tab.

Custom Configuration

Click the Add button to configure Extreme Management Center to automatically run a task (a script or workflow) when discovering a device in a particular device family.

Policy

Add Device to Policy Domain

Select this checkbox to add the device to a policy domain you create on the Policy tab. Once the checkbox is selected, use the Policy Domain drop-down menu to select the policy domain to which the device is added. Extreme Management Center enforces are done automatically once 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 menu.

Extreme Access Control

Add Device to Extreme Access Control Engine Group

Select this checkbox to add the device to an Extreme Access Control Engine Group you create on the Access Control tab. Once the checkbox is selected, use the Extreme Access Control Engine Group drop-down menu to select the engine group to which the device is added.

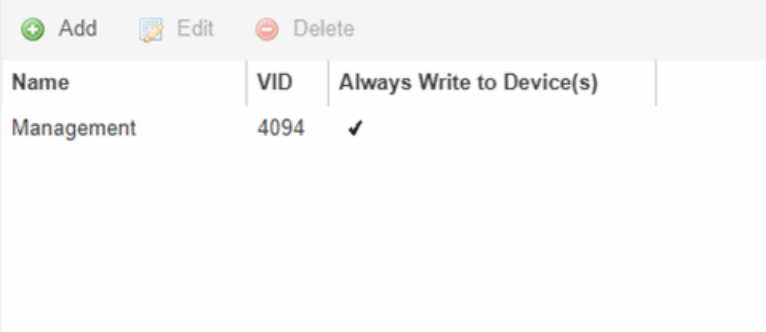
- If the device is an Extreme Access Control engine, it is added as an engine to the engine group.
- If the device is not an engine, it is added as a switch to up to two engines in the engine group. An enforce is run against the engine group if a switch is added.

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.

VLAN Definition

The VLAN Definition tab allows you to configure VLANs on the devices being discovered. To add a new VLAN, click the Add button or edit an existing VLAN by clicking the Edit button. Remove a VLAN by clicking the Delete button.



Name

Displays the name of the VLAN.

VID

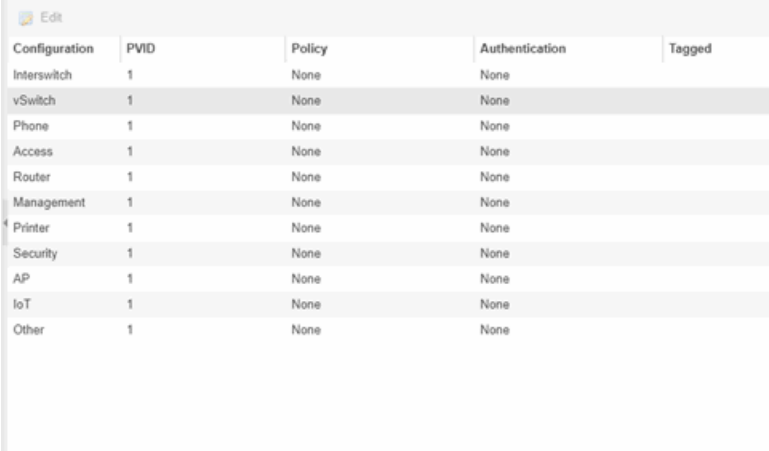
Indicates the VLAN ID for the VLAN. A unique number between 1 and 4094 that identifies a particular VLAN. VID 1 is reserved for the Default VLAN.

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.

Port Templates

The Port Templates tab allows you to configure default port information for those devices discovered in the current site.



Edit

Select a port template and click the Edit button to make changes to the selected port template.

Configuration

Use the drop-down menu 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 are configurable.
- Management — Select this option if the port is used to manage network traffic with Extreme Management Center.
- 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

The port's VLAN ID.

Policy

The policy 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 menu in the Discovered Device Actions section of the tab. Policy assignment to the port is performed after a successful policy domain enforce.

Authentication

Use the drop-down menu 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.

Tagged

Indicates the port's egress state is tagged.

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 Extreme Management Center 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

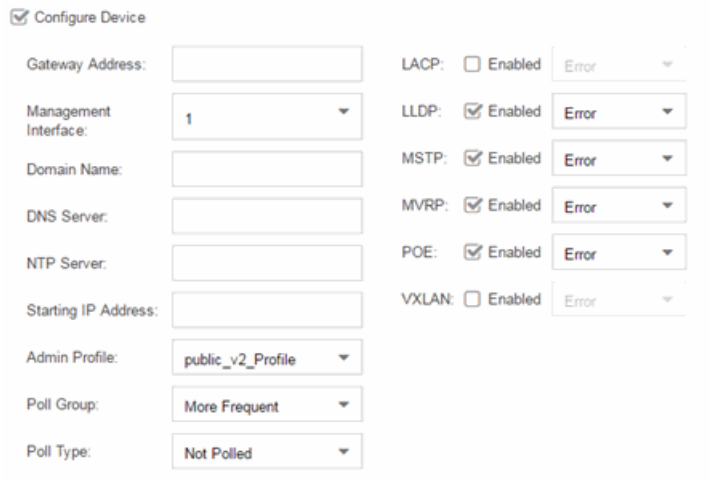
Indicates that the Multiple VLAN Registration Protocol (MVRP) has been enabled for the port. If MVRP has been enabled globally, interswitch ports are automatically enabled and access ports default to disabled. Select the checkbox to enable ZTP+ devices being discovered to broadcast MVRP (Multiple VLAN Registration Protocol) information. Select the appropriate logging level from the drop-down menu.

Collection

Indicates the port's egress state is untagged.

ZTP+ Device Defaults

The **ZTP+ Device Defaults** tab contains basic information about a device with ZTP+ (Zero Touch Provisioning Plus) enabled.



Configure Device

Select this checkbox to enable ZTP+ functionality for a device. ZTP+ allows you to quickly add a supported device to your network with minimal configuration.

Gateway Address

Enter the Gateway Address for the ZTP+ devices associated with the site.

Management Interface

Select the interface the ExtremeXOS device uses for Management and assigns the device IP to that interface.

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.

NTP Server

The NTP Server field allows you to set the NTP server address on 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.

Admin Profile

Use the drop-down menu to select the access Profile that gives Extreme Management Center 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 menu to select a Poll Group for the discovered ZTP+ devices. Extreme Management Center 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 will overwrite 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 menu to select the Poll Type used to discover devices. Valid options are SNMP, Ping, and Not Polled. When SNMP is specified, the SNMP version (SNMPv1 or SNMPv3) is determined by the Profile specified for the IP range. If the Profile is set to Ping Only, the Poll Type must be set to Ping. If you discover an existing device using a different poll type than the device is already using in the database, saving the device overwrites the Poll Type currently being used in the database.

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 Console as a user with Administrative privileges.

LACP

Select the checkbox to enable ZTP+ devices being discovered to broadcast LACP (Link Aggregation Control Protocol) information. Select the appropriate logging level from the drop-down menu.

LLDP

Select the checkbox to enable ZTP+ devices being discovered to broadcast LLDP (Link Layer Discovery Protocol) information. Select the appropriate logging level from the drop-down menu.

MSTP

Select the checkbox to enable ZTP+ devices being discovered to broadcast MSTP (Multiple Spanning Tree Protocol) information. Select the appropriate logging level from the drop-down menu.

MVRP

Select the checkbox to enable ZTP+ devices being discovered to broadcast MVRP (Multiple VLAN Registration Protocol) information. Select the appropriate logging level from the drop-down menu.

POE

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

VXLAN

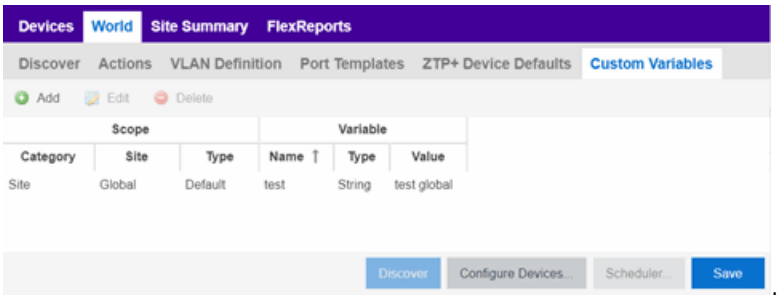
Select the checkbox to indicate the ZTP+ devices being discovered for this site use VXLAN to tunnel Layer 2 traffic over a Layer 3 network.

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.

Custom Variables

The Custom Variables tab allows you to add, edit, or delete variables used in Extreme Management Center. 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 Extreme Management Center, while the fields in the Variable section allow you to define a value for the variable. After you create a variable, Extreme Management Center automatically substitutes the Value you define in the appropriate feature of Extreme Management Center when the criteria specified in the Scope section is met. Variables you create on the Site tab can then be used in a 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 Extreme Management Center. To view and reference the variables, use the Northbound Interface functionality in the Diagnostics tab.



Scope

Category

Displays where the variable is used in Extreme Management Center. Select Port Template, Site, or Topology from the drop-down menu, depending on the purpose of the variable.

Site

Defines the site in which the variable is used.

- Global indicates Extreme Management Center uses the variable for all sites.
- Selecting /World indicates Extreme Management Center 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 menu change depending on what Category you select.

- Port Template — Indicates the Port Configuration for which the variable is used by Extreme Management Center.
- Topology — Displays the type of network topology for which the variable is used by Extreme Management Center.

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 menu.

Value

Displays the value Extreme Management Center 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).

Cancel

Click the Cancel button to cancel the new variable or the changes you made to an existing 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 click **Edit** to make changes to a custom variable.

Update

Click the **Update** button when you finish adding a new or editing an existing custom variable.

Delete

Select a variable in the table and click **Delete** to remove a custom variable from the table.

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 clicking **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 clicking **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 Extreme Management Center
- Devices
- Maps
- How to Create and Edit Maps
- Advanced Map Features

Compare Device Configurations

You can compare archived device configurations in Extreme Management Center 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 Configuration/Firmware > Compare Last Configurations.

From the Reports tab:

Use the **Reports** tab to compare two configuration files selected from all archived files for the device.

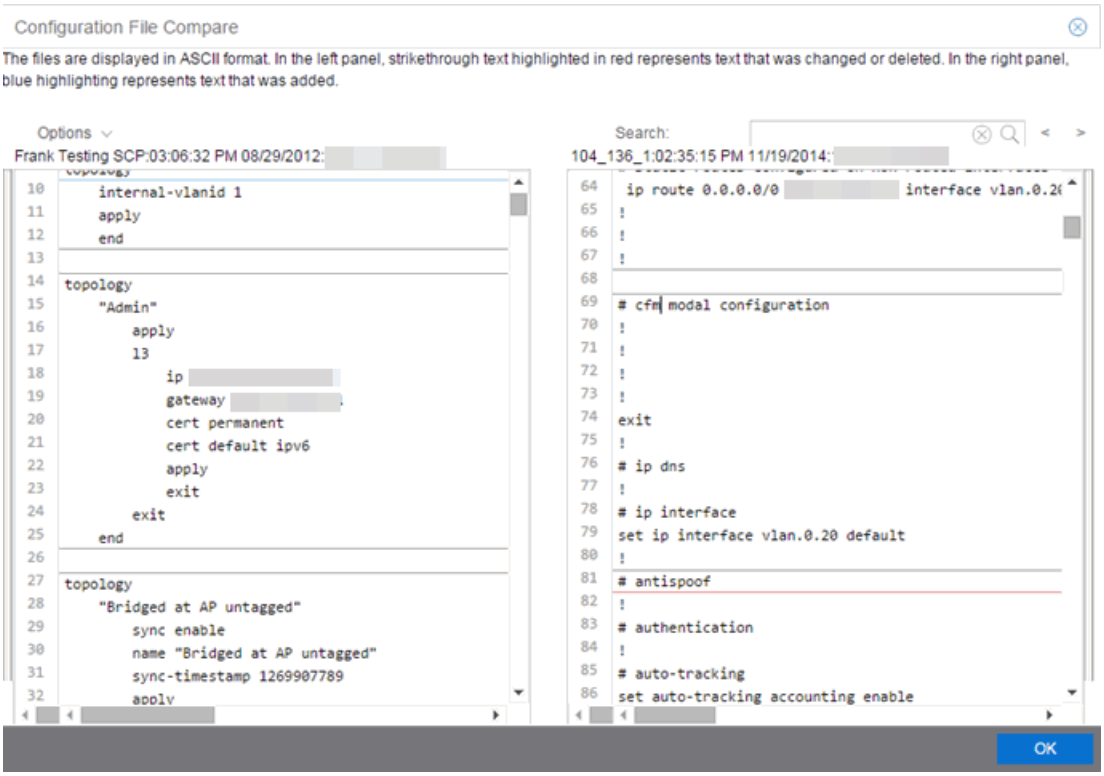
Select the Device > Device Archives report. Click on the **Archive Details** tab in the right panel and then click on the **Archives by Device** sub-tab.

The tab displays all the Extreme Management Center archives by device IP address. Select two files to compare and click **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:

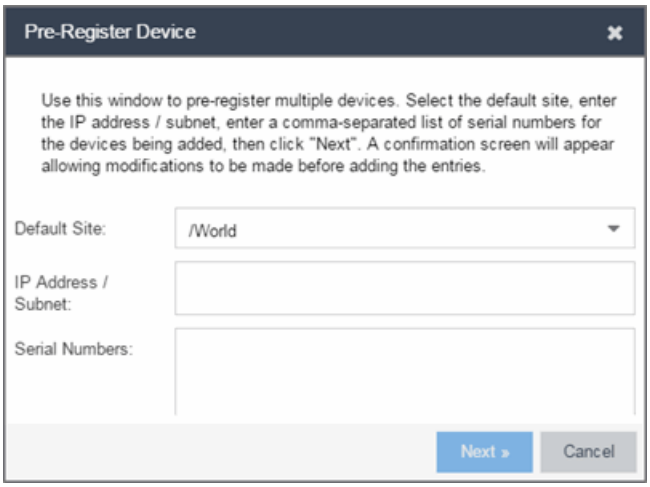
- Network
- Reports

Pre-Register Device

Use this window to add multiple ZTP+ enabled devices to Extreme Management Center.

This window is also accessible on the Network > Discovered tab by clicking the Pre-Register Device button or by right-clicking an existing device and selecting Pre-Register Device.

Pre-Register Device Window



Default Site

The site to which the devices are added.

IP Address/Subnet

Enter the device's IP address and subnet in this field. The subnet can be separated from the IP address by a slash (/) or period (.). This field is required.

Serial Number

Enter the manufacturer-assigned serial numbers of the devices being added, separated by commas.

Next

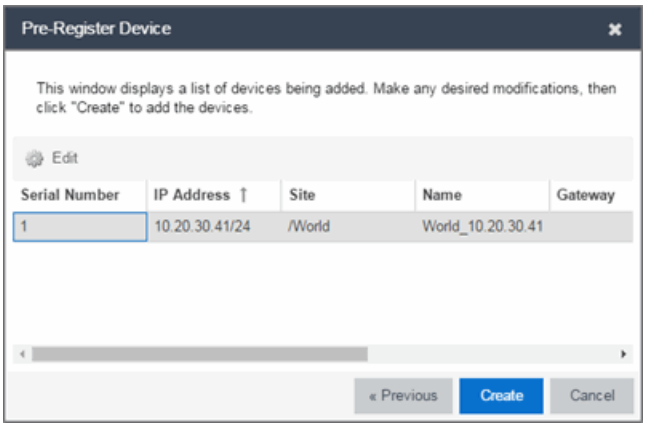
Click the Next button to open a confirmation window allowing you to verify the device information entered.

Cancel

Click the Cancel button to close the window with no changes saved.

Pre-Register Device Confirmation Window

Use this window to confirm device information before adding devices to Extreme Management Center.



Configure

Select a device and click the **Configure** button to change the information for that device.

NOTE: The **Site** can not be changed from this window.

Serial Number

The serial number of the device.

IP Address

The device's IP address.

Site

The site to which the device is added. To change the **Site**, use the Configure Device window.

Name

The name assigned to the device. The default **Name** lists includes the **Site** to which the device is assigned followed by the device's IP address.

Gateway

Enter the IP address of the switch's Access Control Gateway, if necessary.

Domain Name

Enter a value in the **Domain Name** field to configure the domain name on the devices being discovered, if necessary.

DNS Server

Enter a DNS server address for the devices being discovered, if necessary.

NTP Server

Enter the NTP server address for the devices being discovered, if necessary.

Create

Click the **Create** button to add the devices listed to the Extreme Management Center database.

Related Information

For information on related windows:

- Discovered

Maps Overview

The Extreme Management Center Maps feature on the **Network** > **Devices** tab lets you view and search geographic and topology maps of the 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.

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

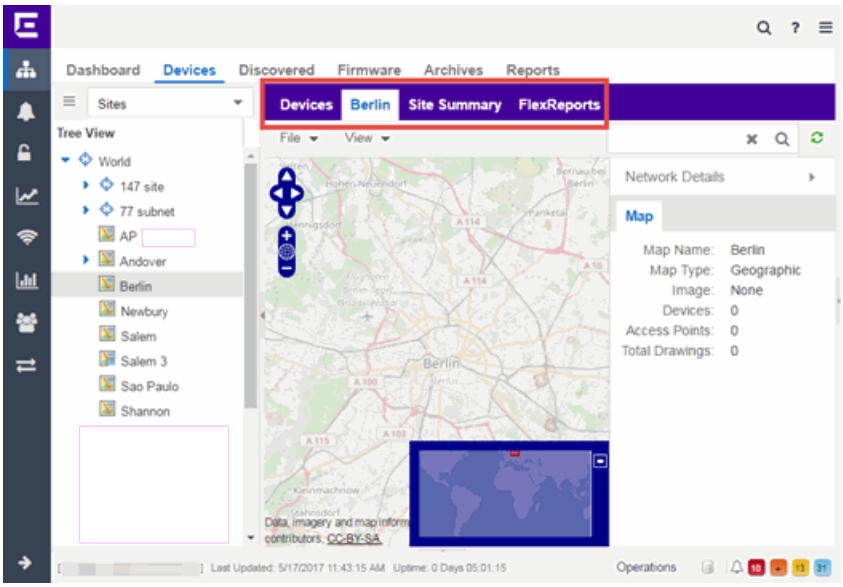
Access the **Network** > **Devices** tab and select **Sites** from the left-panel drop-down menu.

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 menu, 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, three types of maps are available, Topology, 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.

For information on advanced location (triangulation) and wireless coverage maps (available with the NMS-ADV license), see Advanced Map Features.

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 Extreme Management Center to automatically create FlexReports on a scheduled basis by clicking 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

Navigating the Extreme Management Center Map Tab

The Extreme Management Center 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.

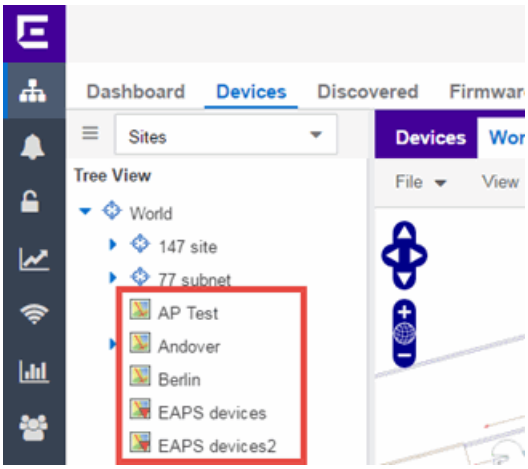
To view or search maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read Access or Maps Read/Write Access capability.

Accessing the Map Tab

1. Launch Extreme Management Center.
2. Click the Network > Devices tab.
3. Select Sites from the left-panel drop-down menu. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.

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

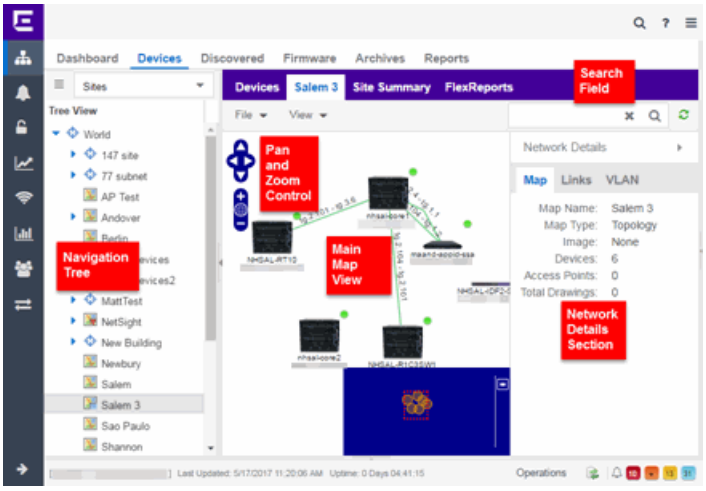
You can also import a saved map by right-clicking a map in the navigation tree and selecting **Maps** > **Import Map**. This opens the Import Map window.

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:

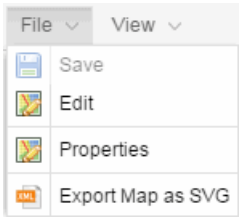
- File, View, and Tool Menus
- Pan and Zoom Control
- Search Field



File, View, and Tool Menus

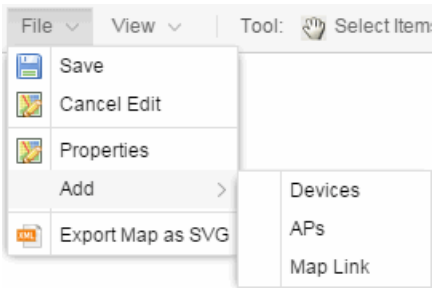
File Menu

The **File** menu allows you to change the map information, the devices, APs, and links displayed on the map, and export the map from Extreme Management Center.



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.

Clicking **Edit** opens the map in Edit mode and the **Add** menu is available, as shown below.



Clicking **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.

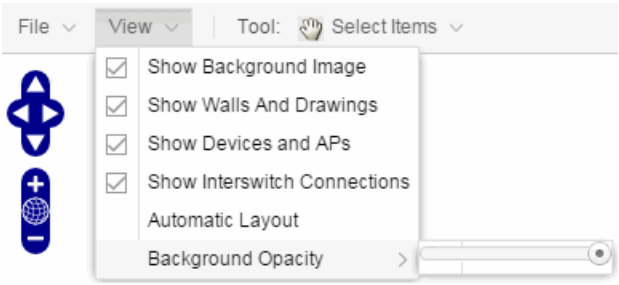
When exporting a map in SVG format, the exported SVG file may open in a new tab or window, depending on how your browser is configured. The SVG file displays your exact view when you select **Export Map as SVG**. For example, if your map is zoomed in to only show two devices and the VLANs associated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

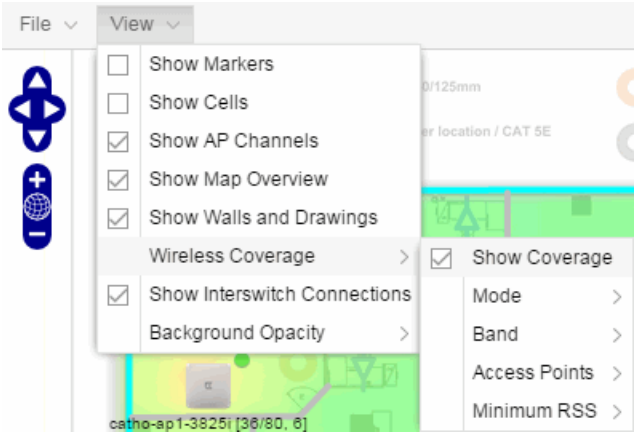
Additionally, by clicking **Edit** in the **File** menu, the map changes to Edit mode and the **Add** submenu is available, from which you can add devices, APs, and map links to the map. Edit mode also allows you to manipulate the existing devices, APs, and map links currently displayed on the map. Click **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: The floorplan map type is only available with the NMS-ADV license.

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 Click on 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. Click 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. Click once and draw the first line of the polygon. Click at 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. Click and drag to draw the rectangle. When you are finished drawing, right-click to release the draw rectangle tool.
	Add Text Click the map to open the Enter Text window. When you are finished entering your text, click OK. Position the cursor where you want to place the text and click 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. Click 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. Click once and draw the line. Click 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 Click on 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 clicking 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. Clicking 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.

Clicking 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 click 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 Extreme Management Center 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, click the **more** link in the pop-up to access the DeviceView or additional information about the AP for a device or AP, respectively.

Accessing Device Information

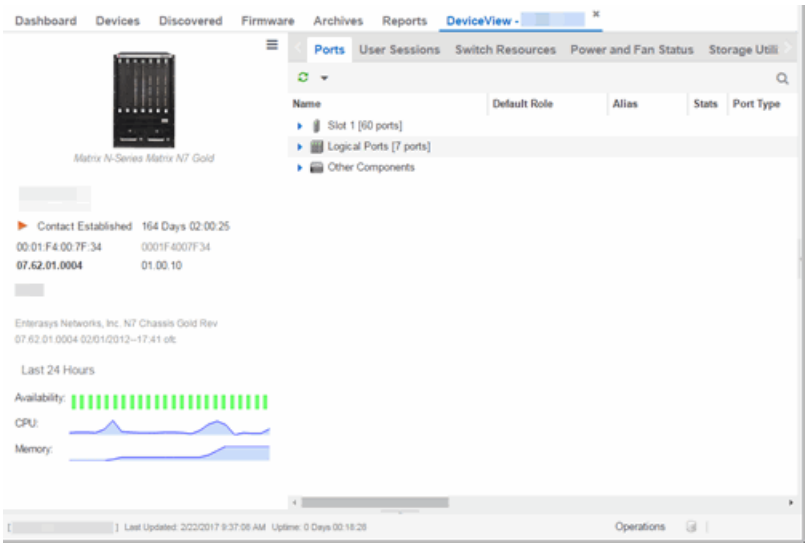
There are two ways to access additional device information from a map.

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 **DeviceView** or right-click on an AP in a map and select **AP Summary** to open a DeviceView (like the example shown below) or AP PortView window where you can see a device image and other important device information.



Additionally, the DeviceView and AP PortView windows contain tabs with additional information about the device or AP.

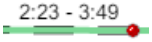
Link Information

Links are displayed on Topology maps. Each connection type is represented by a different line style:

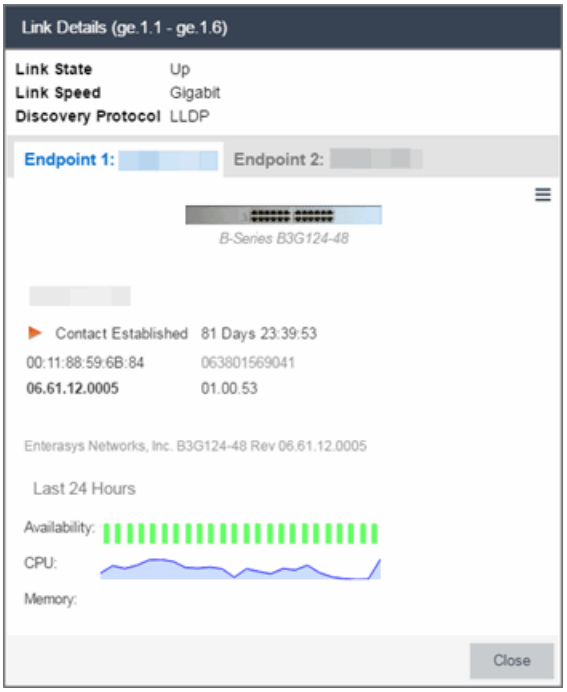
- Basic links appear as thin green lines with no outlining.

- 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

Related Information

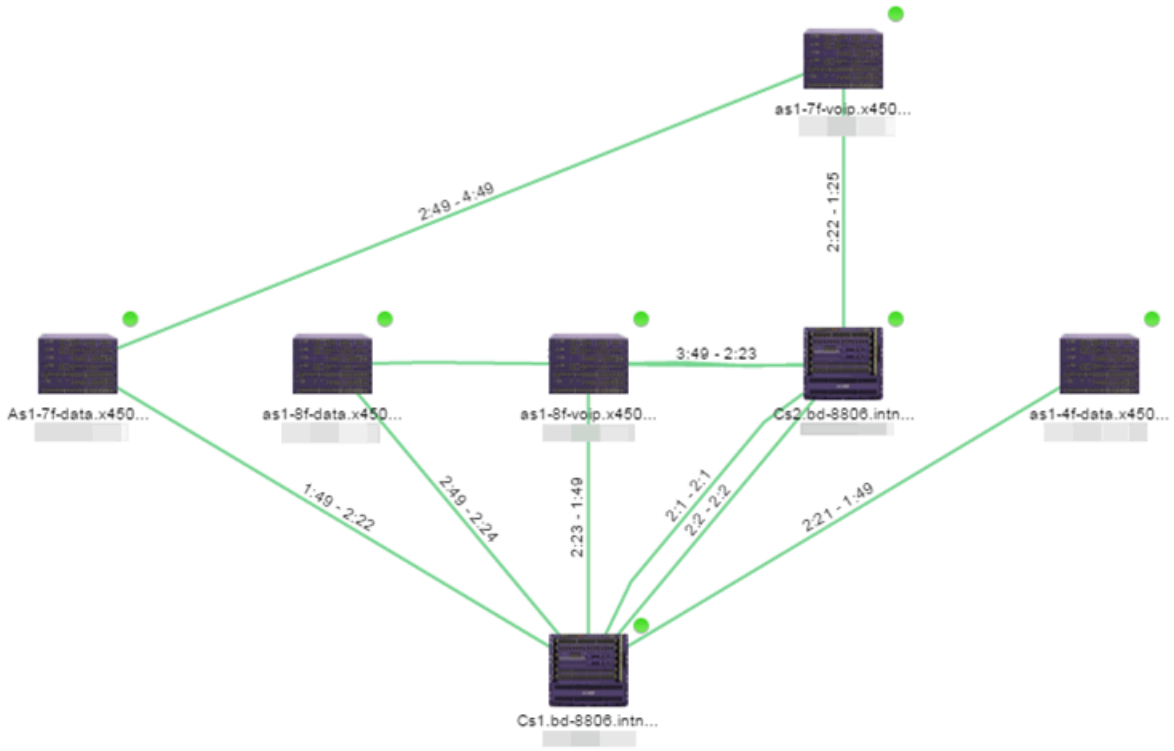
- Extreme Management Center Maps
- Advanced Map Features

Extreme Management Center Maps

Extreme Management Center allows you 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. Maps are configured in various places on the Network > Devices tab.

Using Extreme Management Center 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.



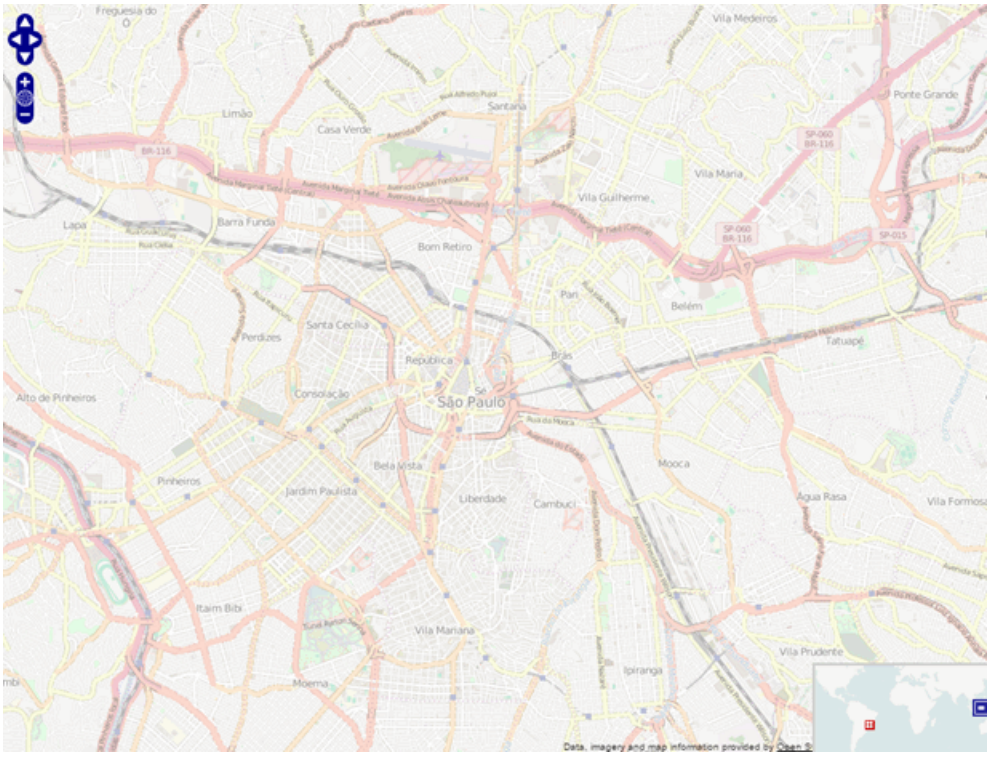
For additional information about devices and links in a Topology map, see the Viewing Alarm and Device Status and Link Information sections.

- 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: The floorplan map type is only available with the NMS-ADV license. 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 (available with the NMS-ADV license), see Advanced Map Features.

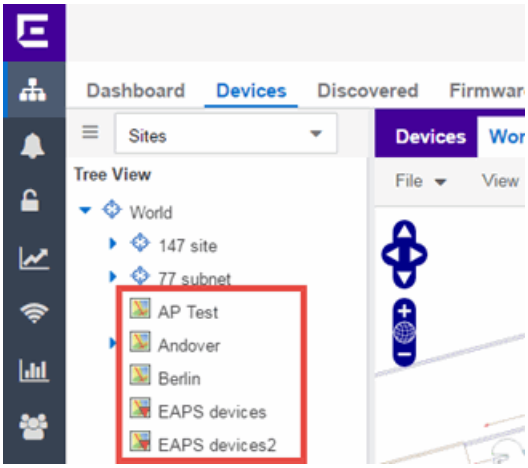
To view or search Maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read Access or Maps Read/Write Access capability.

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. Edit mode allows you to add new or move existing devices, APs, and map links on a map.

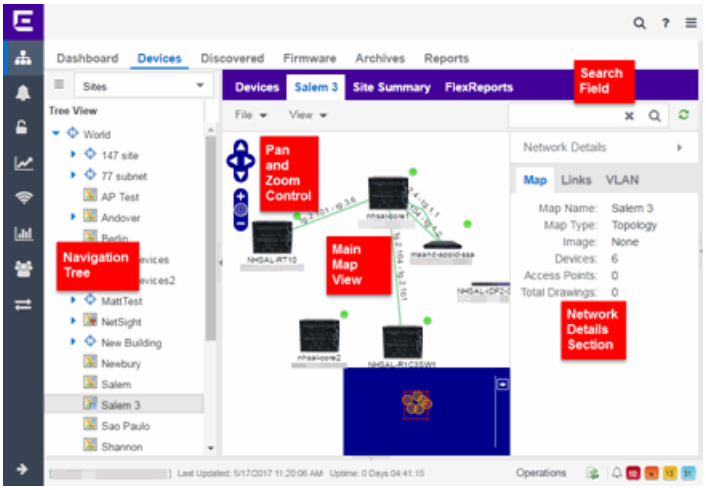
Import Map

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:

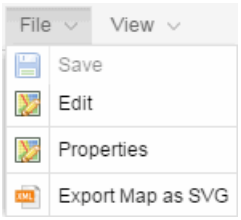
- File, View, and Tool Menus
- Pan and Zoom Control
- Search Field



File, View, and Tool Menus

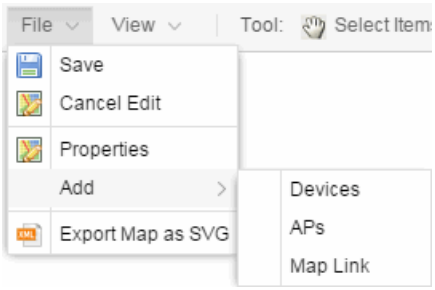
File Menu

The **File** menu allows you to change the map information, the devices, APs, and links displayed on the map, and export the map from Extreme Management Center.



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.

Clicking **Edit** opens the map in Edit mode and the **Add** menu is available, as shown below.



Clicking **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**.

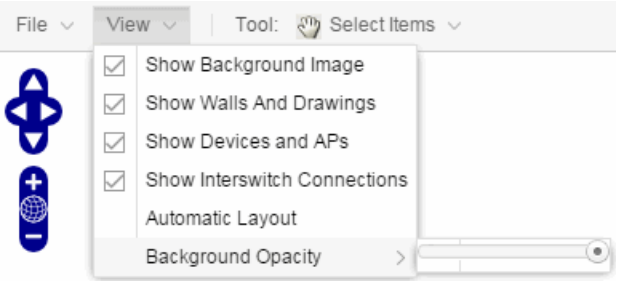
NOTE: For additional information regarding displaying VLANs in a map, see the VLAN tab section.

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 Extreme Management Center.

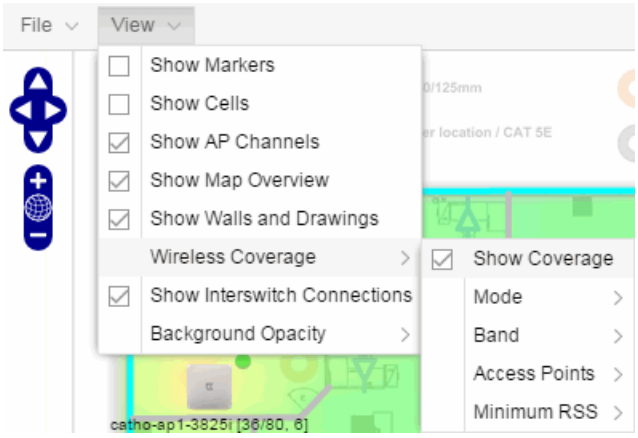
Additionally, by clicking **Edit** in the **File** menu, the map changes to Edit mode and the **Add** submenu is available, from which you can add devices, APs, and map links to the map. Edit mode also allows you to manipulate the existing devices, APs, and map links currently displayed on the map. Click **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: The floorplan map type is only available with the NMS-ADV license. 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** Click on 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. Click 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. Click once and draw the first line of the polygon. Click at 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. Click and drag to draw the rectangle. When you are finished drawing, right-click to release the draw rectangle tool.

Drawing Tool	Definition
	Add Text Click the map to open the Enter Text window. When you are finished entering your text, click OK. Position the cursor where you want to place the text and click 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. Click 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. Click once and draw the line. Click 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 Click on 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 clicking 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. Clicking 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.

Clicking 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 click 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 Extreme Management Center 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, click the **more** link in the pop-up to

access the DeviceView or additional information about the AP for a device or AP, respectively.

Accessing Device Information

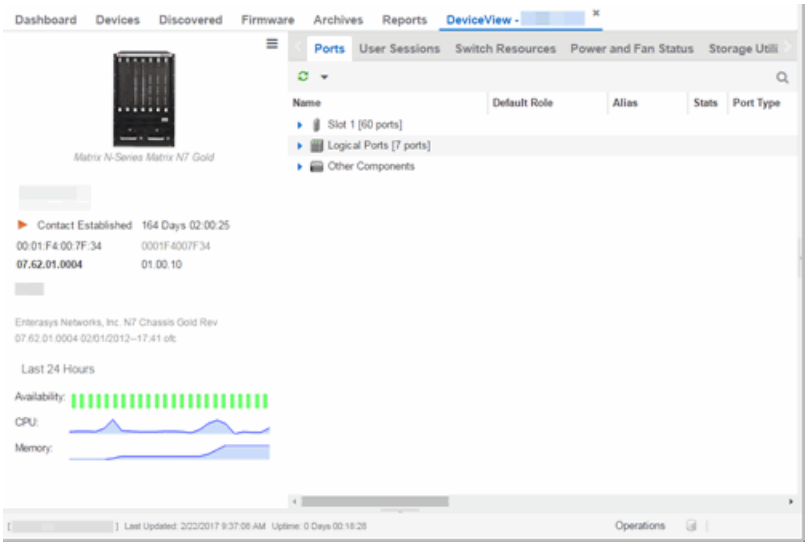
There are two ways to access additional device information from a map.

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 **DeviceView** or right-click on an AP in a map and select **AP Summary** to open a DeviceView (like the example shown below) or AP PortView window where you can see a device image and other important device information.



Additionally, the DeviceView and AP PortView windows contain tabs with additional information about the device or AP.

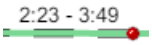
Link Information

Links are displayed on Topology maps. Each connection type is represented by a different line style:

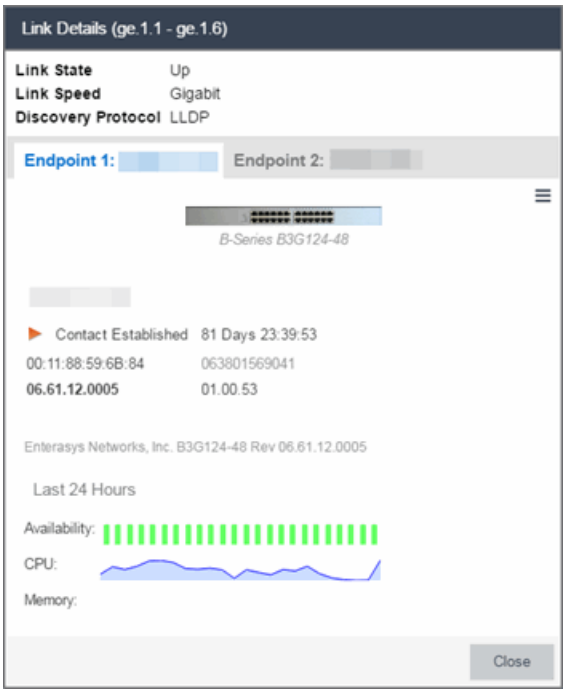
- Basic links appear as thin green lines with no outlining.

- 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.



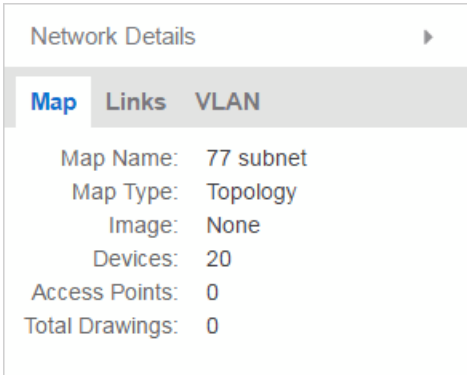
Network Details Section

The Network Details section is available in topology and geographic maps. It contains 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

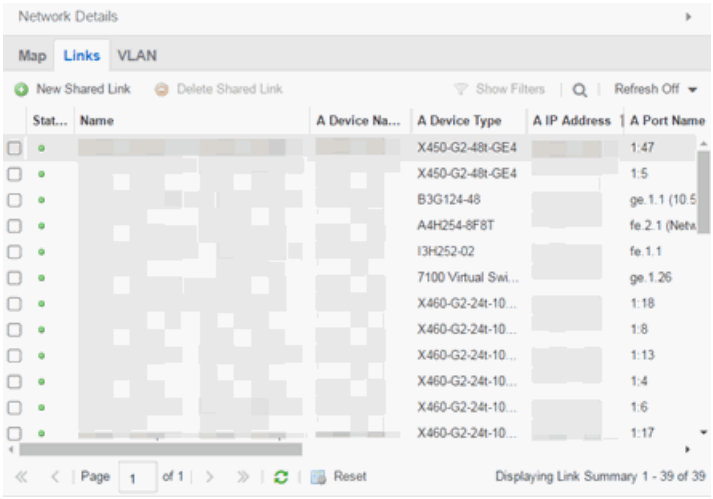
Map tab

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.



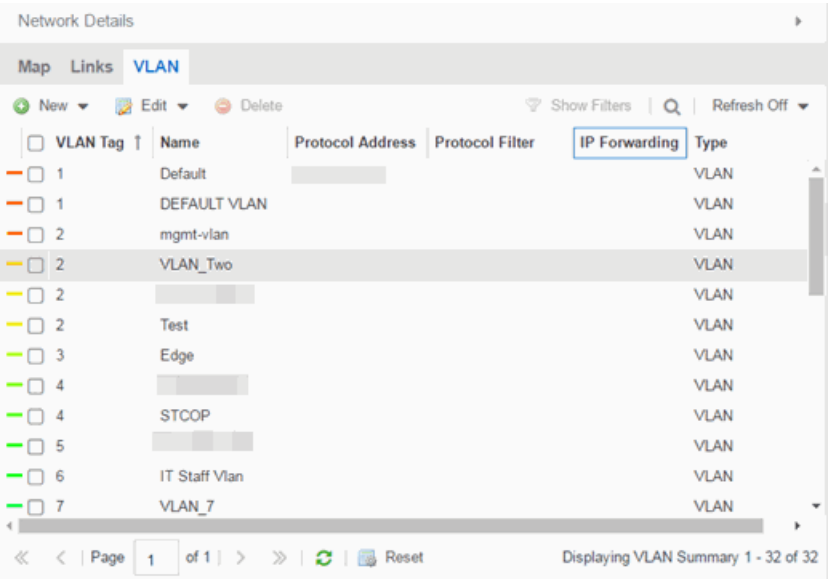
The top of the **Links** tab contains a search field, which allows you to find a particular Link by entering specific criteria. Additionally, you can manually browse links using the scroll bar and page navigation at the bottom of the section.

Double-clicking a link opens the Link Details window.

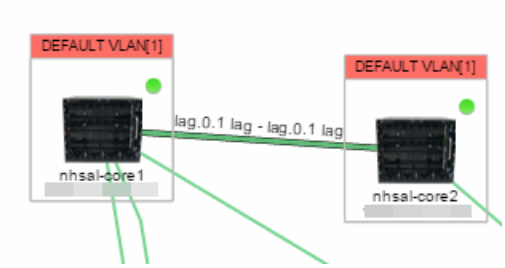
The top of the window displays information about the link, while information about the devices it connects are contained on two tabs, Endpoint 1 and Endpoint 2.

VLAN tab

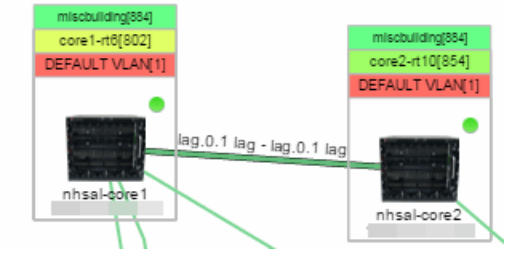
The **VLAN** tab displays VLANs configured as part of devices included in the map. Columns in the **VLAN** tab provide additional information, including the VLAN tag, the name of the VLAN, any protocol filters applied for devices on which the VLAN is configured, and whether or not IP forwarding is enabled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



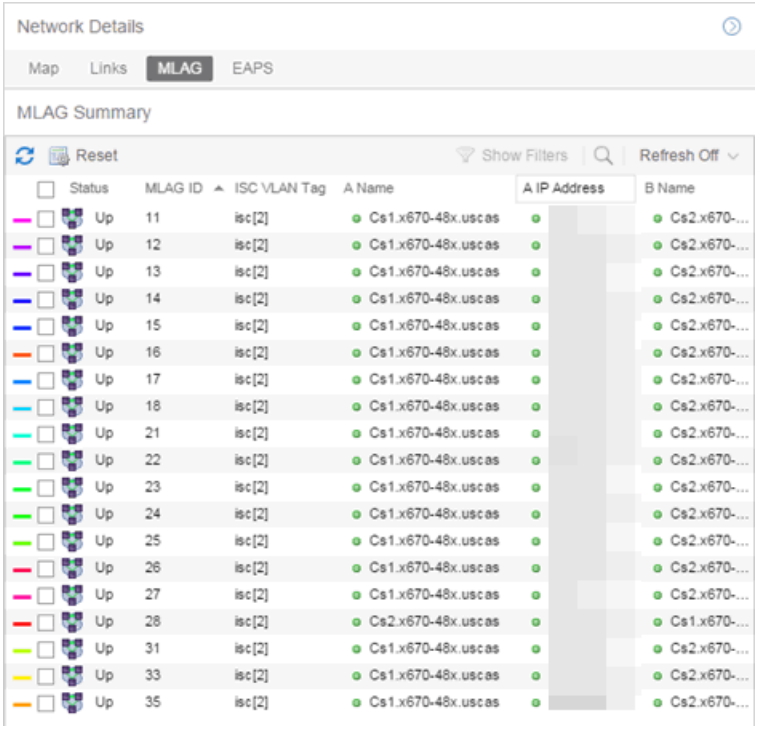
Selecting multiple VLANs assigned to the same device adds a new title bar to the box that displays the VLAN name and associated color.



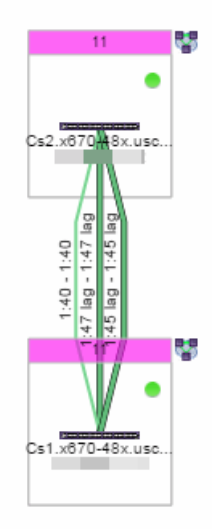
Additionally, from the **VLAN** tab, you can create a new VLAN and create a VLAN protected by an EAPS domain via the New drop-down menu or edit the ports, name, and devices associated with an existing VLAN via the **Edit** drop-down menu. For more information, see How to Create and Edit VLANs.

MLAG tab

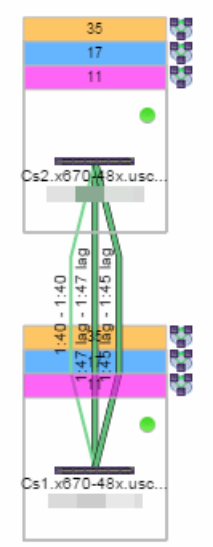
The MLAG tab provides a list of the MLAGs (ports combined as a common logical connection on devices) included in the map. The list provides the MLAG's status, ID, ISC VLAN tag, the names and addresses of the devices configured as part of the MLAG, and the ports on those devices assigned as part of the MLAG. Additionally, the Connected IP column displays the IP of the switch to which the MLAG is connected.



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.

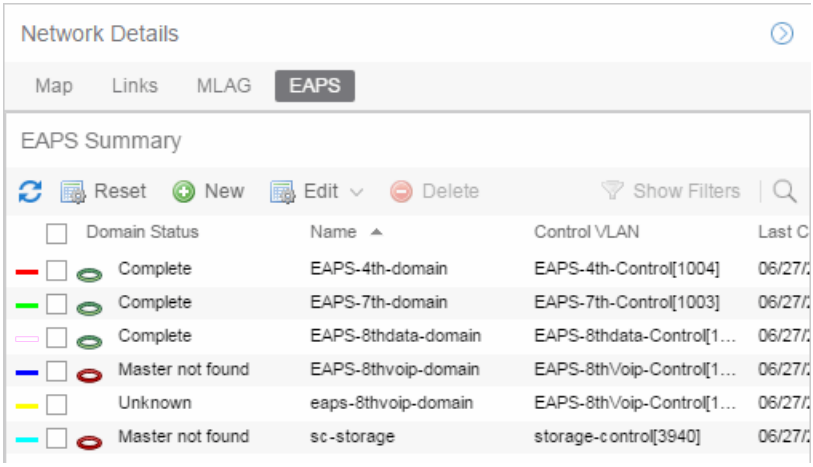


Selecting multiple MLAGs assigned to the same device adds a new title bar to the box containing the VLAN name and associated color.

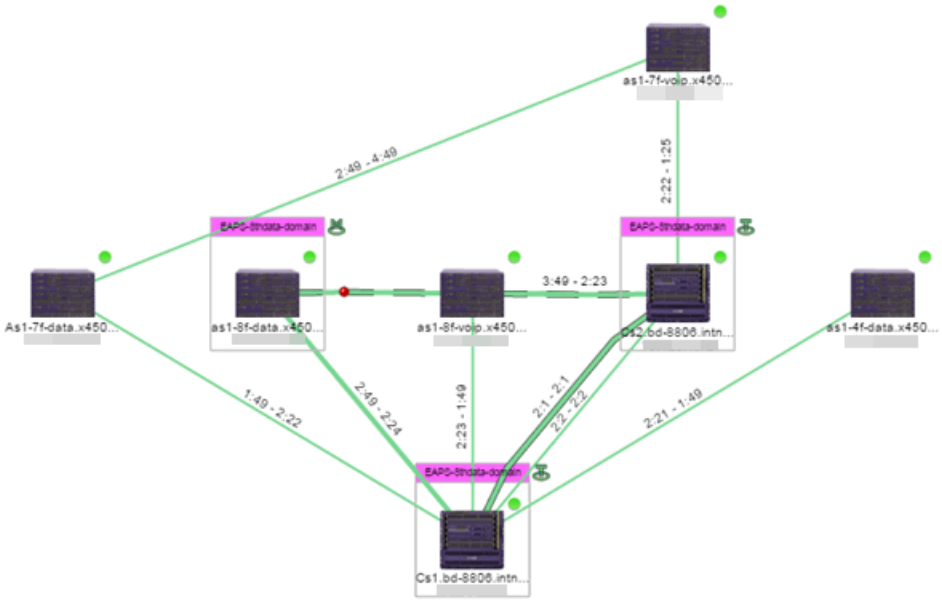


EAPS tab

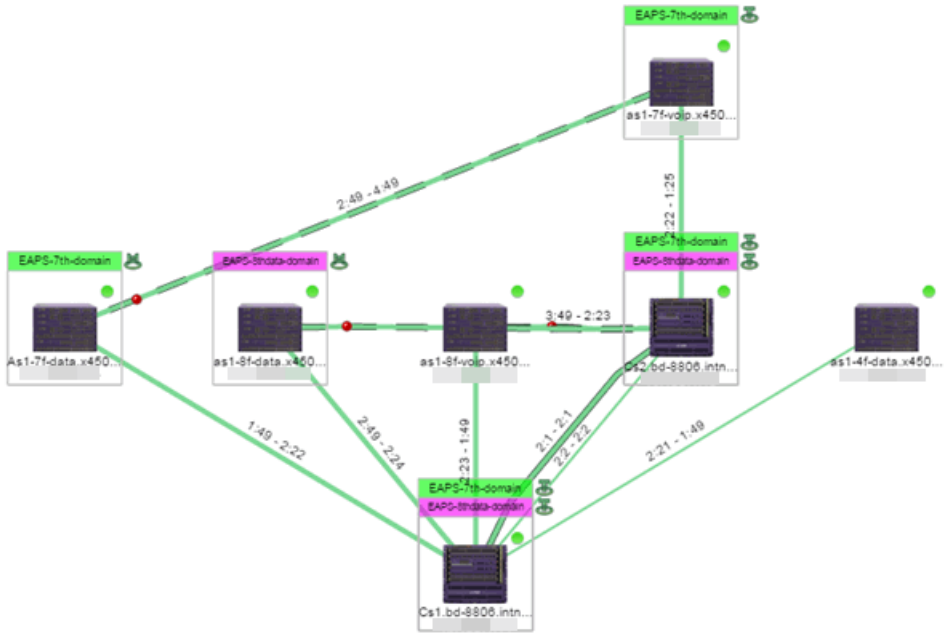
The EAPS tab displays a list of the EAPS domains, including their status, name, the control VLAN name, and the IP addresses of the devices utilizing the EAPS domain.



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.

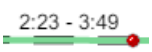


An icon next to the title bar indicates if the node is a master node, indicated by an "M" icon, or if the node is a transit node, indicated by a "T" icon.

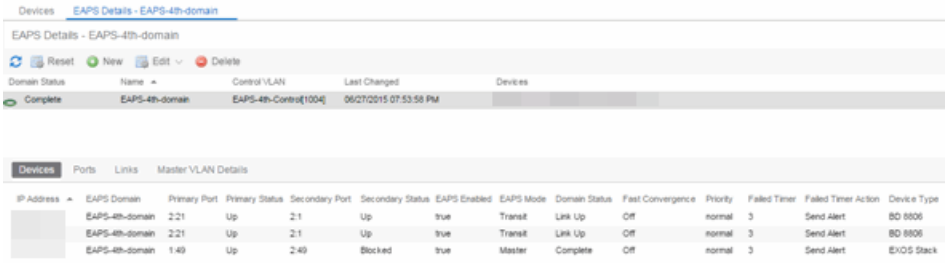
The color of the ring icon indicates the status of the domain:

- 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.

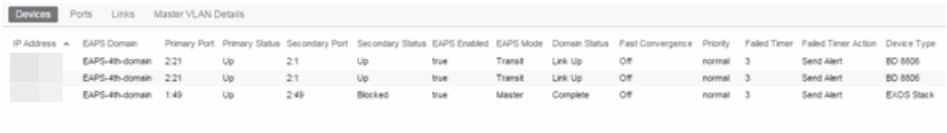


You can view additional details about the EAPS domain by right-clicking an EAPS domain on the **EAPS** tab and selecting **EAPS Details** to open the EAPS Detail view.

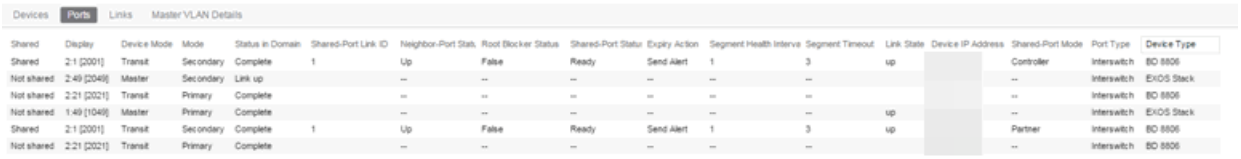


The top of the EAPS Details view displays a summary of the EAPS domain, identical to the information displayed in the EAPS tab. At the bottom of the window are three sub-tabs, which display additional information:

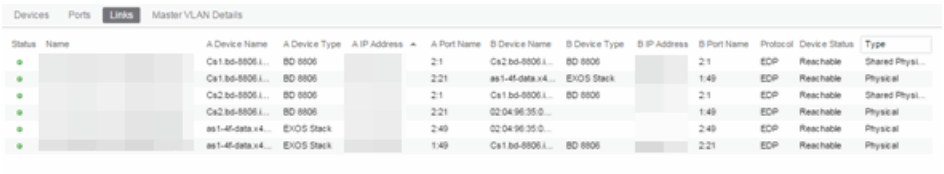
- Devices — Displays information about the devices using the EAPS domain.



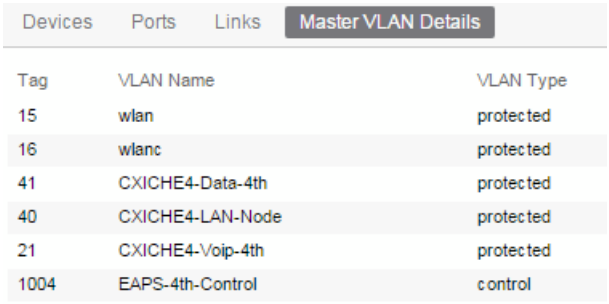
- Ports — Displays information about the shared ports associated with the EAPS domain.



- Links — Displays links between devices using the EAPS domain.



- Master VLAN Details — Displays details about the master VLAN associated with the EAPS domain.



Clicking 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 menu, enter the MAC Address, IP Address, hostname, user name, AP serial number or Extreme Access Control custom field information, and press **Enter**.

You can also search for specific wireless clients, access points, devices, and wired clients from different locations in Extreme Management Center, outlined below.

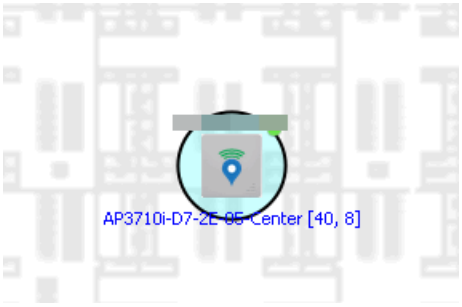
Finding a Wireless Client

From the Search Field on the Network Tab

You can locate a wireless client connected to an AP added to a map by selecting a map or the map navigation tree and use the **Search** field on the **Network** tab. To start a search for a wireless client, enter a MAC address, IP address, hostname, or user name in the map **Search** field and press **Enter** .

The search uses RSS-based (Received Signal Strength) location services to locate the wireless client and display the approximate location of the client on the map. For more information, see Advanced Map Features.

The map opens with the AP centered on the map, with a circle showing the possible area where the client is located. If that information is not available, a square is drawn around the AP last associated with the client.



From the Wireless Tab

In addition to using the **Network** tab Search, you can locate a wireless client from the **Wireless** tab. Select a client in the Clients view, right-click and select **Search Maps**. The map opens centered on the AP, with a circle showing the possible area where the client is located. Mouse over the client icon to see a tooltip with client information.

NOTE: Tooltip information is based on current data from the wireless domain unless the client icon displays a clock in the center. In that case, the tooltip information is based on historic data from the Wireless > Clients page.

Radius Distance Calculation

The following distance calculation defines the radius of the circle displayed around the wireless client located on the map.

Path loss per meter in free space =
L1 = 20 * log (10) (f) - 28

where:

- [f] is the frequency in MHz
  (Uses Source SNMP MIB dot11ExtSmtCurrentChannel
  or if that value is 0, uses MIB dot11ExtSmtCurChanSelectedByAP)
- [L1] is the path loss on distance of 1 meter

Radial distance for location =
d(RSS,n) = 10 ^(pTx - RSS - L1)/(10*n)

where:

- [n] is the coefficient for the environment
- [pTx] is the transmit power (dB)

- [RSS] is the Received Signal Strength
- [d] is the distance in meters

Finding an Access Point

From the Wireless Tab

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

From the Reports Page

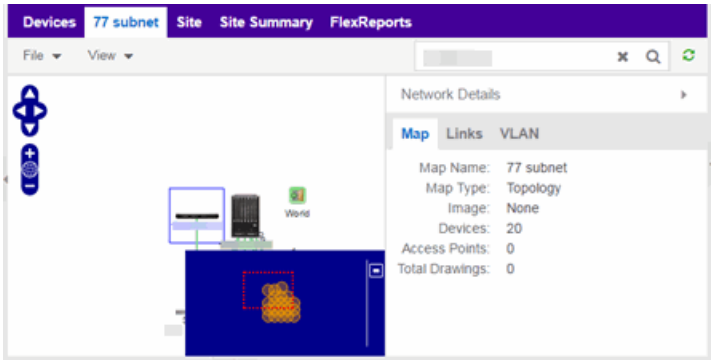
You can locate an AP from the Wireless > APs Summary report on the **Reports** tab. Select an AP in the table, right-click and select **Search Maps**. If a map contains the AP, the map opens with the AP centered on the map.

Finding a Device

From the Network Page Search Field

Select a map or the map navigation tree, enter an IP address or hostname for the device in the **Network** tab **Search** box and press **Enter** to start a search.

The search locates a device added to a map. The map centers on the device. The screen shot below shows the results for a search on a specific IP address.



Finding a Wired Client

From the Network Tab Search Field

Select a map or the map navigation tree, enter a MAC address, IP address, hostname, or user name in the **Network** tab **Search** box and press **Enter** to start a

search for a wired client.

The search locates a wired client if the client is Extreme Access Control authenticated and is connected to a switch added to a map. The map centers on the wired client.

From the Control Tab

You can also locate an Extreme Access Control authenticated wired client from the **Control > Extreme Access Control** tab. Select an end-system in the End-Systems view, right-click and select **Search Maps**. If the end-system is connected to a switch added to a map, the map opens with the end-system centered on the map.

Using Map Links

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

For example, the following map link lets you jump to the Second Floor map. The link is green, indicating that there are no devices with alarms on the Second Floor map.

The following map link lets you jump to the First Floor map. The link is red, indicating that there is an alarm for a device on the First Floor map.

Additionally, you can use map links to display Application data based on Application Analytics 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

How to Create and Edit Maps

The Extreme Management Center 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 Extreme Management Center, see Extreme Management Center Maps.

This Help topic provides the following information on creating and editing maps.

For information on creating custom floor plans, advanced location (triangulation), and wireless coverage maps (available with the NMS-ADV license), 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 Extreme Management Center and click on the Network tab.
2. Open the Devices tab.
3. In the left-panel select Sites.

4. Right-click a site or map and click **Maps/Sites** > **Create Map**.

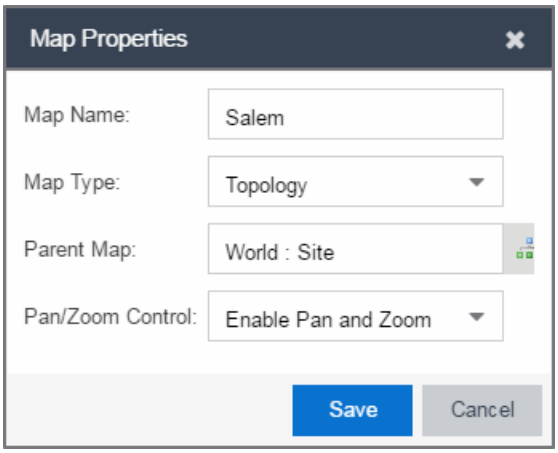
   NOTE: You cannot create a new map if you are currently editing another map.

5. Enter a name for the map and click **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, clicking 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.

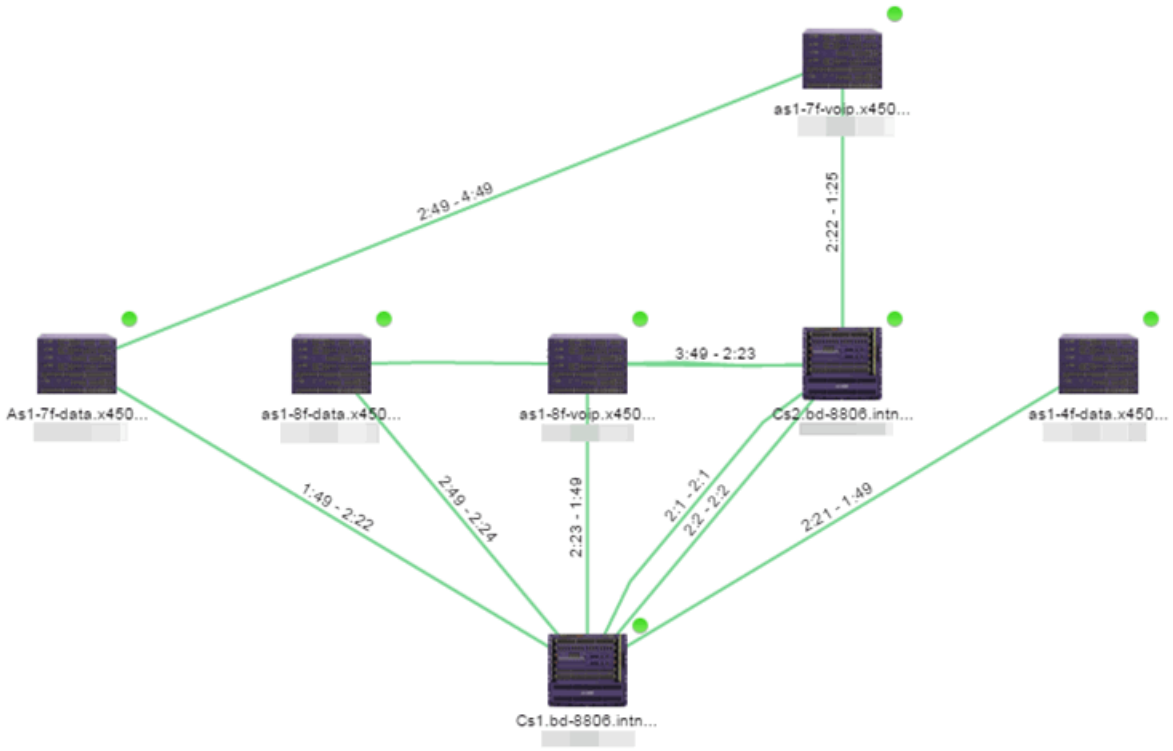
6. Click **File** > **Properties** to open the Map Properties window from which you can edit the map criteria.



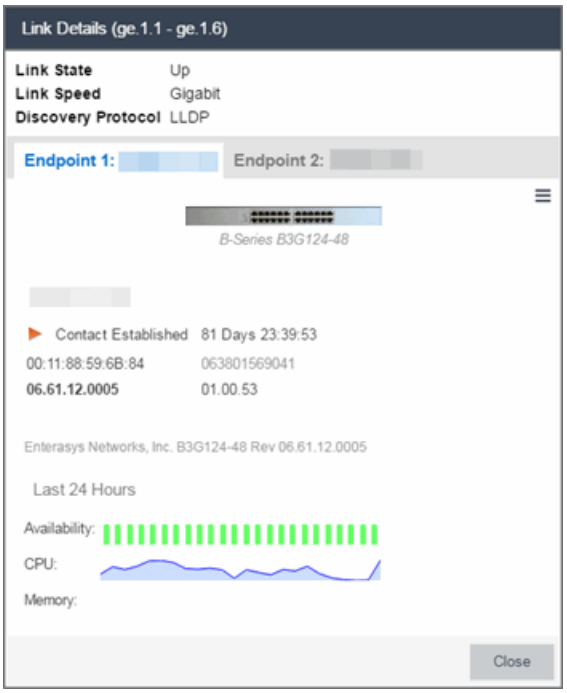
   a. In the **Map Name** field, change the name for the map, if necessary.

   b. In the **Map Type** drop-down menu, 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, .gif, and .jpg 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 menu to select an image or click the button to open a window where you can select a local image and upload it to the Extreme Management Center 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 — For customers with a NMS-ADV license, use this option to create custom floor plans. For more information, see Advanced Map Features.

An additional Floor Plan option is available for users with the Extreme Management Center NMS-ADV license. 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 menu to select an image or click **Add** (⊕) to open a window where you can select a local image and upload it to the Extreme Management Center server.

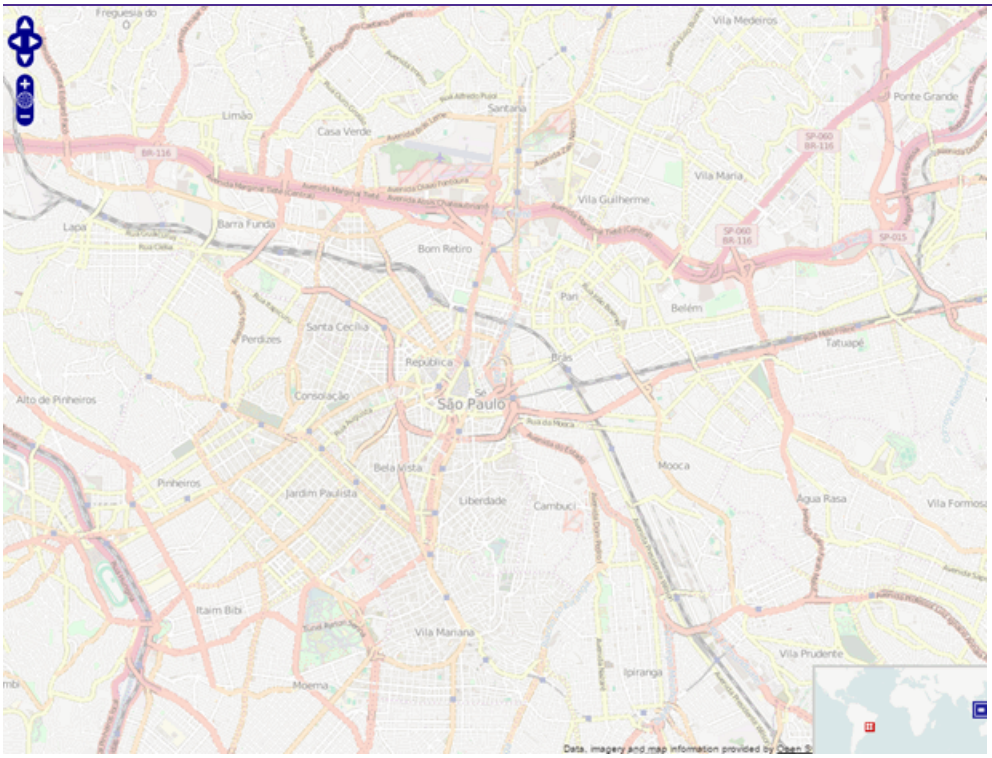
NOTE: If you upload a map image and an image with the same name already exists, the existing image is replaced.

The Map feature supports images in the .png, .gif, and .jpg 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.

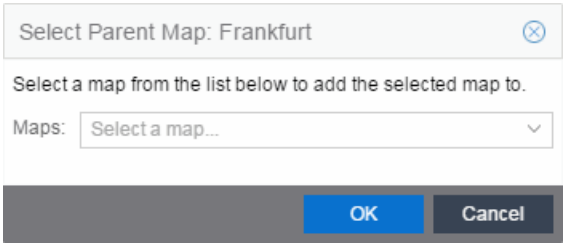
CAUTION: Increasing the oneView.maxImageSize value may cause stability issues and performance issues when generating a heatmap.

- 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. Click 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, or Links to the map you are currently editing by clicking 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 menu in the Add Link To Map window. Click the Add button to add the device, AP, or link to your network map.

8. 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 clicking 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. Click 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 click 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 Extreme Management Center and click on 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. Click **Import**.

Adding Devices/APs from Extreme Management Center Devices and Wireless

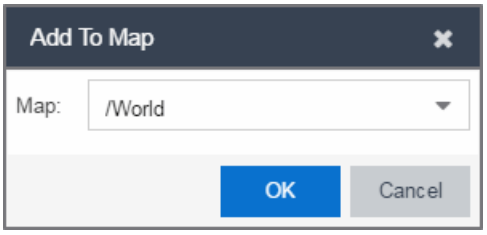
You can quickly add devices and APs to your maps directly from the Devices list or from the navigation tree on the Extreme Management Center **Network** and **Wireless** tabs. You can add them to a specific map, or create new maps based on device or AP system location.

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 menu 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, click 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 menu to select the desired map. Click **OK** to add the devices or APs to the map.



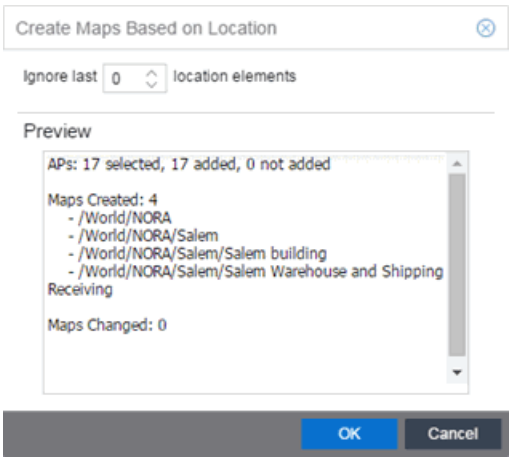
4. Open the Maps page and select the map to which you added the devices. Right-click on the map and select **Edit Map**. You can now position the devices as desired.
5. Click the **Save** button to save the device to the map.

Add to New Maps Based on Location

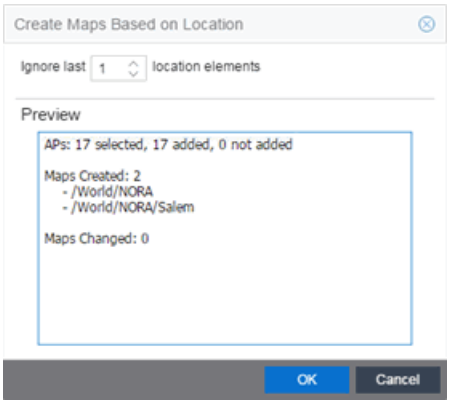
Use these steps to add devices or APs to new maps based on well-named system locations that reflect the desired map structure. For example, if your devices are assigned system locations according to the following structure: US/Boston/Third Floor/Closet One/Rack One/Shelf One, typically, a map would be 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, click on 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. Click **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. Click 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 menu.
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. Click **OK** to add the link to the map.

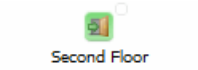
NOTES: The **Link State** for a manual link is derived from the **Status** of the ports to which it connects.

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.

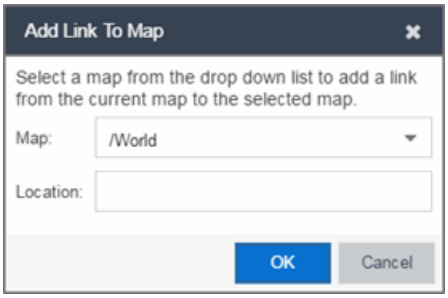


The following map link lets you jump to the First Floor map. The link is red, indicating there is an alarm for a device on the First Floor map.

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 click **File** > **Edit** button in the map properties panel.

2. The map's property panel opens in Edit mode. Click **File** > **Add** > **Map Link**.
3. The **Add Link to Map** window opens.



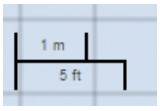
4. From the **Map** drop-down menu, select the map to which you want to link.
5. Enter information in **Location** about the location to which the link connects and click **OK**.
6. The map link is added to the map and can be repositioned, if desired.
7. Click the **Save** button to save the map and close the properties panel.

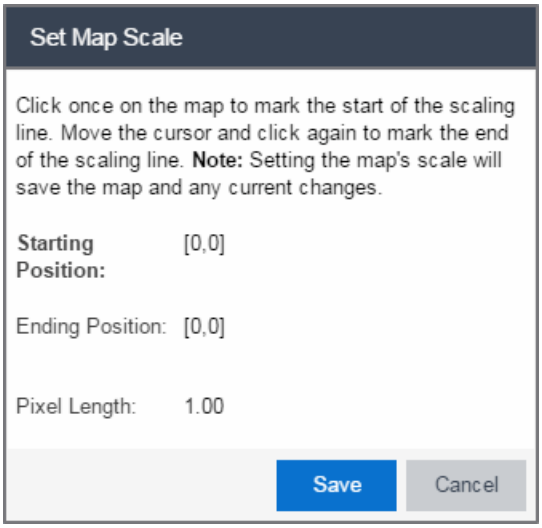
Setting the Map Scale

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 click the **File** > **Edit** button in the map properties panel.
2. Click on the map scale in the map's footer panel to open the Set Map Scale window. (Users with the Extreme Management Center NMS-ADV license 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. Click once on the map to mark the start of the scaling line. Move the cursor and click again to mark the end of the scaling line.
    b. Enter the line length and units.
4. Click Save. The map scale is automatically adjusted and the map is saved.

Related Information

- Extreme Management Center Maps
- Advanced Map Features

How to Add Devices and APs to Maps

Adding Devices/APs from Extreme Management Center Devices and Wireless

Using the Extreme Management Center Maps feature, you can quickly add devices and wireless access points (APs) to your maps directly from the Devices

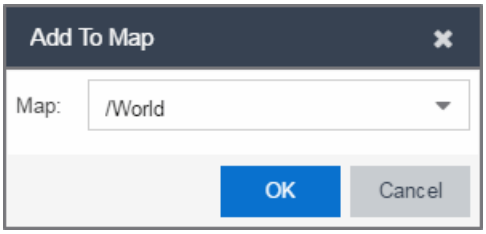
list or from the navigation tree on the Extreme Management Center **Network** and **Wireless** tabs. You can add them to a specific map, or create new maps based on device or AP system location.

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 menu 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, click 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 menu to select the desired map. Click **OK** to add the devices or APs to the map.



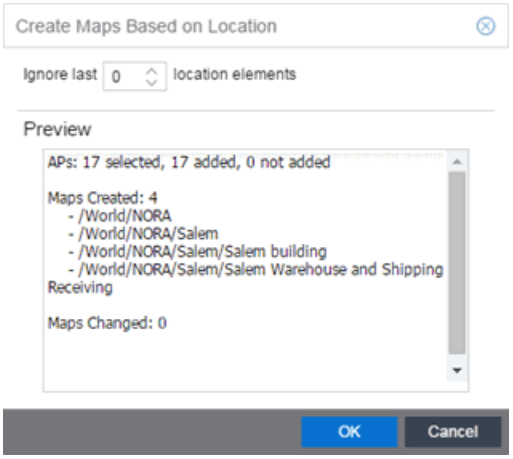
4. Open the Maps page and select the map to which you added the devices. Right-click on the map and select **Edit Map**. You can now position the devices as desired.
5. Click the **Save** button to save the device to the map.

Add to New Maps Based on Location

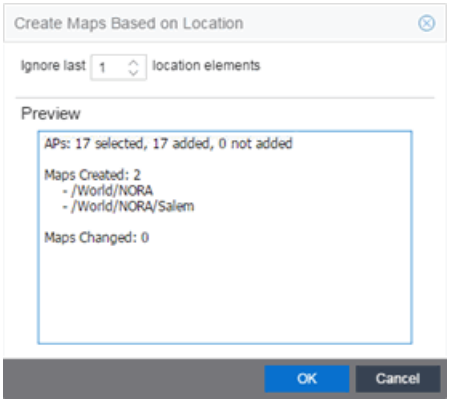
Use these steps to add devices or APs to new maps based on well-named system locations that reflect the desired map structure. For example, if your devices are assigned system locations according to the following structure: US/Boston/Third Floor/Closet One/Rack One/Shelf One, typically, a map would be 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, click on 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. Click **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. Click the **Save** button to save the devices/APs to the map.

Related Information

- Extreme Management Center Maps
- Advanced Map Features

How to Create Maps Using the

The Extreme Management Center 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.

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

Accessing the Map Tab

1. Launch Extreme Management Center.
2. Click the **Network** > **Devices** tab.
3. Select **Sites** from the left-panel drop-down menu. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.

Creating a Map

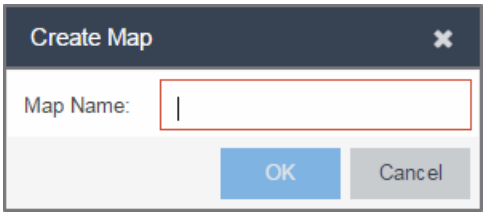
To create a new Device map:

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**.

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

The Create Map window, shown below, opens.

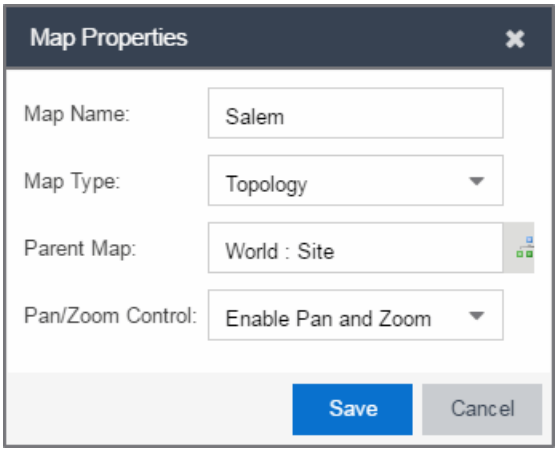
2. Enter a name for the map and click **OK**.



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, clicking 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.

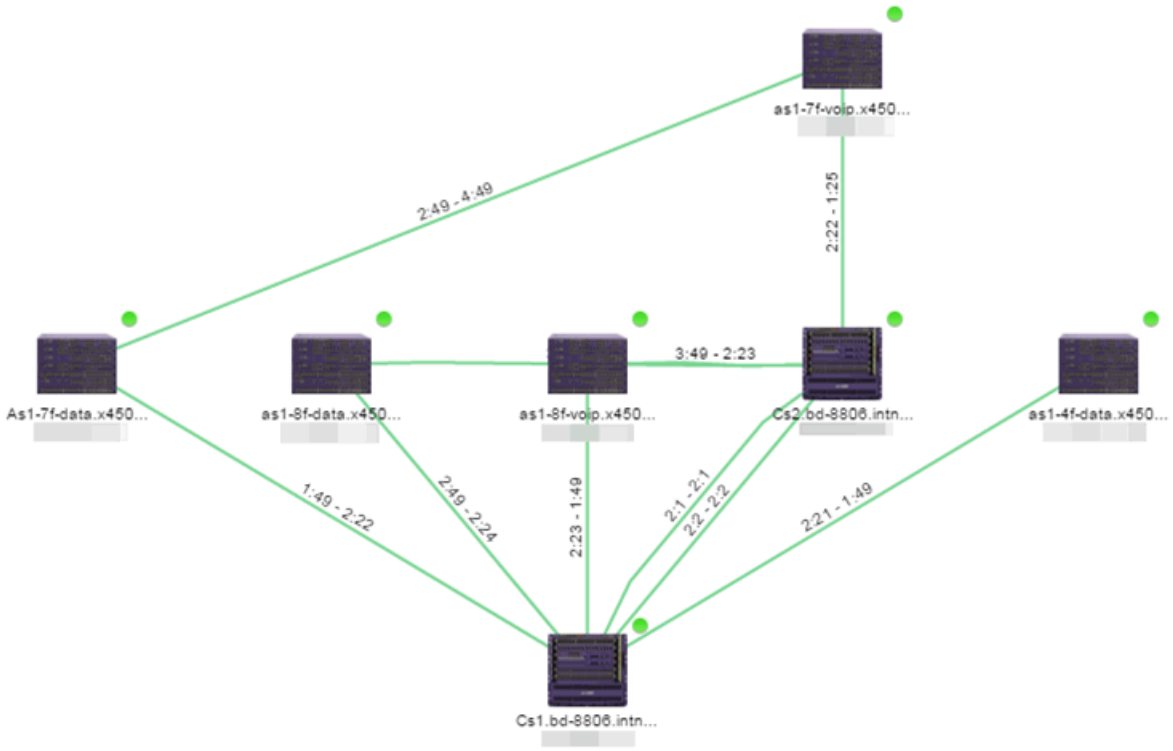
3. Click **File** > **Properties** to open the Map Properties window from which you can edit the map criteria.



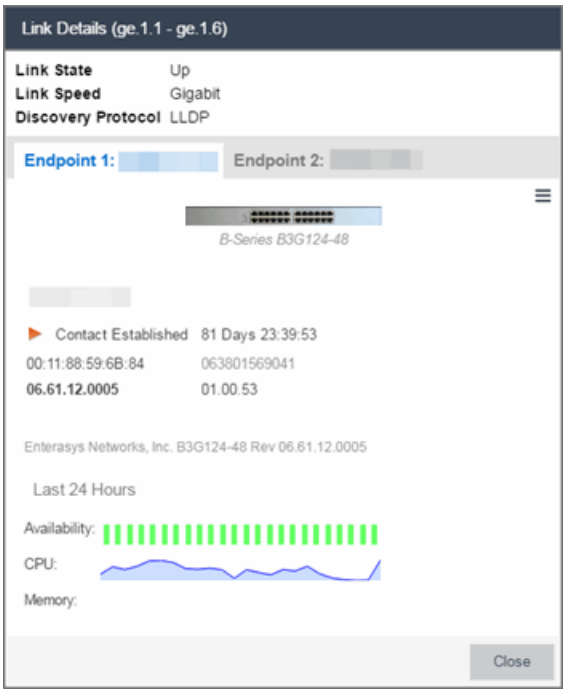
a. In the **Map Name** field, change the name for the map, if necessary.

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

- Topology *(default)* - A topology map shows the state and speed of the network connections between devices as well as the state of the devices in the network.



Double-clicking a connection opens the Link Details window from which you can view additional details about the network connection and the devices it links.



- Topology - Background — Use a custom image to serve as the background of your map. The Map feature supports images in .png, .gif, and .jpg 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 menu to select an image or click the button to open a window where you can select a local image and upload it to the Extreme Management Center 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 — For customers with a NMS-ADV license, use this option to create custom floorplans.

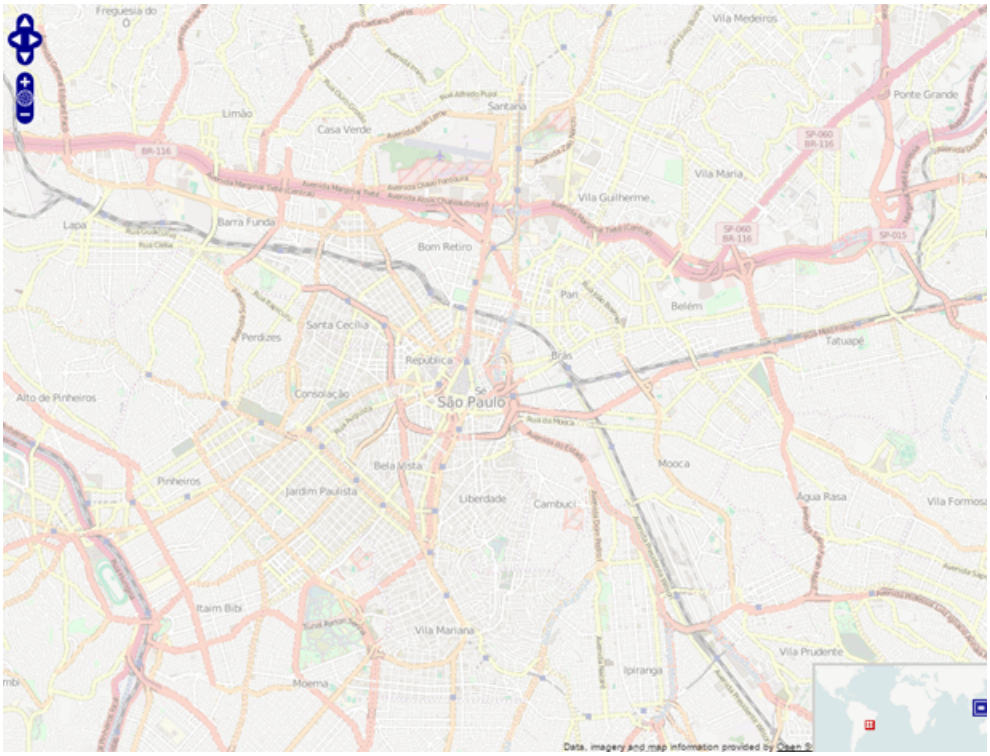
An additional Floor Plan option is available for users with the Extreme Management Center NMS-ADV license.

A **Map Image** field is displayed under the **Environment** field. In the **Map Image** field, use the drop-down menu to select an image or click **Add** (⊕) to open a window where you can select a local image and upload it to the Extreme Management Center server.

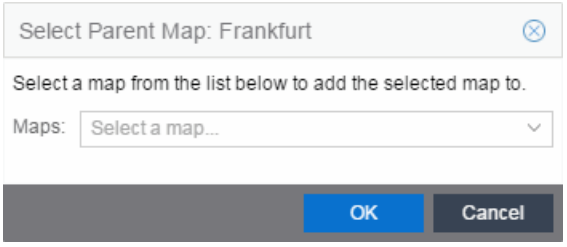
NOTE: If you upload a map image and an image with the same name already exists, the existing image is replaced.

- 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. Click 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 clicking **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 menu in the Add Link To Map window. Click 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 clicking **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. Click **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 click the **Edit** button in the Map Properties panel.

Related Information

- Extreme Management Center Maps
- Advanced Map Features

How to Edit Maps

The Extreme Management Center 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.

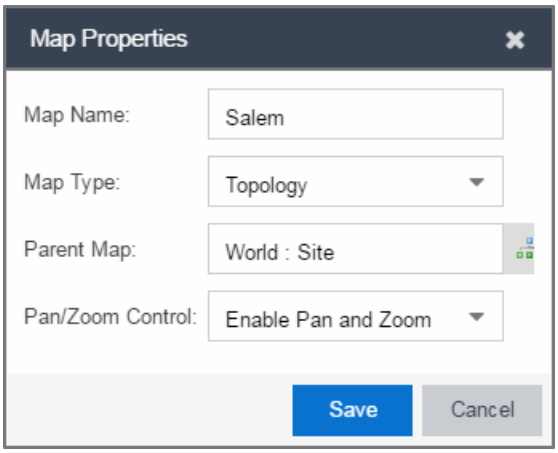
Accessing the Map Tab

1. Launch Extreme Management Center.
2. Click the Network > Devices tab.
3. Select Sites from the left-panel drop-down menu. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.

Editing a Map

To edit a new Device map properties:

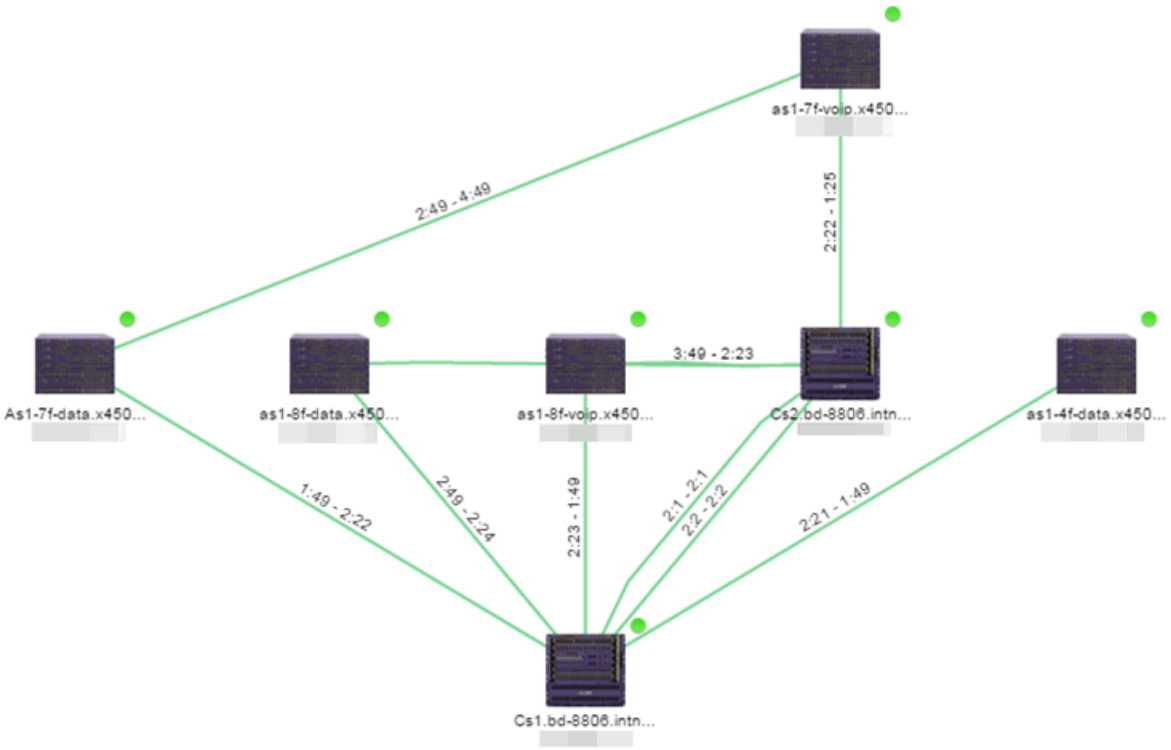
1. Select a new map from the left-panel. The new map is initially blank unless you create it from a device or AP by selecting the device or AP, clicking the Menu icon (≡) or right-clicking the device or AP and selecting Maps > Create Map.
2. Click File > Properties to open the Map Properties window from which you can edit the map criteria.



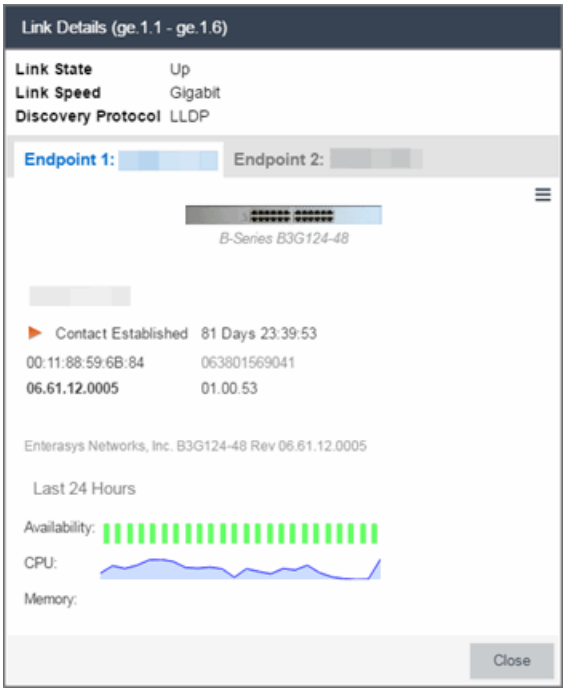
a. In the **Map Name** field, change the name for the map, if necessary.

b. In the **Map Type** drop-down menu, 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, .gif, and .jpg 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 menu to select an image or click the button to open a window where you can select a local image and upload it to the Extreme Management Center 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 — For customers with a NMS-ADV license, use this option to create custom floorplans.

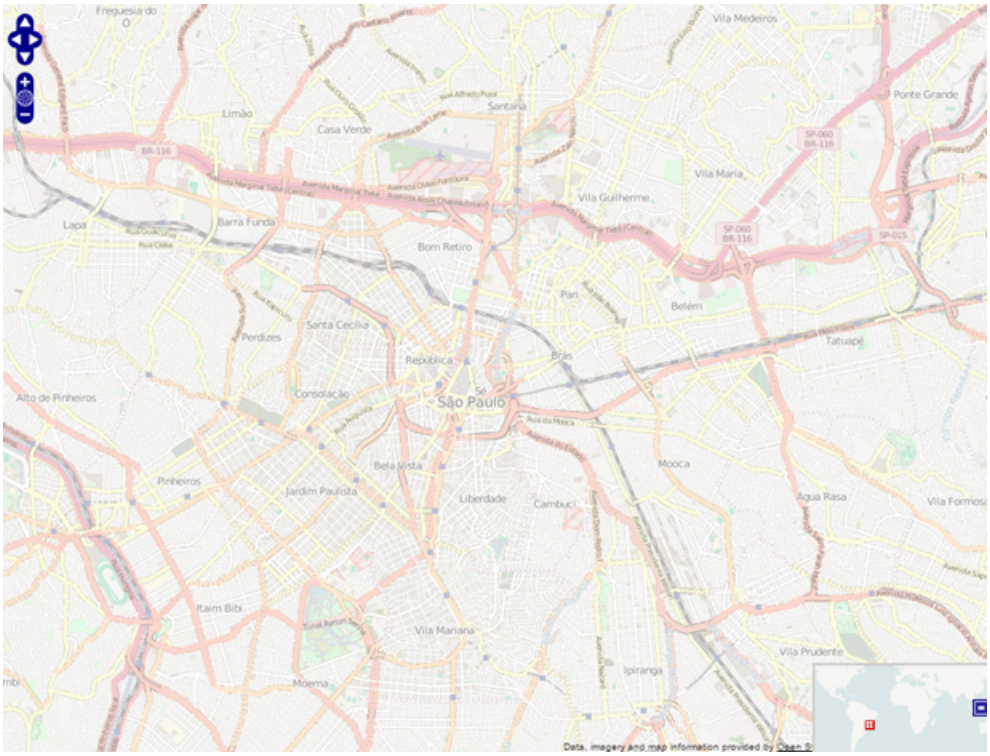
An additional Floor Plan option is available for users with the Extreme Management Center NMS-ADV license.

A **Map Image** field is displayed under the **Environment** field. In the **Map Image** field, use the drop-down menu to select an image or click **Add** () to open a window where you can select a local image and upload it to the Extreme Management Center server.

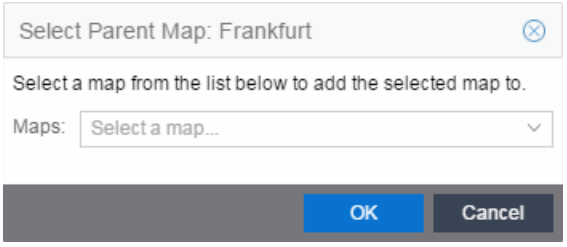
NOTE: If you upload a map image and an image with the same name already exists, the existing image is replaced.

- 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. Click 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. Click 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 menu in the Add Link To Map window. Click 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 clicking 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. Click 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 click the **Edit** button in the Map Properties panel.

Related Information

- Extreme Management Center 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 (available with the NMS-ADV license) include custom floor plan design, triangulated wireless client location, and wireless coverage maps to identify coverage trouble spots for your wireless network.

Overview

Extreme Management Center 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 Application Analytics network locations to display network application flow data in a map.

Prerequisites

Review the following prerequisites for using the Extreme Management Center advanced Map features:

- To access the advanced Map features, the Extreme Management Center server must be running version 6.2 with an Extreme Management Center (NetSight) Advanced license (NMS-ADV).
- In order to create or edit Maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

The following requirements pertain to wireless location and coverage features:

- The ExtremeWireless Controller must be a model C25 or better, running firmware version 8.31 or higher.
- The Location Engine on the wireless controller must be enabled. (For information on how to enable the Location Engine, refer to the *Extreme Networks Wireless Convergence Software User Guide.*)
- The Access Points must be model 37xx, 38xx, or 39xx.

Related Information

For information on related topics:

- Extreme Management Center 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 (available with the NMS-ADV license) 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

Extreme Management Center 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 Application Analytics network locations to display network application flow data in a map.

Prerequisites

Review the following prerequisites for using the Extreme Management Center advanced Map features:

- To access the advanced Map features, the Extreme Management Center server must be running version 6.2 with an Extreme Management Center (NetSight) Advanced license (NMS-ADV).

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

The following requirements pertain to wireless location and coverage features:

- The ExtremeWireless Controller must be a model C25 or better, running firmware version 8.31 or higher.
- The Location Engine on the wireless controller must be enabled. (For information on how to enable the Location Engine, refer to the *Extreme Networks Wireless Convergence Software User Guide.*)
- The Access Points must be model 37xx, 38xx, or 39xx.

Designing a Floorplan

You can design and enhance floorplans of your wired and wireless network environment by editing your maps using the drawing and style tools. These editing tools allow you to create detailed visual representations of your network. You can also use floorplans to provide greater accuracy in the calculation of AP client location and in determining signal strength coverage for the wireless devices on your network.

NOTE: You can only use an AP in one floorplan.

Managed wireless controllers are automatically synchronized to match map floorplan data. If the floorplan data defined in Extreme Management Center maps is not consistent with data on the controller, the controller is updated accordingly.

NOTE: To prevent the automatic synchronization between Extreme Management Center 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

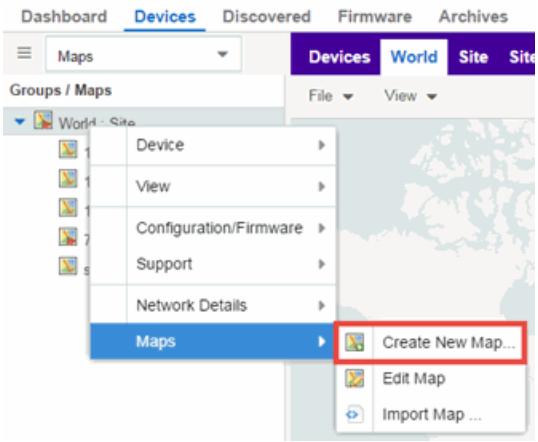
given access point. Extreme Management Center uses the wall information to provide accuracy in determining wireless device signal strength.

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, .gif, and .jpg 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.

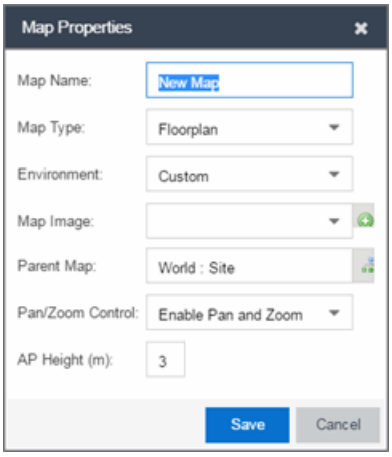
1. Create and configure a new map.
    a. Launch Extreme Management Center and click on the Network > Devices tab.
    b. In the left-panel Groups/Maps navigation tree, right-click on the World map (or any other map that you want as the parent of the new map) and select Maps > Create New Map.



The Create New Map window opens.

c. Enter a name for the Map.

d. Open the Map Properties window by clicking **File** > **Properties**.



e. Change the **Map Type** drop-down menu 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, .gif, and .jpg 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.

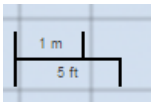
h. Set the **AP Height** property. This value is the distance from the floor to the AP position on the wall or ceiling in meters. This is a single value used for all access points. Setting a reasonable value helps with the accuracy of the location feature. The default for this value is three meters,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

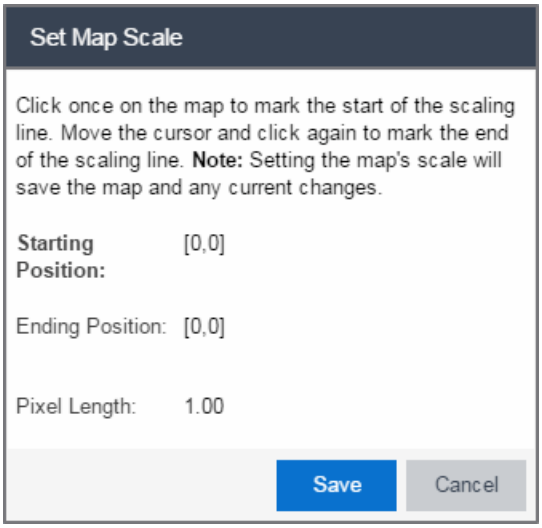
i. Click **Save** to save the map and display the image.

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. Click **File** > **Edit** to open the map in edit mode.

b. Click on 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. Click once on the map to mark the start of the scaling line. Move the cursor and click again to mark the end of the scaling line.
    ii. Enter the line length and units.
d. Click **OK**. The map scale is automatically adjusted and the map is saved.

3. **Draw floorplan walls.** Click 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 menu 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.

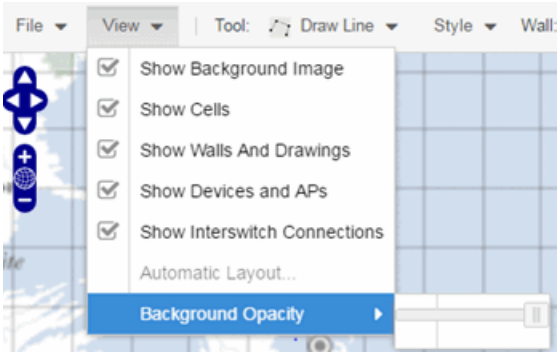
d. Use these same steps to draw the remaining walls on your floorplan. Be sure to deselect the **Exterior** checkbox for the other walls.

   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, click **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.

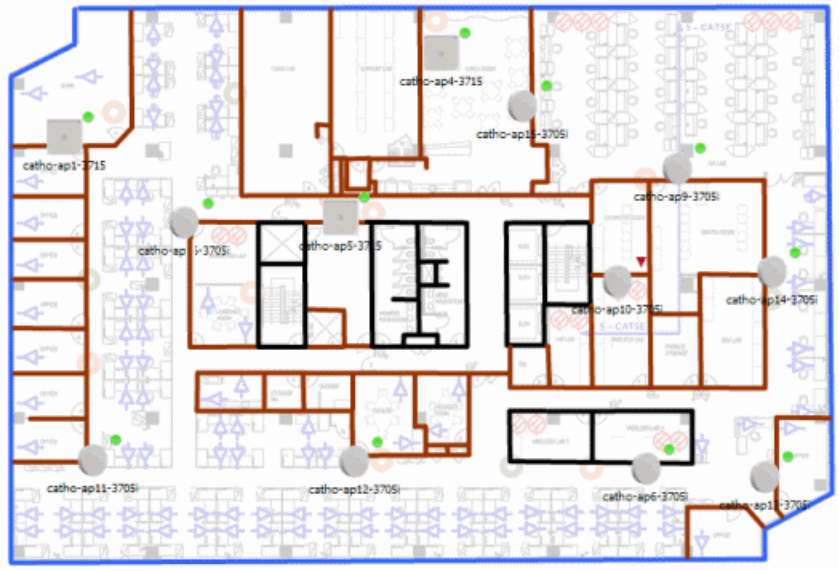
e. While editing, use the **View** menu to select whether to view or hide the background image, map cells, floorplan walls and drawings, devices and APs, and interswitch connections. You can also select an automatic layout and set the background image opacity.



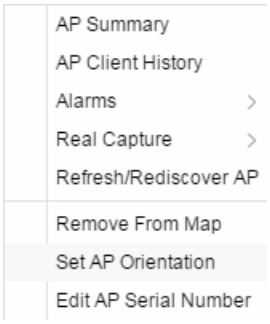
4. **Add your APs to the map.** In Edit mode, a panel that lists equipment available to add to the map is visible beneath the properties panel. The display is filtered on either the currently discovered devices or the APs known to wireless controllers on your network, depending on your selection (APs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

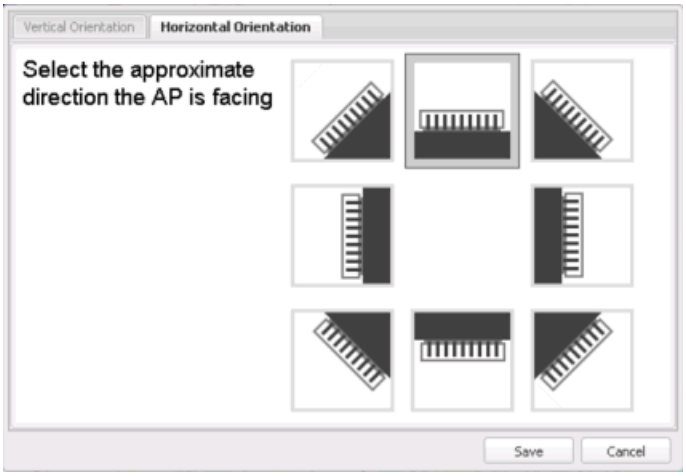


5. Set AP orientation.
    a. Right-click on an AP in the map and select **Set AP Orientation**.



    b. Click on 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. Click **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.

Over AP
Orientation: Wall facing east

6. Click **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 menu 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 Click on 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. Click 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. Click once and draw the first line of the polygon. Click at each corner of the area location. To open the Configure Area window with the Draw Area tool active, double-click the area line. To open the Configure Area window and close the Draw Area tool, right-click the area line.
	Draw Polygon Position your cursor where you want to start drawing the polygon shape. Click once and draw the first line of the polygon. Click at each corner of the polygon. Double-click to release the polygon line. When you are finished drawing, right-click to release the draw polygon tool.

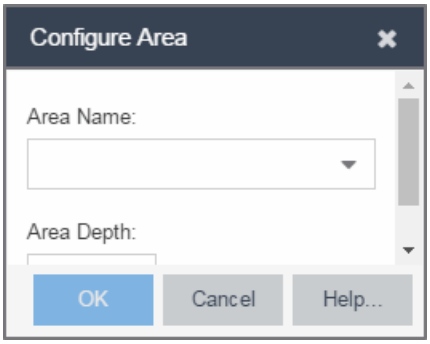
Drawing Tool	Definition
	Draw Rectangle Position the cursor where you want the rectangle. Click and drag to draw the rectangle. When you are finished drawing, right-click to release the draw rectangle tool.
	Add Text Click the map to open the Enter Text window. When you are finished entering your text, click OK. Position the cursor where you want to place the text and click 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. Click 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. Click once and draw the line. Click 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 Click on the shape you want to rotate. Use the blue handle to rotate the shape to the desired position. (You can also right-click on an image and select Rotate Shape from the menu.)
	Set Scale Opens the Set Map Scale window from which you can determine the scale of your map.

Configure Area Window

The Configure Area window, accessible from the Draw Area tool, allows you to name and determine the depth of an area.

- Area Name — The name of the area you are creating.
- Depth — A unique identifier for the area used when two areas overlap. In the event a client is located in a location shared by two areas, the client displays in the area with the higher Depth value.

NOTE: The Depth must be a value of 10 or higher. Values of 1 - 9 are reserved by the system.



Area locations allow you to define up to 16 specific areas per floor on your map to determine whether a client position is inside or outside of each area. Additionally, you can create areas located inside of other areas. A client can only be located in one area at a time and based on the area in which the client is located, you can apply different policies to the client. For example, a client accessing the network from an area located in a classroom may be granted different access than a client accessing the network in an area located in a professor's office.

Style Menu

Use the Style menu to define the characteristics of the walls and other shapes you add to your custom floorplans. Following are definitions of the Style menu options.

Style Option	Description
Font Color	Specify the color of the text added to the map.
Font Size	Specify the size of the text added to the map.
Line Thickness	Specify the thickness of the shape border in pixels.
Line Color	Specify the color used in shape borders.
Line Opacity	Specify the opacity of the shape borders. This allows you to shade the floorplan.
Shape Filled	Select the checkbox to fill shapes with the specified shape color.
Shape Color	Select the color used to fill the shapes you create.
Shape Opacity	Specify the opacity of the shape color.

Wireless Client Location

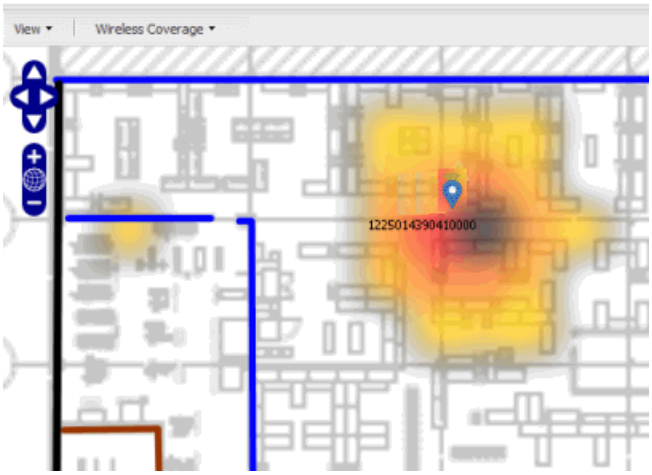
The wireless location feature requires you enable the location engine on the wireless controller. Once you add APs to your custom floorplan and save the map, a copy of the floorplan is sent to each controller. The location engine incorporates information defined in the floorplan data and signal information from a client's contact with APs in order to calculate a client's precise location in the covered area. Client information from within a short time frame must be reported by at least three APs in order to determine a client's triangulated location.

To search for a wireless client, enter a MAC address, IP address, hostname, or user name in the map Search box and press Enter. (The client must be connected to an AP added to a map.)

The map containing the AP is displayed with an icon for the client. A colored distribution of location confidence is shown on the map with black being highest confidence, red medium confidence, and yellow lowest confidence. You can use the Min. Location Confidence slider on the View menu to filter out lower confidence colors. As you drag the slider, colors below the selected confidence level are no longer displayed. If you set the slider to the right-most point, only black is displayed.

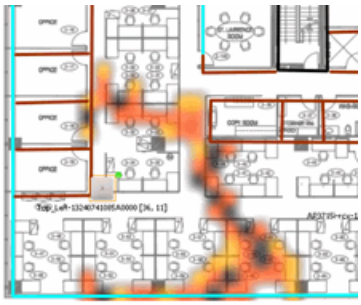
Mouse over the client icon to see a tooltip with client information.

NOTE: The tooltip information is based on current data from the wireless domain unless the client icon displays a clock in the center. In that case, the tooltip information is based on historic data from the Wireless > Clients tab and the confidence colors are not displayed.

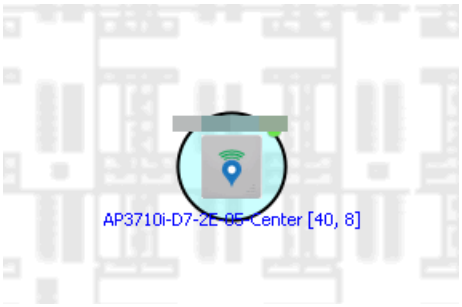


If the location result is based on only one AP, the map displays probabilities for the location but with a few differences:

- No client icon is displayed.
- The location confidence distribution area is larger and generally displayed in a circular pattern.
- The associated AP is highlighted.
- The distance is shown beside the confidence legend at the foot of the map.



If there is insufficient data to provide triangulated results, the map displays the AP in the center, with a circle showing the possible area where the client may be located, based on the client's RSS (Received Signal Strength).



Time-Lapse Location

The wireless location feature provides the ability to view time-lapse location coverage for a client, using historic triangulated location results. This allows you to understand a wireless client's movement through the network and provides for better network troubleshooting.

When a current triangulated location search result displays, a checkbox is available in the upper right corner to enable time-lapse location.

When the checkbox is selected, a set of controls appears to the left of the checkbox, indicating the date of the displayed result. If there are historic events available, the Rewind arrow is enabled and you can scroll through the history. Note that for a historic location, the client icon displays a small clock inside it.

The Rewind and Fast-Forward arrows are disabled if there is no more history in that direction. After viewing historic locations, if you fast forward to the current location and it changed, the location updates.

Wireless Coverage

After you finish your custom floorplan and saved the map, the map is ready to display wireless coverage information. Select View > Wireless Coverage > Show Coverage to show wireless coverage of the APs on the map and to enable the wireless coverage options. Use the View > Wireless Coverage menu available at the top of the map to select from the following coverage display options.

- Mode — Select from the different options for coverage display:
  - Signal Strength— Use this mode to view AP signal strength. Set the Band, Access Points, and Minimum RSS options.
  - Channel Coverage — Use this mode to view channel coverage and AP health. Set the Select Channel, Band, and Access Points options. This mode provides a

graphical overview of channel allocation, helping to visualize radio management issues or locate potential interference.

- Data Rate — This mode shows a coverage map indicating the expected physical rate for all of the cells on the floor. Set the Minimum Physical Rate, Band, and Access Points options. Use this mode to ensure proper wireless performance throughout the network.

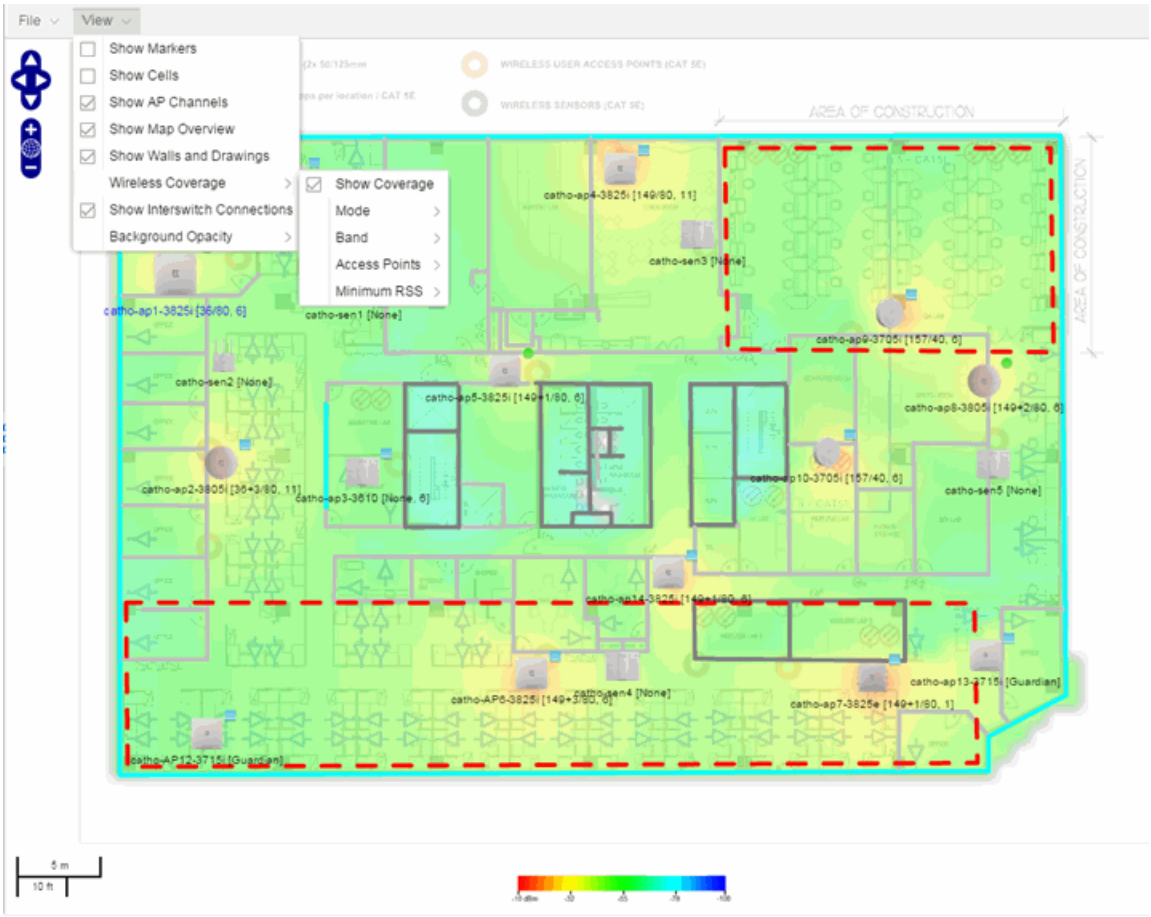
NOTE: Wireless coverage maps are divided into cells. Each cell displays a signal strength with which it is associated, used to determine wireless coverage and the location probability of a user.

- Location Readiness — Use this mode to view the expected quality of location search results for each map cell, given the current placement of APs. Colors denote readiness for each cell:
  - Green — Good readiness. There are four or more APs with visibility of the cell, with at least three of them within 20 meters.
  - Yellow — Moderate readiness. There are three APs with visibility of the cell, with at least two within 20 meters.
  - Orange — Poor readiness. There are less than three APs with visibility of the cell.
  - Red — No triangulation. Only Cell of Origin location results are available in this area.

- Select Channel — Used to select the channels to view for Channel Coverage mode. If "All" is selected, each distinct channel is assigned a color as shown in the legend at the foot of the map, and the color brightness varies to indicate coverage intensity. Selecting a single channel shows a coverage map for that one channel's signal strength and displays a Channel Health window that shows the average and maximum utilization and noise levels for each applicable AP.
  - Utilization — The percentage of busy time for the channel during the last 100 seconds. A channel is busy either because of an interference with energy above a threshold (-62dBm) or because of an active transmission of other stations or APs. This is an indicator of the congestion and interference on the channel.
  - Noise — The noise floor measured by the AP on the 802.11 channel over the last 30 seconds. Noise floor is measured during the quiet time, between the valid transmission or reception of 802.11 frames.

- Min. Physical Rate — Used for Data Rate mode to set the minimum physical rate to display. A legend for the Physical Rate by color is visible at the bottom of the map.
- Band — Select the desired band (radio frequency).
- Access Points — Select which access points to include. These buttons allow you to select or deselect all APs. This option also contains a checkbox that allows you to use default values if a radio is off. When this checkbox is selected, you can view an estimate of coverage using default values; otherwise, no coverage is shown.
- Minimum RSS — Used to set the minimum RSS to display (default is -80) for Signal Strength mode. A legend for the RSS by color is visible at the bottom of the map.

Once 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 Extreme Management Center floorplan maps. The map export function exports floorplan maps to a ZIP file.

Importing Maps

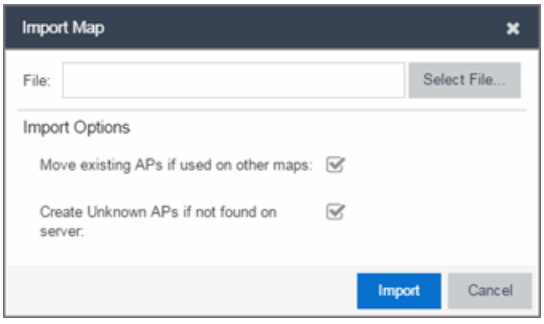
The map import function gives you the ability to import Ekahau maps into Extreme Management Center floorplan maps and gives you the ability to import floorplan maps are previously exported from Extreme Management Center maps.

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 Extreme Management Center, each Ekahau map is re-created into an individual map again.

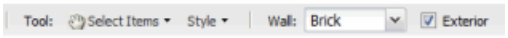
When a map is imported, it is added as a child map of the World map. If the map's name is not unique, a number is appended to the end of the name. After the map is imported it can be moved and renamed, if desired.

To import a map:

1. Launch Extreme Management Center and click on the Network > Devices tab.
2. In the left-panel, select Maps from the drop-down menu.
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 Extreme Management Center, a placeholder AP is created. Once 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. Click 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 click Edit to edit the map.
   b. Click on the exterior wall and then select the Exterior checkbox. This designates the wall as an exterior wall.



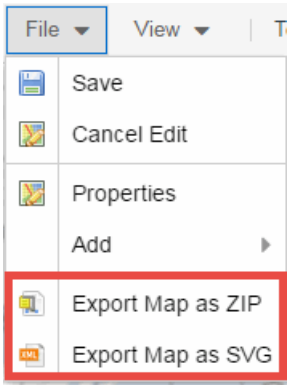
   c. Click Save to save the map.

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 Extreme Management Center and click on 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. Click 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.

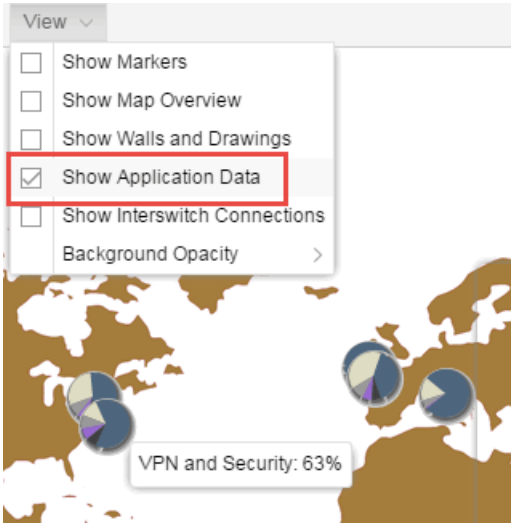
NOTE: The Export Map as ZIP option is only available for Floorplan map types.

Show Application Data

You can display application data in maps by creating map links tied to Application Analytics network locations. Application data for the location tied to the link displays in the map.

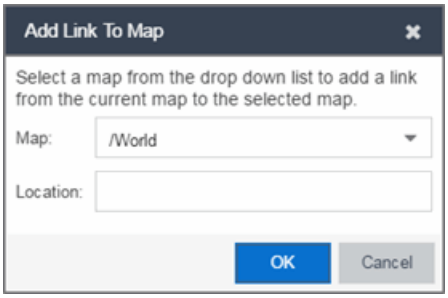
When the Show Application Data checkbox in the View menu is selected, a pie chart is generated for every map link on the current map. The application data in the pie chart is based on the Location field specified for the link and corresponds to a network location defined in the Application Analytics feature. For more information on network locations, see the section on Network Locations in the Application Analytics user guide.

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 click **File** > **Edit** in the map properties panel.
2. The map's property panel opens in Edit mode. Click **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 network location defined in Application Analytics and click **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. Click 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

- Extreme Management Center 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 (available with the NMS-ADV license) 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 Extreme Management Center maps is not consistent with data on the controller, the controller is updated accordingly.

NOTE: To prevent the automatic synchronization between Extreme Management Center 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. Extreme Management Center uses the wall information to provide accuracy in determining wireless device signal strength.

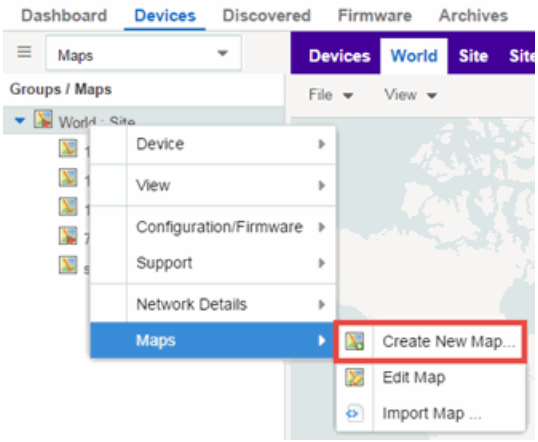
A floorplan can be created with or without a reference background image; however it is much easier to use the drawing features with an existing image. (The Map feature supports images in .png, .gif, and .jpg formats.) For example, you can trace the outline of a floorplan image using the drawing tools 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.

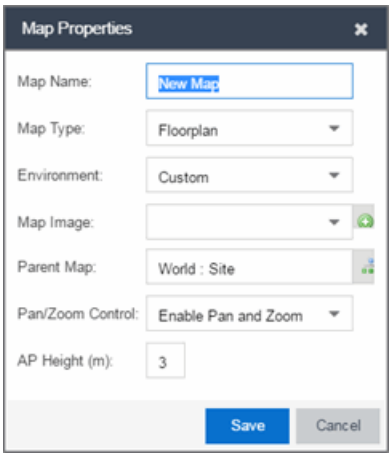
1. Create and configure a new map.
    a. Launch Extreme Management Center and click on the **Network** > **Devices** tab.
    b. In the left-panel Groups/Maps navigation tree, right-click on the World map (or any other map that you want as the parent of the new map) and select **Maps** > **Create New Map**.



The Create New Map window opens.

    c. Enter a name for the Map.

d. Open the Map Properties window by clicking **File** > **Properties**.



e. Change the **Map Type** drop-down menu 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, .gif, and .jpg 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.

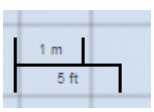
h. Set the **AP Height** property. This value is the distance from the floor to the AP position on the wall or ceiling in meters. This is a single value used for all access points. Setting a reasonable value helps with the accuracy of the location feature. The default for this value is three meters,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

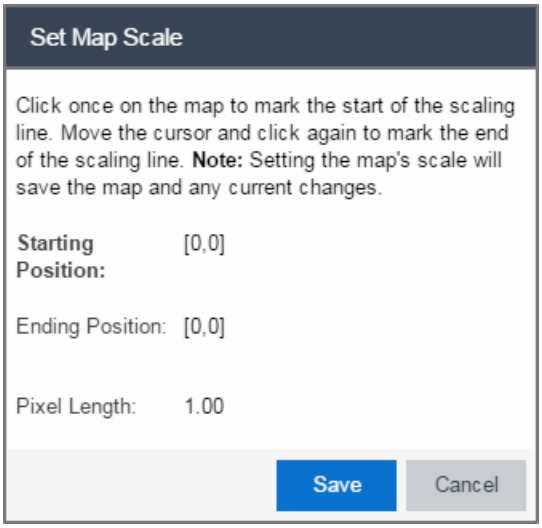
i. Click **Save** to save the map and display the image.

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. Click **File** > **Edit** to open the map in edit mode.

b. Click on 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. Click once on the map to mark the start of the scaling line. Move the cursor and click again to mark the end of the scaling line.

   ii. Enter the line length and units.

d. Click **OK**. The map scale is automatically adjusted and the map is saved.

3. **Draw floorplan walls.** Click 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 menu 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.

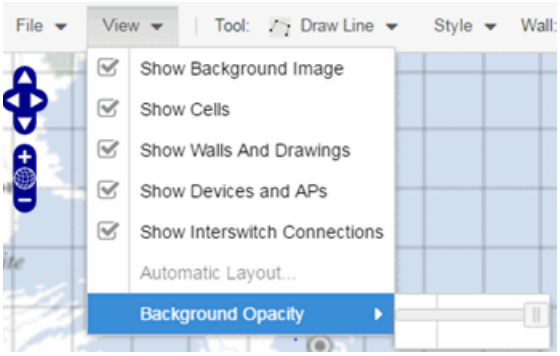
d. Use these same steps to draw the remaining walls on your floorplan. Be sure to deselect the **Exterior** checkbox for the other walls.

   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, click **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.

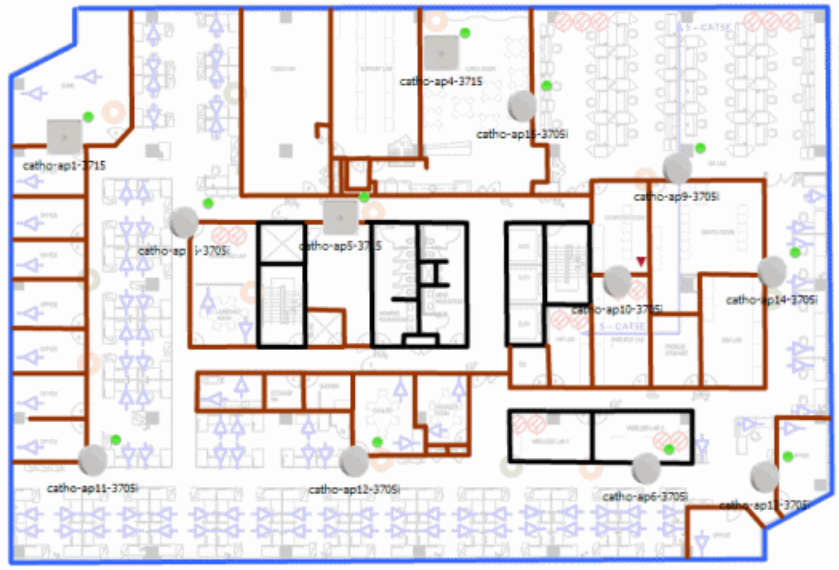
e. While editing, use the **View** menu to select whether to view or hide the background image, map cells, floorplan walls and drawings, devices and APs, and interswitch connections. You can also select an automatic layout and set the background image opacity.



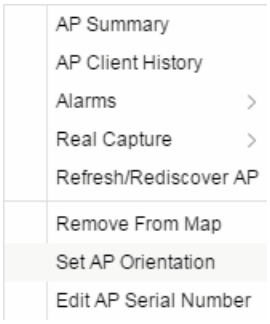
4. **Add your APs to the map.** In Edit mode, a panel that lists equipment available to add to the map is visible beneath the properties panel. The display is filtered on either the currently discovered devices or the APs known to wireless controllers on your network, depending on your selection (APs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

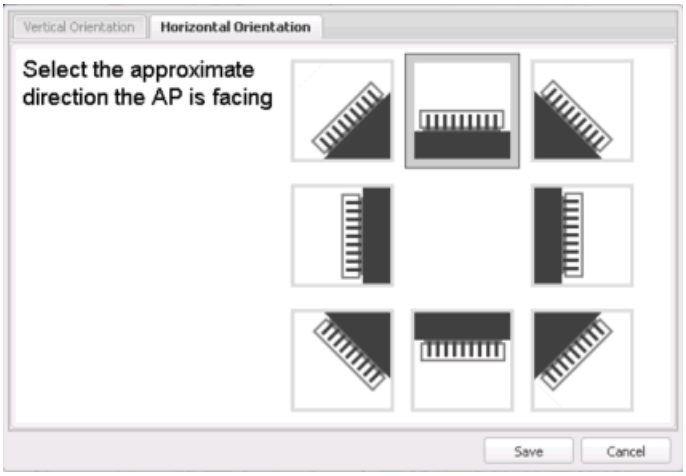


5. Set AP orientation.
    a. Right-click on an AP in the map and select **Set AP Orientation**.



    b. Click on 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. Click **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.

Over AP
Orientation: Wall facing east

6. Click **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 menu 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 Click on 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. Click 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. Click once and draw the first line of the polygon. Click at each corner of the area location. To open the Configure Area window with the Draw Area tool active, double-click the area line. To open the Configure Area window and close the Draw Area tool, right-click the area line.
	Draw Polygon Position your cursor where you want to start drawing the polygon shape. Click once and draw the first line of the polygon. Click at each corner of the polygon. Double-click to release the polygon line. When you are finished drawing, right-click to release the draw polygon tool.

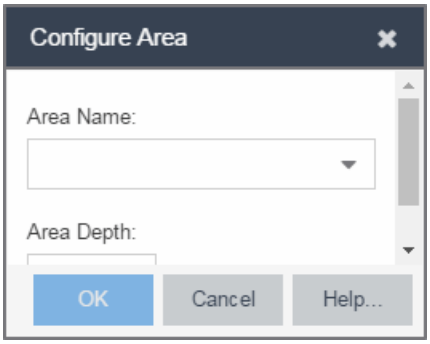
Drawing Tool	Definition
	Draw Rectangle Position the cursor where you want the rectangle. Click and drag to draw the rectangle. When you are finished drawing, right-click to release the draw rectangle tool.
	Add Text Click the map to open the Enter Text window. When you are finished entering your text, click **OK**. Position the cursor where you want to place the text and click 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. Click 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. Click once and draw the line. Click 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 Click on 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

- Extreme Management Center Maps
- Advanced Map Features

How to Add Devices and APs to Maps

Adding Devices/APs from Extreme Management Center Devices and Wireless

Using the Extreme Management Center 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 Extreme Management Center **Network** and **Wireless** tabs. You can add them to a specific map, or create new maps based on device or AP system location.

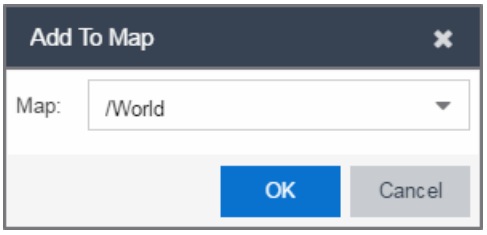
In order to edit maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

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 menu 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, click 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 menu to select the desired map. Click **OK** to add the devices or APs to the map.



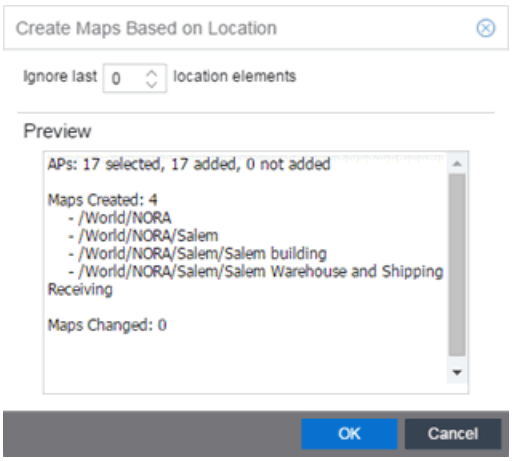
4. Open the Maps page and select the map to which you added the devices. Right-click on the map and select **Edit Map**. You can now position the devices as desired.
5. Click the **Save** button to save the device to the map.

Add to New Maps Based on Location

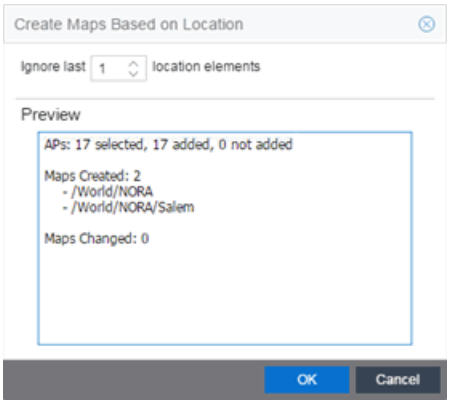
Use these steps to add devices or APs to new maps based on well-named system locations that reflect the desired map structure. For example, if your devices are assigned system locations according to the following structure: US/Boston/Third Floor/Closet One/Rack One/Shelf One, typically, a map would be 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, click on 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. Click **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. Click the **Save** button to save the devices/APs to the map.

Related Information

- Extreme Management Center Maps
- Advanced Map Features

How to Display Map Application Data

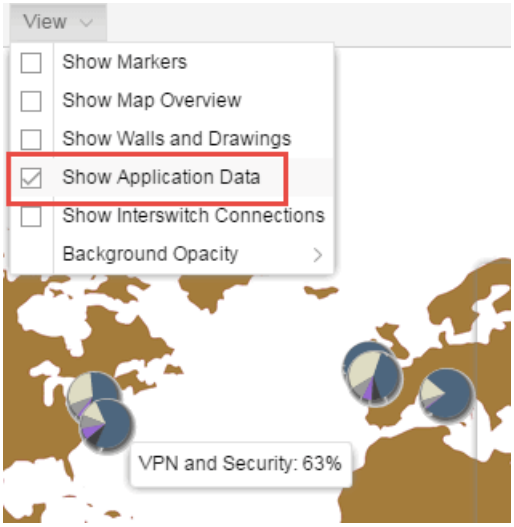
The Network > Devices tab contains Map features that let you create geographic and topological maps of the devices and floor plans of wireless access points (APs) on your network. The advanced Map features (available with the NMS-ADV license) allows you to display application data in maps by creating map links tied to ExtremeAnalytics network locations. Application data for the location tied to the link displays in the map.

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 Location field specified for the link and corresponds to a network location defined in the ExtremeAnalyticsfeature. For more information on network locations, see the section on Network Locations in the ExtremeAnalytics user guide.

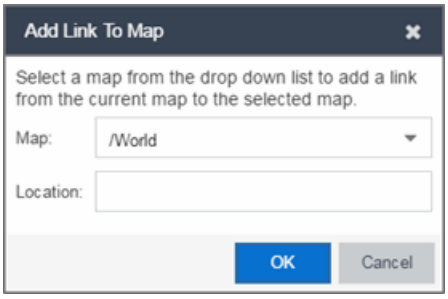
The pie chart displays the top five application groups (by bytes transferred) for the location specified for the map link.

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 click **File** > **Edit** in the map properties panel.
2. The map's property panel opens in Edit mode. Click **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 network location defined in ExtremeAnalytics and click **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. Click 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:

- Extreme Management Center Maps
- Advanced Map Features

How to Use Maps to Locate Wireless Clients

The **Network** > **Devices** tab in the Extreme Management Centercontains 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 (available with the NMS-ADV license) 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. Once 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 Extreme Management Center.
2. In the SearchNetwork box, click Advanced .
3. Enter the MAC Address, IP Address, hostname, user name, AP serial number or Extreme Access Control 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.

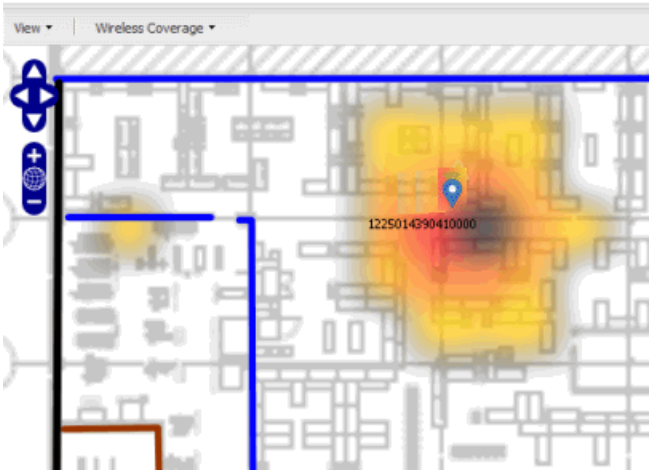
5. On the View tab, use the Min. Location Confidence slider to filter out lower confidence colors:

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.

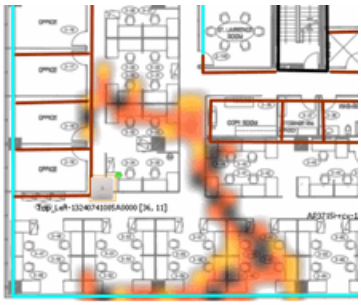
6. Mouse over the client icon to see a tooltip with client information.

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.

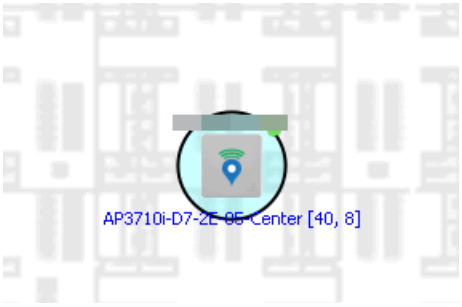


If the location result is based on only one AP, the map displays probabilities for the location but with a few differences:

- 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. Click 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. Click the left arrow to rewind.

b. Click 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:

- Extreme Management Center 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 (available with the NMS-ADV license) include wireless coverage maps to identify coverage trouble spots for your wireless network.

Wireless Coverage

After you finish your custom floor plan and save the map, the map is ready to display wireless coverage information.

1. Select View > Wireless Coverage > Show Coverage to show wireless coverage of the APs on the map and to enable the wireless coverage options.
2. Use the View > Wireless Coverage menu available at the top of the map to select from the following coverage display options.
    - Mode — Select from the different options for coverage display:
        - Signal Strength— Use this mode to view AP signal strength. Set the Band, Access Points, and Minimum RSS options.
        - Channel Coverage — Use this mode to view channel coverage and AP health. Set the Select Channel, Band, and Access Points options. This

mode provides a graphical overview of channel allocation, helping to visualize radio management issues or locate potential interference.

- Data Rate — This mode shows a coverage map indicating the expected physical rate for all of the cells on the floor. Set the Minimum Physical Rate, Band, and Access Points options. Use this mode to ensure proper wireless performance throughout the network.

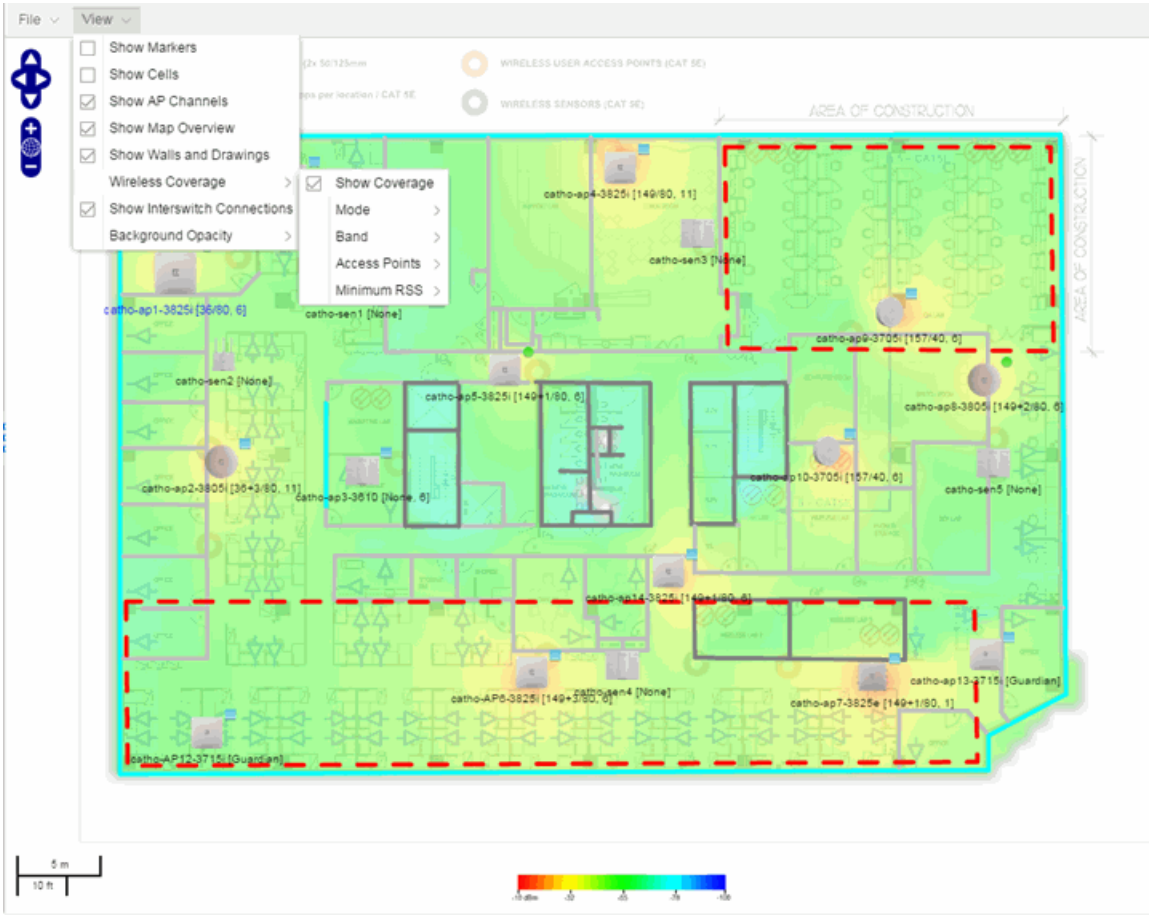
NOTE: Wireless coverage maps are divided into cells. Each cell displays a signal strength with which it is associated, used to determine wireless coverage and the location probability of a user.

- Location Readiness — Use this mode to view the expected quality of location search results for each map cell, given the current placement of APs. Colors denote readiness for each cell:
    - Green — Good readiness. There are four or more APs with visibility of the cell, with at least three of them within 20 meters.
    - Yellow — Moderate readiness. There are three APs with visibility of the cell, with at least two within 20 meters.
    - Orange — Poor readiness. There are less than three APs with visibility of the cell.
    - Red — No triangulation. Only Cell of Origin location results are available in this area.

- Select Channel — Used to select the channels to view for Channel Coverage mode. If "All" is selected, each distinct channel is assigned a color as shown in the legend at the foot of the map, and the color brightness varies to indicate coverage intensity. Selecting a single channel shows a coverage map for that one channel's signal strength and displays a Channel Health window that shows the average and maximum utilization and noise levels for each applicable AP.
    - Utilization — The percentage of busy time for the channel during the last 100 seconds. A channel is busy either because of an interference with energy above a threshold (-62dBm) or because of an active transmission of other stations or APs. This is an indicator of the congestion and interference on the channel.
    - Noise — The noise floor measured by the AP on the 802.11 channel over the last 30 seconds. Noise floor is measured during the quiet time, between the valid transmission or reception of 802.11 frames.

- Min. Physical Rate — Used for Data Rate mode to set the minimum physical rate to display. A legend for the Physical Rate by color is visible at the bottom of the map.
- Band — Select the desired band (radio frequency).
- Access Points — Select which access points to include. These buttons allow you to select or deselect all APs. This option also contains a checkbox that allows you to use default values if a radio is off. When this checkbox is selected, you can view an estimate of coverage using default values; otherwise, no coverage is shown.
- Minimum RSS — Used to set the minimum RSS to display (default is -80) for Signal Strength mode. A legend for the RSS by color is visible at the bottom of the map.

Once these options are set, the map displays the selected coverage information. The following map shows signal strength coverage.



Wireless Map Limits

The following sections provide information about limits for wireless client location and wireless coverage maps.

Active Client Tracking

The number of active clients the location engine on the wireless controller can track simultaneously depends on the wireless controller model. Refer to your wireless controller documentation for information.

Maximum Number of Maps

A wireless controller on which version 10.01.01 or higher is installed can store a maximum of 200 maps. Wireless controllers running a version lower than 10 can store a maximum of 100 maps.

Maximum Number of APs per Floor Plan

A single floor plan allows a maximum of 2,000 APs when version 10.01.01 is installed on the wireless controller. A floor plan with a wireless controller on which a version lower than 10 is installed allows 100 APs.

Related Information

For information on related topics:

- Extreme Management Center Maps
- Advanced Map Features

How to Export Maps

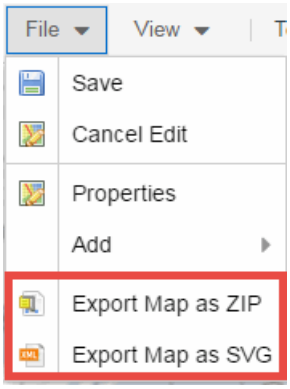
The Extreme Management Center Maps lets you import saved maps of devices and wireless access points (APs) from your local drive or network, and configure the behavior of the imported maps.

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 (available with the NMS-ADV license) 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 Extreme Management Center and click on 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. Click 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

- Extreme Management Center 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 (available with the NMS-ADV license) 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 Extreme Management Center maps is not consistent with data on the controller, the controller is updated accordingly.

NOTE: To prevent the automatic synchronization between Extreme Management Center 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. Extreme Management Center uses the wall information to provide accuracy in determining wireless device signal strength.

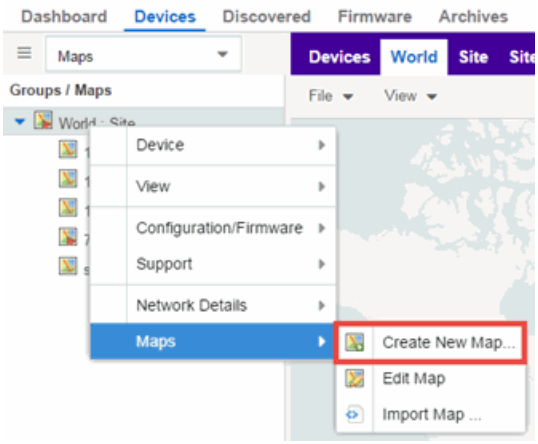
A floorplan can be created with or without a reference background image; however it is much easier to use the drawing features with an existing image.

(The Map feature supports images in .png, .gif, and .jpg 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.

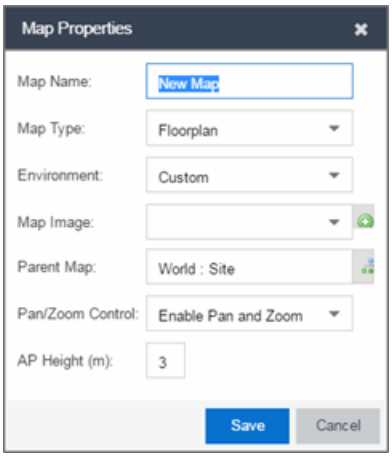
1. Create and configure a new map.
    a. Launch Extreme Management Center and click on the Network > Devices tab.
    b. In the left-panel Groups/Maps navigation tree, right-click on the World map (or any other map that you want as the parent of the new map) and select Maps > Create New Map.



The Create New Map window opens.

    c. Enter a name for the Map.

d. Open the Map Properties window by clicking **File** > **Properties**.



e. Change the **Map Type** drop-down menu 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, .gif, and .jpg 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.

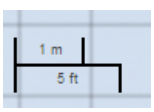
h. Set the **AP Height** property. This value is the distance from the floor to the AP position on the wall or ceiling in meters. This is a single value used for all access points. Setting a reasonable value helps with the accuracy of the location feature. The default for this value is three meters,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

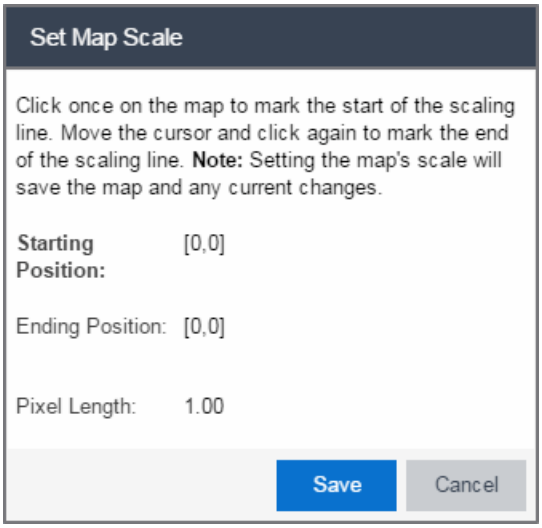
i. Click **Save** to save the map and display the image.

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. Click **File** > **Edit** to open the map in edit mode.

b. Click on 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. Click once on the map to mark the start of the scaling line. Move the cursor and click again to mark the end of the scaling line.
    ii. Enter the line length and units.
d. Click **OK**. The map scale is automatically adjusted and the map is saved.

3. **Draw floorplan walls.** Click 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 menu 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.

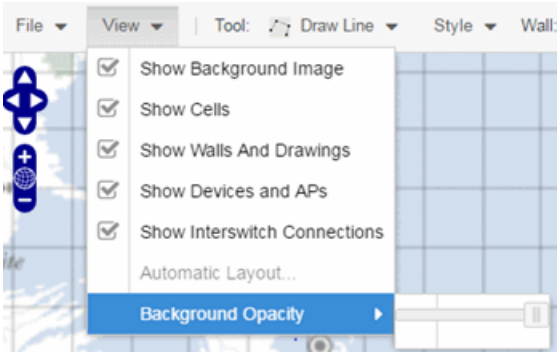
d. Use these same steps to draw the remaining walls on your floorplan. Be sure to deselect the **Exterior** checkbox for the other walls.

   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, click **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.

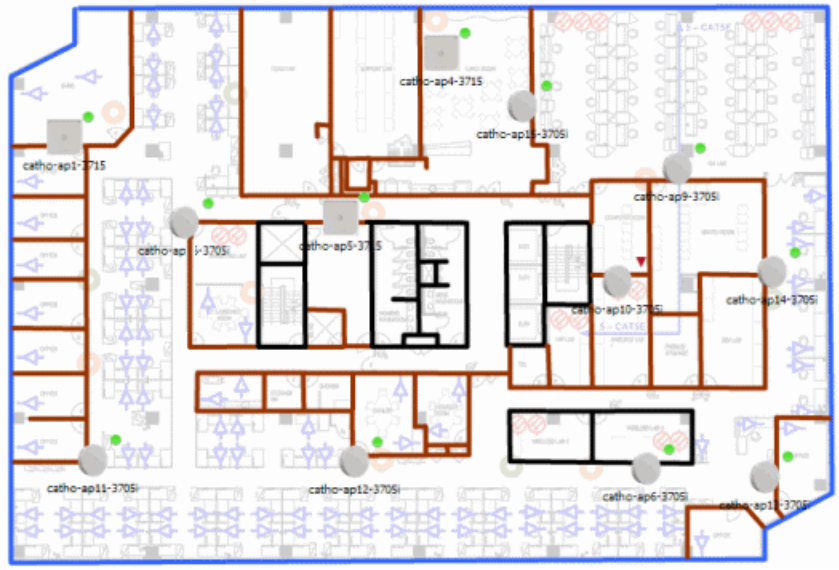
e. While editing, use the **View** menu to select whether to view or hide the background image, map cells, floorplan walls and drawings, devices and APs, and interswitch connections. You can also select an automatic layout and set the background image opacity.



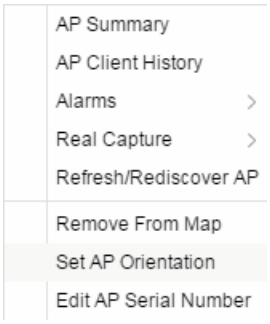
4. **Add your APs to the map.** In Edit mode, a panel that lists equipment available to add to the map is visible beneath the properties panel. The display is filtered on either the currently discovered devices or the APs known to wireless controllers on your network, depending on your selection (APs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

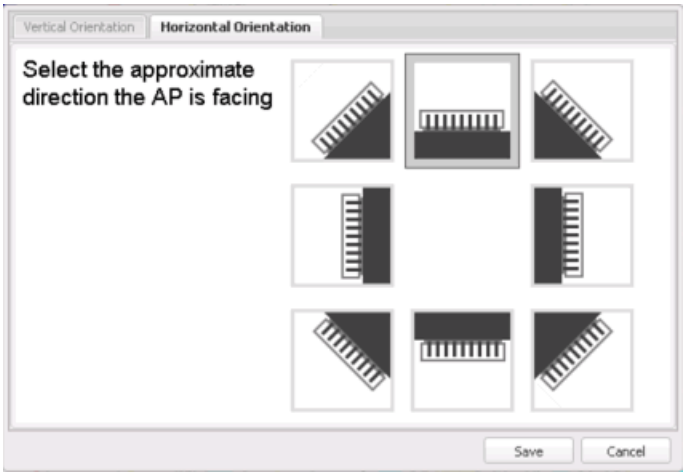


5. Set AP orientation.
    a. Right-click on an AP in the map and select **Set AP Orientation**.



    b. Click on 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. Click **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.

Over AP
Orientation: Wall facing east

6. Click **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 menu 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 Click on 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. Click 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. Click once and draw the first line of the polygon. Click at each corner of the area location. To open the Configure Area window with the Draw Area tool active, double-click the area line. To open the Configure Area window and close the Draw Area tool, right-click the area line.
	Draw Polygon Position your cursor where you want to start drawing the polygon shape. Click once and draw the first line of the polygon. Click at each corner of the polygon. Double-click to release the polygon line. When you are finished drawing, right-click to release the draw polygon tool.

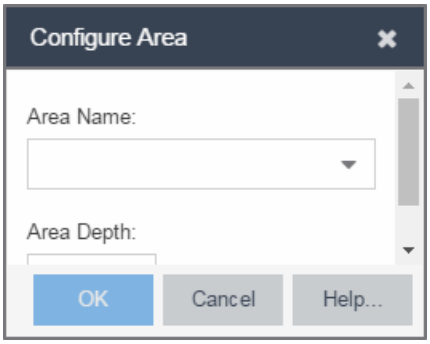
Drawing Tool	Definition
	Draw Rectangle Position the cursor where you want the rectangle. Click and drag to draw the rectangle. When you are finished drawing, right-click to release the draw rectangle tool.
	Add Text Click the map to open the Enter Text window. When you are finished entering your text, click **OK**. Position the cursor where you want to place the text and click 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. Click 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. Click once and draw the line. Click 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 Click on 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

- Extreme Management Center Maps
- Advanced Map Features

How to Export Maps

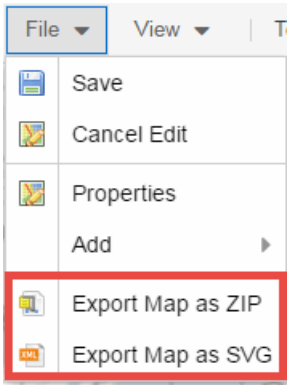
The Extreme Management Center Maps lets you import saved maps of devices and wireless access points (APs) from your local drive or network, and configure the behavior of the imported maps.

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 (available with the NMS-ADV license) 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 Extreme Management Center and click on 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. Click 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

- Extreme Management Center Maps
- Advanced Map Features

Network Details on the Extreme Management Center Map Tab

The Extreme Management Center 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.

Accessing the Map Tab

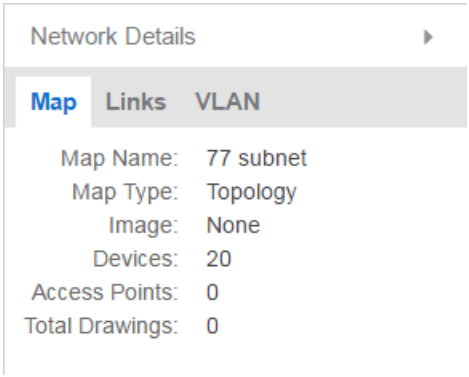
1. Launch Extreme Management Center.
2. Click the **Network** > **Devices** tab.
3. Select **Sites** from the left-panel drop-down menu. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.

Accessing Network Details

1. Right-click the map or map tree in the left-panel.
2. Click **Network Details** from the drop-down menu. 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

NOTE: For an alternate way to access the additional tabs:

1. Click Network > Devices
2. Click 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:

- Extreme Management Center Maps
- Advanced Map Features

Accessing the EAPS tab in Network Details on the Extreme Management Center Map Tab

The Extreme Management Center 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.

Accessing the Map Tab

1. Launch Extreme Management Center.
2. Click the Network > Devices tab.
3. Select Sites from the left-panel drop-down menu. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.

Accessing Network Details

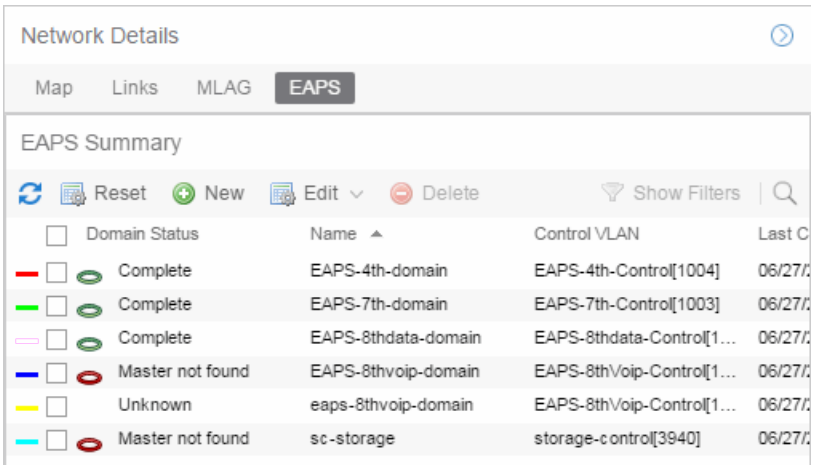
1. Right-click a map or map tree in the left-panel.
2. Select Network Details from the drop-down menu.
3. Select EAPS Summary.

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

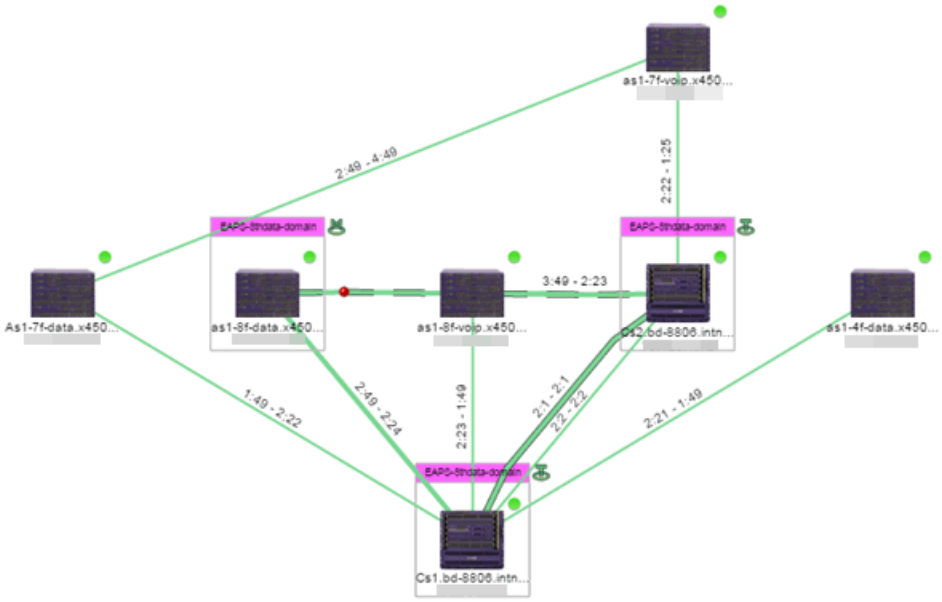
1. Click Network > Devices.
2. Click the second tab of the open Devices window, which is the Map Tab for the map you selected.
3. The EAPS tab will be included in the Network Details panel at the far right of the open Devices window.

EAPS Summary Tab

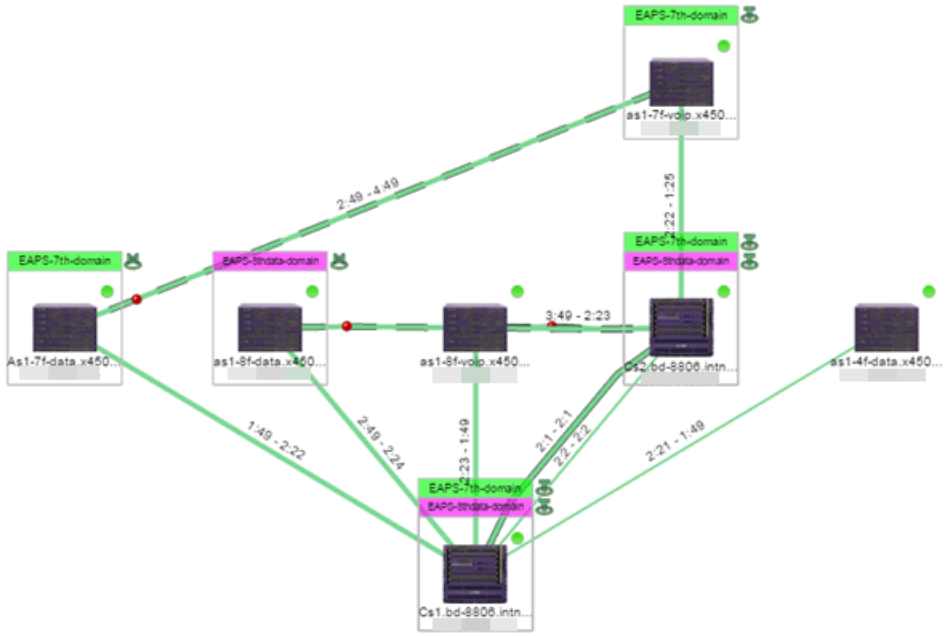
The EAPS Summary tab displays a list of the EAPS domains, including their status, name, the control VLAN name, and the IP addresses of the devices utilizing the EAPS domain.



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.

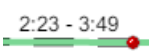


An icon next to the title bar indicates if the node is a master node, indicated by an "M" icon, or if the node is a transit node, indicated by a "T" icon.

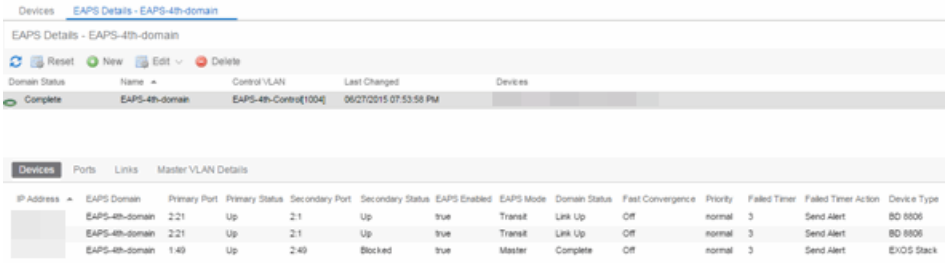
The color of the ring icon indicates the status of the domain:

- 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.

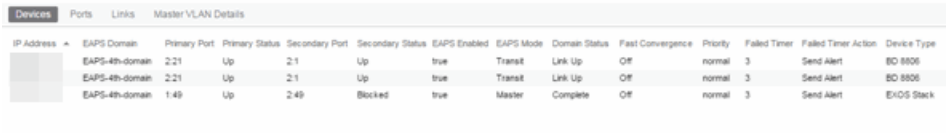


You can view additional details about the EAPS domain by right-clicking an EAPS domain on the **EAPS** tab and selecting **EAPS Details** to open the EAPS Detail view.

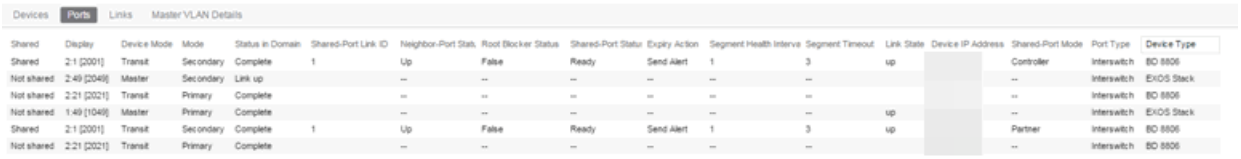


The top of the EAPS Details view displays a summary of the EAPS domain, identical to the information displayed in the EAPS tab. At the bottom of the window are three sub-tabs, which display additional information:

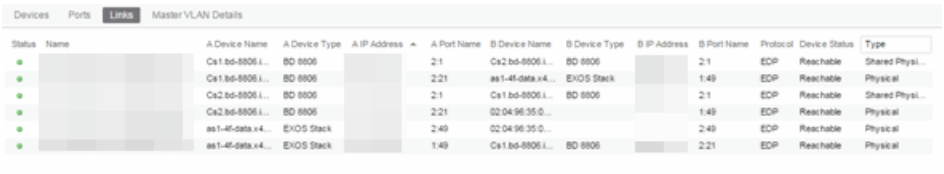
- Devices — Displays information about the devices using the EAPS domain.



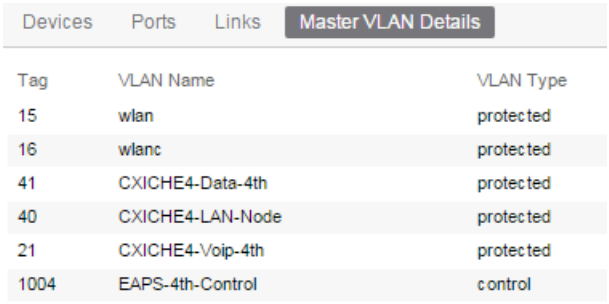
- Ports — Displays information about the shared ports associated with the EAPS domain.



- Links — Displays links between devices using the EAPS domain.



- Master VLAN Details — Displays details about the master VLAN associated with the EAPS domain.



Clicking 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:

- Extreme Management Center Maps
- Advanced Map Features

Accessing the Link Tab in Network Details on the Extreme Management Center Map Tab

The Extreme Management Center 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 Link Summary tab displays information about the network connections between devices.

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 the Map Tab

1. Launch Extreme Management Center.
2. Click the **Network** > **Devices** tab.
3. Select **Sites** from the left-panel drop-down menu. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.

Accessing Network Details

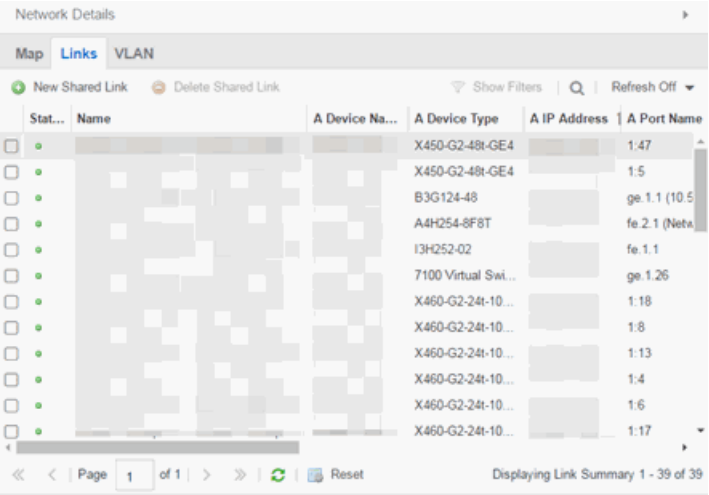
1. Right-click a map or map tree in the left-panel.
2. Select **Network Details** from the drop-down menu.
3. Select **Link Summary**.

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

1. Click **Network > Devices**.
2. Click 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.

Link Summary tab

The **Link Summary** 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 Link Summary 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:

- Extreme Management Center Maps
- Advanced Map Features

Accessing the VLAN tab in Network Details on the Extreme Management Center Map Tab

---

The Extreme Management Center 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 VLAN tab Lists any virtual local area networks within the map.

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 the Map Tab

1. Launch Extreme Management Center.
2. Click the Network > Devices tab.
3. Select Sites from the left-panel drop-down menu. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.

Accessing Network Details

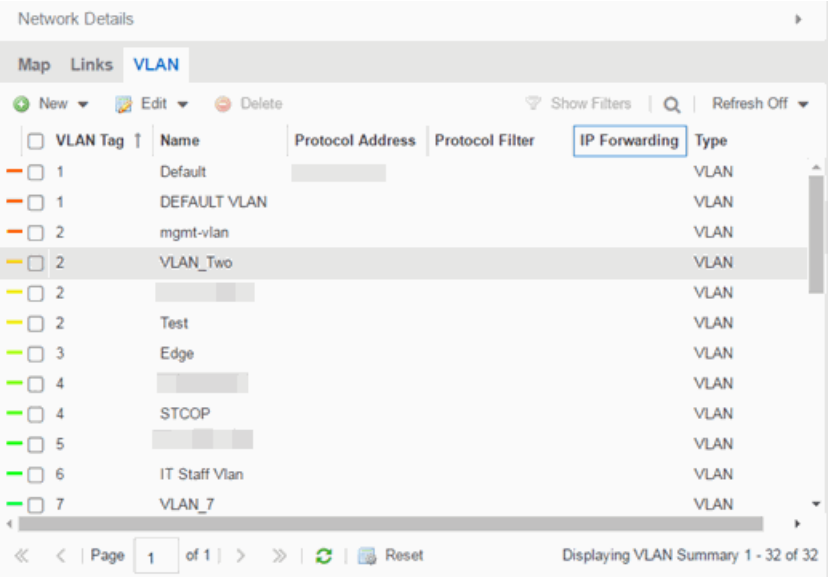
1. Right-click a map or map tree in the left-panel.
2. Select Network Details from the drop-down menu.
3. Select VLAN Summary.

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

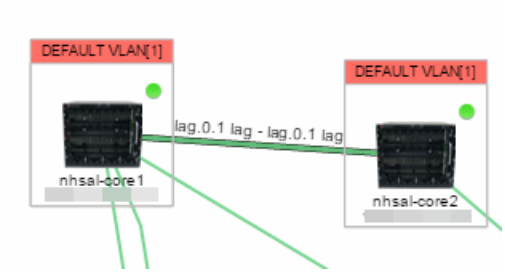
1. Click Network > Devices.
2. Click the second tab of the open Devices window, which is the Map Tab for the map you selected.
3. The VLAN tab will be included in the Network Details panel at the far right of the open Devices window.

VLAN Summary tab

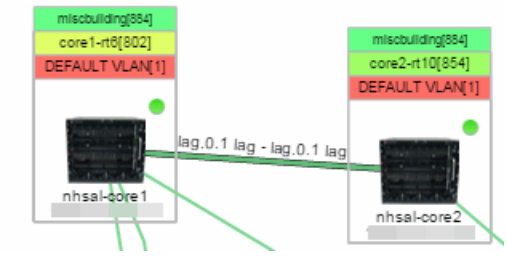
The VLAN Summary tab displays VLANs configured as part of devices included in the map. Columns in the VLAN tab provide additional information, including the VLAN tag, the name of the VLAN, any protocol filters applied for devices on which the VLAN is configured, and whether or not IP forwarding is enabled 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 menu. You can edit the ports, name, and devices associated with an existing VLAN via the **Edit** drop-down menu.

Related Information

For information on related topics:

- Extreme Management Center Maps
- Advanced Map Features

Accessing the MLAG tab in Network Details on the Extreme Management Center Map Tab

The Extreme Management Center 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 **MLAG** tab lists devices configured in a multi-switch link aggregation group.

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 the Map Tab

1. Launch Extreme Management Center.
2. Click the **Network** > **Devices** tab.
3. Select **Sites** from the left-panel drop-down menu. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.

Accessing Network Details

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

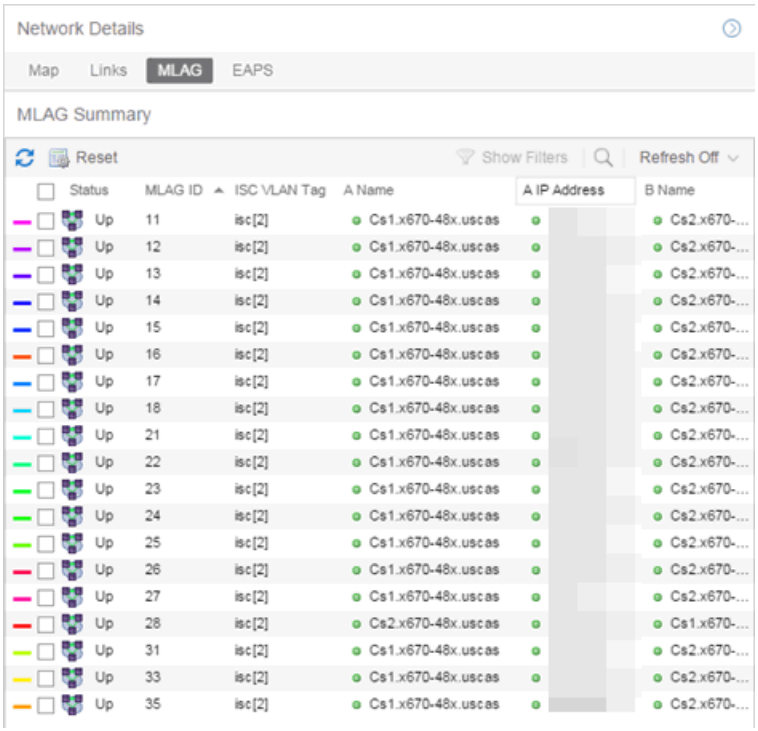
3. Select **MLAG Summary**.

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

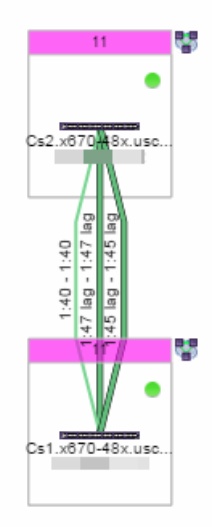
1. Click **Network > Devices**.
2. Click the second tab of the open **Devices** window, which is the **Map Tab** for the map you selected.
3. The **MLAG** tab will be included in the **Network Details** panel at the far right of the open **Devices** window.

MLAG Summary tab

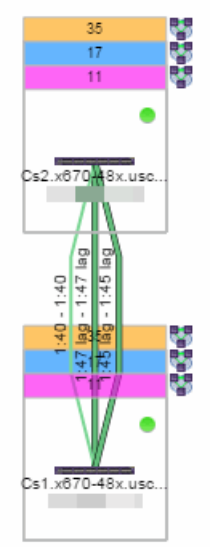
The **MLAG** Summary tab provides a list of the MLAGs (ports combined as a common logical connection on devices) included in the map. The list provides the MLAG's status, ID, ISC VLAN tag, the names and addresses of the devices configured as part of the MLAG, and the ports on those devices assigned as part of the MLAG. Additionally, the Connected IP column displays the IP of the switch to which the MLAG is connected.



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:

- Extreme Management Center Maps
- Advanced Map Features

Accessing the VPLS tab in Network Details on the Extreme Management Center Map Tab

The Extreme Management Center 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 VPLS tab displays information about site connectivity within a private VLAN.

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 the Map Tab

1. Launch Extreme Management Center.
2. Click the Network > Devices tab.
3. Select Sites from the left-panel drop-down menu. Sites are groups of devices that share a configuration. Within each site, you can add maps for devices, depending on their physical location.

Accessing Network Details

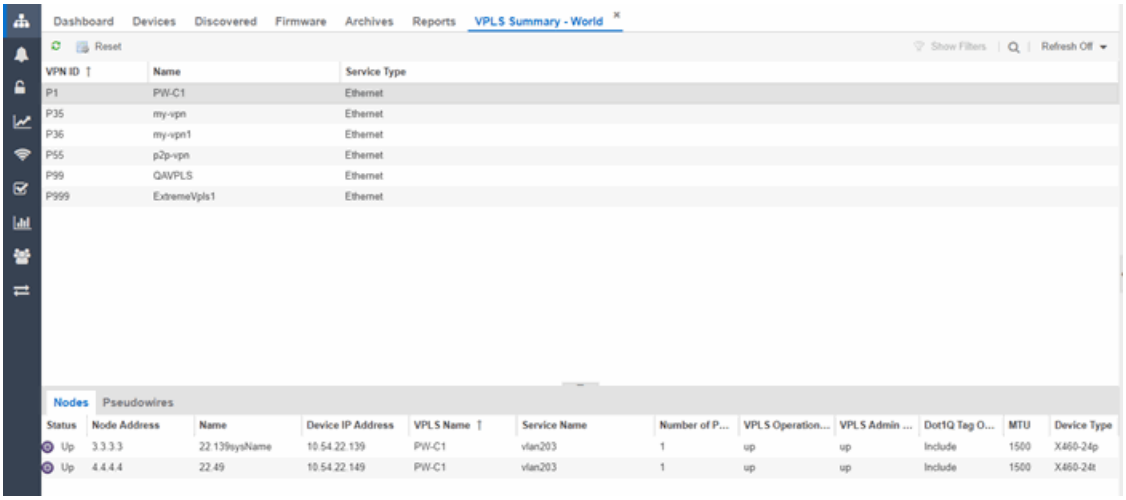
1. Right-click a map or map tree in the left-panel.
2. Select Network Details from the drop-down menu.
3. Select VPLS Summary.

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

1. Click **Network > Devices**.
2. Click 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

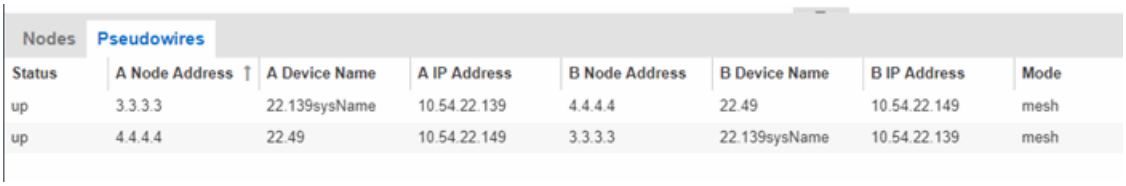
The **Nodes tab** includes the following:

- 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

Click 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.



Related Information

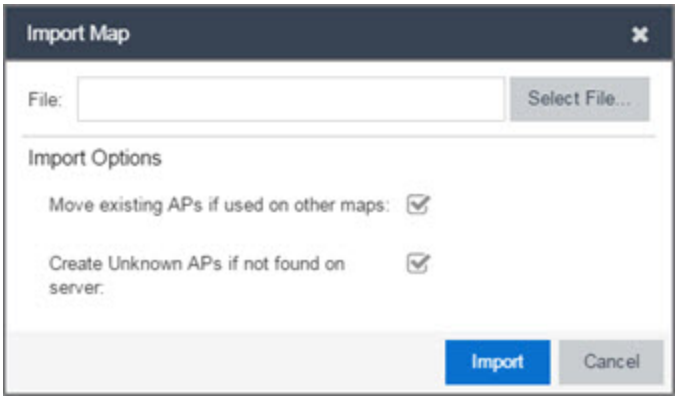
For information on related topics:

- Extreme Management Center Maps
- Advanced Map Features

Extreme Management Center 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. Click 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.

Move existing APs if used on other maps

Select this checkbox to move APs currently located on another map in Extreme Management Center 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 Extreme Management Center server are created as unknown APs.

Related Information

For information on related topics:

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

Extreme Management Center Map Types

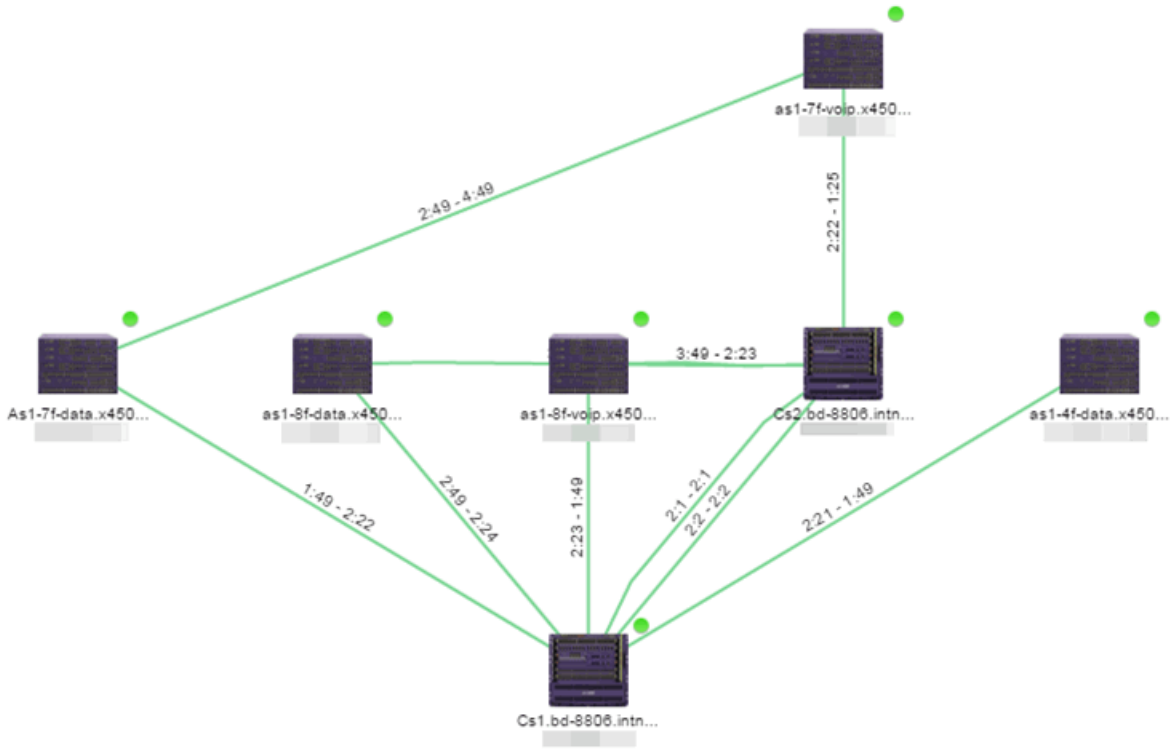
Extreme Management Center allows you to create geographic and topology maps of devices and floorplans of wireless access points (APs) on your network.

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 Extreme Management Center 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.

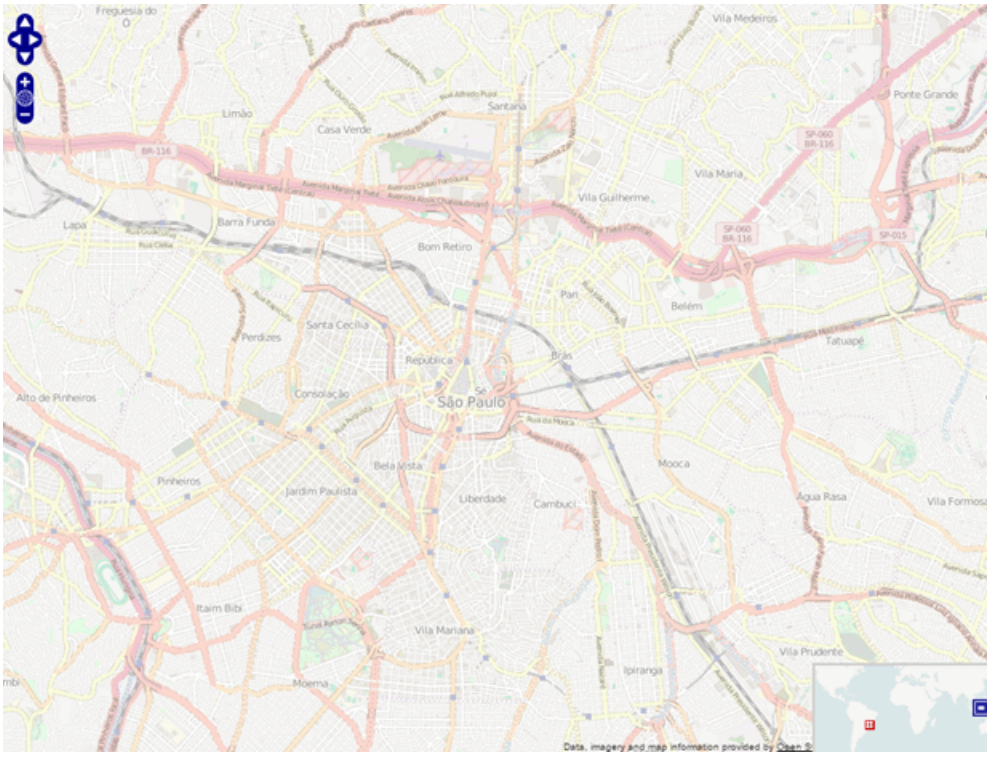


- Floorplan — The floorplan map displays the location of APs in a floorplan you configure. Using information about the size and composition of the building, this map provides an overview of the coverage of wireless APs.

NOTE: The floorplan map type is only available with the NMS-ADV license.

- 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

- Extreme Management Center Maps
- Advanced Map Features

How to Perform a Search Using Extreme Management Center Maps

Using Extreme Management Center 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 Extreme Management Center.

Performing a Search

To search for a wireless client, an AP, a device, or a wired client:

1. Launch Extreme Management Center.
2. In the **Search Network** box, click **Advanced** .
3. Enter the MAC Address, IP Address, hostname, user name, AP serial number or Extreme Access Control custom field information in the open **Search** box.
4. Press **Enter**.

You can also search for specific wireless clients, access points, devices, and wired clients from different locations in Extreme Management Center.

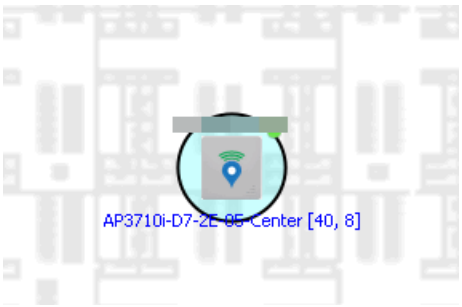
Finding a Wireless Client

From the Search Field on the Network Tab

1. Launch Extreme Management Center and click the **Network > Devices** tab.
2. Select Sites from the left-panel drop-down menu.
3. Select the map or map navigation tree.
4. Enter the MAC Address, IP Address, hostname, user name, AP serial number or Extreme Access Control 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 Extreme Management Center.
2. Click **Wireless > Clients.**
3. Select a client in the Clients view.
4. Right-click and select **Search Maps**.
5. The map opens centered on the AP, with a circle showing the possible area where the client is located.
6. Mouse over the client icon to see a tooltip with client information.

NOTE: Tooltip information is based on current data from the wireless domain unless the client icon displays a clock in the center. In that case, the tooltip information is based on historic data from the Wireless > Clients page.

Radius Distance Calculation

The following distance calculation defines the radius of the circle displayed around the wireless client located on the map.

Path loss per meter in free space =
L1 = 20 * log (10) (f) - 28

where:

- [f] is the frequency in MHz
  (Uses Source SNMP MIB dot11ExtSmtCurrentChannel
  or if that value is 0, uses MIB dot11ExtSmtCurChanSelectedByAP)
- [L1] is the path loss on distance of 1 meter

Radial distance for location =
d(RSS,n) = 10 ^(pTx - RSS - L1)/(10*n)

where:

- [n] is the coefficient for the environment
- [pTx] is the transmit power (dB)
- [RSS] is the Received Signal Strength
- [d] is the distance in meters

Finding an Access Point

From the Wireless Tab

1. Launch Extreme Management Center.
2. Click **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

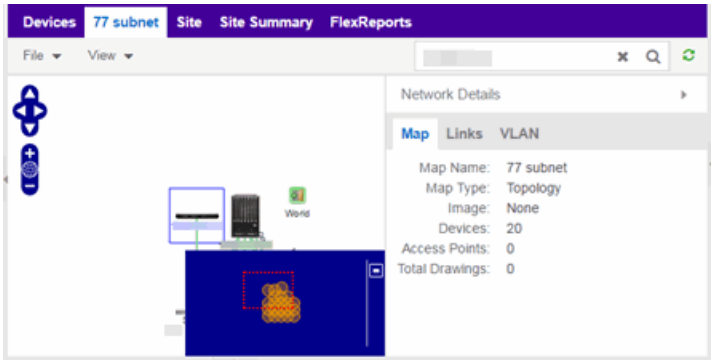
1. Launch Extreme Management Center.
2. Click the **Wireless** tab.
3. On the **Reports** tab, click the APs Summary from the **APs Summary** drop-down menu.
4. Right-click an AP in the table.
5. Select **Maps > Search Maps**.
6. If a map contains the AP, the map opens with the AP centered on the map.

Finding a Device

From the Network Page Search Field

1. Launch Extreme Management Center and click the **Network > Devices** tab.
2. Select Sites from the left-panel drop-down menu.
3. Select the map or map navigation tree. Click 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 Extreme Management Center and click the **Network > Devices** tab.
2. Select Sites from the left-panel drop-down menu.
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 Extreme Access Control authenticated and is connected to a switch added to a map. The map centers on the wired client.

From the Control Tab

1. Launch Extreme Management Center.
2. Click **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:

- Extreme Management Center Maps
- Advanced Map Features

How to Import Maps

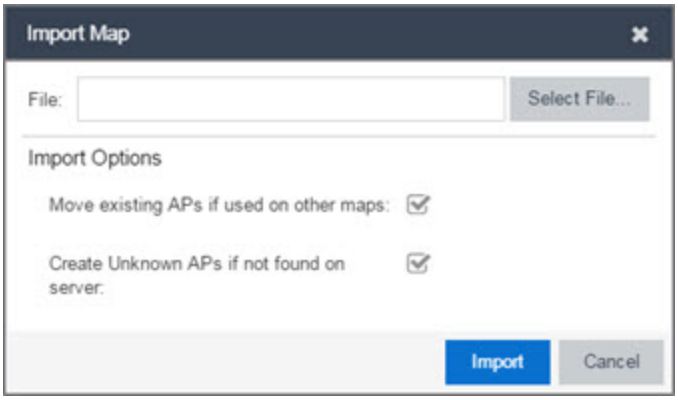
The Extreme Management Center Maps lets you import saved maps of devices and wireless access points (APs) from your local drive or network, and configure the behavior of the imported maps.

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. Click 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 APs on the map being imported:
   a. Select the **Move existing APs if used on other maps** checkbox to move APs currently located on another map in Extreme Management Center to the map being imported.
   b. 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 Extreme Management Center server.
4. Click **Import**.

Related Information

- Extreme Management Center Maps
- Advanced Map Features

How to Create Links Between Devices and Maps

Using the Extreme Management Center 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 menu.
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. Click 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

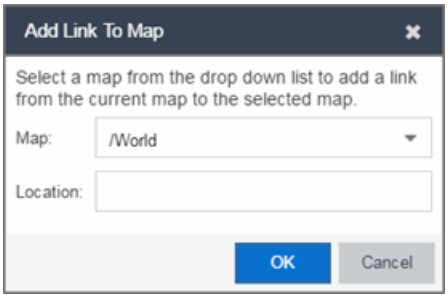
Map links display the name of the map and an aggregated alarm/device status for the linked map. Double-click on the link to go to the linked map.

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 click **File** > **Edit** button in the map properties panel.
2. The map's property panel opens in Edit mode. Click **File** > **Add** > **Map Link**.
3. The **Add Link to Map** window opens.



4. From the **Map** drop-down menu, select the map to which you want to link.
5. Enter information in **Location** about the location to which the link connects and click **OK**.
6. The map link is added to the map and can be repositioned, if desired.
7. Click the **Save** button to save the map and close the properties panel.

Related Information

- Extreme Management Center Maps
- Advanced Map Features

How to Set the Map Scale

You can use the Extreme Management Center Maps feature to set the scale of a map of devices or wireless access point (APs) in your network.

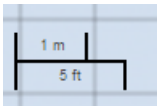
In order to edit maps, you must be a member of an authorization group assigned the OneView > Maps > Maps Read/Write Access capability.

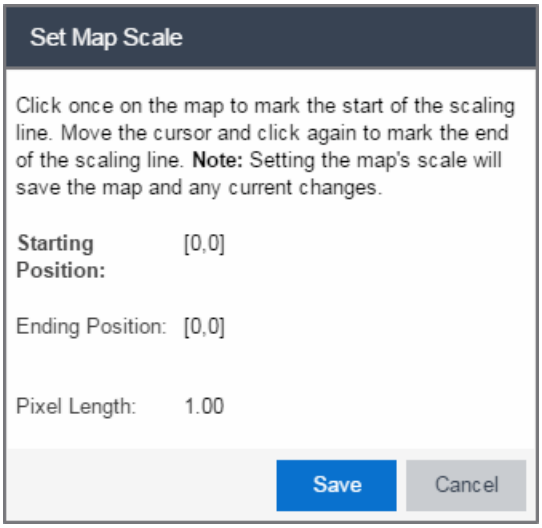
Setting the Map Scale

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 click the File > Edit button in the map properties panel.
2. Click on the map scale in the map's footer panel to open the Set Map Scale window. (Users with the Extreme Management Center NMS-ADV license 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. Click once on the map to mark the start of the scaling line. Move the cursor and click again to mark the end of the scaling line.
    b. Enter the line length and units.
4. Click Save. The map scale is automatically adjusted and the map is saved.

Related Information

- Extreme Management Center Maps
- Advanced Map Features

Extreme Management Center Restart Devices

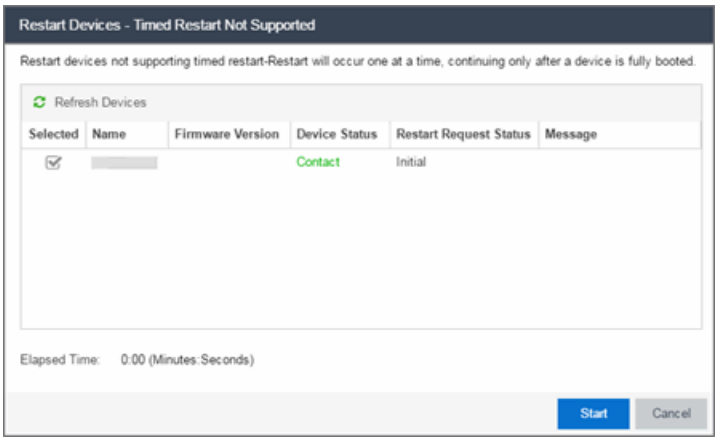
Use this window to restart a device. Devices can be restarted manually, or scheduled at a future date and time, if a timed restart is supported by the device. The window varies depending on the devices you select to restart:

- Timed Restart Not Supported
- Timed Restart Supported

You can access the Restart Devices window from the Network tab by clicking the **Menu** icon or right-clicking a device in the table and selecting **Configuration/Firmware** > **Restart Device**.

Timed Restart Not Supported

To restart a device, select it in the list by clicking the **Selected** checkbox, and click **Start**.



Refresh Devices

Click 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 once the device restart is complete (update the field by clicking Refresh Device).

Device Status
The connection status between Extreme Management Center 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.

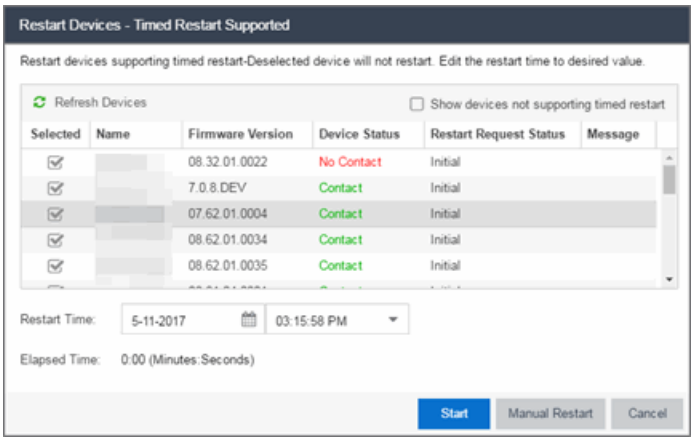
Elapsed Time
The time elapsed since the restart began.

Start
Click Start to restart the device.

Close
Click 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
Click 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 once the device restart is complete (update the field by clicking Refresh Device).

Device Status
The connection status between Extreme Management Center 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
Click this button to schedule the device restart now, or at the time selected in the Restart Time field.

Close
Click 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

How to Create an EAPS Domain in Extreme Management Center

This section outlines how to create an EAPS domain, from the Network tab.

To create a new EAPS Domain:

1. Launch Extreme Management Center.
2. Open the **Network** > **Devices** tab and select a map within the World map navigation tree.
3. Click the EAPS tab in the Network Details section of the window. The EAPS Summary pane opens.
4. Click 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 click 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. Click **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 click 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. Click **Next >**. The Results window opens.
2. Verify the EAPS domain is properly created.

   NOTE: If the EAPS domain is not created correctly, click the **< Back** button to change the values in the New EAPS Domain wizard.

3. Click **Close** to exit the New EAPS Domain wizard. The EAPS domain is created.

Related Information

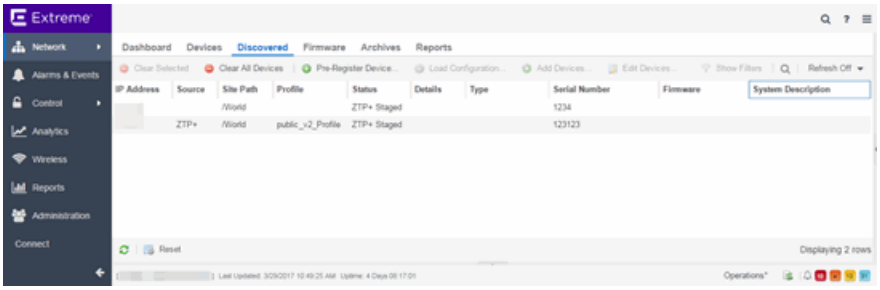
For information on related topics:

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

Discovered

The **Discovered** tab allows you to view devices new to your network not yet added to the Extreme Management Center database.

To access the **Discovered** tab open the **Network** tab and select the **Discovered** tab.



Devices appear on the **Discovered** tab when they are:

- Added via the Site tab without the **Automatically Add Devices** checkbox selected in the Discovered Device Actions section of the tab.
- Added using the Pre-Register Device window for your ZTP+ (Zero Touch

Provisioning Plus) enabled ExtremeXOS devices.

NOTE: ZTP+ functionality requires an ExtremeXOS device on which version 21.1 is installed.

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

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

For instructions about how to discover devices and add them to the Extreme Management Center database, see How to Discover Devices in Extreme Management Center.

Columns

The columns on the **Discovered** tab display the details about the devices available to be added to the Extreme Management Center database.

IP Address
The **IP Address** column displays the IP address assigned to the discovered device.

Source
The **Source** column displays the IP address of the device that discovered the device and added it to the **Discovered** tab in Extreme Management Center.

Site Path
The **Site Path** column shows the site to which the device is assigned. To change the site, click the **Add Devices** button for devices with a Status of **New** or the **Edit Devices** button for devices with a Status of **Exists** and use the **Default Site** drop-down menu 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 as its administrative SNMP and CLI credentials. To change the profile, click the **Add Devices** button for devices with a Status of **New** or the **Edit Devices** button for devices with a Status of **Exists** and use the **Admin Profile** drop-down menu 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 Extreme Management Center database:

- New — The device is discovered by Extreme Management Center, but it has not yet been added to the Extreme Management Center database.
- Exists — The device already exists in the Extreme Management Center database and you can monitor the device using Extreme Management Center.

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, the column displays Reject Profile and another profile must be selected before the device can be added to Extreme Management Center.

Type

The Type column displays the device type.

Serial Number

The Serial Number column displays the serial number of the device.

Firmware

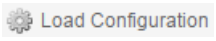
The Firmware column shows the version number of the firmware or boot PROM image.

System Description

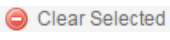
The System Description provides a complete description of the device.

Toolbar Buttons

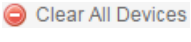
The toolbar at the top of the tab allows you to perform various tasks on the devices on the Discovered tab.

Load Configuration 

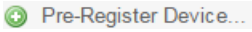
Click to open the Load a configuration on a Discovered Device window, which allows you to use a saved configuration for an existing device on a ZTP (zero touch provisioning) enabled device.

Clear Selected 

Click to remove the currently selected device from the Discovered tab.

Clear All Devices 

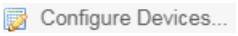
Click to remove all devices listed on the Discovered tab.

Pre-Register Device 

Click to open the Pre-Register Device window, where you can configure a ZTP+ (zero touch provisioning plus) enabled ExtremeXOS device.

Add Devices 

Opens the Add Selected Devices window, where you can configure newly discovered devices and add them to the Extreme Management Center database.

Configure Devices 

Opens the Configure Device window, where you can edit an existing device's configuration.

Related Information

For information on related windows:

- Network Tab
- Devices Tab

For information on related tasks:

- How to Discover Devices in Extreme Management Center
- How to Upgrade Firmware

Load Configuration on a Discovered Device

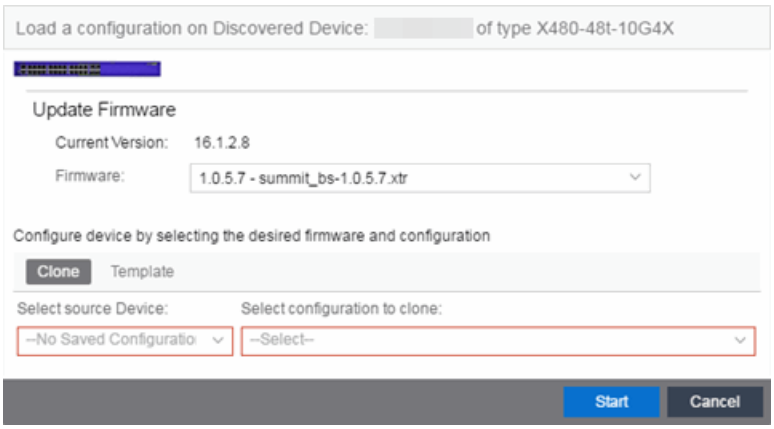
Use this window to use a saved device configuration on a device you are adding to Extreme Management Center. Devices to which you load a saved configuration must have ZTP (Zero Touch Provisioning) enabled.

This window is accessible by clicking 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 Extreme Management Center as a template.

Clone



Current Version

Displays the current version of firmware installed on the device.

Firmware

Use the drop-down menu to select a new firmware version to install on the device.

Select source Device

Use the drop-down menu to select a device currently added to Extreme Management Center from which to copy the device configuration.

Select configuration to clone

Use the drop-down menu to select the configuration on the device listed in the Select source Device drop-down menu that is being cloned to the new device.

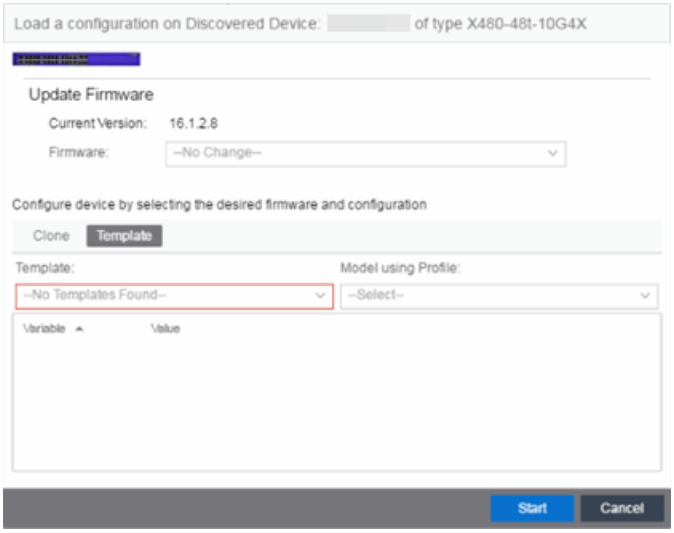
Start

Click the Start button to copy the configuration from the selected device to the new device.

Cancel

Click 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 menu to select a new firmware version to install on the device.

Template
: Use the drop-down menu to select a device configuration template saved to Extreme Management Center.

Model using Profile
: Use the drop-down menu to select the profile to use when modeling the template on the new device.

Start
: Click the **Start** button to copy the configuration from the selected device to the new device.

Cancel
: Click 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 Extreme Management Center.

This window is also accessible on the **Network** > **Discovered** tab by clicking the **Pre-Register Device** button or by right-clicking an existing device and selecting **Pre-Register Device**.

Pre-Register Device Window

Default Site

The site to which the devices are added.

IP Address/Subnet

Enter the device's IP address and subnet in this field. The subnet can be separated from the IP address by a slash (/) or period (.). This field is required.

Serial Number

Enter the manufacturer-assigned serial numbers of the devices being added, separated by commas.

Next

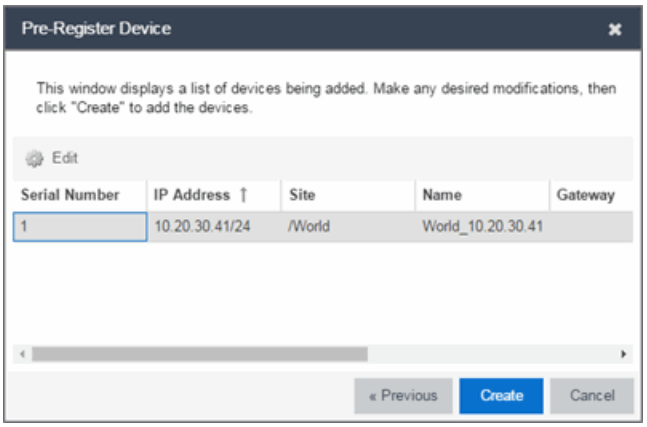
Click the **Next** button to open a confirmation window allowing you to verify the device information entered.

Cancel

Click the **Cancel** button to close the window with no changes saved.

Pre-Register Device Confirmation Window

Use this window to confirm device information before adding devices to Extreme Management Center.



Configure

Select a device and click the **Configure** button to change the information for that device.

NOTE: The **Site** can not be changed from this window.

Serial Number

The serial number of the device.

IP Address

The device's IP address.

Site

The site to which the device is added. To change the **Site**, use the Configure Device window.

Name

The name assigned to the device. The default **Name** lists includes the **Site** to which the device is assigned followed by the device's IP address.

Gateway

Enter the IP address of the switch's Access Control Gateway, if necessary.

Domain Name

Enter a value in the **Domain Name** field to configure the domain name on the devices being discovered, if necessary.

DNS Server
Enter a DNS server address for the devices being discovered, if necessary.

NTP Server
Enter the NTP server address for the devices being discovered, if necessary.

Create
Click the Create button to add the devices listed to the Extreme Management Center database.

Related Information

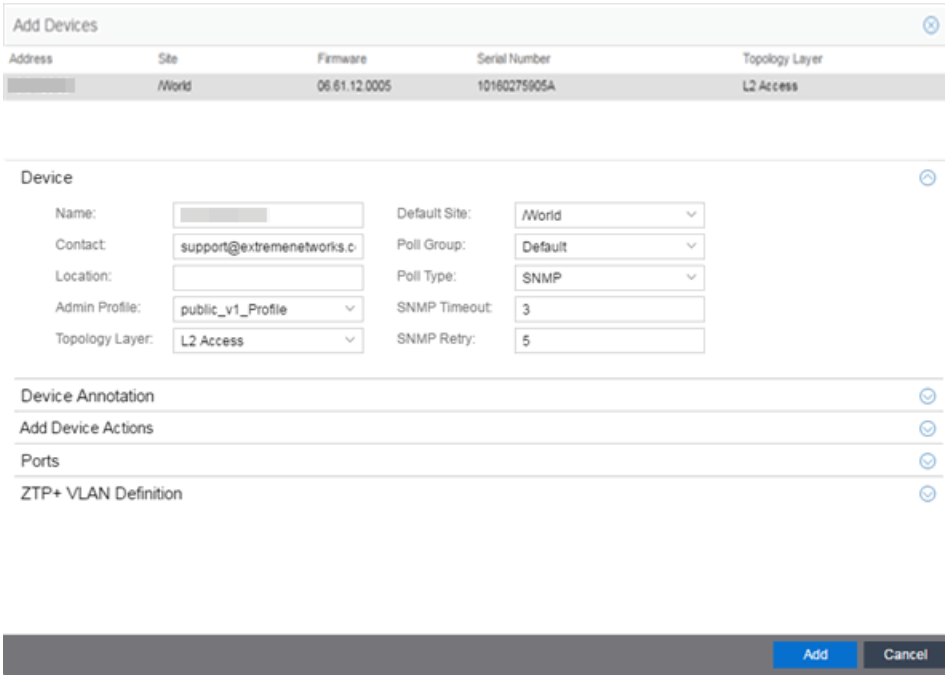
For information on related windows:

- Discovered

Add Devices

Use this window to configure a newly discovered device before you add it to the Extreme Management Center 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.

This window is accessible by clicking 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.

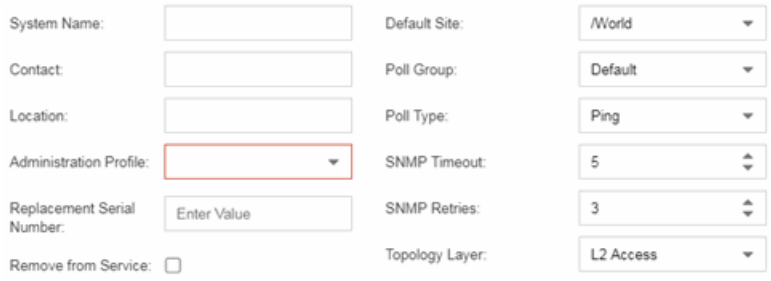
When you first open the window, only the Device section is expanded. Click a section heading to expand that section.

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 menu 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 menu to select the map to which the device is associated.

Poll Group

Use the drop-down menu to select a Poll Group for the discovered devices. Extreme Management Center 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: If Poll Type is Not Polled is specified, the Poll Group is only used if/when the Poll Type is changed to SNMP or Ping.

Poll Type

Use the drop-down menu to select the Poll Type used to discover devices: SNMP, Ping or Not Polled. When SNMP is specified, the SNMP version (SNMPv1 or SNMPv3) is determined by the Profile specified for the IP Range. If the Profile is set to Ping

Only, the Poll Type must be set to Ping.

NOTE: On a Windows platform, device operational status cannot be determined for devices with their Poll Type set to Ping unless you are logged on and running Extreme Management Center as a user with Administrative privileges.

SNMP Timeout

The amount of time (in seconds) that Extreme Management Center 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.

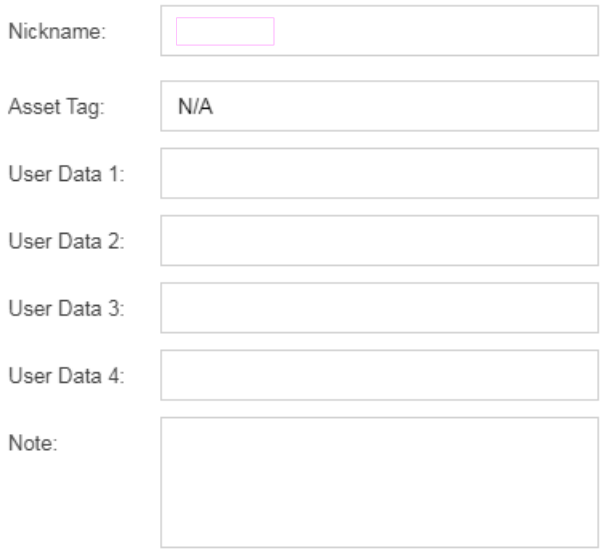
SNMP Retry

The number of attempts Extreme Management Center makes to contact a device after an attempt at contact fails. The value for this setting must be between 1 and 60 tries.

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

Device Annotation

The Device Annotation section allows you to add user-defined information about the device.



Nickname

The user-defined nickname for the selected device. This is the name for this device that appears in the device tree in the left panel when nickname is selected in the How to Display Devices in Tree menu option in the OneView options menu in the Administration > Options tab.

User Data

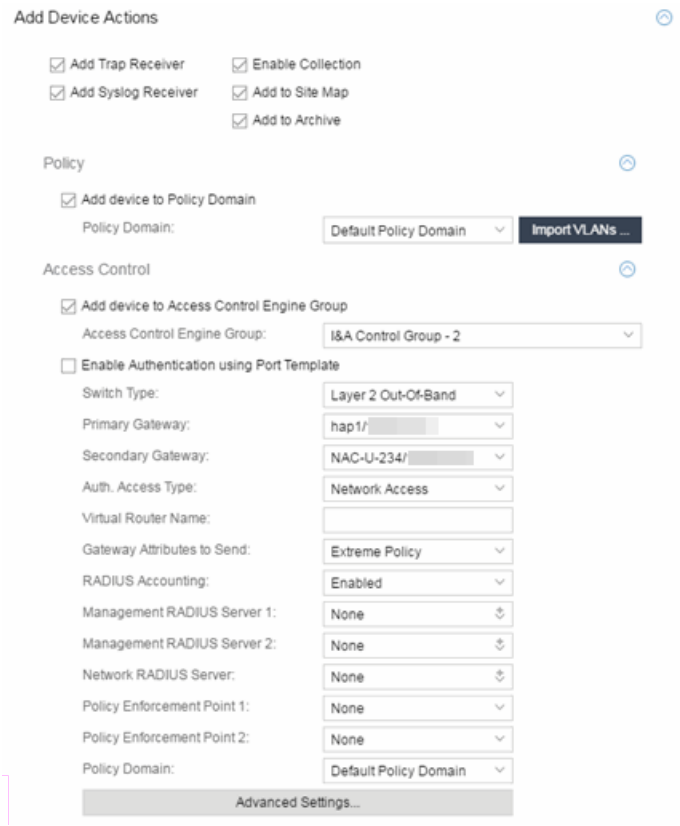
The user-defined information displayed in the devices table in the User Data columns.

Notes

Additional user-defined information displayed in the devices table in the Notes column.

Add Device Actions

The Add Device Actions section indicates the actions taken by the device upon being discovered.



Add Trap Receiver

Select this checkbox if you want the devices being discovered to receive trap information it sends to Extreme Management Center.

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 Extreme Management Center reports.

Add to Site Map

Select this checkbox to add the devices being discovered to the map associated with the currently accessed site.

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. Once the checkbox is selected, use the Policy Domain drop-down menu to select the policy domain to which the device is added.

Click the Import VLANs button to import the VLAN definitions from the policy selected in the Policy Domain drop-down menu.

Extreme Access Control

Add device to Extreme Access ControlEngine Group

Select this checkbox to add the device to an Extreme Access ControlEngine Group you create on the Access Control tab. Once the checkbox is selected, use the Access Control Engine Group drop-down menu 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 menu 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 Extreme Access Control 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 Extreme Access Control engine, Extreme Access Control removes the end-system authentication from their prior port/switch. This allows VMs that quickly move from one server to another and then back again to still have their location updated in Extreme Management Center, because only one authenticated session is allowed per end-system in Extreme Management Center.
- Layer 2 RADIUS Only — In this mode, Extreme Management Center 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 Extreme Access Control 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 Extreme Management Center is unable to apply policies to restrict access after the user is granted access.

Primary Gateway

Use the drop-down menu to select the primary Extreme Access Control Gateway for the selected switches. If load balancing has been configured for the engine group, the Extreme Management Center server determines the primary and secondary gateways at Enforce, and this field displays Determined by Load Balancer.

Secondary Gateway

Use the drop-down menu to select the secondary Extreme Access Control Gateway for the selected switches. If load balancing has been configured for the engine group, the Extreme Management Center server determines the primary and secondary gateways at Enforce, and this field displays Determined by Load Balancer.

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

Auth. Access Type

Use the drop-down menu 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. Extreme Access Control 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 Extreme Access Control Profile" to grant proper access to users. Also, verify that the current switch CLI credentials for the admin user are defined in the database that Extreme Management Center 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 Extreme Access Control authentication type precedence from highest to lowest is: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.
- Monitoring - RADIUS Accounting - the switch monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. Extreme Management Center learns about these session via RADIUS accounting. This allows Extreme Management Center 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 Extreme Access Control authentication type precedence from highest to

lowest is: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.

- Manual RADIUS Configuration - Extreme Management Center 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 Extreme Management Center 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 menu to select the RADIUS attributes included as part of the RADIUS response from the Extreme Access Control engine to the switch. You can also select Edit RADIUS Attribute Settings from the menu to open the RADIUS Attribute Settings window where you can define, edit, or delete the available attributes.

RADIUS Accounting

Use the drop-down menu to enable RADIUS accounting on the switch. RADIUS accounting can be used to determine the connection state of the end-system sessions on the Extreme Access Controlengine, providing real-time connection status in Extreme Management Center.

Management RADIUS Server 1 and 2

Use the drop-down menu to specify RADIUS servers used to authenticate requests for administrative access to the selected switches. Select from the RADIUS servers you have configured in Extreme Management Center, 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 Extreme Access Controlengine. (This option is only available if a Secondary Gateway is not specified.) Select from the RADIUS servers you have configured in Extreme

Management Center, or select New or Manage RADIUS Servers to open the Add/Edit RADIUS Server or Manage RADIUS Servers windows.

Policy Enforcement Point 1 and 2

Select the Policy Enforcement Points used to provide authorization for the end-systems connecting to the VPN device you are adding. The list is populated from the N-Series, S-Series, and K-Series devices in your Console device tree. If you do not specify a Policy Enforcement Point, then Extreme Access Control is unable to apply policies to restrict end user access after the user is granted access.

Policy Domain

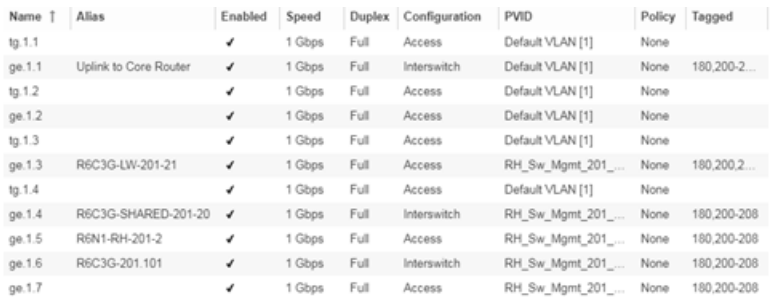
Use this option to assign the switch to a policy domain and enforce the domain configuration to the switch. The switch must be an Extreme Networks switch.

Advanced Settings

Click 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. Click the **Add** button to add a new port to the list. Click the **Delete** button to remove a device from the list.



Name	Alias	Enabled	Speed	Duplex	Configuration	PVID	Policy	Tagged
tg.1.1		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
ge.1.1	Uplink to Core Router	✓	1 Gbps	Full	Interswitch	Default VLAN [1]	None	180,200-2...
tg.1.2		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
ge.1.2		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
tg.1.3		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
ge.1.3	R6C3G-LW-201-21	✓	1 Gbps	Full	Access	RH_Sw_Mgmt_201_...	None	180,200,2...
tg.1.4		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
ge.1.4	R6C3G-SHARED-201-20	✓	1 Gbps	Full	Interswitch	RH_Sw_Mgmt_201_...	None	180,200-208
ge.1.5	R6N1-RH-201-2	✓	1 Gbps	Full	Access	RH_Sw_Mgmt_201_...	None	180,200-208
ge.1.6	R6C3G-201.101	✓	1 Gbps	Full	Interswitch	RH_Sw_Mgmt_201_...	None	180,200-208
ge.1.7		✓	1 Gbps	Full	Access	RH_Sw_Mgmt_201_...	None	180,200-208

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 menu 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 Extreme Management Center.

Policy

The policy assigned to the selected port.

Add

Click the Add button to add the device to the Extreme Management Center database with the current configuration.

Cancel

Click the Cancel button to close the window without adding the device to the Extreme Management Center database.

ZTP+ VLAN Definition

The ZTP+ VLAN Definition section allows you to configure VLANs on the device you are adding. To add a VLAN, click the Add button. You can remove a VLAN by clicking the Delete button.

Name

Displays the name of the VLAN.

VID

Indicates the VLAN ID for the VLAN. A unique number between 1 and 4094 that identifies a particular VLAN. VID 1 is reserved for the Default VLAN.

Dynamic Egress

Indicates if the associated dynamic egress setting for the VLAN (Enable or Disable) is written to the device(s) when you enforce.

Protocol Filter
Indicates the VLAN uses an X-Pedition Protocol Filter.

Management
Indicates which VLAN the ExtremeXOS 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

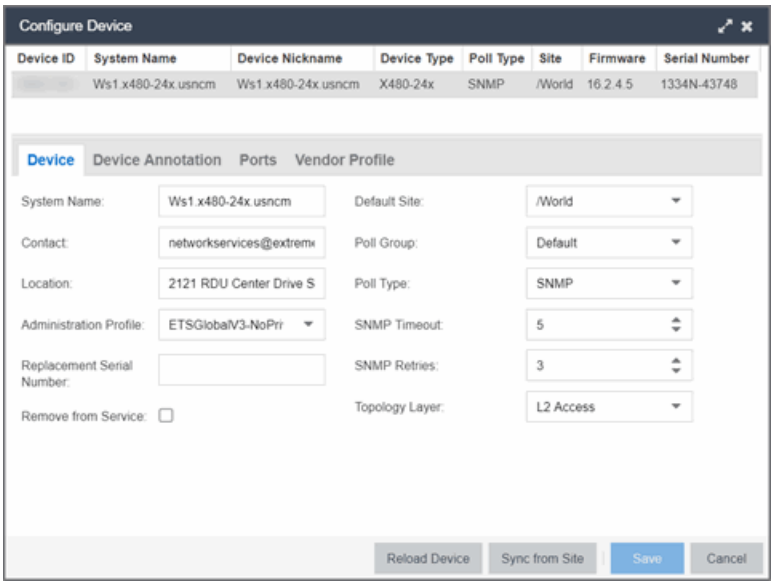
Configure Device

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. Click the Menu icon (≡) or right-click on a device.
4. Select Device > Configure Device.

This window is also accessible by clicking the Configure Device button on the Discovered and Site tabs.



When you first open the window, the **Device** tab opens.

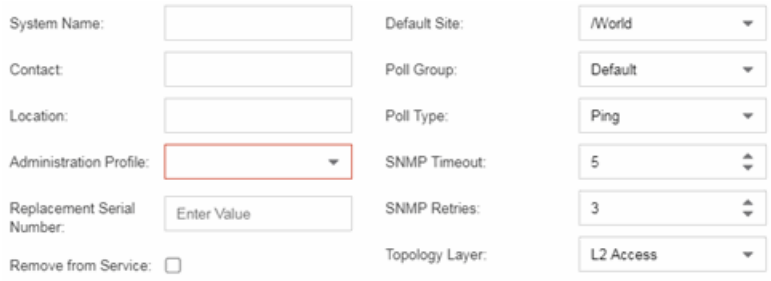
The **Configure Device** window contains the following tabs:

- Device
- Device Annotation
- VLAN Definition
- 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 menu 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, Extreme Management Center restores the most recent archive of the device removed from service.

Remove from Service

Select this checkbox if the device is being removed from the network. When Remove from Service is selected, the device is not polled and alarms are not triggered for the device.

Default Site

Use the drop-down menu to select the map to which the device is associated. For additional information, see the Maps Overview topic.

Poll Group

Use the drop-down menu to select a Poll Group for the discovered devices. Extreme Management Center 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: If **Poll Type** is **Not Polled** is specified, the **Poll Group** is only used if/when the **Poll Type** is changed to **SNMP** or **Ping**.

Poll Type

Use the drop-down menu to select the Poll Type used to discover devices:

- Select **Not Polled** if you do not want to poll the devices.
- 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** once maintenance on the device is complete.
- Select **SNMP** to poll the device using SNMP. The SNMP version (SNMPv1 or SNMPv3) is determined by the Profile specified for the IP Range.
- Select **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 Extreme Management Center as a user with Administrative privileges.

SNMP Timeout

The amount of time that Extreme Management Center 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 Retries

The number of attempts Extreme Management Center makes to contact a device after an attempt at contact fails. The value for this setting must be between 1 and 60 tries.

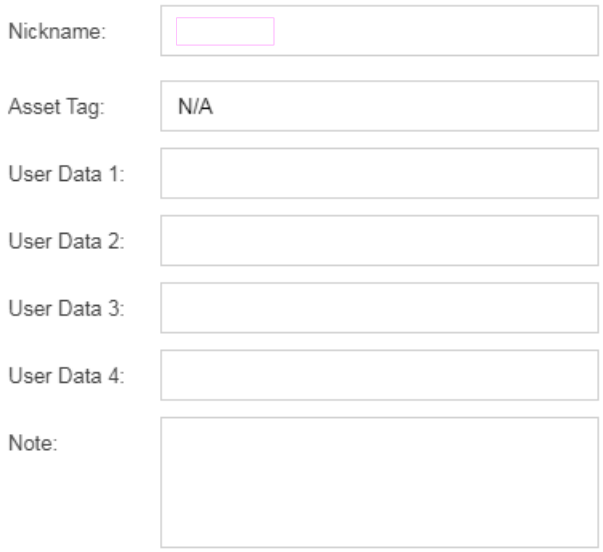
The value entered in this field overrides the default entered in the SNMP Advanced view in the Administration > Options tab.

Topology Layer

The layer and networking attributes for the device.

Device Annotation

The Device Annotation tab 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 Extreme Management Center options menu in the 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.

VLAN Definition

The VLAN Definition tab allows you to configure VLANs on the device. To add a VLAN, click the Add button. You can remove a VLAN by clicking the Delete button.

Name
Displays the name of the VLAN.

VID
Indicates the VLAN ID for the VLAN. A unique number between 1 and 4094 that identifies a particular VLAN. VID 1 is reserved for the Default VLAN.

Dynamic Egress
Indicates if the associated dynamic egress setting for the VLAN (Enable or Disable) is written to the device(s) when you enforce.

Protocol Filter
Indicates the VLAN uses an X-Pedition Protocol Filter.

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.

Ports

The Ports tab allows you to enter information about the ports on a device. Click the Add button to add a new port to the list. Click the Delete button to remove a device from the list.

Name ↑	Alias	Enabled	Speed	Duplex	Configuration	PVID	Policy	Tagged
tg.1.1		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
ge.1.1	Uplink to Core Router	✓	1 Gbps	Full	Interswitch	Default VLAN [1]	None	180,200-2...
tg.1.2		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
ge.1.2		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
tg.1.3		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
ge.1.3	R6C3G-LW-201-21	✓	1 Gbps	Full	Access	RH_Sw_Mgmt_201_...	None	180,200,2...
tg.1.4		✓	1 Gbps	Full	Access	Default VLAN [1]	None	
ge.1.4	R6C3G-SHARED-201-20	✓	1 Gbps	Full	Interswitch	RH_Sw_Mgmt_201_...	None	180,200-208
ge.1.5	R6N1-RH-201-2	✓	1 Gbps	Full	Access	RH_Sw_Mgmt_201_...	None	180,200-208
ge.1.6	R6C3G-201.101	✓	1 Gbps	Full	Interswitch	RH_Sw_Mgmt_201_...	None	180,200-208
ge.1.7		✓	1 Gbps	Full	Access	RH_Sw_Mgmt_201_...	None	180,200-208

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.

Configuration

Use the drop-down menu 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 are configurable.
- Management — Select this option if the port is used to manage network traffic with Extreme Management Center.
- 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).

Authentication

Use the drop-down menu 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.

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 Extreme Management Center 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.

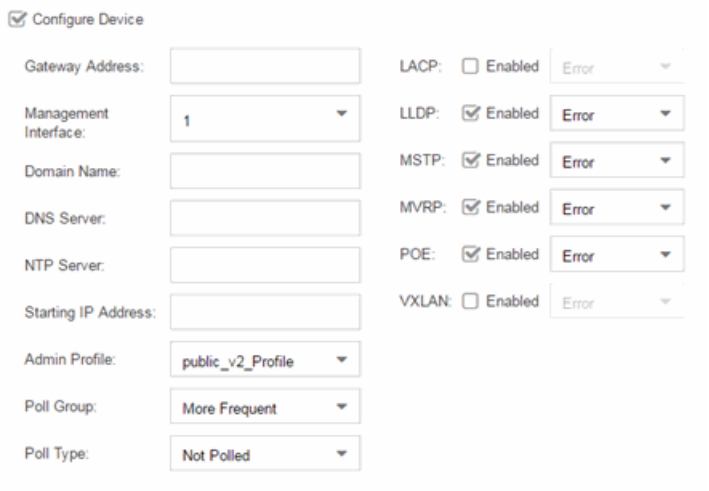
MVRP
Indicates that the Multiple VLAN Registration Protocol (MVRP) has been enabled for the port. If MVRP has been enabled globally, interswitch ports are automatically enabled and access ports default to disabled. Select the checkbox to enable ZTP+ devices being discovered to broadcast MVRP (Multiple VLAN Registration Protocol) information. Select the appropriate logging level from the drop-down menu.

Update
Click Update to save any changes made to the device configuration.

Cancel
Click Cancel to close the window and discard any changes.

ZTP+ Device Settings

The ZTP+ Device Settings tab contains basic information about the device being discovered.



Configure Device

Select this checkbox to enable ZTP+ (Zero Touch Provisioning Plus) functionality device being discovered. ZTP+ allows you to quickly add a supported device to your network with minimal configuration.

Gateway Address

Enter the Gateway Address for the ZTP+ devices being discovered.

Management Interface

Select the interface the ExtremeXOS device uses for Management and assigns the device IP to that interface.

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 being discovered

NTP Server

The NTP Server field allows you to set the NTP server address on the ZTP+ devices being discovered.

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 being discovered.

Admin Profile

Use the drop-down menu to select the access Profile that gives Extreme Management Center administrative access to the ZTP+ devices you wish to discover. 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, saving the device overwrites the profile currently being used in the database.

Poll Group

Use the drop-down menu to select a Poll Group for the discovered ZTP+ devices. Extreme Management Center 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 will overwrite 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 menu to select the **Poll Type** used to discover devices. Valid options are **SNMP**, **Ping**, and **Not Polled**. When **SNMP** is specified, the SNMP version (SNMPv1 or SNMPv3) is determined by the **Profile** specified for the IP range. If the **Profile** is set to **Ping Only**, the **Poll Type** must be set to **Ping**. If you discover an existing device using a different poll type than the device is already using in the database, saving the device overwrites the **Poll Type** currently being used in the database.

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 Console as a user with Administrative privileges.

LACP

Select the checkbox to enable ZTP+ devices being discovered to broadcast LACP (Link Aggregation Control Protocol) information. Select the appropriate logging level from the drop-down menu.

LLDP

Select the checkbox to enable ZTP+ devices being discovered to broadcast LLDP (Link Layer Discovery Protocol) information. Select the appropriate logging level from the drop-down menu.

MSTP

Select the checkbox to enable ZTP+ devices being discovered to broadcast MSTP (Multiple Spanning Tree Protocol) information. Select the appropriate logging level from the drop-down menu.

MVRP

Select the checkbox to enable ZTP+ devices being discovered to broadcast MVRP (Multiple VLAN Registration Protocol) information. Select the appropriate logging level from the drop-down menu.

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.

Flow Sources

The Flow Sources tab allows you to configure devices to act as flow sources for an Application Analytics 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 Application Analytics engine or used to create the GRE tunnel.

Source Ports

Displays the ports on which flow collection is enabled.

NOTE: Policy mirrors the first 15 packets of each flow received on the Source Ports to the Application Analytics engine.

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 Application Analytics 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

Click Add to open a window from which you can select a device in Extreme Management Center to add as a flow source.

Remove

Select a flow source device in the table and click Remove to remove the device as a flow source.

Edit

Click Edit to open a window from which you can change the configuration of a flow source device.

Test

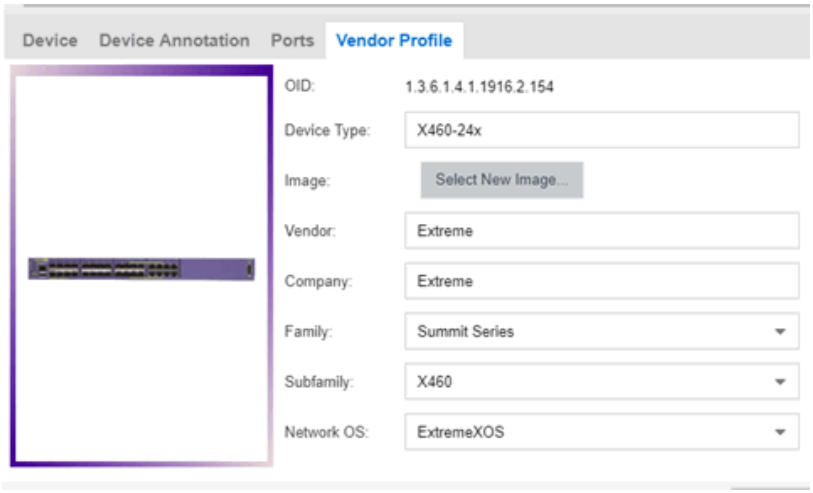
Click Test to verify the GRE tunnel end-points can communicate.

NOTE: Test is only available if Tunnel is enabled.

Vendor Profile

The **Vendor Profile** tab allows you to edit configurations for devices. The configuration you select allows you to enter information about the device to help identify it in Extreme Management Center.

NOTE: To remove all user-defined Vendor Profile configurations and restore the default system configurations, click the **Restore to Defaults** button on the **Administration** > **Diagnostics** > **System** > **Vendor Profile Cache** tab.



OID

Displays the Object Identifier for the device.

Device Type

Displays the specific type of device.

NOTE: When **Device Type** is blank:

- The tab is named **New Vendor Profile**.
- If a device's Vendor is recognized, but Extreme Management Center does not have a profile for the device's unique **OID**, the **Device Type**, **Family** and **Subfamily** values are empty, but Extreme Management Center supplies the **Vendor** and **Company** values.
- 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 DeviceView and Maps. Click 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 Extreme Management Center.

Subfamily
Displays a smaller grouping to which the device belongs, if applicable.

Network OS
The operating system that the device type uses.

Buttons

Reload Device
Click to read configuration information from the device to populate Extreme Management Center. Reload Device reads the configuration (e.g. VLAN Definition, Ports, Port VLANs) from the device and reloads it in Extreme Management Center.

NOTE: Clicking 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
Click 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
Click to copy the default configurations from the site to Extreme Management Center's representation of the devices. The Enforce Preview button displays, which you can use to decide whether to save the settings to the device.

Save
Click to save any changes you make to a device in Extreme Management Center.

Cancel

Click to discard any unsaved changes and close the window.

Related Information

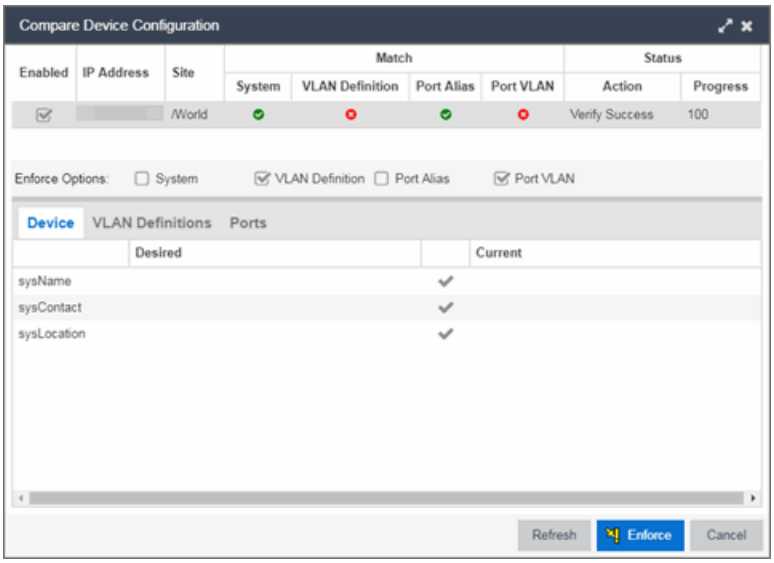
For information on related windows:

- 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 click **Enforce Preview** in the Configure Device window.



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 bottom of the window.

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 (✖). The System column indicates the whether the information on the **Device** tab matches, the VLAN Definition column indicates whether the

information on the VLAN Definitions tab matches, and the Port Alias and Port VLAN columns indicate whether the information on the Ports tab matches.

The Enforce Options section of the window allows you to select the changes you want to make on the device. Select System to push changes you make on the Device tab to the device, select VLAN Definition to push changes you make on the VLAN Definitions tab, select Port Alias to push changes you make to the top table on the Ports tab, and select Port VLAN to push changes you make to the Port VLAN Details table on the Ports tab.

NOTE: By default, the checkboxes in the Enforce Options section of the window are not selected. To configure Extreme Management Center 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`

In each tab, the configurations are separated into two columns:

- 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.

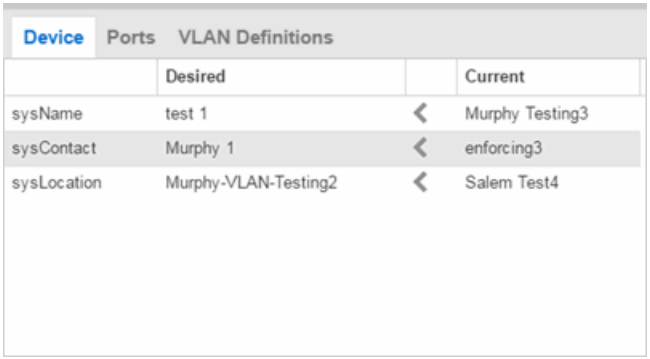
A check mark between the columns (✔) indicates the Current configuration matches the Desired configuration.

A left arrow icon (<) indicates the configurations do not match. Clicking it copies the Current configuration to the Desired configuration so no configuration change is made when enforcing the device.

Click Enforce to save your changes to 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

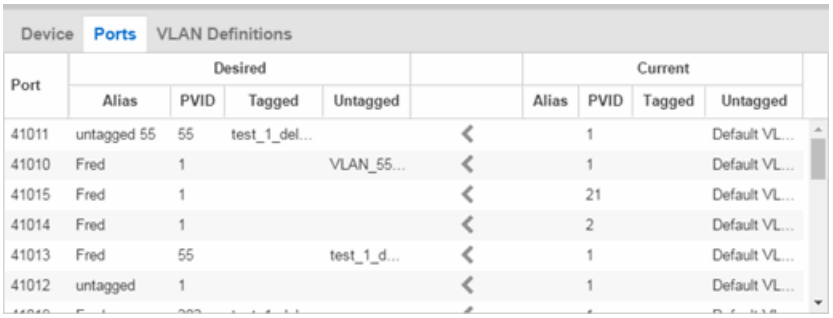
Allows you to specify contact information for the person maintaining the device.

sysLocation

The physical location of the device.

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

Shows the alias for the port, if one is assigned.

PVID

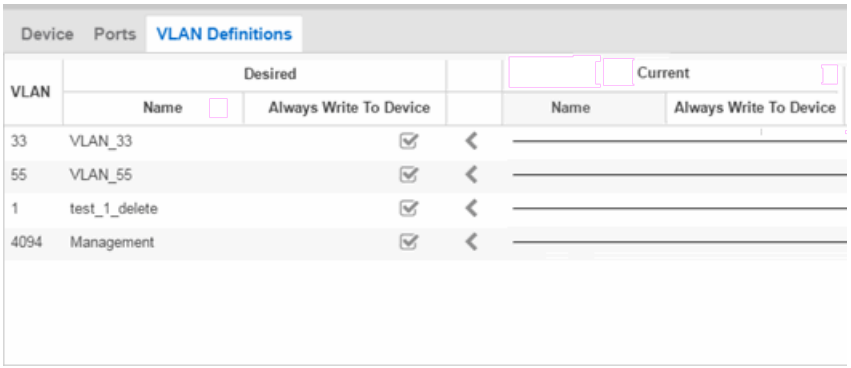
The port's VLAN assignment. Possible values are 1 through 4094.

Tagged
The port is added to the list with the egress state set to Tagged (frames are forwarded as tagged).

Untagged
The port is added to the list with the egress state set to Untagged (frames are forwarded as untagged).

VLAN Definitions

The VLAN Definitions tab displays any changes to the VLANs defined for the device selected at the top of the window.



VLAN
A unique numerical identifier of the VLAN.

Name
The name of the VLAN.

Always Write to Device(s)
Indicates whether or not the VLAN is written to the device(s) when you enforce, or compared to the actual VLANs on the device(s) when you verify.

Related Information

For information on related topics:

- VLAN Concepts
- Configure Device
- Site Tab

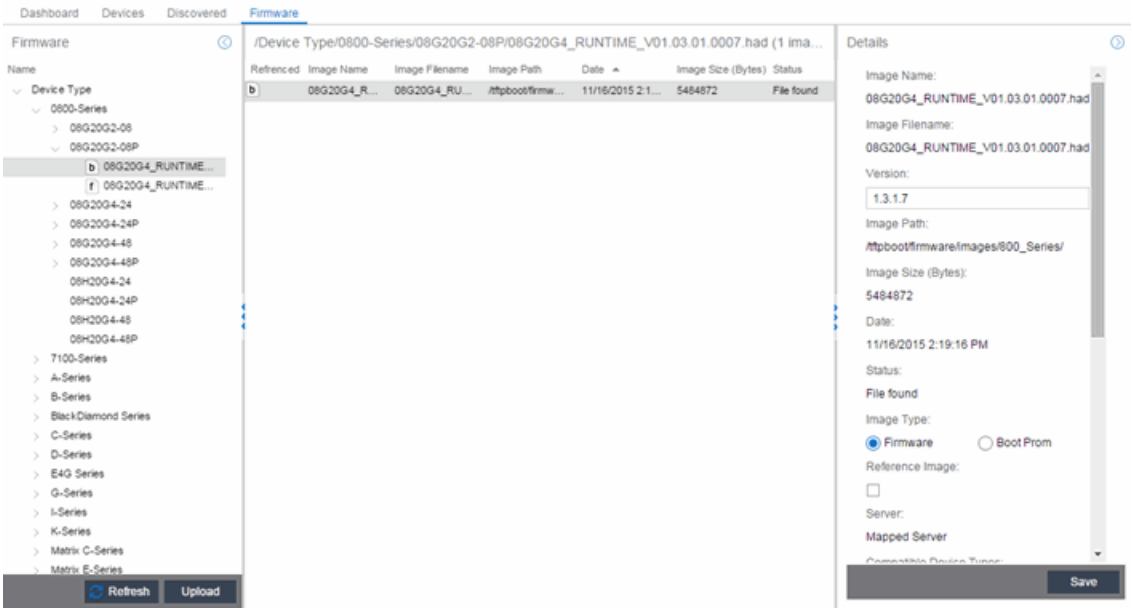
Firmware

The **Firmware** tab allows you to upload firmware and boot PROM images to Extreme Management Center 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

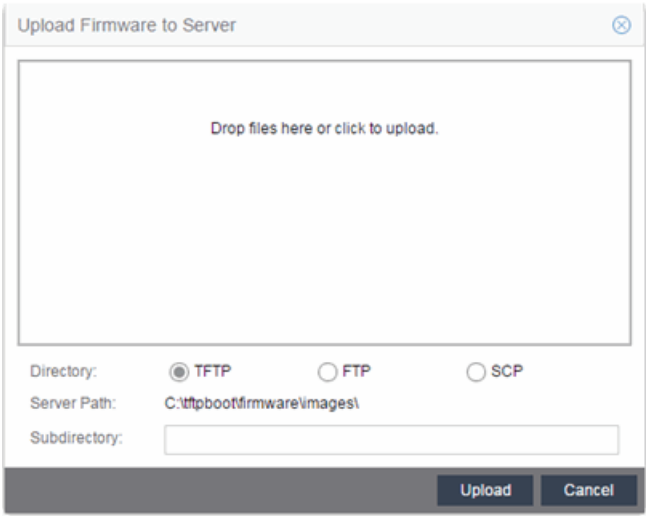
The **Firmware** tree in the left panel displays firmware and boot PROM images grouped according to product family and device type. It provides pre-defined firmware groups and automatically organizes the images stored in your firmware directory under the appropriate group when you perform a firmware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

Click the Upload button to open the Upload Firmware to Server window from which you can save image files to the Extreme Management Center server. This allows anyone with access to Extreme Management Center to download the image file to a device.



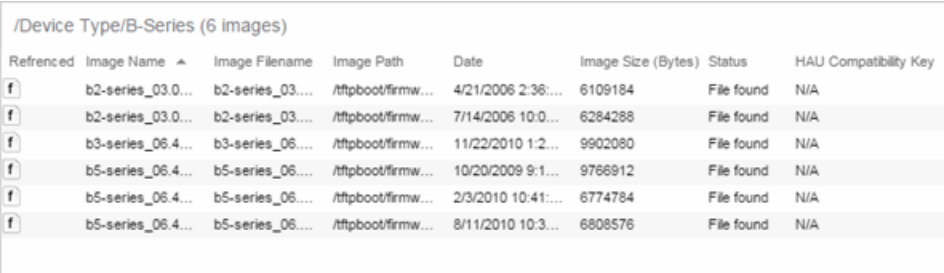
For additional information on how to upload a firmware or boot PROM image, see How to Upgrade Firmware.

Refresh

Click the Refresh button to synchronize the images displayed in the Firmware left-panel with the firmware and boot PROM images on the Extreme Management Center server. Clicking 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 Extreme Management Center server and adds or removes images from the Firmware left-panel in Extreme Management Center 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, Extreme Management Center 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

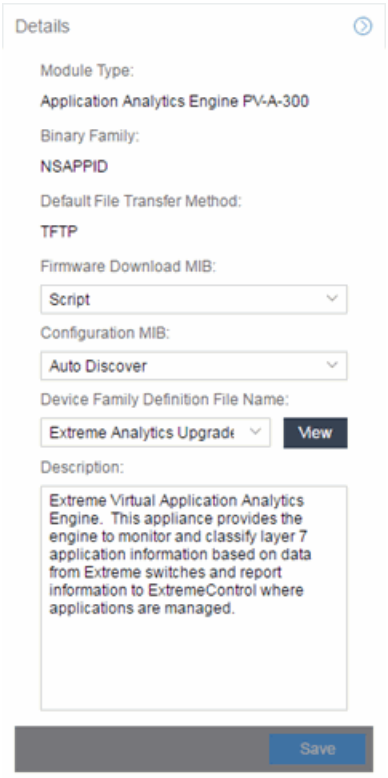
NOTE: Firmware images that were discovered with a NetSight version prior to 4.4 need to be removed from Extreme Management Center (right-click the image on the **Firmware** tab and select **Delete Image**) and then rediscovered in order to populate the compatibility key field.

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.



Module 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 menu to select the desired MIB. In addition to a list of MIBs, other menu options include:

- Auto Discover — Extreme Management Center reads the Firmware Download MIB on the first device of this device type that you add or import and displays

it here. Extreme Management Center 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.
- Script — Allows the firmware download function to be executed through the use of a script. This option is used when upgrading Extreme Access Control and Application Analytics engines as well as for third-party devices that do not support the required SNMP MIBs. For information on using scripts to upgrade Extreme Access Control and Application Analytics engines, refer to How to Upgrade Firmware.

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 — Extreme Management Center reads the Configuration MIB on the first device of this device type that you add or import and displays it here. Extreme Management Center 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 Extreme Management Center function for specific third-party devices in this file.

Extreme Management Center provides sample Definition Files for Extreme, Enterasys, Cisco Systems, and Hewlett Packard devices. Click 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.

Click Save to save any changes.

Firmware/boot PROM Image Details

Use this section to edit the version number of the image, the type of image (firmware or boot PROM), and enter a description for the image.

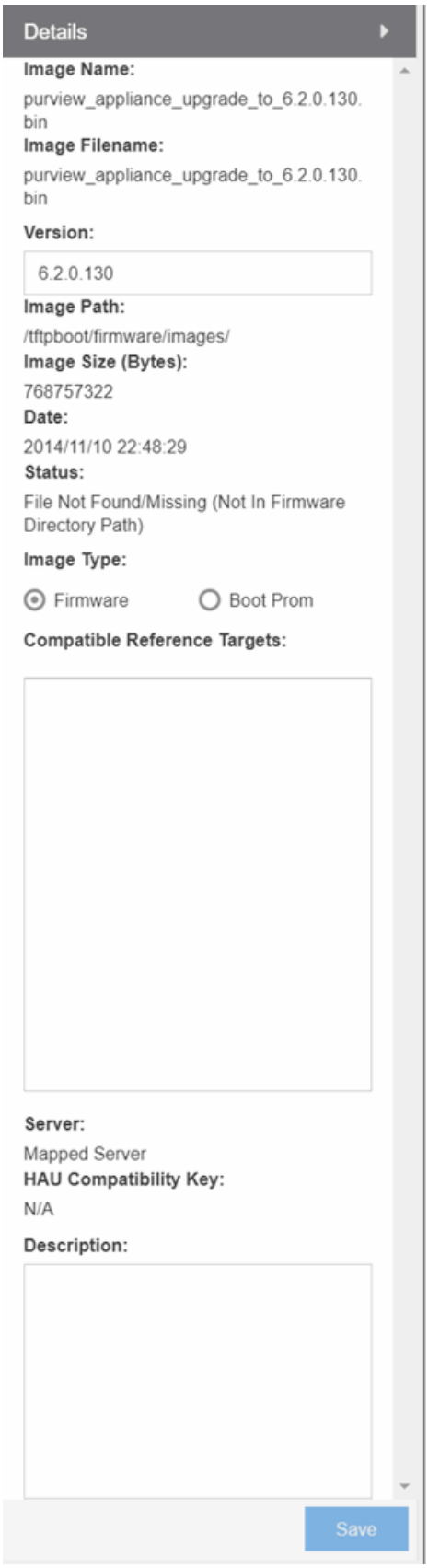

Details
Image Name:
purview_appliance_upgrade_to_6.2.0.130.bin
Image Filename:
purview_appliance_upgrade_to_6.2.0.130.bin
Version:
6.2.0.130
Image Path:
/tftpboot/firmware/images/
Image Size (Bytes):
768757322
Date:
2014/11/10 22:48:29
Status:
File Not Found/Missing (Not In Firmware Directory Path)
Image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

Image Name

The name of the image as it is displayed in the left-panel Firmware tree. The maximum length of the displayed name is 50 characters. Longer names will be truncated to the 50-character maximum with a (2), (3), and so on, appended if there are multiple images with the same name.

Image Filename

The full name of the image as it appears in your firmware images directory.

Version

The version number of the firmware or boot PROM image. If the version number is not available from the image file, and Inventory Manager has not performed a firmware or boot PROM upgrade using this image, this field displays N/A (not available). Enter a version number and click 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, Extreme Management Center 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 Extreme Management Center 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. Click 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

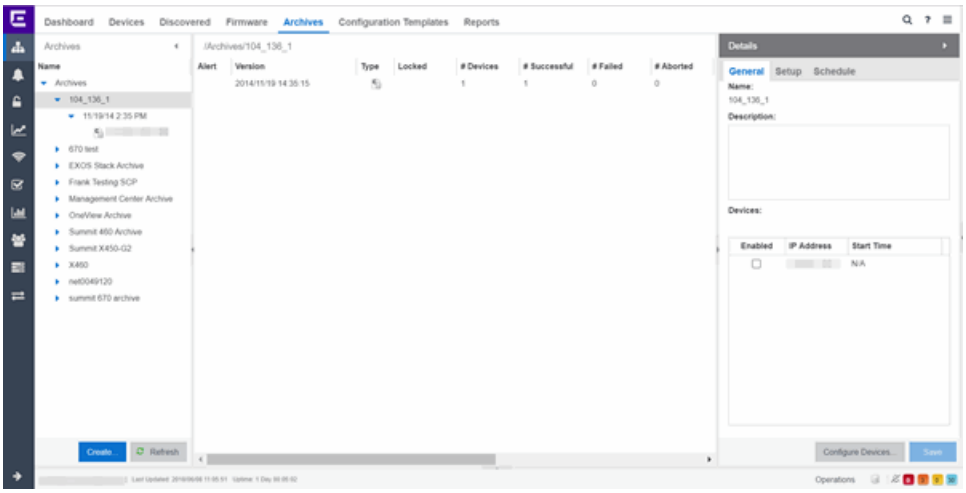
For information on related tasks:

- 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 a governance 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.
  - 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.
  - 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.

- 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, while the **Custom Attributes** 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 **Archive Wizard** 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 **Archive** 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.

Archive 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 archive (as specified

in the Archive Wizard) is reached. To lock and unlock an archive version, right-click the archive version in the left-panel **Archive** 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 abored 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

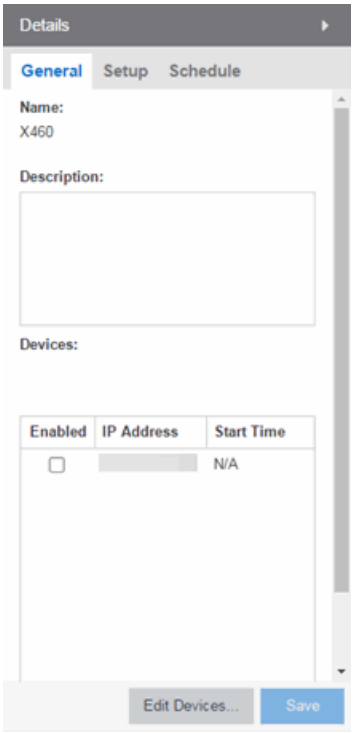
For information on related tasks:

- 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 **Archive** 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 **Archive** tab, and then select **Rename**.

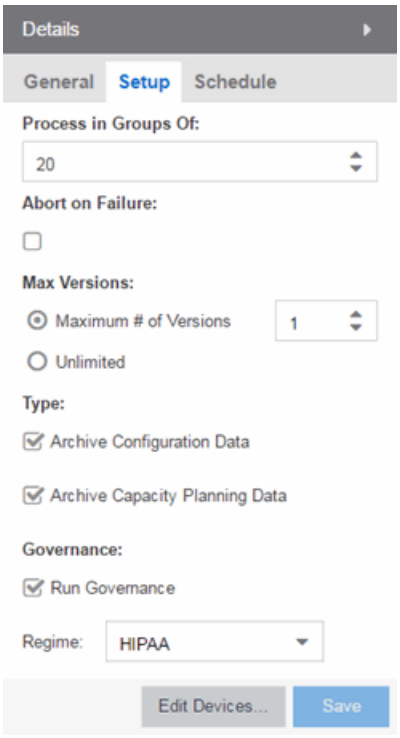
Description

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, click Edit Devices.

Setup



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. Once 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.

Governance

Select the Run Governance checkbox to perform a governance audit on the archive using the regime you select in the Regime drop-down menu.

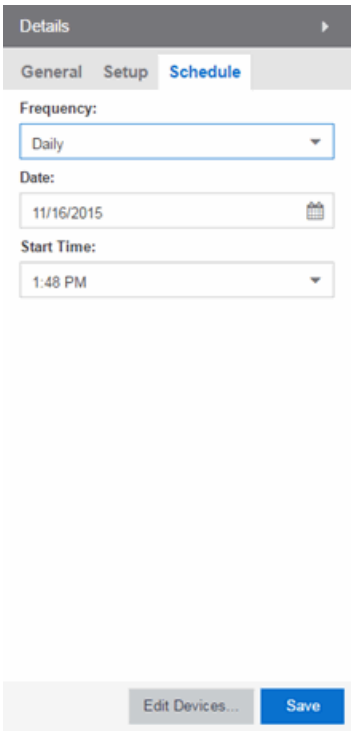
Save

Saves any changes made to the archive attributes. Selecting a Frequency of Now performs the archive immediately.

Edit Devices

Opens the Select Devices 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 menu 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 menu 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 clicking on the calendar. You can use the arrows on either side of the drop-down menu 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 **Archive** 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 Extreme Management Center 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:

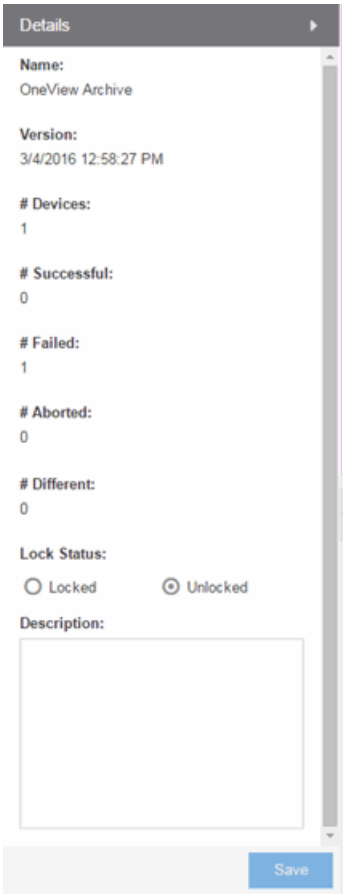
- Archive Version Right-Panel
- Archive File Right-Panel

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 **Archive** 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 Archive Wizard) is reached. To lock and unlock an archive version, right-click the archive version in the left-panel of the **Archive** 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

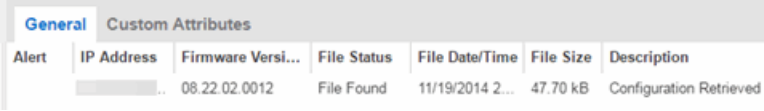
The Archive File panel appears when you select an archive configuration file in the left-panel of the **Archive** tab. It contains information about specific archive configurations.

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 Extreme Management Center 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.

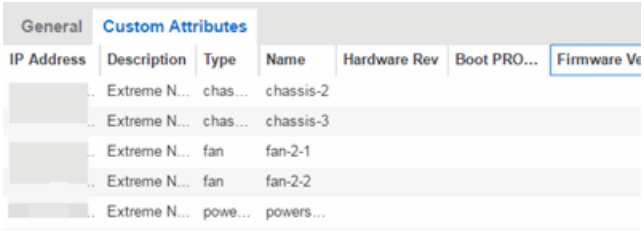
File Size
The size of the saved configuration in bytes.

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 Extreme Management Center 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 master, backup master, or slave 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:

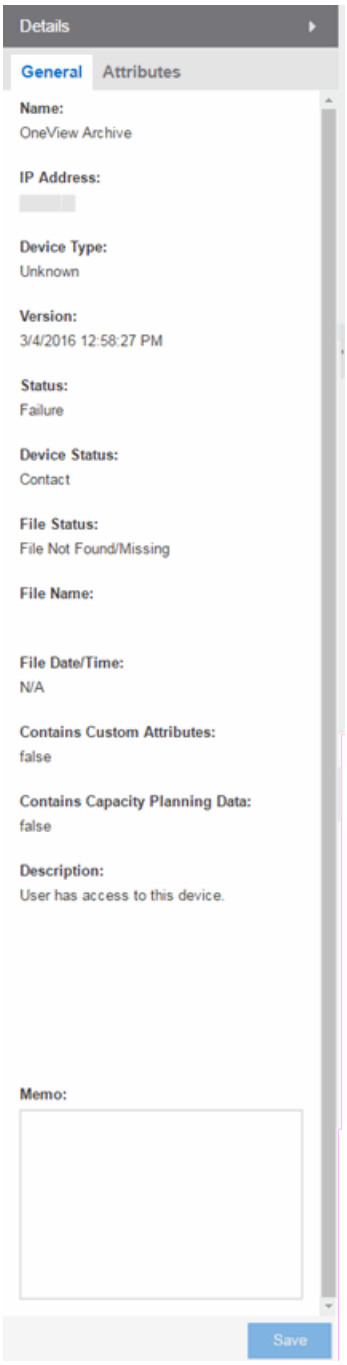
- Archive File Right-Panel

Archive File (Right-Panel)

The Archive File right-panel appears when you select an archive configuration in the left panel of the **Archive** 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



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 Extreme Management Center 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.

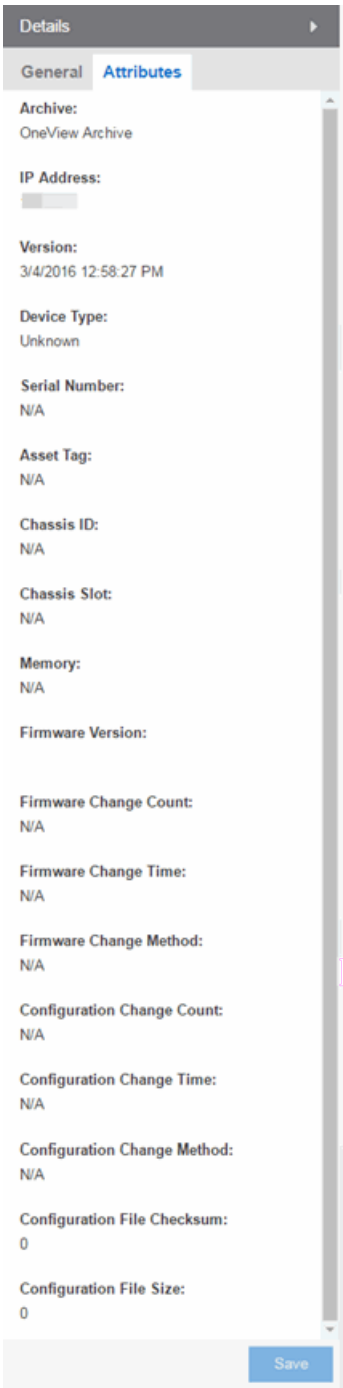
Description

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



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:

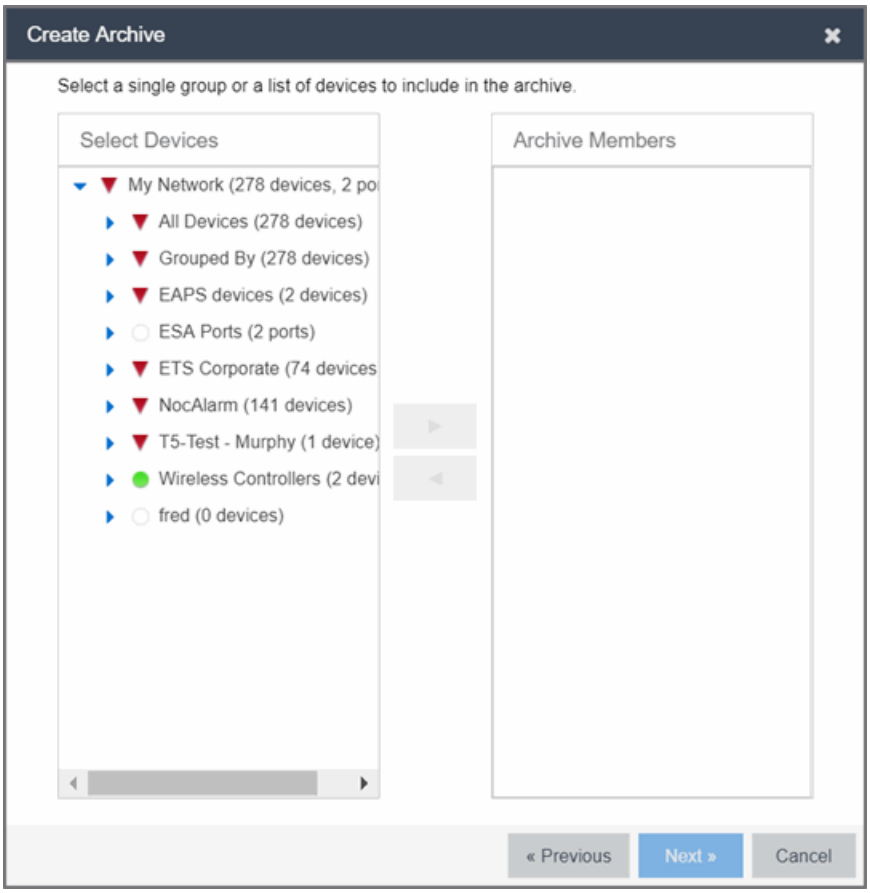
- Archive File Panel

For information on related tasks:

- How to Archive
- How to Restore an Archive

Select Devices

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. Click 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 click the left arrow button **<**.

Right Arrow Button

Click **>** to add the selected device(s) or device group to the Archive Members list.

Remove Button

Click < 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

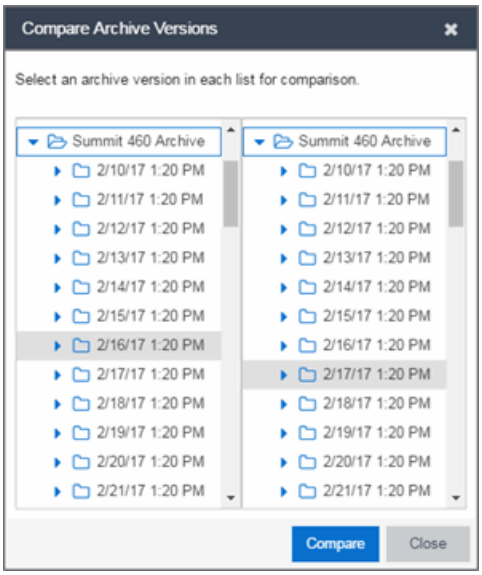
For information on related tasks:

- 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

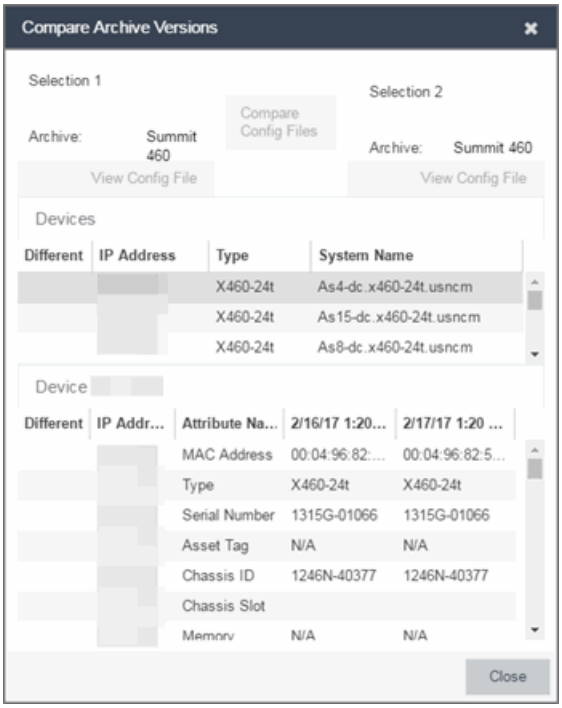
For information on related tasks:

- How to Archive
- How to Compare Archives

Compare Archive Versions

The Compare Archives window lets you compare two different archives for the same device and monitor any changes in device attributes. Extreme Management Center compares archives using a set group of saved attributes from when the archive occurred. The values for these attributes are displayed in a table with any differences between the values flagged by a yellow **Diff** icon in the **Different** column.

For information on how to perform a compare archive operation, see How to Compare Archives.



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:

- View Config File — Opens the Configuration File Viewer and displays the archived config file of the selected device. This option is only available when there are no differences between the two config files being compared.
- Compare Config Files — Opens the Configuration File Compare window and displays the two archived config files for the selected device. This option is only available when there are 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 Diff icon displays in the Different column. Select the device whose comparison results you wish to see. The results display in the Comparison Results table.

Device 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 Diff icon () in the Different column. For a definition of each attribute, see Archive File right-panel.

Diff

A yellow Diff 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.

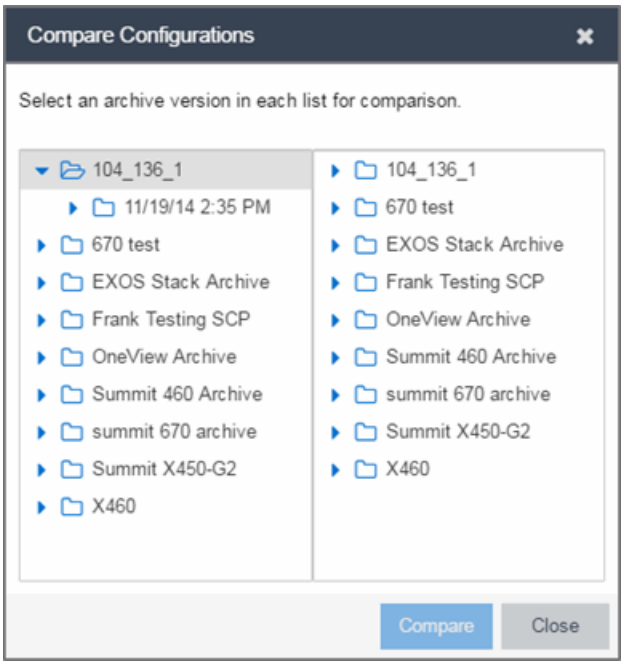
Related Information

For information on related tasks:

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

Select 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

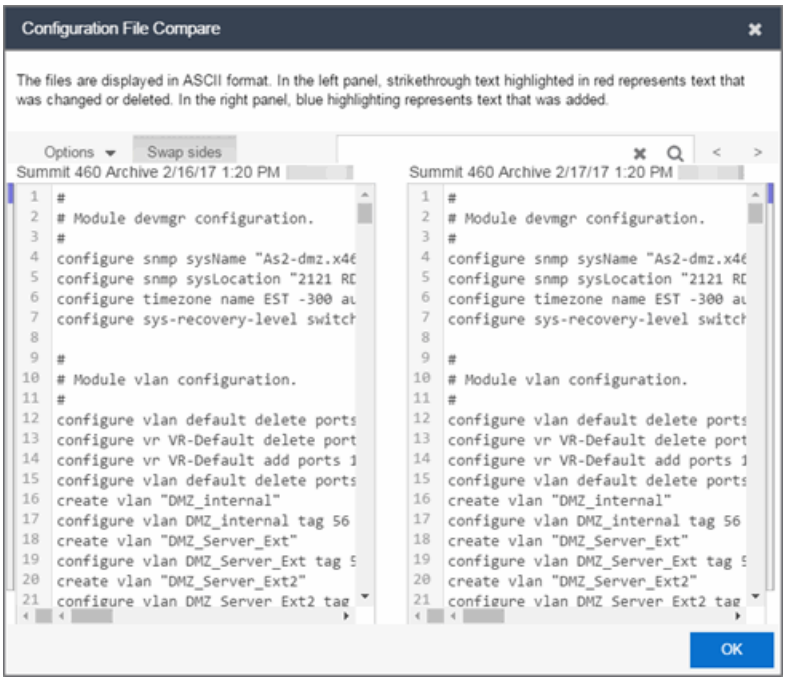
Configuration File Compare

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. Click **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. Click **OK**.
- In the Compare Archives window, click 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

Click this button to clear the search parameters from the Search box.

Find Previous Row/Find Next Row Buttons

Click 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

Clicking this button switches the sides on which each archive configuration is located.

Options Options

The Options drop-down menu 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

Click 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:

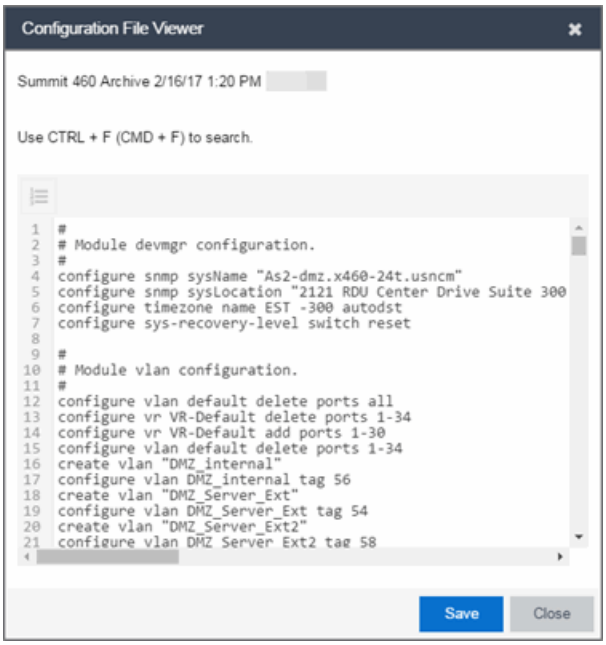
- How to Archive
- How to Compare Archives

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 clicking 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

Click Save to automatically save the configuration file to your default download folder in CFG format.

Close

Click 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:

- How to Archive
- How to Compare Archives

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, Extreme Management Center lets you schedule archives to be performed at a future time, and/or on a routine basis. Once 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 e-mail 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, Extreme Management Center generates an event log message. Using the Extreme Management Center Alarms & Events tab, you can create an alarm that monitors the log for the text "Configurations Are Different" and define an e-mail to be executed as the specific alarm action.

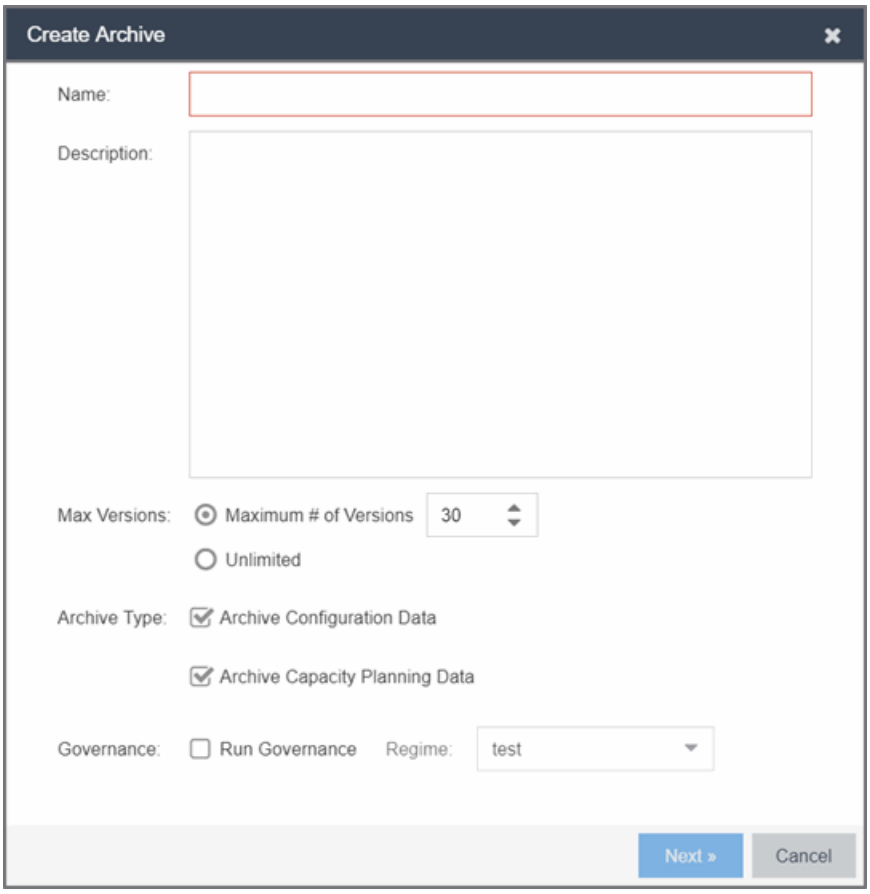
Once an archive operation is created, it is listed by name in the left-panel Archives folder. Below the archive name are the archive versions, displayed by the date and time of the creation of the version. Under the versions are individual configurations, listed by the IP address of the device whose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

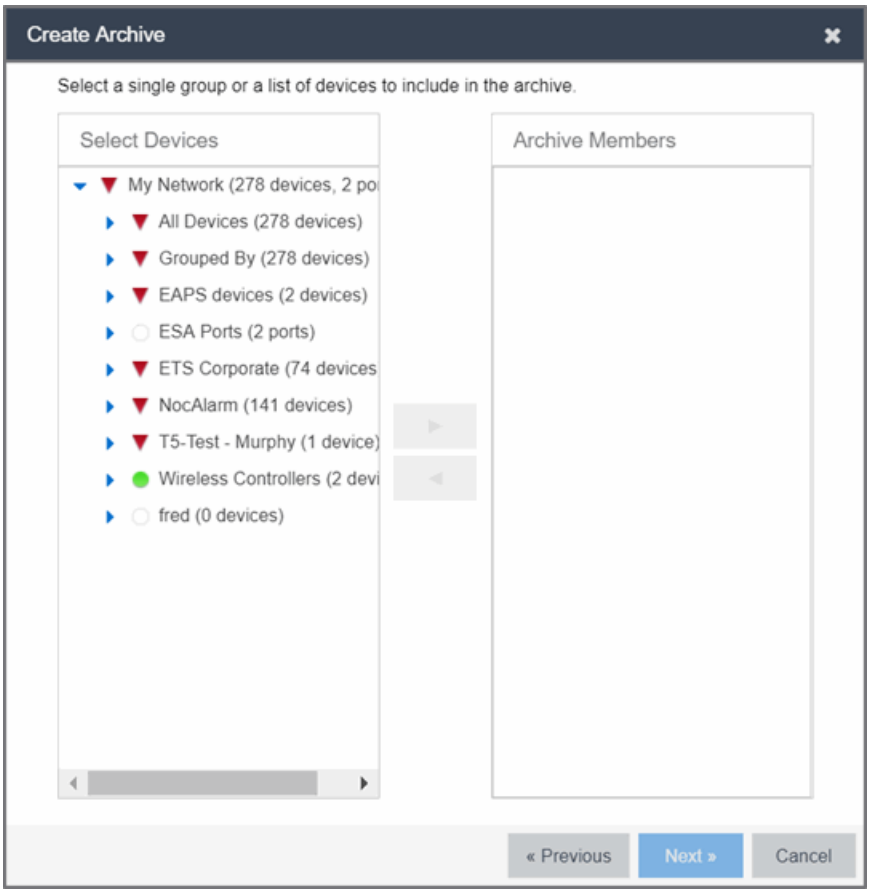
Run Governance

Select the checkbox to indicate that you want to perform a governance audit on the device archive. Select the appropriate Regime from the drop-down menu.

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. Click 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 click 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

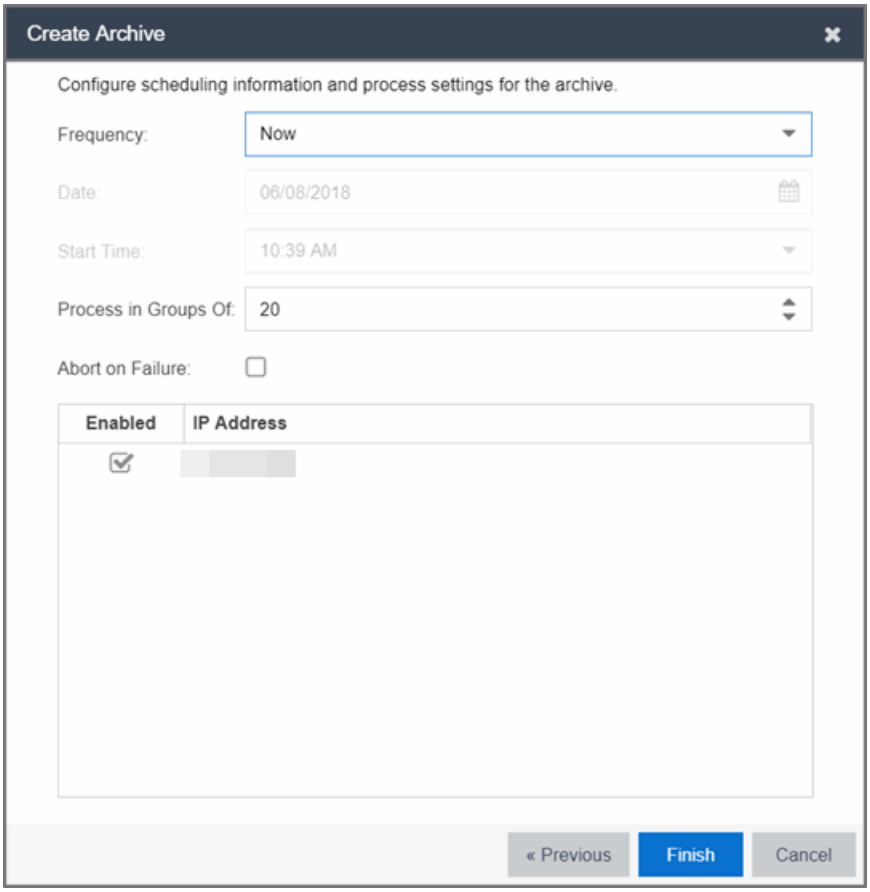
In the Devices tree, select the device(s) or device group you want to archive, and click **>** to add it to the Archive Members list.

Left Arrow Button

Select a device or device group in the Archive Members list, and click **<** 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 menu 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 menu 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 clicking on the calendar. You can use the arrows on either side of the drop-down menu 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 Archive 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

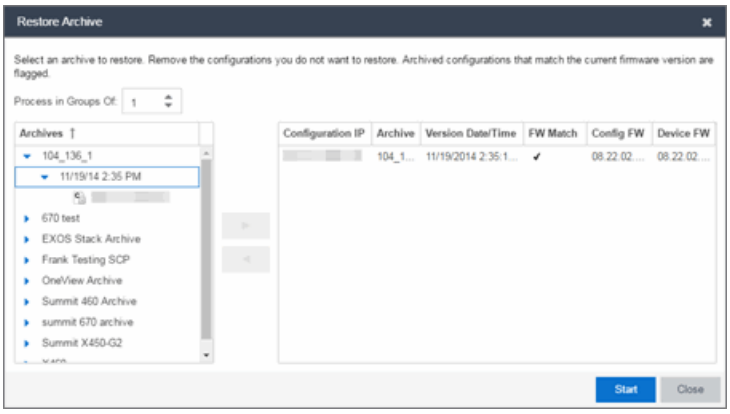
Use the **Restore Archive** window to restore saved (archived) device configuration files to one or more devices. Saved configurations are listed in the left-panel of the **Archive** tab under the appropriate archive and version. Each configuration displays an icon that identifies the type of saved data: 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 **Archive** 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 click 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. Click 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 click **>** to add it to the Configurations to Restore table.

Left Arrow Button
Select a configuration in the Configurations to Restore table, and click **<** 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
Once 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. Once 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

Once the restore is started, this area updates with status information for the restore operation.

Restore Type

The restore is performed in parallel (simultaneously) on the number of devices specified in the Process in Groups Of field. By default, the restores occur in sequential order (Process in Groups Of: 1). This is to protect against possible isolation of other devices on the restore list.

CAUTION: Because some devices automatically restart following a restore operation, performing a Restore Type greater than 1 may isolate other devices in the restore list, causing their restores to fail. Use a Process in Groups Of value of 1 (perform the restore serially,) unless you know it is safe for the selected network devices to restart simultaneously.

Start Button

Initiates the restore operation. The table at the top of the window and the status area in the bottom left of the window update with status information.

Related Information

For information on related tasks:

- How to Archive
- How to Restore an Archive

How to Archive

You can archive (save) device configuration data and/or capacity planning data using the Archive Wizard. 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, Extreme Management Center lets you schedule archives to be performed at a future time, and/or on a routine basis. Once 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.

Once 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.

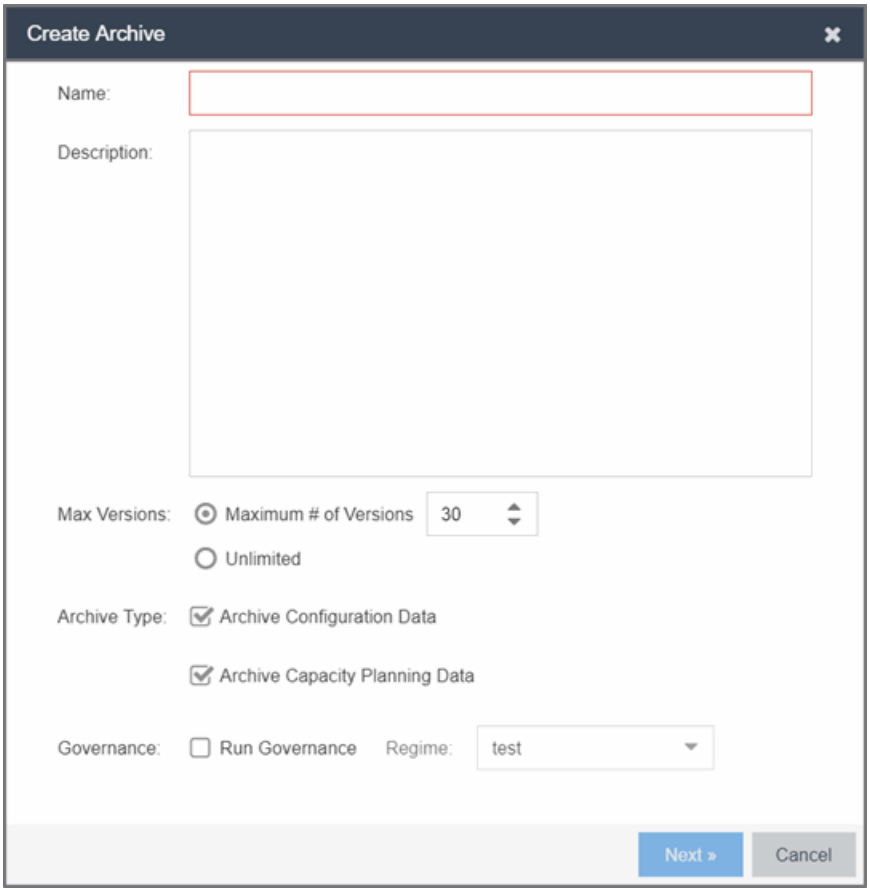
Instructions on:

- 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.

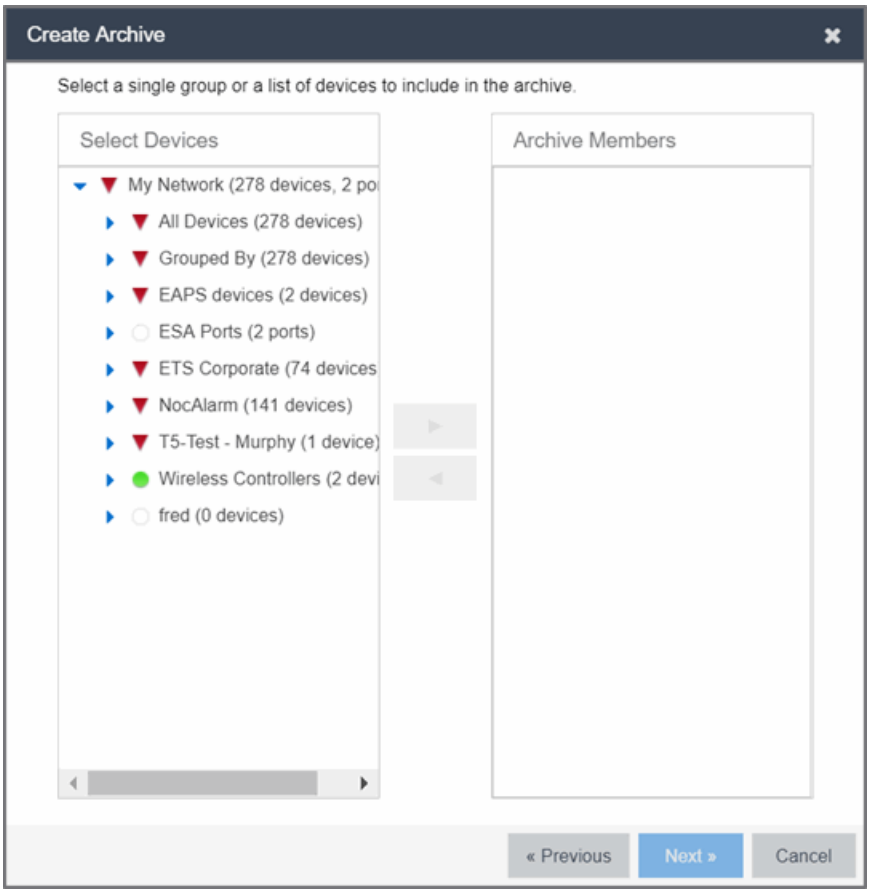


2. Enter a name and description *(optional)* of the archive operation.
3. Configure the archive setup:
    a. Specify either the maximum number of versions to be saved for this archive in the **Max Versions** field or select **Unlimited** to retain all archives. Entering a value in the **Max Versions** field allows you to limit the number of versions saved for each archive and once 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. Click 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 click the right arrow button > to move the devices to the Archive Members list.

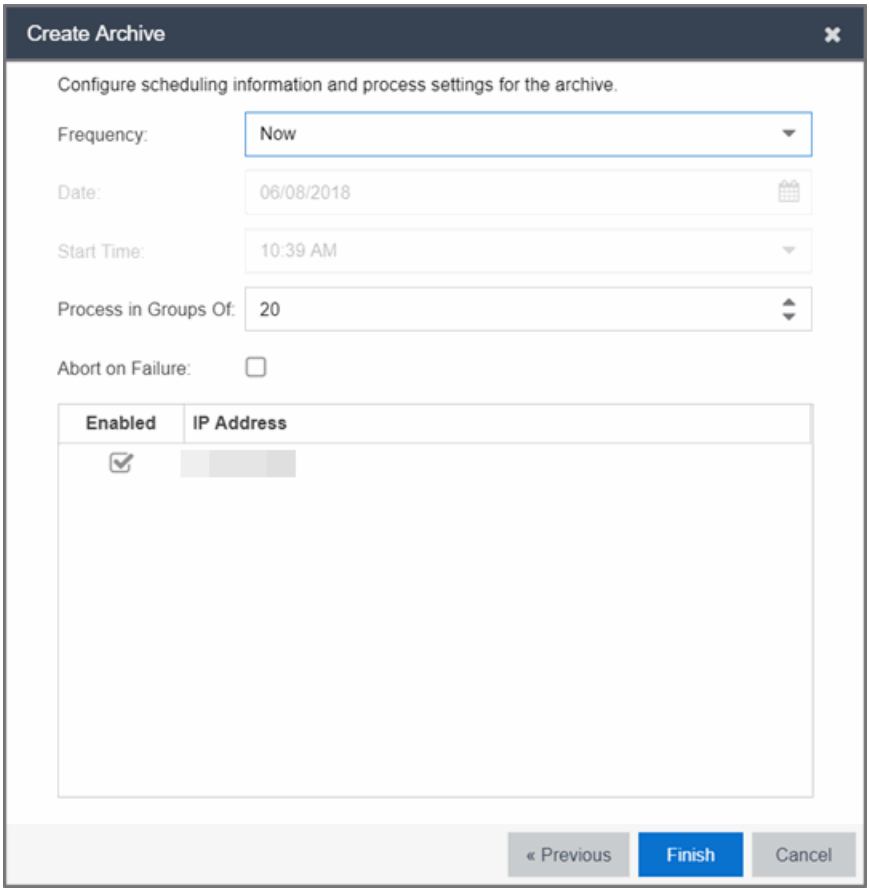
NOTE: If you select multiple tree nodes representing the same device, but with varying SNMP contexts, an archive save is performed for each context. However, the context must provide access to the MIBs required for the archive save operation or the archive for that context fails. It is recommended you 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 click the left arrow button **<**.

c. Click **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.

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. Click **Finish** to create the archive. The archive is listed by name in the left-panel of the **Archive** 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.

TIP: You can set up an e-mail 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, Extreme Management Center generates an event log message.

Saving a New Archive Version

Once 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

Once 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. Select the right-panel Archive Name right-panel.

3. Edit the archive Description and use the **Enabled** checkboxes in the Devices table to select or deselect devices to be archived, if desired.
4. Click 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 once 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 Governance** checkbox and select a **Regime** to run on the device archive, if necessary.
10. Click 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. Click **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 **Archive** tab, right-click and select **Rename** from the menu. The Rename Archive window opens.
2. Enter the new name, and click **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. Click 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

Extreme Management Center lets you compare two different archives for the same device and monitor any changes in device attributes. Extreme Management Center 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 . Use the Select Archive Versions window to select the configurations you want to compare, and the Compare Archives window to view the comparison results.

1. Access the Select Archive Versions window from the Archive tab by right-clicking an archive name, archive version, or configuration file in the right-panel navigation tree or by right-clicking in the main panel and selecting Compare Archives.
   The Select Archive Versions window opens.
2. The Select 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). Click the Compare button.

3. The 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 Configuration File — Opens the Configuration File Viewer and displays the archived config file of the selected device. This option is only available when there are no differences between the two config files being compared.
- Compare Configuration Files — Opens the Configuration File Compare window and displays the two archived config files for the selected device. This option is only available when there are differences between the two config 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

Archive 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. Click 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 click the left arrow button **<**.
   c. Click **Start**.

TIPS: If you open the Restore Archive window from an archive version or configuration in the left-panel of the **Archives** tab, the selected configuration(s) is automatically displayed under Configurations to Restore.

Check the FW Match column to see if the current firmware version on the device matches the firmware version on the device at the time of the archive.

---

3. **Initiate the Restore operation:**
   a. Specify the **Restore Type** option. The restore is performed in parallel (simultaneously) on the number of devices specified in the **Process in Groups Of** field. By default, the restores occur in sequential order (**Process in Groups Of**: 1). This is to protect against possible isolation of other devices in the restore list.

CAUTION: Because some devices automatically restart following a restore operation, performing a Restore Type greater than 1 may isolate other devices in the restore list, causing their restores to fail. It is recommended you leave the Process in Groups Of value at 1 (perform the restore serially), unless you know it is safe to simultaneously restart the selected network devices.

b. Click 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. Click 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 in Extreme Management Center

You can back up (archive) and restore device configurations as well as compare two configuration files, using the Network tab in Extreme Management Center. 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.

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 (archive) without going into the **Archives** tab:

1. Select a device in the Device list.
2. Click the **Menu** icon (≡) or right-click in the Devices list.
3. Select **Configuration/Firmware** > **Backup Configuration**.

   This performs a single configuration archive for the device. You can refer to the Extreme Management Center 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 Extreme Management Center backup creates a single archive that is not recurring, use the Archive Wizard 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. Click the **Menu** icon (≡) or right-click in the Devices list.
3. Select **Configuration/Firmware** > **Restore Configuration**.

   For additional information about restoring a device's configuration, see Restore Device Configuration in Extreme Management Center.

Compare Device Configurations

You can compare the last two archived configuration files for a selected device, without going into the **Archives** tab.

1. Select a device in the Device list.
2. Click the **Menu** icon (≡) or right-click in the Devices list.

3. Select Configuration/Firmware > Compare Last Configurations.

   For additional information about comparing device configurations, see Compare Device Configurations in Extreme Management Center.

Related Information

For information on related windows:

- Network Tab
- Devices Tab
- Firmware Tab

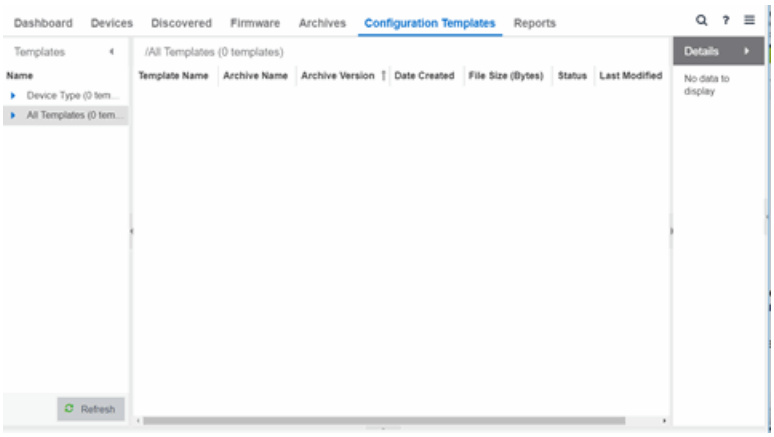
Extreme Management Center Configuration Templates

The Configuration Templates tab displays configuration templates grouped according to product family and device type. Extreme Management Center 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.

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
- All Templates
- 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 lists the product families and device types to which you can assign the firmware or boot PROM image.

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 have created.

All Templates

Extreme Management Center automatically lists each configuration template under the All Templates folder. The Details View tab appears when you select the All Templates folder in the left panel's Configuration Templates tab. The Details View displays information for each template.

Template Name

The name of the configuration template.

Archive Name

The name of the archive that contained the configuration file the template was based on.

Archive Version
The archive version that contained the configuration file the template was based on.

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. This shows whether the template is still present in the database.

Last Modified
The date and time the template was last modified.

Details View

The Details View tab appears in the right panel when you select the Device Type folder in the left panel of the Configuration Templates tab. The Details View displays information about all the configuration templates listed in the left panel under the template groups and subgroups.

Extreme Management Center provides pre-defined template groups based on product family and device type, and automatically organizes each template under the appropriate group. All of these template groups are organized in the Device Type folder.

Related Information

For information on related windows:

- Extreme Management Center Network Tab

Alarms & Events

The Alarms & Events tab displays 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 Extreme Management Center.

This Help topic provides information on the following topics:

Access Requirements

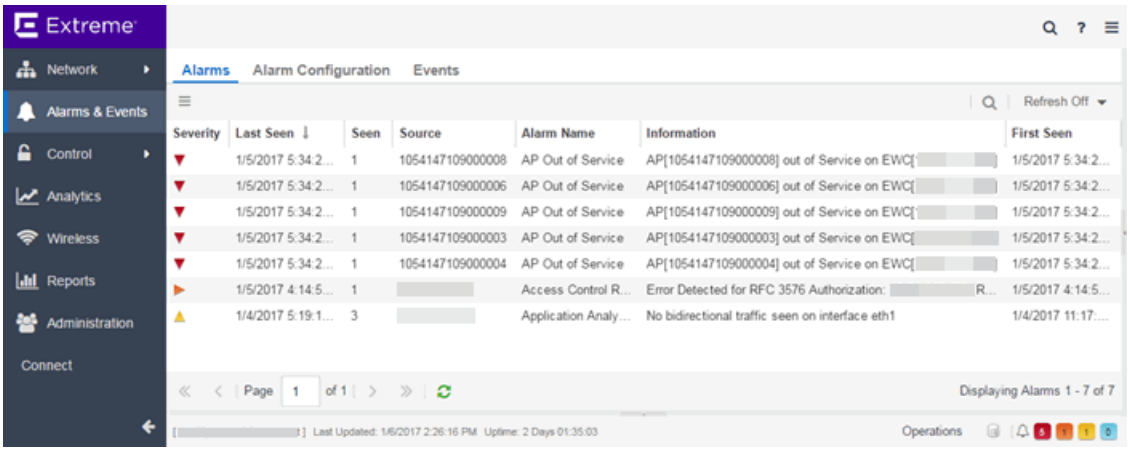
To view the information in the Alarms and Event logs, you must be a member of an authorization group assigned the appropriate Extreme Management Center capabilities:

- 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 Extreme Management Center 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 click 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 click the **Menu** icon (≡) and select **Alarm History** > **By Alarm Name** to view an Alarm History for a specific alarm.
- Right-click on the alarm or click the **Menu** icon (≡) and select **Alarm History** > **All** to view the Alarm History for all devices.
- Right-click on an alarm to clear the selected alarm or to clear all alarms. Supply a reason the alarm cleared, if necessary. which is recorded in the Alarm History.
- Right-click on an alarm or select an alarm and click the **Menu** icon (≡) and select **Edit Alarm Definition** to open the alarm in the Alarm Configuration window, from which you can edit the criteria which triggers the alarm.
- Double-click on any row in the table to open a window that displays Alarm Details.

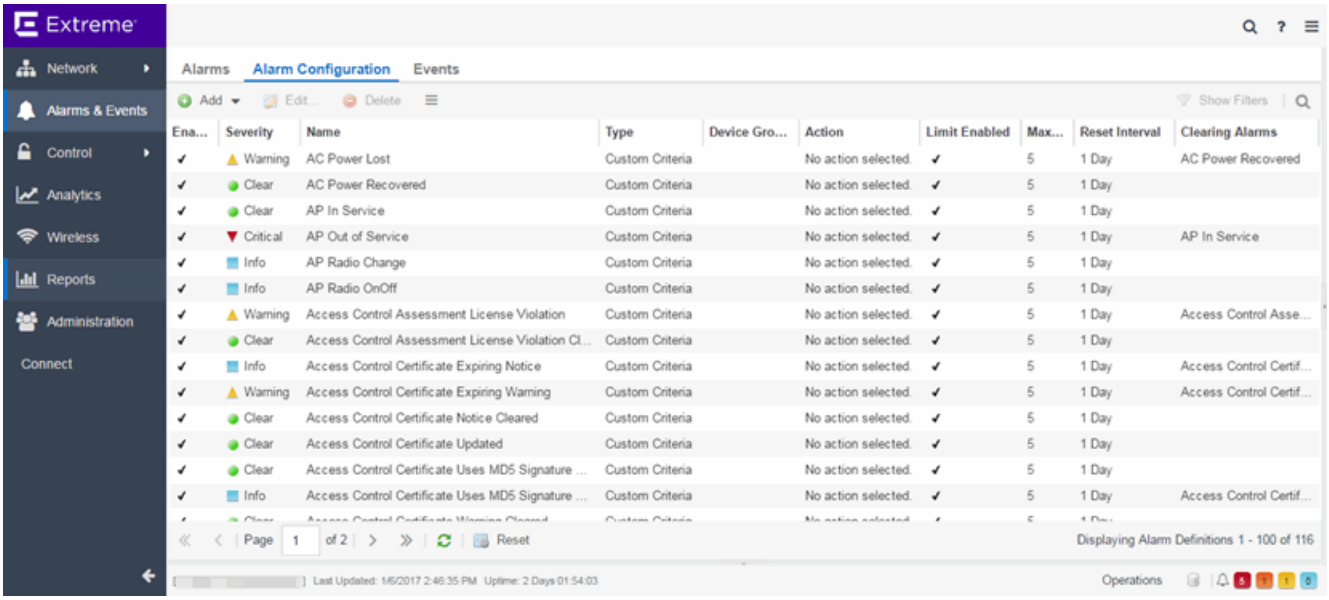
Alarm Summary

Every Extreme Management Center 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. Click on 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

The Alarm Configuration tab in the Alarms & Events tab allows you 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.

Extreme Management Center ships with a set of default alarm definitions, which you can use as is, or delete or modify them as desired.

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 — This column indicates the seriousness of an alarm definition, which posses 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. Once 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

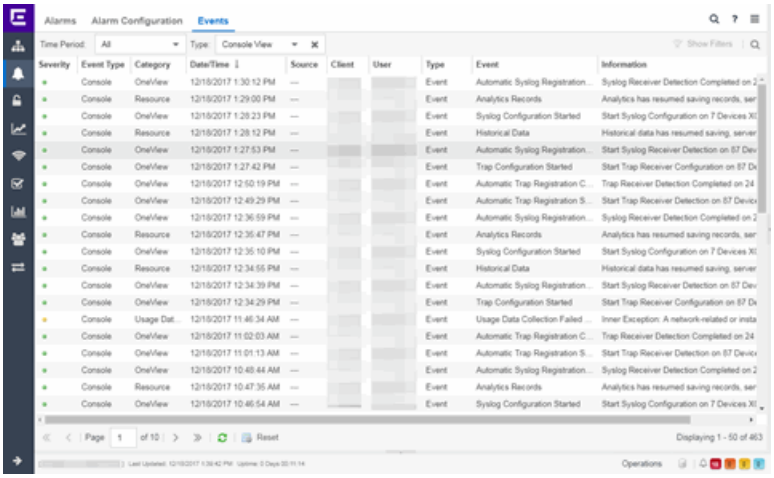
the set of configured actions is performed, not for each individual action. If Limit Enabled is not checked, there is no limit placed on the number of times the action is performed.

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. Once the count is reset, actions are executed until the Max Count is reached again. If the reset interval is set to "None", then once 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

Open the Events tab in the Alarms & Events tab to access the event log, as well as the event logs for Extreme Management Center, legacy applications, and Extreme Access Control Audit events and Wireless Audit events. In addition, you can access an event log for Extreme Management Center Scheduler events.



Use the drop-down menu 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 Extreme Management Center event logs for Extreme Management Center and legacy components (Console, Inventory, Policy, NAC Manager, and Wireless) present the same data as the event logs in the actual applications.
- The Extreme Access Control Audit event log provides information on Extreme Access Control Registration events such as when a device or user is added during the registration process, or an end-system is added/removed/updated via the registration administration web page.
- The Extreme Access Control Engine event log displays engine events.

NOTE: Installed certificates using an MD5 RSA signature algorithm now generate an event in Extreme Management Center version 7.

The Wireless Audit event log allows you to view the configuration activity on Wireless Manager.

The Application Analytics event log displays Application Analytics engine events as well and Application Analytics 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 Extreme Management Center server and database administrative events, and Extreme Management Center 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:

- Click the drop-down arrow to open the drop-down menu and select an application to include in the Events table.
- Click on the column headings to sort column data in ascending or descending order.
- Hide or display different columns by clicking on a column heading drop-down arrow and selecting the column options from the menu.
- Double-click on 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).

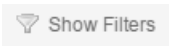
Event — Shows the type of event or trap. For traps, this column shows the name of the event as defined in the `trapd.conf` file.

Information — Shows an summary explanation of the event or trap.

Event Configuration

Select 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



— The **Show Filters** button becomes active when any filters are applied. It opens a window that shows all active filters.

 — The Search function allows you to search for full or partial matches on all fields. Enter the full or partial value you are searching for and click the **Search** button. Matching items are displayed in the table. Click the **Reset** button to clear the Search results and refresh the table.

— The paging toolbar provides four buttons that let you easily page through the table: first, previous, next, and last page. It also displays an indicator of the current and total number of pages. Enter a page number in the Page field and press Enter to quickly move to that page.

— Refreshes the page.

— 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

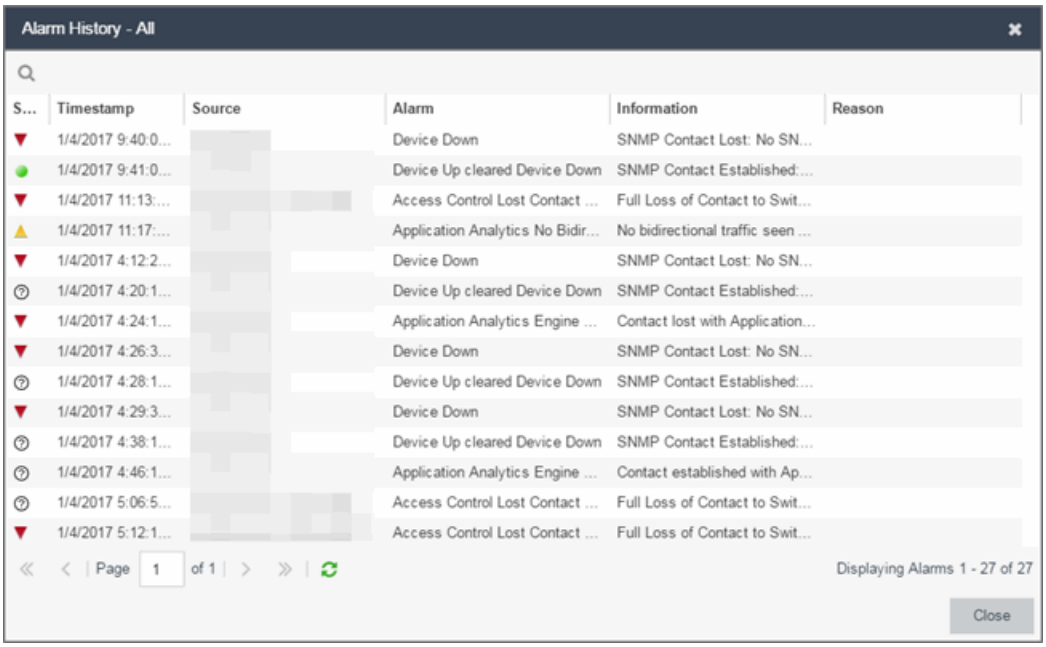
Alarm History

Extreme Management Center records alarm information whenever an alarm is raised and whenever an alarm is cleared, and displays the records 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 clicking 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. Click the Menu icon (≡).
3. Select the criteria by which the alarm history is displayed from the Menu drop-down menu:
    a. Select Alarm History > All to view the Alarm History for all devices.
    b. 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.
    c. Select Alarm History > By Alarm Name to view an Alarm History for a specific alarm.



Alarm Limits

To configure alarm action limits or 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 clicking 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:

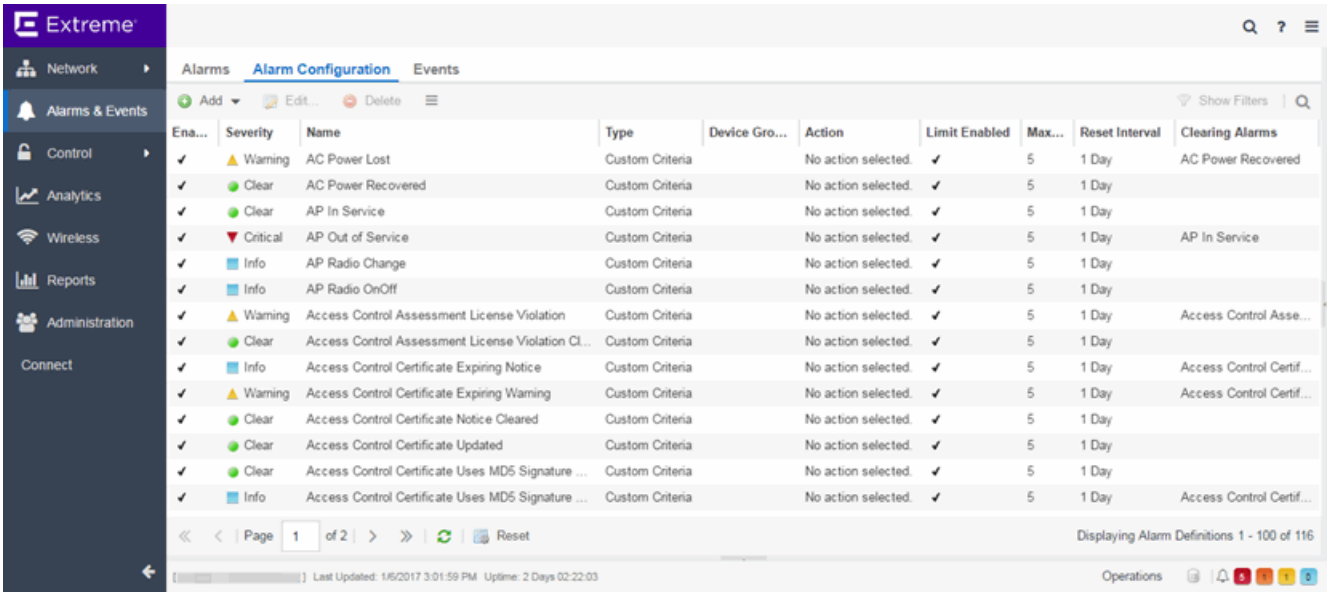
- Alarm Options

For information on related tasks:

- How to Configure Alarms

How to Configure Alarms

The Alarm Configuration tab lets you 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 Extreme Management Center. 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.

Extreme Management Center 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

You can 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.

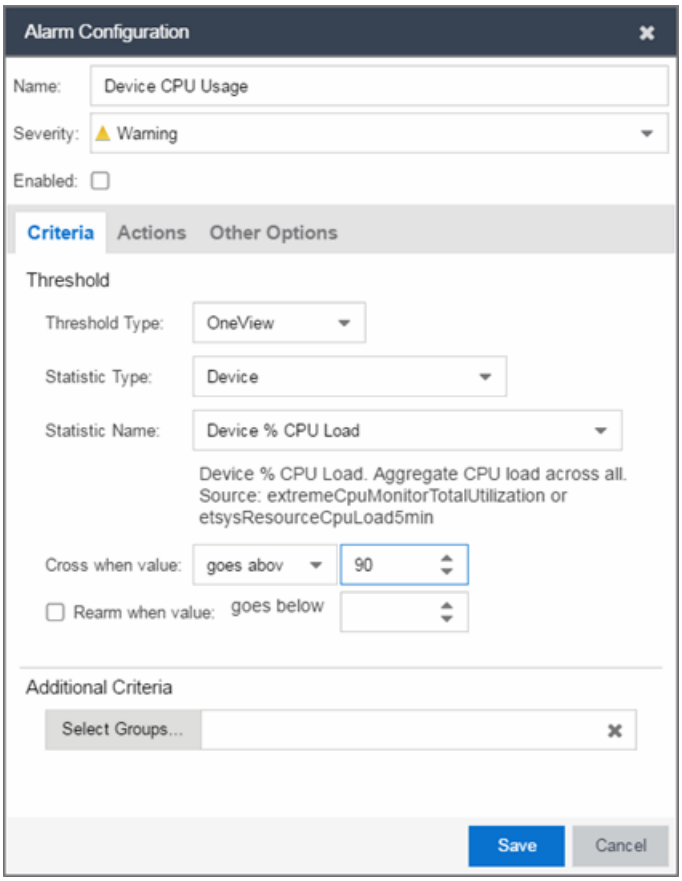
- Custom Criteria Alarm — Triggers an alarm when very specific criteria you define is met.
- Flow Alarm — Flow alarms are used for reporting network traffic flow anomalies detected by the NetFlow flow collector. An alarm triggers when a flow matches criteria you configure.
- Selected Trap Alarm — Triggers an alarm when a specific trap occurs. You are able to select from all the Trap IDs available for the devices modeled in the Extreme Management Center 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 Application Analytics. This option is disabled if your Extreme Management Center license does not include Extreme Management Center features that support threshold alarms (such as device statistics collection) and you do not have an Application Analytics license.

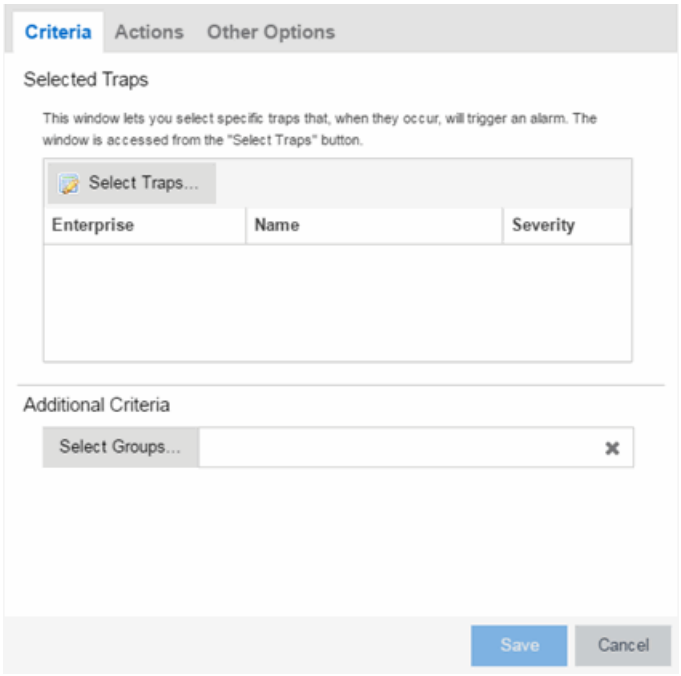
To create a new alarm definition:

1. Click the Add button and select the type of Alarm you are creating from the drop-down menu. The Alarm Configuration window opens.



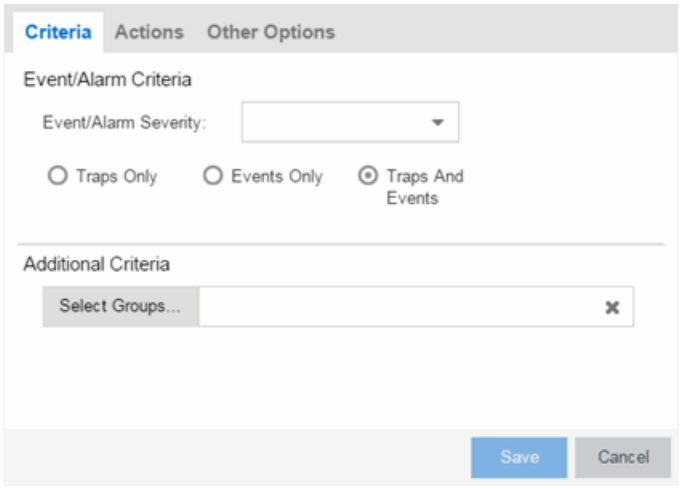
2. Enter a name for your new alarm definition in the **Name** field.
3. Select the appropriate severity level of the alarm definition in the **Severity** drop-down menu. The alarm can have its own specified severity regardless of the severity of the event or trap from which it is triggered.
    - (question 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. Click the **Select Traps** button. The Select Traps window opens.
    b. Select the traps that trigger the alarm.
    c. Click **Save**.
    d. Click **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 click **OK**. Not selecting any device groups means the alarm applies to all devices.
    e. Click the **Actions** tab to configure the actions performed when the alarm is triggered. Proceed to Step 6 for information about configuring rule actions.

- Severity Alarm



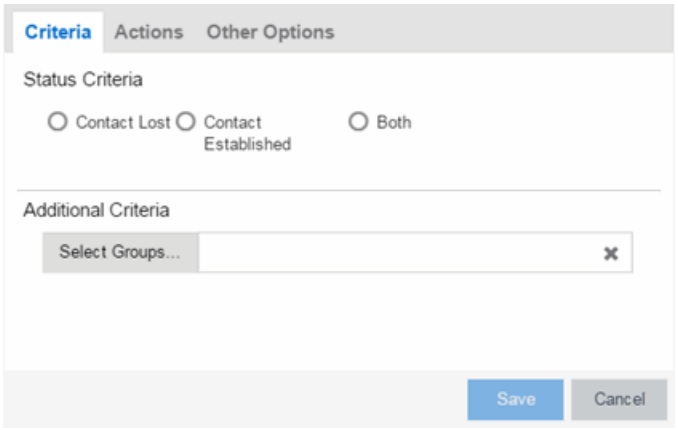
a. Select the severity of the event or trap required to generate the alarm from the drop-down menu (Emergency, Alert, Critical, Error, Warning, Notice, or Info). Traps or Events that occur and match the severity in this drop-down menu trigger the alarm. For example, you can create a severity alarm with an **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. Click **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 click **OK**. Not selecting any device groups means the alarm applies to all devices.

d. Click the **Actions** tab to configure the actions performed when the alarm is triggered. Proceed to Step 6 for information about configuring rule actions.

- Status Change Alarm

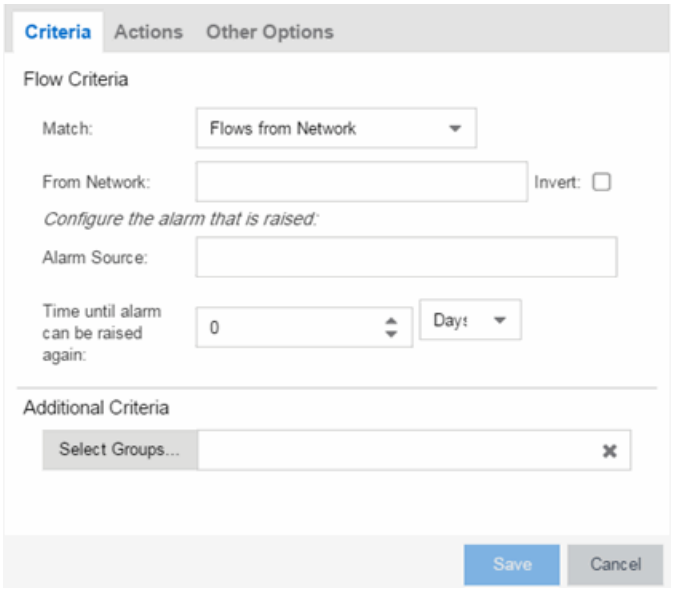


a. Select whether the alarm triggers when contact with a device is lost (Contact Lost), restored (**Contact Established**), or when contact is lost and when contact is regained (**Both**).

b. Click **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 click **OK**. Not selecting any device groups means the alarm applies to all devices.

c. Click the **Actions** tab to configure the actions performed when the alarm is triggered. Proceed to Step 6 for information about configuring rule actions.

- Flow Alarm



a. Select how the flow is matched to trigger a flow alarm in the **Match** drop-down menu. 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.

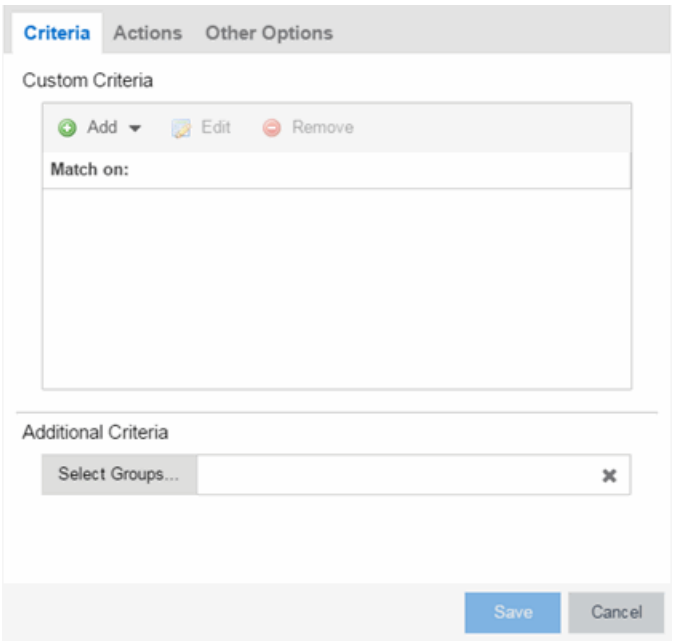
c. Enter a phrase in the **Alarm Source** field used as the source of the alarm.

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. Once you manually clear the alarm, it can be triggered again.

e. Click **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 click **OK**. Not selecting any device groups means the alarm applies to all devices.

f. Click the **Actions** tab to configure the actions performed when the alarm is triggered. Proceed to Step 6 for information about configuring rule actions.

- Custom Criteria Alarm



a. Click the **Add** drop-down menu 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.

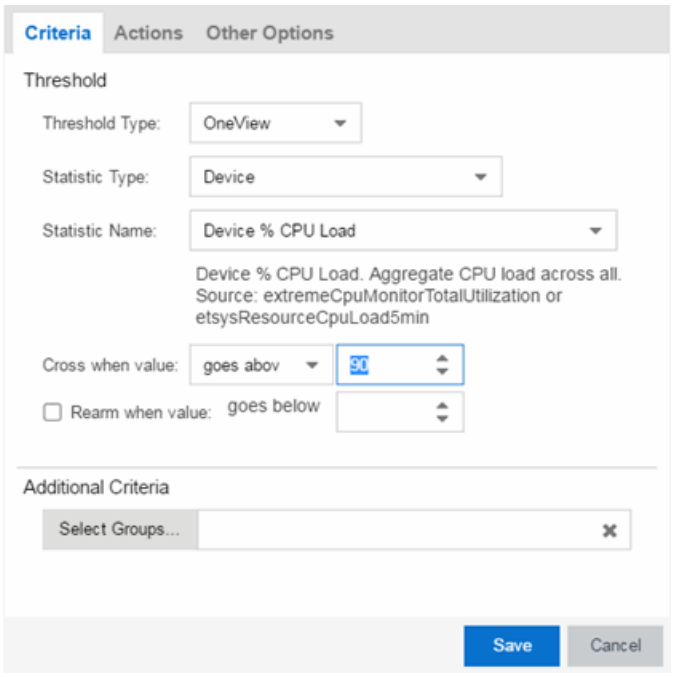
    - Match Selected — The reported Category is matched against any of the categories selected in the list.
    - Exclude Selected — The reported Category matches if it is not one of the categories selected in the list.
- Type Criteria — Select one or more message types (Event, Inform, Trap) to match against 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 clicking 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 clicking 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. Click 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 click OK. Not selecting any device groups means the alarm applies to all devices.

c. Click the Actions tab to configure the actions performed when the alarm is triggered. Proceed to Step 6 for information about configuring rule actions.

- Threshold Alarm



a. Select a Threshold Type.

- OneView — The Extreme Management Center (formerly OneView) Collector gathers historical reporting data over time, which is then

used in Extreme Management Center reports. Threshold alarms are raised when the reporting data matches a threshold alarm criteria.

- Application Analytics — The Application Analytics engine generates Application Analytics 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 Application Analytics 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 Application Analytics can be used in alarms.

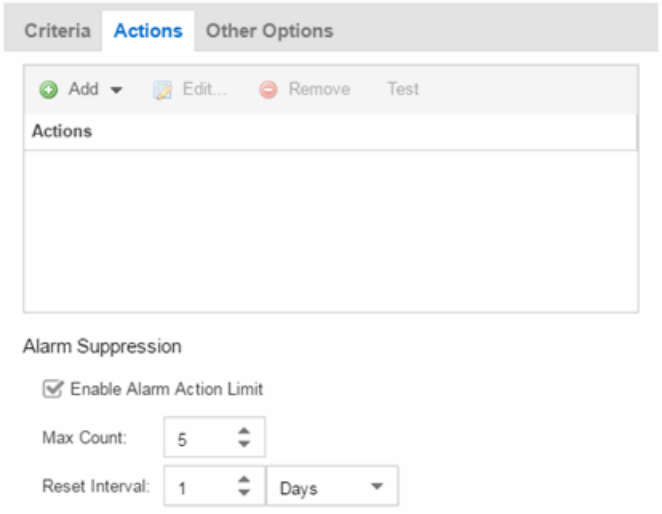
b. Select the criteria against which the threshold is compared.

c. Enter the threshold value. When the value crosses the established threshold for the criteria you select, the alarm triggers.

d. Click 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 click OK. Not selecting any device groups means the alarm applies to all devices.

e. Click the Actions tab to configure the actions performed when the alarm is triggered. Proceed to Step 6 for information about configuring rule actions.

6. Click the Add drop-down menu to select the actions performed when the alarm is triggered.

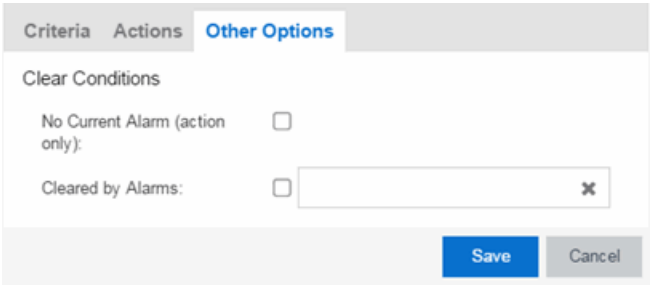


- Add Email Action — Sends an email when the alarm is triggered. Use the Destination drop-down menu to select one of your pre-defined email lists. Extreme Management Center comes preloaded with a default email list called Helpdesk. You can rename this list, but it cannot be deleted. Click the Edit Email Lists button to define a new list. (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 clicking Show Keywords. Click 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 clicking Show Keywords. Click 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 menu, 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 clicking **Show Keywords**. Click 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 Extreme Management Center 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 clicking **Show Keywords**. Click the **Save** button to save the email action to the list of actions for the alarm definition.
- **Add Task Action** — Runs a task action when the alarm is triggered. Tasks are configured on the **Tasks** tab and include scripts and workflows. Selecting **Task Action** from the **Add** drop-down menu opens the **Add Task Action** window, from which you can select a task from the **Tasks** drop-down menu.
- **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. Once 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 may 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 once the alarm limit is reached, the alarm does not reset unless manually reset.
- You can test an alarm action by clicking the **Test** button. (You must save an alarm before you can test it.) You can also override the action.

7. In the **Other Options** subtab, select how you want to clear the alarm.

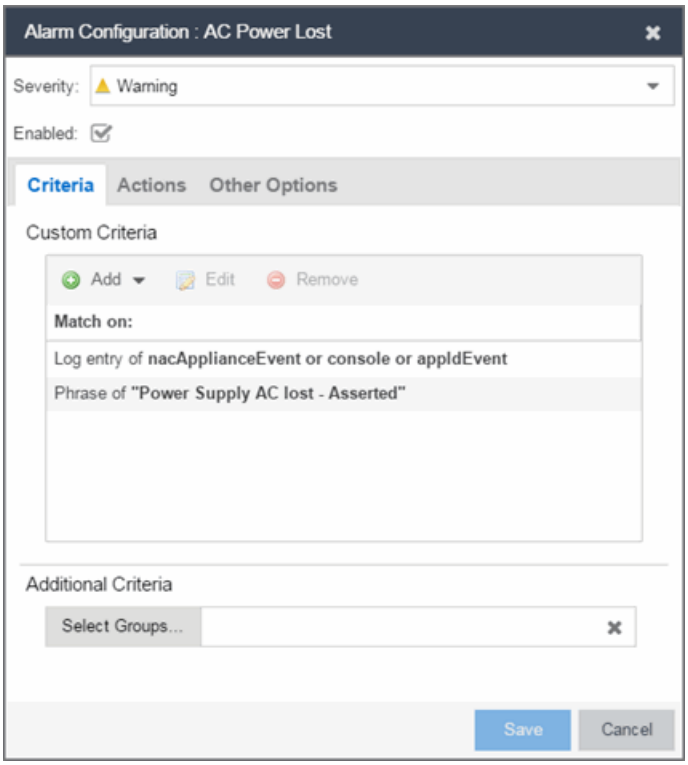


- No Current Alarm (action only) — When this option is selected, the trigger event causes the system to perform the configured actions, but does not raise an alarm that becomes associated with the alarm source. The alarm status of the alarm source does not change, and no alarm is added to the system.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

8. Click 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. Double-click the Alarm Definition. You can also click 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. Click **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 click **OK**. You can then edit the alarm to the desired configuration.

Disabling Alarms

There may 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 Extreme Management Center.

To delete an alarm, open the Alarm Configuration view, select the alarm definition you want to delete, and click the **Delete** button.

Configuring Email Settings

From the **Alarm Configuration** tab, you can configure or edit the email address to which alarm information is sent for an alarm definition when the alarm is triggered.

To configure the email address 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, click 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.

Resetting Alarm Action Limits

Once 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, click 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 once.

To enable or disable all of your alarms, open the **Alarm Configuration** tab, click 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, click 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

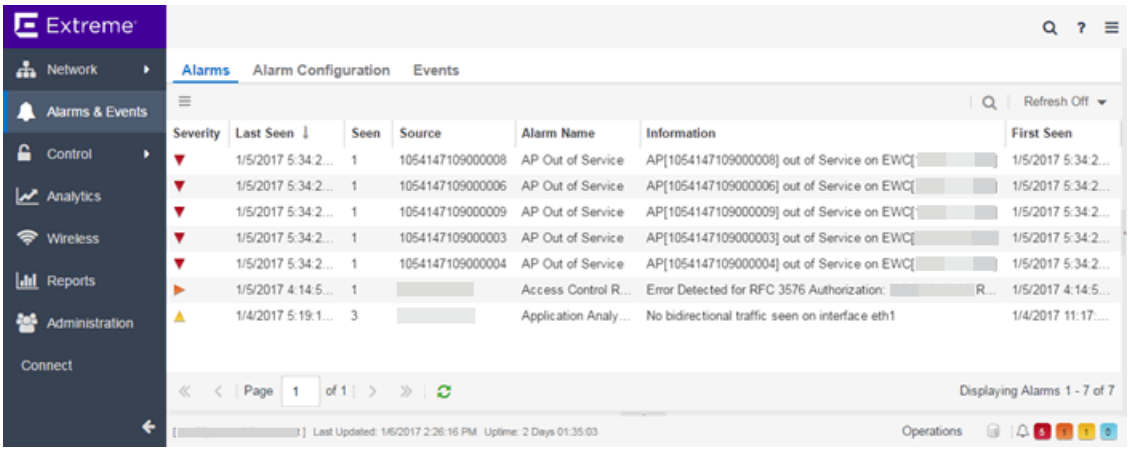
You can view device/alarm status in multiple places throughout Extreme Management Center.

Extreme Management Center

Every Extreme Management Center 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. Click on an indicator to open the **Alarms** tab filtered to display the alarms of that severity.

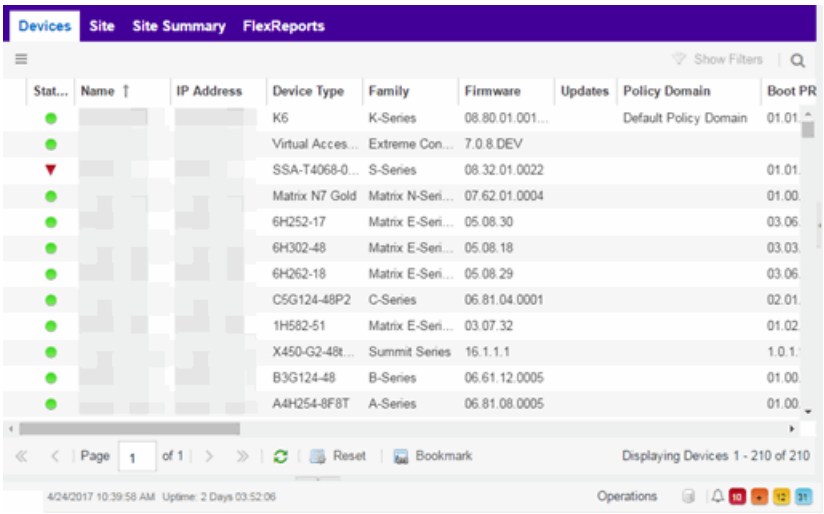
Alarms & Events Tab

You can 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.



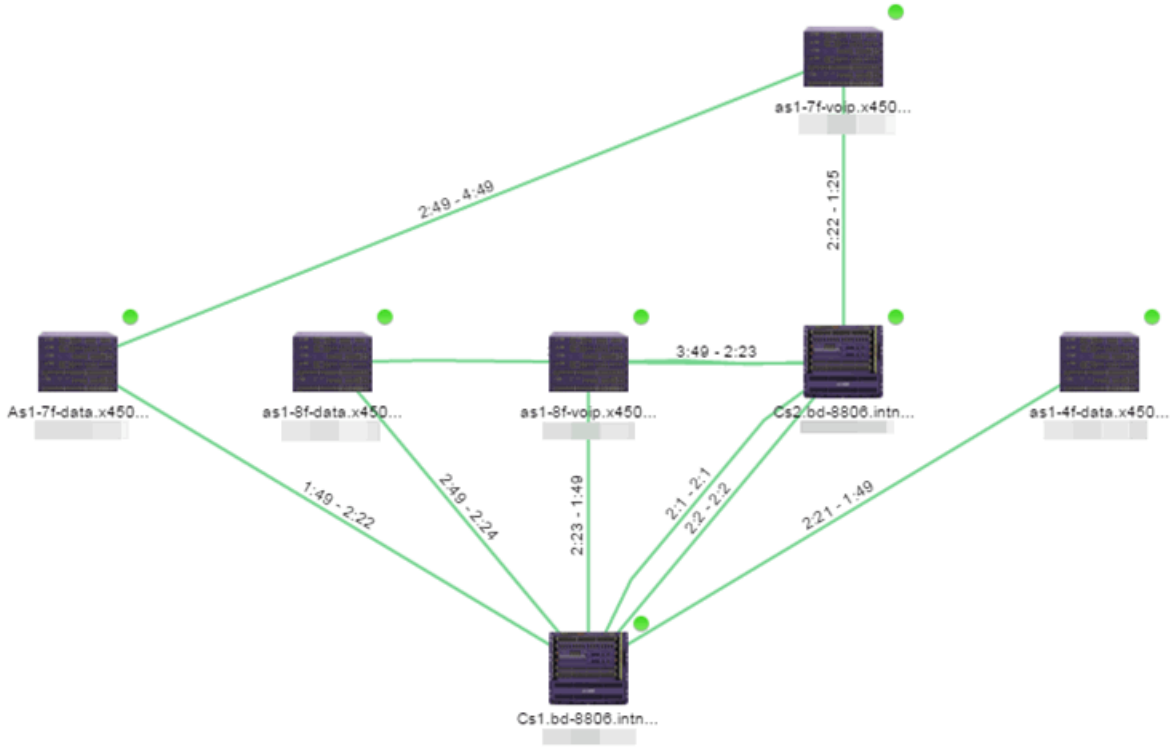
Network Tab

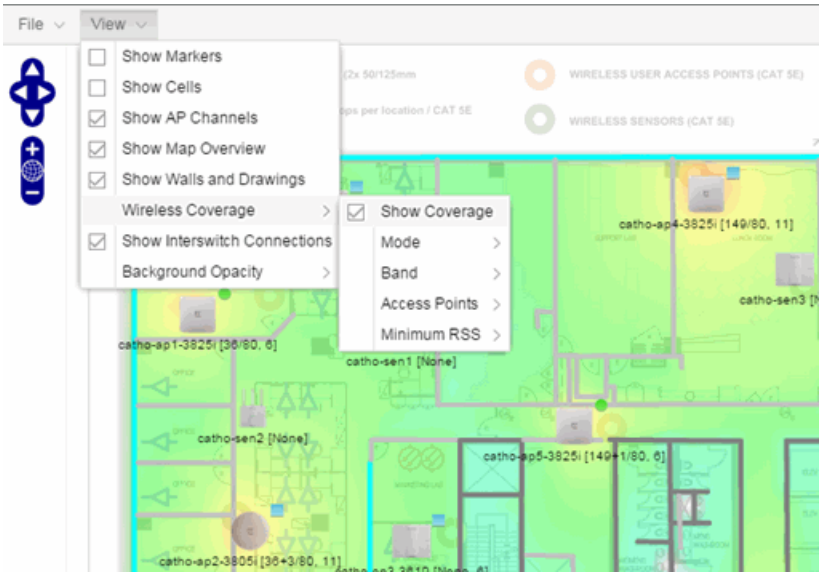
You can view the alarm status for a device in the **Status** column from within the My Network navigation tree on the **Network** tab. The colored circle indicates the severity of the most severe alarm on the device. A green icon indicates that there are no alarms and the device is up. A red icon indicates a critical alarm or the device is down. Double-click on 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.



You can also 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.





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.

In addition, a threshold alarm can be configured to "self-clear". For additional information, see How to Clear Threshold Alarms in Extreme Management Center. This is called re-arming the alarm. Re-arming allows the threshold alarm to clear itself when the monitored statistic is restored to an acceptable range, without requiring a clearing alarm. When an alarm self-clears, no action is triggered.

Related Information

For information on related concepts:

- Alarms & Events

For information on related tasks:

- How to Configure Alarms in Alarms Manager

Event Configuration Tab

The **Event Configuration** tab displays the event types used in the **Events** tab and allows you to add, edit, or delete those event types. This allows you to filter events in the event log based on event types you define.

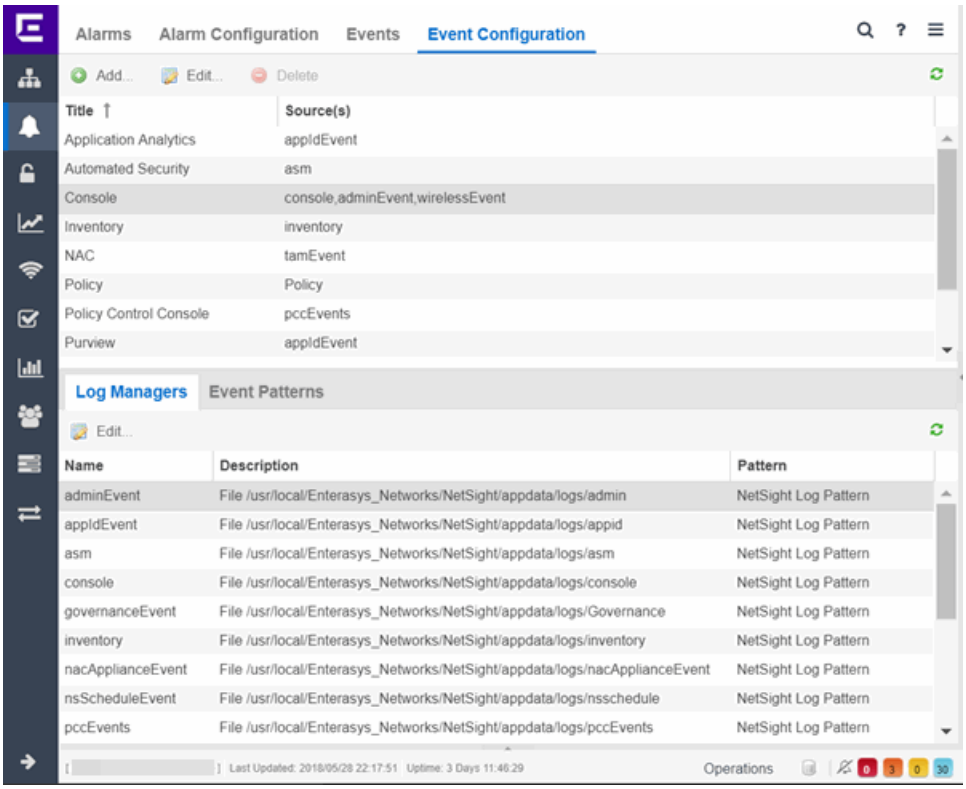
NOTE: **Access Control Audit**, **Access Control Engine**, **Admin**, **Console View**, **Governance**, **Wireless**, and **Wireless Audit** Event Types are not configurable and not displayed on the **Event Configuration** tab.

The tab contains three sections:

- Event Type
- Log Managers
- Event Patterns

Event Type

The Event Type section of the tab provides a list of the event types configured in Extreme Management Center. Event types provide you with the ability 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 Extreme Management Center 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 an Event Type** window opens, which allows you to enter a **Name** and select a **Source** from the drop-down menu.

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.

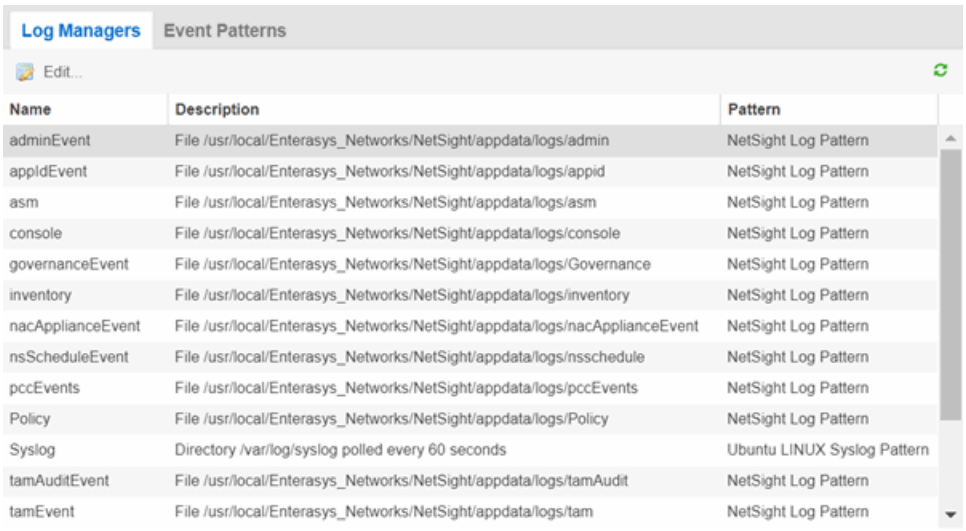
Delete

Deletes an event type you select from the list.

NOTE: You can only delete user-defined event types.

Log Managers

The **Log Managers** 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. By default, **Names** indicate the location in Extreme Management Center from which the event is generated.

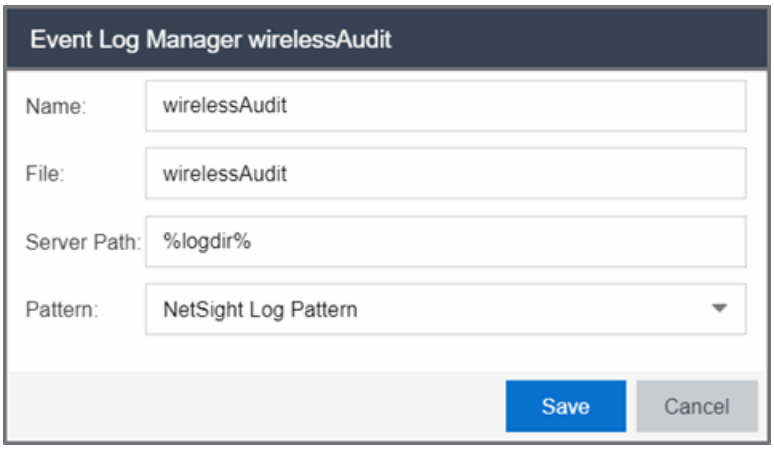
Description

Displays the name and location of the log file.

Pattern

Displays the pattern Extreme Management Center uses when generating the log file. This is vendor-specific depending on the type of device on which Extreme Management Center is generating the log. You can configure the pattern on the Event Patterns tab.

Click the **Edit** button to open the **Edit Log Manager** 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

Click to open the Add an Event Pattern window, which allows you to create a new event pattern. In the Add an Event Pattern window, enter a Name and define a format

Edit

Click 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

Click to delete an existing user-defined event pattern.

Field Types

Click 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 — Extreme Management Center 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 — Extreme Management Center 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

Click 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

Control

Extreme Management Center's Control tab provides end-system and user identity reports and control capabilities, allowing better visibility and control for IT analysts, troubleshooters, and the helpdesk.

Additionally, the Legacy menu in the Control tab menu provides access to the following Java-based legacy applications:

- NAC Manager
- Policy Manager

Access Requirements

To view the reports in the Control tab, you must be a member of an authorization group that has been assigned the appropriate capabilities:

- Extreme Management Center (NetSight) OneView > Access OneView
- Extreme Management Center (NetSight) OneView > Extreme Access Control > Access OneView Identity and Access Reports
- Extreme Management Center (NetSight) OneView > Extreme Access Control > OneView End-Systems Read Access or Read/Write Access

Navigating the Control Tab

Clicking on Control in the Menu Bar at the top of Extreme Management Center opens the Control tab. The Control tab provides access to four sub-tabs:

- Dashboard — Displays summary Extreme Management Center data including end-system data, system-level information, system events, Access Control engine information, and network health.
- Policy — Enables you to create policy profiles, called roles, assigned to the ports in your network.
- Access Control — Allows you to configure how end-users connect to your network.
- End-Systems — Displays information about end-users connected to your network.
- Reports — Provides a variety of system reports that give information about your devices, ports, and network traffic.

Additionally, the Menu icon (☰) at the top of the screen provides links to additional information about your version of Extreme Management Center.

Dashboard

Select the Dashboard tab to view information about engines and end-systems.

Overview

Provides an overview of end-system connection information. For a description of each report, click the Info button in the upper right corner of the view. Enable and disable data display in each chart by clicking on the data set in the chart legend. For example, if one segment represents a disproportionately large percentage of the total, mouse over the segment legend to the right of the chart and click on it to remove it from the pie chart.

System

Provides system-level information for engines and end-systems. For a description of each report, click the Info button in the upper right corner of the view.

Health

Provides reports on end-system assessment and state information. For a description of each report, click the Info button in the upper right corner of the view.

Data Center

The Data Center reports provide an overview of all virtual machines on the network broken down into VM distribution per Extreme Access Control 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.

Policy

Clicking the Policy tab lets you create policies for your network. It allows you to create policies for users and ports, enabling network engineers, information technology administrators, and business managers to work together to create the appropriate network experience for each user in their organization.

Access Control

The Access Control tab lets you manage the end user connection experience and control network access based on a variety of criteria including

authentication, user name, MAC address, time of day, and location. The **Access Control** tab comes with a default Extreme Access Control Configuration which is automatically assigned to your Extreme Access Control engine. You can use this default configuration as is, or make changes to the default configuration, if desired.

End-Systems

Clicking the **End-Systems** tab displays end-system connection information, and lets you monitor end-system events and view the health results from an end-system's assessment. Double-click on any row in the table to open a browser window that displays End-System Details.

Reports

The **Reports** tab allows you to view information about the end-systems connecting to your network, Extreme Access Control authentication information, and the top services and roles based on policy rules. Available reports are accessible via the **Reports** drop-down menu at the top of the tab and are grouped into the following reporting areas:

- End-Systems
- Access Control
- Access Control — Health
- Policy

Related Information

For information on related topics:

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

Policy

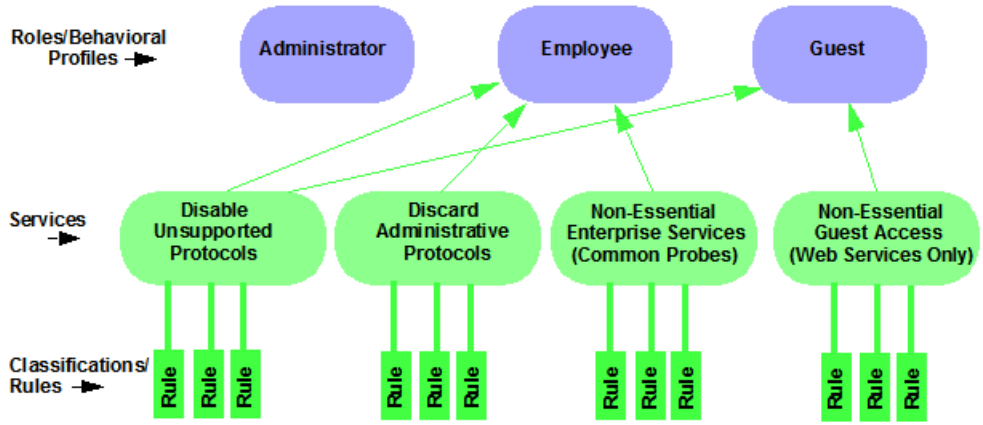
The Policy tab, contained in the Control tab of Extreme Management Center is a configuration tool that simplifies the creation and enforcement of policies on networks, enabling network engineers, information technology administrators, and business managers to work together to create the appropriate network experience for each user in their organization.

The Policy tab enables you to create policy profiles, called roles, which are assigned to the ports in your network. These roles are based on the existing business functions in your company and consist of services that you create, made up of traffic classification rules. Roles provide four key policy features: traffic containment, traffic filtering, traffic security, and traffic prioritization.

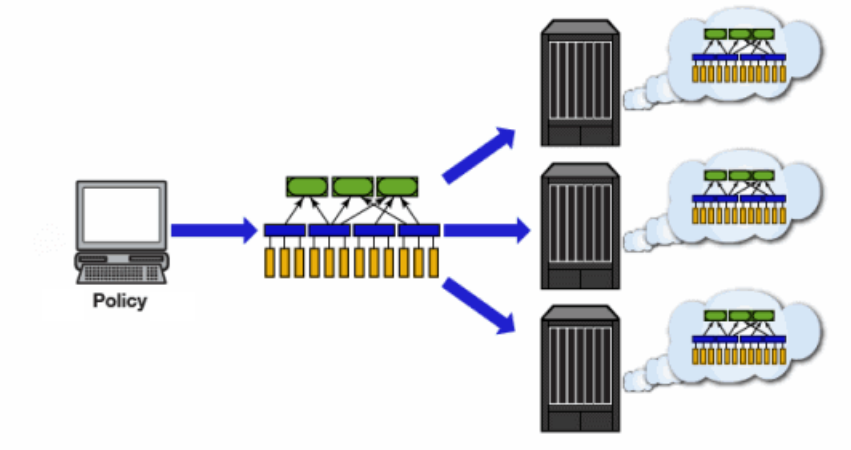
Use the following summary to guide you through the basic steps for using the Policy tab.

1. Create your Policy Domains (see How to Create and Use Domains.)
2. Add your devices to the Extreme Management Center Database and assign them to the appropriate domain.
3. If desired, group your ports into port groups (see How to Create a Port Group).
4. Create services (see How to Create a Service).
5. If desired, group services into service groups (see How to Create a Service Group).
6. Create roles (see How to Create a Role).
7. Write your configuration to your devices (see Enforcing).

The illustration below shows the Policy tab relationship hierarchy, with Rules at the base to define specific packet handling behaviors, Roles at the top to identify specific job functions in the organization, and Services in the middle, providing the interface between the two layers.



Using policy configuration tools, you can create multiple roles tailored to your specific needs and set a default policy for some or all of your network devices and ports. These policies can be deployed on multiple devices throughout your switch fabric.



The topic covers the following features:

- Understanding Policy Domains
- Understanding Roles
- Understanding Services
- Working with Service Groups
- Understanding Traffic Classification Rules
- Adding Devices
- Viewing Port Configuration Information

- Working with Port Groups
- Working with VLANs
- Viewing Classes of Service
- Saving the Domain
- Enforcing
- Verifying
- AP Aware

Understanding Policy Domains

The **Policy** tab provides the ability to create multiple policy configurations by allowing you to group your roles and devices into Policy Domains. A Policy Domain contains any number of roles and a set of devices that are uniquely assigned to that particular domain. Policy Domains are centrally managed in the database and shared between **Policy** tab clients.

The first time you launch the **Policy** tab, you are in the Default Policy Domain. You can manage your entire network in the Default Policy Domain, or you can create multiple domains each with a different policy configuration, and assign your network devices to the appropriate domain. The Default Policy Domain is pre-configured with roles and rules. The roles, services, rules, VLAN membership, and class of service in this initial configuration define a suggested implementation of how network traffic can be handled. This is a starting point for a new policy deployment and often needs customization to fully leverage the power of a policy-enabled network.

For more information about domains, see Policy Domains in the Concepts Help topic.

In the Quick Tour, we'll use the Default Policy Domain as a way to explore the basic features and functionality of the **Policy** tab. Later, you may find the Default Policy Domain useful as you create your own Policy Domains.

If you have just launched the **Policy** tab for the first time, you are in the Default Policy Domain and you can proceed to the next step, Understanding Roles. If someone else has been using the **Policy** tab before you, use the following steps to create a demonstration domain you can use for the Quick Tour.

NOTE: If someone uses the Policy tab before you, you may be prompted to save the previous domain's configuration when you create the new domain. Save the previous domain's configuration if you are going to use that configuration in the future.

To create a policy domain:

1. Select Open/Manage Domains > Create Domain. Enter the domain name **`Demonstration Domain`** for the new domain and click OK. The new Demonstration Domain opens.
2. Select Open/Manage Domains > Assign Devices to Domain. Select the devices to add to the Domain and click OK. The device is added to the left-panel Devices tab.
3. Click on the left-panel Roles/Services tab. Right-click on Roles, Services, or Service Groups and select Create Role, Create Services, or Create Service Groups, respectively to create a role, service, or service group for the domain. For additional information on creating a role, service group, or service, see How to Create a Role, How to Create a Service, or How to Create a Service Group.
4. Click on the left-panel Class of Service tab. Right-click on Class of Service and select Create COS to create a class of service for the domain. For more information on creating a class of service, see How to Create a Class of Service.
5. Click on the left-panel VLANs tab. Right-click on Global VLANs and select Create VLAN for the domain. For more information on creating VLANs, see How to Create a VLAN.
6. Click on the left-panel Network Resources tab. Right-click on Network Resources or Global Network Resources (All Domains) and select Create Network Resource to create a network resource for the domain. You can also right-click Network Resource Topologies and select Create Network Resource Topology to create a network resource topology for the domain. For more information on creating a network resource or network resource topology, see How to Create a Network Resource.
7. Select Open/Manage Domains > Save Domain. The data elements are saved to the new Demonstration Domain.

For more information:

- How to Create and Use Domains

Now that you've created the demonstration domain, we can explore the **Policy** tab in a little more depth.

Understanding Roles

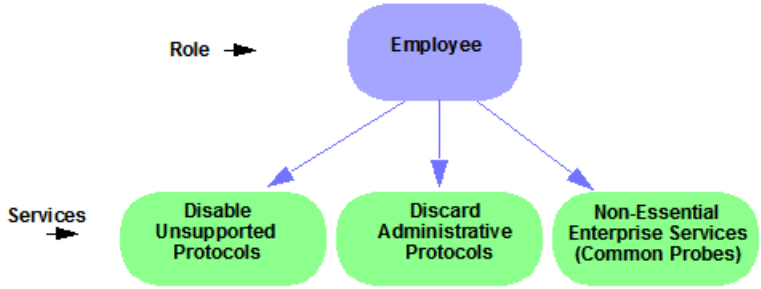
Roles are usually designed to reflect different users in your organization and to provide customized access capabilities based on the role users have in your organization. For example, accounting and engineering personnel have different network access and priority needs and therefore may have different roles.

To view information about existing roles:

1. Click on the left-panel **Roles/Services** tab in the Policy tab main window.
2. Click on the left-panel **Roles** sub-tab in the Roles/Services tab.
3. Click a role name to see a description of the role.
4. Click on the various roles listed in the left panel, and in the right panel you'll see tabs that display specific information for each role. Click the right-panel tabs to see the information they contain.

A role can be made up of one or more network access services defined in the **Policy** tab. These services determine how network traffic is handled at any network access point configured to use that role. A role may also contain default access control (VLAN) and/or class of service designations applied to traffic not handled specifically by the services contained in the role. A role can contain any number of services or service groups.

To filter through roles easily, select the Show Editable Columns drop down and select iif you wannt to hide or show editable information.



Roles are assigned to users during the authentication process. When a user successfully authenticates, the port is opened, and if a role is assigned to the

user, that role is applied to the port. A role can also be directly assigned to a port as a default role for instances when authenticated users are not assigned a role. If an end user on a port is not assigned a role when logging in (authenticating), or if authentication is inactive on a port, then the port uses its default role. However, if a user is assigned a role upon login, then that role overrides any default role on the port.

To create and define a role, right-click **Roles** and select **Create Role**.

To create a role:

1. In the **Policy** tab left panel, select the **Roles/Services** tab.
2. Select the Roles sub-tab.
3. Right-click the Roles folder, and select **Create Role**.
4. Enter the role name **`Office Assistant`** in the highlighted box and press **Ok**.

For more information:

- Role
- How to Create a Role

Role Summary Column

The Summary column shows the data for the row iin a condensed form. Hovering over the cell displays the summary data in an expanded, easy too read format. This includes the rule and service usage information, traffic description, action details, automated service relevant network resources, and toplogy information.

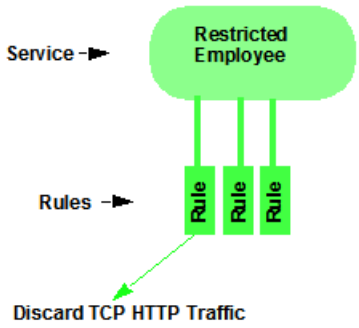
Understanding Services

Roles can be made up of one or more network access services. These services determine how network traffic is handled at any network access point configured to use that role. The **Policy** tab allows you to create Local Services (services unique to the current domain) and Global Services (services common to all domains).

Services can be one of two types:

- Manual Service — Contain customized classification rules you create.
- Automated Service — Associated with a particular set of network resources.

Manual services contain one or more traffic classification rules that define how a network access point handles traffic for a particular network service or application. For example, you might create a Manual service called "Restricted Employee" that contains a classification rule that discards TCP HTTP traffic.



We are creating a Manual service and then adding it to a role. Right now, lets take a look at the services in the domain.

To view information about existing services:

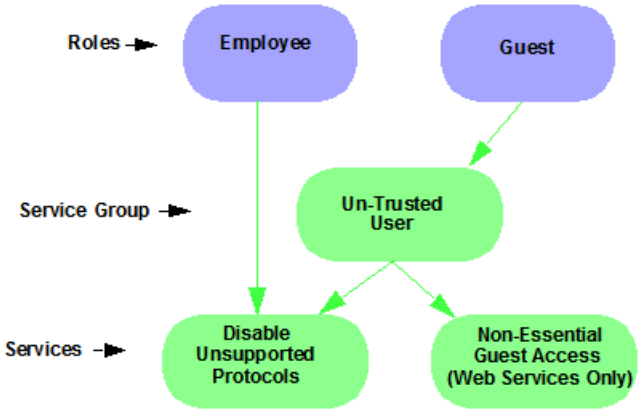
1. Click on the left-panel **Roles/Services** tab in the **Policy** tab main window.
2. Expand the **Service Repository** folder and then the **Local Services** folder.
3. Expand the **Services** folder to view a list of services.
4. Expand a service or two to see the individual classification rules that make up the service.
5. Select a service or two in the left-panel to see the right-panel tabs that display specific information for each service. Click the right-panel tabs to see the information they contain.

For more information:

- Service
- How to Create a Service

Working with Service Groups

Services can be grouped together into Service Groups. This allows you to add a set of services to one or more roles.



To view information about existing service groups:

1. Click on the left-panel **Service Repository** tab in the **Policy** tab main window.
2. Expand the **Service Repository** folder and then the **Local Services** folder. Expand the **Service Groups** folder.
3. Expand the **Acceptable Use Policy** service group to see its services. These services are also listed under the Services folder.

After you have defined and created your services, you can easily create a Service Group and then add your services to the group.

To create a service group:

1. Click on the left-panel **Roles/Services** tab in the **Policy** tab main window.
2. Expand the **Service Repository** folder and then the **Local Services** folder.
3. Right-click the **Service Groups** folder and select **Create Service Group**.
4. Enter the service group name **`Trusted User`** in the highlighted box and press **Enter**.
5. Right-click Service Group, select **Add/Remove Services** and add one or

two of the existing Acceptable Use Policy service groups into the Trusted User service group.

For more information:

How to Create a Service Group

Understanding Traffic Classification Rules

Traffic classification rules allow you to assign access control (VLAN membership) and/or class of service to your network traffic based on the traffic's classification type. Classification types are derived from Layers 2, 3, and 4 of the OSI model and all network traffic can be classified according to specific layer 2/3/4 information contained in each frame.

A traffic classification rule has two main parts:

- Traffic Description — Identifies the traffic classification type for the rule.
- Actions — Apply access control, class of service, security, and/or accounting behavior to packets matching the rule.

To view existing rules:

1. In the left-panel, navigate to the **Service Groups** tab (Roles/Services > Service Repository > Local Services > Service Groups) and expand the **Acceptable Use Policy** service group.
2. Expand the **Deny Unsupported Protocol Access** service and click on the **Discard AppleTalk** rule.
3. Use the **Edit** button to add a description to the service, for example: **AppleTalk not supported on this network**.

For more information:

- Rule
- Traffic Classification Rules
- How to Create or Modify a Rule

Adding Devices

The first step in adding network devices to **Policy** tab, is to add the devices to the Extreme Management Center database. You do this initially, by using the Discovered tab on the **Network** tab. This section assumes you have already done this. If you need more information, refer to the Network tab Help page.

Once you add devices to the Extreme Management Center database, you must assign the devices to a Policy Domain using the **Policy** tab. As soon as the devices are assigned to a domain, they are automatically displayed in the **Policy** tab device tree. Only devices assigned to the domain you are currently viewing are displayed.

To assign devices to a domain:

1. In the **Policy** tab main window, right-click **Devices** and select **Assign Devices to Domain**. The Assign Devices to Domain window opens.

   In the left panel, the Unassigned device tree contains all the devices in the database not assigned to a domain. The right panel displays the devices in the current domain.

2. For the Quick Tour, select a couple of devices to add to the domain and click **Add**. Click **OK** to add the devices.

   You can also use this window to remove a device from the current domain. This removes the device from the current domain and places it in the Unassigned folder. It does not delete the device from the Extreme Management Center database.

For more information:

- How to Add and Delete Devices
- How to Create and Use Domains

Viewing Port Configuration Information

After importing devices into the **Policy** tab, you can view and configure their ports by selecting a device and displaying its ports in the right-panel **Details View** tab or **Ports** tab.

To view port configuration information:

1. Click on the left-panel **Devices** tab in the **Policy** tab main window.
2. Expand the **Devices** folder and select a device.
3. In the right-panel **Ports** tab, expand a **Ports** or **Slot** folder to display ports on the device.
4. Right-click on a port and select **Current Domain > Show Role Details**.
5. Set Default Role, if necessary.

Working with Port Groups

The **Policy** tab allows you to group ports into User-Defined Port Groups, similar to the way you can group services into service groups. Port groups enable you to configure multiple ports on the same device or on different devices, at the same time. The **Policy** tab also provides you with Pre-Defined Port Groups. Every time one of the Pre-Defined Port Groups is accessed, the **Policy** tab goes to the devices in the current domain and retrieves the ports which fit the pre-defined characteristics of the port group.

To view pre-defined port groups:

1. Click on the left-panel **Port Groups** tab in the **Policy** tab main window.
2. Highlight a port group to display information for that port group.

For more information:

- Pre-Defined Port Groups

Working with VLANS

All traffic in a **Policy** tab network is assigned membership in a VLAN. Roles are used to assign VLAN membership to traffic either through the role's default access control or through the role's services which may include traffic classification rules that assign VLAN membership (access control).

When you open a new domain, the Global VLANs folder is prepopulated with the Default VLAN (not to be confused with a default VLAN assigned to a role, although the Default VLAN *could* be a default VLAN for a role). You can then create additional VLANs and assign them as default access control for a role and/or use them to define traffic classification rules. You can view the roles and

services associated with a VLAN by selecting the VLAN in the left-panel. You can also make role and service changes from this window.

Island VLANs are used in Policy VLAN Islands, which enable you to deploy a policy across your network, while restricting user access to only selected local devices. The **Policy** tab allows you to view currently configured Island VLAN information.

To view VLANs:

1. From the **VLANs** tab, expand the **Global VLANs** folder to see individual VLANs.
2. Click on the Default VLAN listed and view the VLAN information in the right panel.

For more information:

- How to Create a VLAN
- General Tab (VLAN)
- Policy VLAN Islands

Viewing Classes of Service

The **Policy** tab lets you create a class of service (CoS) that includes one or more of the following components: an 802.1p priority, an IP type of service (ToS) value, rate limits, and transmit queue configuration. You can then assign the class of service as a classification rule action, as part of the definition of an automated service, or as a role default.

To view Classes of Service:

1. From the **Policy** tab, select the **Class of Service** tab from the left-hand panel. The Class of Service section expands.

   Notice that the window is pre-populated with eight static classes of service, each associated with one of the 802.1p priorities (0-7). You can use these classes of service as is, or configure them to include ToS/DSCP, drop precedence, rate limit, and/or transmit queue values. You can also rename them, if desired. In addition, you can also create your own classes of service (user-defined CoS).

2. Select the Class of Service and all information related to the Class of Service selected is displayed in the right-panel.

For more information:

- Getting Started with Class of Service
- How to Define Rate Limits
- How to Configure Transmit Queues
- How to Create a Class of Service

Saving the Domain

After changing a policy domain, save the domain. This notifies all clients viewing the domain there is a change, which prevents them from saving a domain with an incorrect configuration. The system automatically updates their view with the new configuration.

To save a domain, select Open/Manage Domains > Save Domain.

The domain is saved and automatically updates for all clients viewing the domain. To discard unsaved changes you made to a domain, open the Open/Manage Domains > Open Domain menu and select the domain in which you are currently working.

For more information:

How to Create and Use Domains

Enforcing

Any time you add, make a change to, or delete a role or any part of it (any of its services and/or rules), the devices in your current domain need to be informed of the change so that your revised policy configuration can take effect. This is accomplished by enforcing — writing your policy configuration to a device or devices. Enforce operations are performed only on the current domain.

To enforce to all devices in the current domain, select Open/Manage Domains > Enforce Domain. To enforce to a single device, right-click the device and select Enforce.

Enforce Preview

The Enforce preview tool has a very similar setup to the Enforcing Domain tool. To view the enforce preview, select Open/Manage Domains > Enforce Preview and select the device to preview from the left dropdown.

Note: If the device has a red exclamation type next to it in the left panel, then it is incompatable with the domain configuration and should be corrected.

Enforcing preview shows you a summary of the stats and info, roles, rules, and services on device. The three preview tabs include:

Device Stats & Info: Shows information on supported role/rule counts, etc.

Roles & Rules: Shows a grid panel with roles and rules that will enforce the device. If supported, it will show a green circle. A yellow circle indicates a rule not being supported, and a red circle denotes a role not being supported. Right-click and select View/Edit which will close enforce preview and rbing you to the item you wish to make changes to.

Classes of Service: Shows details of the Class of Service and the related rate limit configuration.

Rule Counts Reported by Devices

Every device has a maximum number of rules that it can follow. Going over the max numberr of rules on a device will create enforce failures. The max supported rules by rule type are mainly a concern for EXOS device, which now report the max a type supports via the value returned for etsysPolicyRuleAttributeMaxCreatable for any rule type in that group. For example, reading either instance 1 (macSource(1)) or 2 (macDestination(2)) will return the supported number of layer 2 (MAC) rules. The 4 rule “types” and the rule types () that these include are:

- MAC
    - macSource(1)
    - macDestination(2)
- IPv4
    - ip4Source(12)
    - ip4Destination(13)

    - ipFragment(14)
    - udpSourcePort(15)
    - udpDestinationPort(16)
    - tcpSourcePort(17)
    - tcpDestinationPort(18)
    - ipTtl(20)
    - ipTos(21)
    - ipType(22),
- IPv6
    - ip6Destination(10)
- L2
    - etherType(25)

The total max supported number of rules for EXOS devices is the sum of these 4 types, NOT the value returned by etsysPolicyRulesMaxEntries (due to that including other things by the FW).

The devices supported number of rules is only read when the device is added to the domain, the firmware is upgraded, or the device is manually refreshed.

For more information:

Enforcing

Verifying

To determine if the roles currently in effect on your domain devices match the set of roles defined in your current Policy Domain configuration, use the Verify feature.

AP Aware

An AP is assigned "AP Aware," all traffic through this port will not need authentication. This new Role default action is configurable via a new AP Aware setting in the role configurations view. To enable AP Aware:

1. Click on the left-panel **Roles/Services** tab in the Policy tab main window.
2. Click on the left-panel **Roles** sub-tab in the Roles/Services tab.
3. Click a role name to see a description of the role.
4. Using the scroll bar, scroll to find the **AP Aware** column.
5. Double-click **Disabled**, and in the drop-down, select **Enabled**.

When enforce or verify occurs, the secondary logic runs which inspects all AP Aware enabled roles, and for each role finds all in-use VLANs (rule actions, role default action) and automatically adds them to that role's tagged VLAN egress list if they are not already present. This is then used for the enforce/verify logic, and returned to the client so the domain is updated accordingly.

The domain data may change from doing an enforce/verify, and needs to be saved.

For more information:

Verifying

Related Information

For information on related concepts:

- Policy Tab Concepts
- Traffic Classification Rules

For information on related windows:

- Main Window

Policy Configuration Considerations

Review the following configuration considerations when installing and configuring Extreme Management Center's **Policy** tab.

- General Considerations
  - Authenticating without Policy
  - Terminating Role Override Sessions
  - Port-Level MAC to Role Mappings

General Considerations

Authenticating without Policy

This section discusses how authentication works in a network where end users must authenticate, but there are no roles (policy) for authenticated users defined on the network devices.

The following table shows Authentication Behavior for each device type when the authenticated role is not defined on the device:

Authentication Type	K-Series, S-Series, N-Series Gold and Platinum	E6/E7	E1	RoamAbout R2 RoamAbout AP3000	C2/B2
802.1X	Successful	Successful	Successful	Successful	Successful
MAC	Successful	Successful	Successful	Successful	Successful
Web-Based	Successful	Successful on firmware version 5.06.x. Failed on older firmware versions.	Successful	Web-Based Auth Not Supported	Successful

The following table shows Authenticated Traffic Behavior for each device type when the authenticated role is not defined on the device:

Authentication Type	N-Series Gold and Platinum 4.11 and earlier	K-Series, S-Series, N-Series 5.01 and later Gold and Platinum	E6/E7	E1	RoamAbout R2 RoamAbout AP3000	C2/B2
802.1X	1	3	2	2	3	2
MAC	1	3	2	2	3	2
Web-Based	1	3	2	2	Web-Based Auth Not Supported	2

1 - Traffic is forwarded based on the 802.1Q PVID and 802.1p priority for the port, regardless of whether the port has been assigned a default role. Authenticated users display a current role of "None" in the Port Usage tab.

2 - Traffic is forwarded based on the port's default role and authenticated users will display the default role as their current role in the Port Usage tab. If no default role has been assigned to the port, the port's 802.1Q PVID and 802.1p priority are used, and the current role will be "None."

3 - Traffic is forwarded based on the Invalid Role Action configuration at the device level in the Policy tab.

Terminating Role Override Sessions

On Port Usage tabs, you cannot terminate Role Override (IP) or Role Override (MAC) sessions created through the CLI (command line interface).

Port-Level MAC to Role Mappings

Enforcing port-level MAC to Role mappings could potentially remove rules as an intrusion detection response.

Import From Device

If you perform a Verify operation following an Import Policy Configuration from Device, the Verify may fail. This is because the import operation imports only roles and rules from the device, not the complete policy configuration.

Also, if you import from more than one device and the configuration is not the same on each device, Verify fails. This is because the imported configuration will not match the configuration on any one device.

Flood Control

Individual Class of Service granularity is unsupported on fixed switches, so if any CoS is assigned a Flood Control rate, all Class of Service on these devices use

that rate.

C1 Considerations

Review the following considerations prior to configuring policy on C1 devices:

Policy Support

Policy support on C1 devices utilizes both a port-level role and a device-level role. In the Policy tab, a role is a set of network access services made up of traffic classification rules. It may also contain default Access Control (VLAN) and/or Class of Service settings applied to traffic not handled specifically by the rules contained in the role. Although both the device-level and port-level roles may contain all of these components, only certain portions of each role are used when applied to a port on a C1 device.

On the C1, classification rules are implemented at the device level through a device-level role. The Policy tab allows you to set a unique device-level role for each C1 device. The device-level role is a regular role that defines how inbound traffic is handled in terms of classification rules and default Class of Service assignment. In other words, all classification rules are taken from the device-level role, and any rules defined in the port-level role are ignored when applied to a port. The Class of Service setting is also implemented through the device-level role and ignored in the port-level role. However, the default Access Control setting of the device-level role is ignored, and is defined through the port-level role.

Classification rules from the device-level role are only applied to ports which also have a port-level role applied (either statically or dynamically). This allows you to exclude the device-level role from uplink ports and hosts ports, by not applying a port-level role to these ports and not enabling authentication on them.

When a port-level role is applied to a port, it overrides any PVID and Class of Service settings defined on the port through Console or local management. When a device-level role is applied to a port, it also overrides these PVID and Class of Service settings, and overrides any Class of Service setting defined in the port-level role. It does not override any default Access Control setting defined in the port-level role.

In addition, if the port-level role's default Access Control is configured to deny traffic, then all inbound traffic will be discarded even if it matches a (forward) classification rule.

Rule Limits

C1 devices limit the number of rules you can create for some classification types. Refer to the C1 information in the Extreme Management Center Release Notes to see which classification types limit the number of rules.

N-Series Considerations

Review the following considerations prior to configuring policy on N-Series devices:

Role Precedence for the N-Series Platinum

The following precedence determines the role (policy) that is being applied on a user/port on a N-Series Platinum device. The precedence used depends on whether the device is configured for multi-user authentication or single user authentication.

Multi-User Authentication:

Devices configured with multi-user authentication use the following precedence when applying a role on a user/port (starting with the highest precedence):

- MAC override policy
- Authenticated role
- MAC-to-Role mapping
- IP override policy
- IP-to-Role mapping
- VLAN-to-Role mapping
- Default port role

Single User Authentication:

Devices configured with single user authentication use the following precedence when applying a role on a user/port (starting with the highest precedence):

- MAC override policy
- MAC-to-Role mapping
- IP override policy
- IP-to-Role mapping
- Authenticated role

VLAN-to-Role mapping
Default port role

C2 and B2 Considerations

Review the following considerations prior to configuring policy on C2 and B2 devices.

- When TCI Overwrite is enabled on a role, C2 and B2 devices support rewriting the 802.1p bit (CoS values) but not the 802.1Q bit (VLAN ID).
- On C2 and B2 gigabit and 10/100 ports, the number of rules per port is restricted. Refer to your C2 and B2 firmware release notes for the maximum number of rules that can be utilized on a port.
- C2 and B2 10/100 ports support two priority-based rate limits (inbound only). When creating a rate limit to be used on C2 and B2 10/100 ports, create the limit with either Low priority to associate the rate limit with priorities 0-3 or High priority to associate the rate limit with priorities 4-7. You can specify both Low and High priorities if you want to associate the rate limit with priorities 0-7.
- C2 and B2 devices do not support setting a default role on a logical port.
- On C2 and B2 devices, it is strongly recommended that you do not enforce rules that assign a Class of Service (CoS) that includes Priority 7. Doing so will interfere with stack communication.
- C2 and B2 devices do not allow a mask for an IP type of service (ToS) rewrite value associated with a class of service (CoS); they will always use ff.
- C2 and B2 devices do not support VLAN ID traffic classification rules. C2 devices (firmware 3.02.xx and newer) and B2 devices (firmware 2.xx.xx) support device-level VLAN to Role mapping. However, VLAN ID traffic classification rules can be configured on C2 devices with firmware versions 3.01.xx or older, using CLI.
- B2 only. Each port on a policy-enabled B2 switch can support up to 100 rules and up to 10 masks. The maximum number of unique rules in a single switch or B2 stack is 100, while the maximum number of unique masks is 18. These unique rules and masks may be shared across any and all ports in a stack or switch.

C3 and B3 Considerations

Review the following considerations prior to configuring policy on C3 and B3 devices.

- B3/C3 devices do not support TCI Overwrite. The B3/C3 does not overwrite 802.1Q VLAN bits, but overwrites the 802.1p Priority bits.
- B3/C3 devices do not support Layer 3 ICMP rules.
- B3/C3 devices support role-based rate limiting. However, on the B3/C3, class of service inbound rate limiting works only on policy roles, not on policy rules.
- C3G and B3 devices have the following additional limitations:
  - Maximum 100 rules per policy role.
  - A system limitation of 768 unique rules.
  - Maximum of 15 roles.
- C3 and B3 devices do not support setting a default role on a logical port.

Mixed-Stack C2/C3 and B2/B3 Considerations

Review the following considerations prior to configuring policy on mixed stacks of C2/C3 and B2/B3 devices.

NOTE: While you can create mixed stacks of C2/C3 devices and mixed stacks of B2/B3 devices, you should not create mixed stacks of C and B devices (e.g. mixed stacks of C2/B2 or C3/B3 devices).

- It is strongly recommended that a C3 device be configured as the master in a mixed C2/C3 stack.
- It is strongly recommended that a B3 device be configured as the master in a mixed B2/B3 stack.
- When you have a mixed stack, all devices in the stack have the rule type and Class of Service limitations of a C3 or B3 device, despite the fact that the stack may report itself as a C2 or a B2. The device type that the stack reports is based on what switch is set as the master.
- Mixed stacks with a B3/C3 master support role-based rate limiting, however, class of service inbound rate limiting works only on policy roles, not on policy rules.
- A mixed stack containing a C2H or a B2 has the following limitations:
  - A single role limitation of 100 rules and 10 masks.
  - A system limitation of 100 unique rules and 18 unique masks.
  - No support for Layer 2 rules or Layer 3 ICMP type rules.

    - Maximum of 15 roles.
    - No support for rate limiting.
- A mixed stack containing a C2G has the following limitations:
    - A single role limitation of 100 rules and 10 masks.
    - A system limitation of 768 unique rules.
    - No support for Layer 2 rules.
    - Maximum of 15 roles.
    - No support for rate limiting.
- When adding a new device to a mixed stack, the ports should not go active unless the stack supports the policy configuration. Once a device has joined the stack, no roles should be enforced that are not supported on all devices. For example:
  A C2K is added to an existing C3 stack.
    - If the number of masks in the C3 stack's current configuration exceed those allowed by the C2K, its ports cannot go active.
    - Once the C2K joins the stack, no roles can be enforced that exceed the limitations of any device.

7100 Considerations

- 7100 devices only support fixed IRL index reference mappings for the static CoS. The IRL Index for the CoS needs to match the priority. This is the default configuration for domains, but if it is changed for a static CoS, enforce will fail.
- 7100 devices only support fixed TXQ index reference mappings for the static CoS. The TXQ Index for the CoS needs to match the priority. This is the default configuration for domains, but if it is changed for a static CoS, enforce will fail.
- 7100 devices only support fixed COS - transmit queue mappings. The transmit queue specified for a Class of Service must match the 802.1p priority, or enforce will fail.
- TCI Overwrite configuration is not supported on the 7100. It is always enabled, and cannot be turned on or off using the Policy tab.

Extreme Access Control Controller Configuration

Review the following considerations prior to configuring policy on Extreme Access Control Controller devices.

Extreme Access Control Controllers Require Separate Domains

Extreme Access Control Controllers must by assigned to their own unique policy domain and cannot be combined with other switch types in a domain.

Modifying Extreme Access Control Controllers Preconfigured Policy

Extreme Access Control Controllers are shipped with a default policy configuration already configured on the device. To modify this default policy configuration, you must create a domain for the Extreme Access Control Controller, assign the Extreme Access Control Controller to the domain, then import the policy configuration from the device into the Policy tab (File > Import > Policy Configuration from Device). You can then alter the policy configuration to define the authorization levels for the Extreme Access Control process, as appropriate for your environment. If assessment will be enabled in the Extreme Networks Extreme Access Control solution, you must add classifications rules to the Quarantine and Assessing policies to allow traffic to be forwarded to the assessment servers deployed on the network. When you have finished modifying the policy configuration, you must enforce it back to the Extreme Access Control Controller.

NOTE: If you are using assisted remediation and quarantined end-users will be required to download remediation files via FTP, you will also need to add a rule to the Quarantine policy configuration that opens up ports 49152-65535. If you are concerned with security, you can configure your FTP server to use a smaller range of ports.

Modifying the Downstream Default Policy

Depending on the network configuration or circumstances, it's possible that traffic from the upstream side could be rerouted to the Extreme Access Control Controller where it would be authenticated using the upstream source IP address. To avoid this problem, add a Layer 3 IP Address Source rule to the downstream default policy configured on the Extreme Access Control Controller, using the upstream IP subnets (or critical servers located in the upstream) and containing the traffic to a VLAN.

Configuring LAG on Extreme Access Control Controllers

This section provides instructions for configuring LAG (link aggregation) on your Extreme Access Control Controller appliance. The instructions vary

depending on whether you are configuring LAG on a Layer 2 or Layer 3 Extreme Access Control Controller.

Configuring LAG on Layer 3 Extreme Access Control Controllers - Upstream Ports

1. Configure LAG on the Extreme Access Control Controller PEP (Policy Enforcement Point) using the CLI (Command Line Interface).
2. Use the **Policy** tab to assign the appropriate upstream role as the default role on the port. For instructions, see Assigning Default Roles to Ports.

Configuring LAG on Layer 3 Extreme Access Control Controllers - Downstream Ports

1. Configure LAG on the Extreme Access Control Controller PEP (Policy Enforcement Point) using the CLI (Command Line Interface).
2. In the **Policy** tab options (Tools > Options), display the Ports panel and uncheck the Hide Logical Ports option.
3. Use the **Policy** tab to assign the appropriate downstream role as the default role on the port. For instructions, see Assigning Default Roles to Ports.

Configuring LAG on Layer 2 Extreme Access Control Controllers - Upstream Ports

1. Configure LAG on the Extreme Access Control Controller PEP (Policy Enforcement Point) using the CLI (Command Line Interface).
2. In the **Policy** tab options (Tools > Options), display the Ports panel and uncheck the Hide Logical Ports option.
3. Use the **Policy** tab to assign the appropriate upstream role as the default role on the port. For instructions, see Assigning Default Roles to Ports.

Configuring LAG on Layer 2 Extreme Access Control Controllers - Downstream Ports

1. Configure LAG on the Extreme Access Control Controller PEP (Policy Enforcement Point) using the CLI (Command Line Interface).
2. In the **Policy** tab options (Tools > Options), display the Ports panel and uncheck the Hide Logical Ports option.

3. Use the **Policy** tab to assign the appropriate downstream role as the default role on the port. For instructions, see Assigning Default Roles to Ports.
4. Use the CLI to set the following command: nodealias maxentries 4096 <lag port>.

ExtremeWireless Controller Configuration

The following sections present information regarding support for the ExtremeWireless Controller in the **Policy** tab. Review the following considerations prior to configuring policy on wireless controller devices.

Version Supported

The Policy tab only supports Wireless Controller version 8.01.03 and higher.

Policy Rules

This section describes wireless controller support for policy rules.

Supported Rule Types

The Wireless Controller supports the following traffic classification rule types:

- Ethertype
- MAC Address Source/Destination/Bilateral
- Priority
- IP Type of Service
- IP Protocol Type[1]
- ICMP
- IP Address Source/Destination/Bilateral
- IP Socket Source/Destination/Bilateral
- IP UDP Port Source/Destination/Bilateral
- IP UDP Port Source/Destination/Bilateral Range
- IP TCP Port Source/Destination/Bilateral
- IP TCP Port Source/Destination/Bilateral Range

[1]Not all IP Protocols are supported for the wireless controller. Supported IP Protocols for this rule type are: ICMP, TCP, UDP, GRE, ESP, AH.

"No Change" Filter Sets

The wireless controller allows administrators to define policies that do not have any filters of their own, but which instead use the set of filters already assigned to a station by a previously applied policy. This type of policy is said to have a "No Change" set of policy rules. The Policy tab does not support policies that have "No change" policy rule sets. Using the ExtremeWireless Assistant, you need to remove any policies containing "No Change" rule sets before the wireless controller can be managed by the Policy tab.

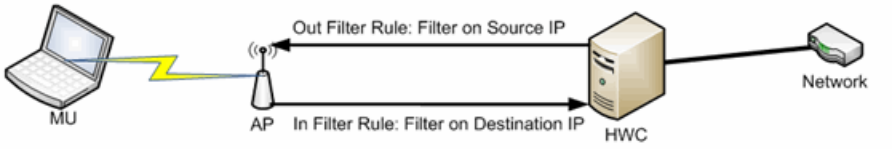
Rule Actions

The following list defines the wireless controller support for rule actions:

- Access Control: Permit, Deny, and Contain to VLAN actions are supported.
- Class of Service is supported.
- TCI Overwrite is not supported.
- System Log, Audit Trap, Disable Port, and Traffic Mirror actions are not supported.

Rule Directions

The Policy tab rules are applied to incoming data packets based on the source or destination address, whereas the wireless controller applies rules to packets based on In/Out direction. On the wireless controller, "In" means coming from the station into the network and "Out" means going from the network out to the station. The wireless controller applies rules to the destination address of inbound packets and to the source address of outbound packets, as shown in the illustration below.



When you create a rule in the Policy tab that allows traffic to a specific destination, that same rule permits data flow from the destination back to the traffic source. This means that Destination rules in the Policy tab map to In/Out rules on the wireless controller. Certain Policy tab rule types do not have a Source or Destination designation (such as ICMP); however, these rules still map to In/Out rules on the wireless controller to indicate the filters are applied to traffic in both directions. Unchecking the In or Out flag for non-directional rules

via the ExtremeWireless Assistant does not affect the way it is reported to the Policy tab. As long as the rule still exists, verify succeeds.

All rules enforced from the Policy tab are created as "In" rules, and "Out" rules created on the controller are not reported to the Policy tab.

When the egress policy feature is enabled for a VNS, egressing traffic is applied to the defined "In" filters as a "reflected" Out rule (with the source and destination fields reversed) and any explicitly defined "Out" filters created on the controller are ignored. Egress policy may be enabled per VNS by selecting Port Properties for that VNS.

The wireless controller reports to the Policy tab any rules created directly on the controller that contain an "In" component. "Out" rules are not reported to the Policy tab. This allows administrators to define and use "Out" rules on the wireless controller in special cases where additional restrictions need to be imposed.

Rule Limits

The wireless controller has a limit of 64 rules per policy role if the policy is enforced at the controller (bridged @ wireless controller or routed topology), and 32 rules per policy role if the policy is enforced at the AP (bridged @ AP).

Role Default Actions

The following list defines the wireless controller support for role default actions:

- Access Control: Permit, Deny, and Contain to VLAN are supported.
- Class of Service: Inbound and outbound rate limits are supported. 802.1p Priority, and ToS/DSCP Marking are supported.
- TCI Overwrite is not supported.
- System Log, Audit Trap, Disable Port, and Traffic Mirror actions are not supported.
- The wireless controller will reject policy configurations that specify a VLAN that does not have an egress port already specified.

Class of Service

The following list defines the wireless controller support for Class of Service (CoS) configuration via the Policy tab:

- Inbound and outbound rate limits are supported at the role-level as Class of Service default actions.
- User-based inbound/outbound rate limits are supported for the Default port group for wireless controllers only.
- 802.1p Priority configuration is supported.
- ToS/DSCP Marking is supported.
- TCI Overwrite is not supported.
- Transmit Queue Rate Shaping is not supported.

Rate Limits

The wireless controller supports inbound and outbound rate limits at the role-level as Class of Service (CoS) default actions. There are three states supported for a rate limit:

- Rate limit traffic at the specified rate.
- No Change (the CoS does not specify a rate, and the rate limit is "inherited" from the port's default role or from the global default policy, if one is defined.)

To explicitly prevent traffic from being rate limited for a role, you can map a rate limit with a value of 0 to a CoS, and set that as the default CoS for the role.

Internal VLAN

The wireless controller uses an *internal VLAN* for processing traffic. For controllers with firmware version 8.01.xx, the internal VLAN is set by default to use VID 1 and the static name of "DEFAULT VLAN." For controllers with firmware version 8.11.xx and later, the internal VLAN uses the VID 4094 and the static name of "INTERNAL VLAN."

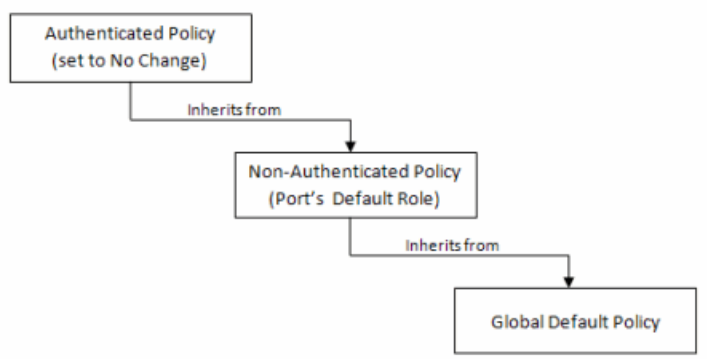
This internal VLAN cannot be used in your **Policy** tab domain configuration to tag traffic. If the VID for the internal VLAN is used in your domain configuration, the **Policy** tab enforce fails with an error message in the Event Log indicating the internal VID cannot be used.

You can use the Web UI (https:\\<controller IP>:5825 > VNS Config > Topologies > Internal VLAN) to change the internal VLAN to a different value, but your policy domain must not use that new value or the **Policy** tab enforce fails.

NOTE: For controllers with firmware version 8.01.xx. Since using a Default VLAN with a VID of 1 is valid on wired devices, the controller's internal VLAN must be changed to another value to prevent issues with the Policy tab enforcing a configuration that uses this VLAN.

Policy Inheritance

The wireless controller uses the concept of policy inheritance, which specifies that if the authenticated policy's access control (VLAN) or class of service (CoS) is set to "No Change," then the policy inheritance hierarchy is used to determine the VLAN and/or CoS. The policy inheritance hierarchy is as follows:



If the authenticated policy's VLAN and CoS are set to "No Change," then the VLAN and CoS settings for the port's default role is used. If the port's default role does not specify the VLAN and CoS, then the global default policy (specified via the ExtremeWireless Assistant) is used. (In wireless controller terminology, a VNS port's default role is the VNS's default policy.)

It is important to note that the Policy tab does not support "No Change" rules (filter set). If any policy's rules (filter set) are set to "No Change," then the Policy tab is not able to manage the device until the policy containing the "No Change" configuration is removed.

Configuring RADIUS Servers

When configuring RADIUS authentication and accounting servers, keep in mind the following differences:

- The "Number of Retries" and "Timeout Duration" settings for RADIUS authentication servers are configured on a per-server basis for wireless controller devices. For all other devices, these settings are global to all RADIUS servers, and are specified per device as client defaults.

- The "Update Interval" setting for RADIUS accounting servers is configured on a per-server basis for wireless controller devices. For all other devices, this setting is global to all RADIUS servers, and is specified per device as client defaults.
- For wireless controller devices, the Client Status (Enabled or Disabled) is automatically set to Enabled when a RADIUS server exists and Disabled when it does not. For all other devices, Client Status is configured for each device, allowing you to enable and disable communication between the device and the RADIUS servers.
- If Strict Mode is enabled, up to three RADIUS servers are automatically associated to each WLAN service. If Strict Mode is disabled, RADIUS servers must be manually added to a WLAN service via the ExtremeWireless Assistant.

Other Considerations

- The wireless controller does not support authentication configuration.
- The wireless controller does not support viewing user sessions in the Port Usage tabs.
- The wireless controller must have any VLANs used in a Role's default action already defined on the device and configured with an egress port. If the Policy tab enforces a domain configuration to the wireless controller using a VLAN that does not have an egress port specified, enforce fails.

Extreme Management Center™ Policy Help

Extreme Management Center Policy enables the creation and deployment of role-based policies that dynamically control user access, network security, application prioritization and other parameters. Policy management and role-based administration are keys to effectively enforcing business and IT rules in the network infrastructure.

Contact your sales representative for information on obtaining an Extreme Management Center software license.

Policy Tab Overview

The Policy tab simplifies the configuration of policies on networks, and deploys the policies on multiple devices throughout the switch fabric.

With the Policy tab, you can create policy profiles, called roles, assigned to the ports in your network. These roles provide four key policy features: traffic containment, traffic filtering, traffic security, and traffic prioritization. When authentication is enabled, users identify themselves to the network and are given customized access capabilities based on the role they serve in the organization.

Using the Policy tab configuration tools, you can create multiple roles tailored to your specific needs, and set a default role for all or some of your network devices and ports. Basic Policy tab operations include creating, editing, and deleting roles. You can also view role configuration on a per device and per port basis. In addition, the Policy tab allows you to verify the roles enforced on your network device match the roles currently configured in the application. The Policy tab supports a maximum of 1,000 devices (25,000 ports) and 50 roles per policy domain, and can process a maximum of 250 classification rules with a maximum of 50 classification rules per role.

Extreme Management Center Details View

Some Details View tabs display a simple list of items for the current selection in the left panel. However, other Details View tabs present more complex tables of information. To access Help topics on those tabs, expand the Details View Tabs folder in the Policy tab Help Table of Contents. The Help topics are named to reflect the item selected in the left-panel tree. For example, the Help topic for the Details View tab with a device selected in the left panel is named Details View Tab (Device).

Most Details View tabs provide the following features:

- *Right-click menus:* Right-click an item for a menu of options.
- *Sorting, filtering and finding:* Clicking on column headings sorts the column. Click the magnifying glass icon to open a Search field.

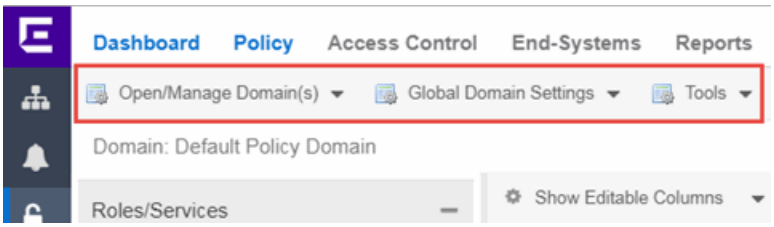
Extreme Management Center General

A General tab is available in the right panel of the Policy tab main window for many items selected in the left-panel tab. It provides general properties information about the selected item.

Help topics for the right-panel General tabs are named to reflect the item selected in the left-panel tree. For example, the Help topic for the General tab with a device selected in the left panel is named General Tab (Device). For more complete information on the different General tabs, expand the General Tabs section and select the desired tab.

Policy Menus

The two drop-down menus on the Policy tab provide access to Policy tab functions. The Open/Manage Domains menu provides options for the domain currently accessed. The Global Domain Settings drop-down menu allows you to configure global Policy tab settings.



Open/Manage Domains Menu

The Open/Manage Domains provides the following options for the **Policy** tab:

Open Domain
Provides a list of the available Policy Domains. Selecting a domain opens that domain, allowing you to make changes.

Lock Domain
Lets you lock the current Policy Domain for editing purposes. The **Policy** tab automatically locks the domain when you begin to edit the domain configuration. Other **Policy** tab users are notified that the domain is locked and they are not able to save their own domain changes until the lock is released. For more information, see Controlling Client Interactions with Locks.

Save Domain
Lets you save any changes you made to the current Policy Domain. Only users with the capability to Enforce are able to save the domain.

Enforce Domain
Writes the role and/or any changes you have made to it (rules, services) to all the devices in your current domain. See Enforcing for more information.

Verify Domain
Compares the roles in your current domain to the roles currently enforced on all the devices in the current domain. This is useful for ensuring the roles in your domain are enforced, or, if you use more than one domain, ensuring that the roles in the domain you are currently using matches what is on the devices. See Verifying for more information.

Assign Devices to Domain
Opens the Assign Devices to Domain window where you can assign devices that are in the Extreme Management Center database to the current Policy Domain.

Create Domain
Lets you create and name a new (blank) Policy Domain.

Delete Domain(s)
Opens a window where you can select one or more Policy Domains to delete.

Rename Domain
Lets you rename the current Policy Domain.

Import/Export > Import From Domain
Opens the Import from Domain window where you can import policy configuration data from one Policy Domain into another domain. (This menu option is not available if only one domain exists, as there are no other domains from which to import data.)

Import/Export > Import From File
Opens the Import from File window, which enables you to import policy data from a .pmd file into the current Policy Domain. Be aware that the import overwrites any existing data in the Policy Domain. Any devices in the .pmd file must already exist in the Console database or they won't be imported.

Import/Export > Export to File
Lets you save policy data from the current Policy Domain to a .pmd file or .xml file with the file name and location of your choosing. This file stores all information about roles, services, and rules configured in the current Policy Domain. This allows you to save a Domain configuration prior to making changes so that you can restore the original Domain configuration if required (via Import/Export > Import From File).

Global Domain Settings Menu

The Global Domain Settings Menu provides the following options:

GVRP > Ignore GVRP
To ignore GVRP status on the devices in the current domain, select this menu option and enforce. This means that the Policy tab ignores the GVRP configuration on a device during an Enforce operation, allowing you to configure some network devices with GVRP enabled and others with GVRP disabled (using MIB Tools or local management), according to their configuration requirements. Be aware that for devices with GVRP set to disabled, ignoring GVRP configuration during an Enforce may affect connectivity on ports with VLANs that rely on Dynamic Egress.

GVRP > Enable GVRP
To enable GVRP on the devices in the current domain, select this menu option and enforce. If the current domain configuration contains rules that use VLAN

containment, Dynamic Egress and GVRP must be enabled on the devices in the domain, or the VLANs must be properly pre-configured on the devices outside of the Policy tab.

GVRP > Disable GVRP

If you do not want GVRP enabled on the devices in the current domain, select this menu option and enforce. Be aware that disabling GVRP may affect connectivity through ports with VLANs that rely on Dynamic Egress.

Port Level Role Mappings Enabled

Check this box to enable any port-level Tagged Packet VLAN to role mappings or port-level MAC to role mappings that have been configured and enforced for the current domain. If the box is not checked, all port-level mappings are ignored.

NOTE: This functionality is not yet available.

Do Not Use Global Services

Check this box to hide the display of Global Services in the left-panel Services tab for this domain. If you use Global Services in some domains but not in others, this option allows you to hide global services in the domains where they are not used so that they won't be inadvertently used or modified.

Tools Menu

Authentication Configuration

Opens the Authentication Configuration wizard, where you can configure authentication settings on a device.

RADIUS Configuration

Opens the RADIUS Configuration wizard, where you can configure RADIUS authentication and accounting settings on a device.

Policy Event Log

Opens the Events tab filtered to display only Policy events.

Related Information

For information on related windows:

- Main Window

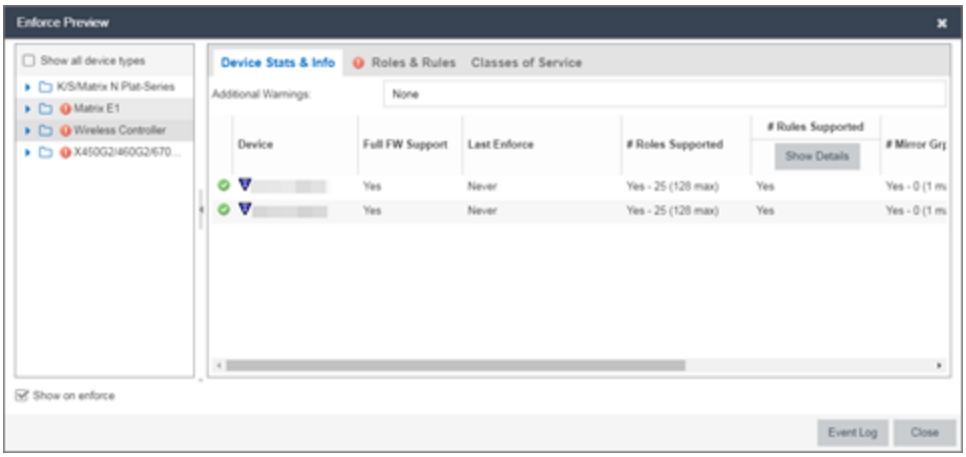
Extreme Management Center Enforce Preview Window

Use the Enforce Preview window in the Policy tab to view the information you are writing to your devices, before you actually enforce. Use this window when enforcing to devices that only support certain aspects of policy management. For example, some devices support only the policy features of policy management; some devices support the policy features and classification rules, but do not support VLAN forwarding for certain classification rules; and some devices fully support all policy management features, including policy, classification rules, and VLAN forwarding for all classification rules.

The Enforce Preview window appears in the Policy tab by selecting Open/Manage Domain(s) > Enforce Preview, or clicking the enforce icon in the left panel and selecting Enforce Preview. You can control whether this view automatically appears when you click Enforce with the Show on Enforce checkbox.

What you see in the window depends on whether you are enforcing to all devices or to a subset of devices. The title bar indicates the devices to which the enforce applies. After viewing the information in this window, you can either click Close to back out and make changes, or Enforce to go ahead with the enforce.

You can view device support for specific roles, services, and rules on the Roles & Rules tab. Refer to the Extreme Management Center Firmware Support tables for complete information on device support for Policy features, and VLAN and Priority classification rules.



Show on Enforce

When this checkbox is checked, the Enforce Preview window appears any time you enforce, before the actual enforcement takes place.

Left Panel

The left panel of the Enforce Preview window displays folders for different device types. Expand the folders to see your network devices and device groups organized according to device type. The warning icon ( ) alerts you that Extreme Management Center is not writing a staged change to this device type (e.g. rules not supported on a device).

Show all device types

Select the checkbox in the left panel to display all device types in the left panel. When the checkbox is not selected, only the devices you are changing by enforcing are displayed.

Select a specific device type to display the information Extreme Management Center is writing to those devices when you enforce in the right panel.

Right Panel

The right panel provides information about whether certain policy management features are supported and/or enabled for the device type selected in the left panel.

- Additional Warnings - If there are additional problems detected with the enforce, you will be directed to see the Event Log for details.
- GVRP - Shows whether GVRP is Enabled, Disabled, or Ignored. You can change GVRP status for the domain via the Edit menu.
- Dynamic Egress - Shows whether Dynamic Egress is Supported or Not Supported.

Device Stats & Info Tab

Displays the devices for the device type selected in the left panel and provides information about each device. If the number of roles in the domain exceeds the supported number of roles on a device, the enforce fails.

- # of Roles Supported - The maximum number of roles supported by the device.
- Domain Role Count Supported - This column says "No" if the number of roles in the domain exceeds the supported number of roles on the device. A "Yes" in this column indicates that the number of roles on the device is equal to or less than the maximum number of supported roles.

Role Statistics - Lists information about each role:

- Number of Rules - The number of traffic classification rules the role includes.
- Number of Unique Masks - The number of masks defined for the rules included in the role.

There are six tabs that provide specific information about the Roles, Classification Rules, VLANs, Classes of Service, and Mappings that will be enforced. The information displayed depends on the device type you've selected in the left panel, and whether you have the Show All or the Show Errors and Warnings Only radio button selected. In addition, select a role in the Roles tab to filter the information for just that role.

Roles Tab

Incomplete - Lists any roles with unsupported classification rules. These roles will be written to the devices, but without the unsupported rules.
Complete - Lists any roles which do *not* include unsupported classification rules. These roles will be written to the devices as defined.

NOTE: Select a Role to display only those classification rules and VLANs associated with the selected role.

Classification Rules Tab

Excluded - Lists any unsupported classification rules that have been applied to a role. These rules will not be included when the associated roles are written to the devices.

Included - Lists any supported classification rules that have been applied to a role. These rules will be included when the associated roles are written to the devices.

NOTE: On N-Series Platinum devices, range classification rules are achieved through applying subnet masks to values. As such, in order to achieve a user-specified range, the device may need multiple rules with subnets applied to encompass that range. So, although the user created only one rule with a range, this list may show multiple instances of that rule with the name of the rule followed by the portion of the over-all range it applies to.

VLAN Tab

Excluded - Lists any VLANs associated with unsupported classification rules, or VLANs that are not supported by the device. These VLANs will not be written to the devices.

Included - Lists any VLANs associated with supported classification rules and VLANs associated with roles. These will be written to the devices.

Classes of Service Tab

Class of Service Mode - Lists the Class of Service mode that will be written to the devices.

Classes of Service Subtab - Lists the classes of service that will be written to the devices:

- Class of Service - the name of the class of service.
- 802.1p Priority - the priority associated with the class of service.
- ToS Value - the IP type of service value associated with this class of service, if any. See IP Type of Service for more information.
- Drop Prec - The drop precedence associated with this class of service, if any. See Drop Precedence for more information.
- TxQueue Index - the transmit queue index associated with the class of service.
- IRL Index - the role-based inbound rate limit index associated with the class of service.
- ORL Index - the role-based outbound rate limit index associated with the class of service.

For more information, see Getting Started with Class of Service and How to Create a Class of Service.

Inbound/Outbound Role-Based Rate Limit Mappings Subtabs - Lists the rate limit mappings that will be written to the devices:

- Device - The device where the rate limit mapping will be in effect.
- IRL/ORL Port Grp - The name of the port group that contains the rate limit mapping.
- IRL/ORL Index - The logical inbound rate limit (IRL) or outbound rate limit (ORL) index number. This index number is specified in a class of service and dictates the rate limiting behavior for incoming packets.
- Rate Limit - The actual rate limit that the IRL/ORL index is mapped to.
- IRL/ORL Port Type - The type of ports included in the port group. Port type is based on the number of rate limits the ports support (for example, 8-rate limit ports and 32-rate limit ports).
- Information - Information about mapping support.

Transmit Queue/Rate Shaper Mappings Subtab - Lists the transmit queue rate shaper mappings that will be written to the devices:

- Device - The device where the transmit queue rate shaper mapping will be in effect.
- TxQ Port Grp - The name of the port group that contains the transmit queue rate shaper mapping.
- TxQ Index - The logical transmit queue rate shaper index number. This index number is specified in a class of service and dictates the transmit queue and rate shaper behavior for incoming packets.
- Physical Transmit Queue / Rate Shaper - The actual transmit queue rate shaper that the index is mapped to.
- TxQ Port Type - The type of ports included in the port group. Port type is based on the number of transmit queues the ports support (for example, 4-transmit queue ports and 16-transmit queue ports).
- Information - Information about mapping support.

Mappings Tab

WARNING: Enforcing port-level MAC to Role mappings could potentially remove rules created as an intrusion detection response.

MAC to Role Mapping - Lists the device-level and port-level mappings that will be written to the devices:

- Device/Port Level - indicates whether the mapping is a device-level mapping (all devices) or a port-level mapping (IP address and port description). Port-level mappings on frozen ports will be enforced.
- MAC Address - the MAC address mapped to the role. Masking a MAC address is only supported on N-Series Platinum devices.
- Mask - the mask associated with the MAC address.
- Role - the role mapped to the MAC address.

IP to Role Mapping - Lists the device-level mappings that will be written to the devices:

- IP Address - the IP address mapped to the role.
- Mask - the mask associated with each IP address. Masking an IP address is only supported on N-Series Gold and Platinum devices.
- Role - the role mapped to the IP address.

Tagged Packet VLAN to Role Mapping - Lists the device-level and port-level mappings that will be written to the devices:

- Device/Port Level - indicates whether the mapping is a device-level mapping (all devices) or a port-level mapping (IP address and port description). Port-level mappings on frozen ports will be enforced.
- VLAN - the VLAN mapped to the role.
- Role - the role mapped to the VLAN.

Authentication Based VLAN (RFC 3580) to Role Mapping - Lists the mappings that will be written to the devices:

- VLAN - the VLAN mapped to the role.
- Role - the role mapped to the VLAN.

Event Log Button

Opens the Events tab filtered to display events with an Event Type of Policy.

Enforce Button

Enforces the roles, classification rules and VLANs in the current data file to the devices, based on the level of support available on the devices as indicated in the Enforce Preview window.

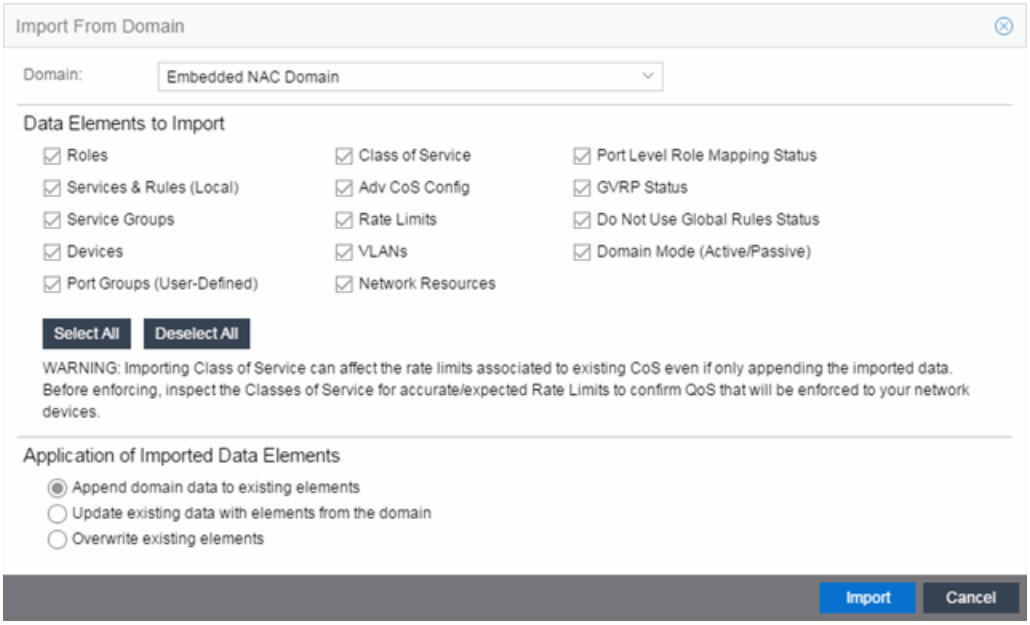
Related Information

For information on related concepts:

- Enforcing

Import from Domain

This window lets you import policy configuration data from one Policy Domain into another domain. To access the Import from Domain window, select Open/Manage Domain > Import/Export > Import From Domain. (This menu option is not available if only one domain exists, as there are no other domains from which to import data.)



Domain

Use the drop-down menu to select the domain whose data you want to import.

Data Elements to Import

In this section, you can choose the specific data elements you want to import. Click Select All to select all the data import options at once.

Roles

Select this option to import roles, including the role's name, description, default VLAN (access control), and default class of service. If a role's services already exist in the current domain, or if you are importing them at the same time as the role, the services are associated with the role. Otherwise, the services are not imported.

Services & Rules (Local)

Select this option to import Local services (services that are unique to a specific domain) and their associated classification rules. When you import rules from another domain, the Policy tab checks for rule conflicts (see Conflict Checking for more information).

Service Groups

Select this option to import service group names. If a service group's services already exist in the current domain, or if you are importing them at the same time as the service group, the services will be associated with the group. Otherwise, the services will not be imported.

Devices

Select this option to import devices. Any devices in the .pmd file must already exist in the Extreme Management Center database or they won't be imported. (See How to Add and Delete Devices for more information on using Console to add devices to the Extreme Management Center database.) Devices that are imported are automatically assigned to the current domain and are displayed in the Policy tab Network Elements tree. If the devices being imported were already assigned to another domain, then those devices are reassigned to the current domain. Any devices that are not imported are listed in an Event Log message along with their device type and firmware version.

Port Groups (User-Defined)

Select this option to import user-defined port groups. If you are importing a port group's ports at the same time as the port group, the ports will be associated with the port group. Otherwise, the ports are not imported.

Class of Service

Select this option to import classes of service, role-based rate limit port groups, and transmit queue port groups. For the purposes of importing, a class of service is

defined as the class of service name, i.e., priority is not a factor in determining uniqueness. After a class of service is imported, its associated roles, services, and rules are updated. When you import class of service data, the relationship between a class of service and its priority is retained; however, rate limiting characteristics of the priorities are not imported. If you also elect to import rate limits, the rate limits are imported first, then the classes of service are imported. You can then redefine the class of service priorities with some or all of the imported rate limits, if desired. Although ToS characteristics are not used to determine the uniqueness of a class of service for importing, if ToS is a part of a class of service, it is imported as an attribute of the class of service. See append, update and overwrite for information on how those specific actions affect the import of classes of service.

Adv CoS Config

Select this option to import the class of service configuration (basic or advanced) for the domain (whether the Advanced Class of Service Configuration option is selected).

Rate Limits

Select this option to import rate limits. For the purposes of importing, a rate limit is defined as [rate + direction] when determining uniqueness. When you append or update rate limits and a duplicate rate limit exists in the current domain, any unique priority and exclusion properties of the imported rate limit replace (if appending) or are added to (if updating) those of the first duplicate rate limit in the existing precedence list. Any other duplicates on the list are not changed. Because rate limits cannot include conflicting priority values, if a priority is already being utilized by an existing rate limit, it will not be imported. If you also elect to import classes of service, the rate limits are imported first, then the classes of service are imported. See append and update for information on how those specific actions affect the import of rate limits.

NOTE: ZTP+ functionality requires an ExtremeXOS device on which version 21.1 is installed.

NOTE: Only those network elements that are recognized by the existing domain can be imported as exclusions. Others are ignored.

VLANs

Select this option to import VLANs.

Policy VLAN Islands

If applicable, Policy VLAN Islands and Island VLANs are imported via the Devices and VLANs options.

- If the Devices option is selected and the Policy VLAN Islands feature is enabled in the current domain as well as the imported domain, the Policy VLAN Islands will be imported. The Policy VLAN Island Base ID and Offset settings from the imported data will be used and those in the current domain will be lost.
- If the VLANs option is selected and the Policy VLAN Islands feature is enabled in the current domain as well as the imported domain, the Island VLANs are imported and are added to any existing Policy VLAN Islands.

Whenever Policy VLAN Islands are imported, all the island VLANs are recalculated and the island ranges may change. It is possible to import more islands and VLANs than can be configured. If this is the case, an error appears in the Event Log, asking that the Base ID and Offset settings be changed.

Network Resources

Select this option to import network resource groups. After a Network Resource is imported, the associated services are updated. If a network resource group no longer exists after an import, the service with which it was associated is changed to a manual service on the Automated Service tab for the service.

Port-Level Role Mapping Status

Select this option to import the Port-Level Role Mappings Enabled status for the domain, as specified in the Edit menu.

GVRP Status

Select this option to import the GVRP status for the domain (as specified in the Edit menu).

Do Not Use Global Services Status

Select this option to import the Do Not Use Global Services status for the domain, as specified in the Edit menu.

Domain Mode

Select this option to import the domain mode (active or passive) as specified in the Edit menu.

Application of Imported Data Elements

In this section, you can choose how you want the data elements selected above to update your current domain.

Append domain data to existing elements

Select this option to import only new data elements into your current domain. If any of the selected data elements already exist in your current domain, they will not be

changed.

Rate Limits: A rate limit will not be appended if: 1) The Rate, Direction, and 802.1P Priority are already defined. 2) The Priority list is empty.

CoS: A class of service will not be appended if: 1) The name is the same as an existing class of service. 2) The class of service names are different but the rate limits for the imported class of service do not match the existing rate limit settings.

Update existing data with elements from domain

Select this option to 1) replace the selected data elements that exist in your current domain with the imported data elements, and 2) import the selected data elements that don't exist in your current domain.

Rate Limits: A rate limit will not be updated if the rate limit and direction do not match.

CoS: A class of service will not be updated if: 1) The name does not match an existing class of service. 2) The class of service name matches but the rate limits for the imported class of service do not match the existing rate limit settings.

Overwrite existing elements

Select this option to replace the selected data elements that exist in your current domain with the imported data elements.

CoS: A class of service will not be overwritten if the rate limits for the imported class of service do not match the existing rate limit settings.

NOTE: If you decide that you want to return to the previous configuration (that the import updated), you can perform a File > Read Policy Domain operation to restore the configuration, as long as you have not saved the data you imported.

Select All Button

Selects all of the data elements.

Import Button

Imports the selected data and closes the window.

Related Information

For information on related tasks:

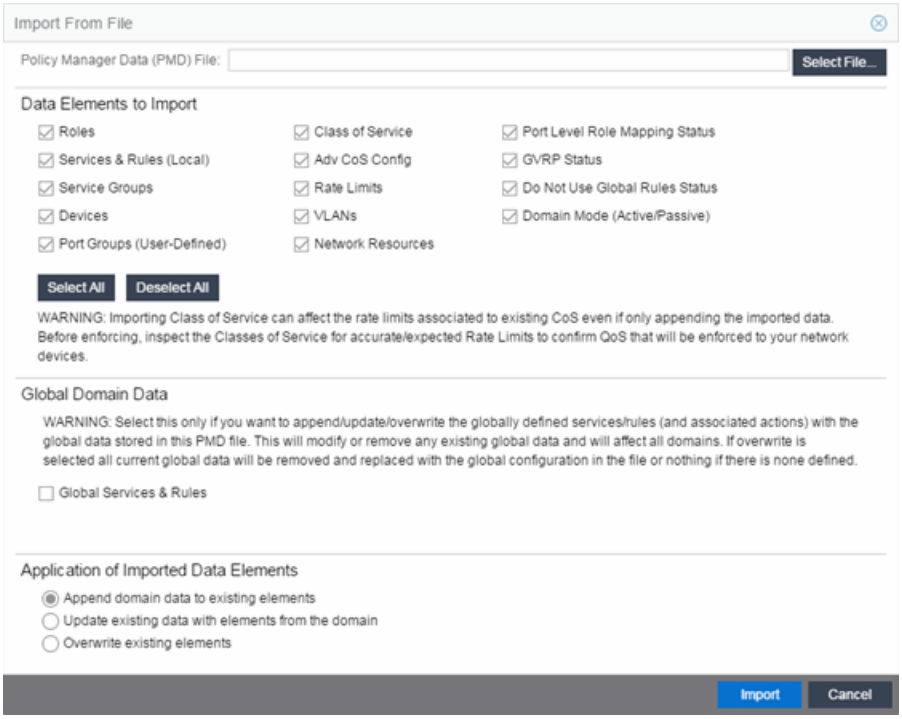
- How to Create and Use Domains

For information on related windows:

- Import From File Window

Import from File

This window lets you import policy data from a .pmd file into a Policy Domain. To access the window, select **Open/Manage Domains > Import/Export > Import From File**.



Policy Manager Data (PMD) File

Enter the name and path for the data file (.pmd) you want to import, or navigate to the file by selecting the **Select File** button.

Data Elements to Import

In this section, you can choose the specific data elements you want to import. Click **Select All** to select all the data import options at once.

Roles

Select this option to import roles, including the role's name, description, default VLAN (access control), and default class of service. If a role's services already exist

in the current domain, or if you are importing them at the same time as the role, the services will be associated with the role. Otherwise, the services are not imported.

Services & Rules (Local)

Select this option to import Local services (services that are unique to a specific domain) and their associated classification rules. When you import rules from another domain, the **Policy** tab checks for rule conflicts (see Conflict Checking for more information).

Service Groups

Select this option to import service group names. If a service group's services already exist in the current domain, or if you are importing them at the same time as the service group, the services are associated with the group. Otherwise, the services are not imported.

Devices

Select this option to import devices. Any devices in the .pmd file must already exist in the Extreme Management Center database or they won't be imported. (See How to Add and Delete Devices for more information on using Console to add devices to the Extreme Management Center database.) Devices that are imported are automatically assigned to the current domain and are displayed in the Policy tab Network Elements tree. If the devices being imported were already assigned to another domain, then those devices are reassigned to the current domain. Any devices that are not imported are listed in an Event Log message along with their device type and firmware version.

Port Groups (User-Defined)

Select this option to import user-defined port groups. If you are importing a port group's ports at the same time as the port group, the ports are associated with the port group. Otherwise, the ports are not imported.

Class of Service

Select this option to import classes of service, role-based rate limit port groups, and transmit queue port groups. For the purposes of importing, a class of service is defined as the class of service name, i.e., priority is not a factor in determining uniqueness. After a class of service is imported, its associated roles, services, and rules are updated. When you import class of service data, the relationship between a class of service and its priority is retained; however, rate limiting characteristics of the priorities are not imported. If you also elect to import rate limits, the rate limits are imported first, then the classes of service are imported. You can then redefine the class of service priorities with some or all of the imported rate limits, if desired.

Although ToS characteristics are not used to determine the uniqueness of a class of service for importing, if ToS is a part of a class of service, it is imported as an attribute of the class of service. See append, update and overwrite for information on how those specific actions affect the import of classes of service.

Adv CoS Config

Select this option to import the class of service configuration (basic or advanced) for the domain (whether the Advanced Class of Service Configuration option is selected).

Rate Limits

Select this option to import rate limits. For the purposes of importing, a rate limit is defined as [rate + direction] when determining uniqueness. When you append or update rate limits and a duplicate rate limit exists in the current domain, any unique priority and exclusion properties of the imported rate limit replace (if appending) or are added to (if updating) those of the first duplicate rate limit in the existing precedence list. Any other duplicates on the list are not changed. Because rate limits cannot include conflicting priority values, if a priority is already being utilized by an existing rate limit, it will not be imported. If you also elect to import classes of service, the rate limits are imported first, then the classes of service are imported. See append and update for information on how those specific actions affect the import of rate limits.

Note: Only those network elements that are recognized by the existing domain can be imported as exclusions. Others will be ignored.

VLANs

Select this option to import VLANs.

Policy VLAN Islands

If applicable, Policy VLAN Islands and Island VLANs are imported via the Devices and VLANs options.

- If the Devices option is selected and the Policy VLAN Islands feature is enabled in the current domain as well as the imported domain, the Policy VLAN Islands will be imported. The Policy VLAN Island Base ID and Offset settings from the imported data will be used and those in the current domain will be lost.
- If the VLANs option is selected and the Policy VLAN Islands feature is enabled in the current domain as well as the imported domain, the Island VLANs are imported and are added to any existing Policy VLAN Islands.

Whenever Policy VLAN Islands are imported, all the island VLANs are recalculated

and the island ranges may change. It is possible to import more islands and VLANs than can be configured. If this is the case, an error appears in the Event Log, asking that the Base ID and Offset settings be changed.

Network Resources

Select this option to import network resource groups. After a Network Resource is imported, the associated services are updated. If a network resource group no longer exists after an import, the service with which it was associated is changed to a manual service on the Automated Service tab for the service.

Port-Level Role Mapping Status

Select this option to import the Port-Level Role Mappings Enabled status for the domain.

GVRP Status

Select this option to import the GVRP status for the domain.

Do Not Use Global Services Status

Select this option to import the Do Not Use Global Services status for the domain.

Domain Mode

Select this option to import the domain mode (active or passive) as specified in the Edit menu.

Global Domain Data

Use this option only if you want to append, update, or overwrite the globally defined services and rules in your current domain with the global domain data stored in the .pmd file you are importing. This option will modify or remove any existing global data and will affect all domains. If overwrite is selected, all current global data will be removed and replaced with the global configuration in the file, or nothing if there is no configuration defined.

Global Services & Rules

Select this option to import Global services (services that are common to all domains) and their associated classification rules. When you import rules from another domain, the Policy tab checks for rule conflicts (see Conflict Checking for more information).

Application of Imported Data Elements

In this section, you can choose how you want the data elements selected above to update your current domain.

Append domain data to existing elements

Select this option to import only new data elements into your current domain. If any of the selected data elements already exist in your current domain, they will not be changed.

Rate Limits: A rate limit will not be appended if: 1) The Rate, Direction, and 802.1P Priority are already defined. 2) The Priority list is empty.

CoS: A class of service will not be appended if: 1) The name is the same as an existing class of service. 2) The class of service names are different but the rate limits for the imported class of service do not match the existing rate limit settings.

Update existing data with elements from domain

Select this option to 1) replace the selected data elements that exist in your current domain with the imported data elements, and 2) import the selected data elements that don't exist in your current domain.

Rate Limits: A rate limit will not be updated if the rate limit and direction do not match.

CoS: A class of service will not be updated if: 1) The name does not match an existing class of service. 2) The class of service name matches but the rate limits for the imported class of service do not match the existing rate limit settings.

Overwrite existing elements

Select this option to replace the selected data elements that exist in your current domain with the imported data elements.

CoS: A class of service will not be overwritten if the rate limits for the imported class of service do not match the existing rate limit settings.

NOTE: If you decide that you want to return to the previous configuration (that the import updated), you can perform a File > Read Policy Domain operation to restore the configuration, as long as you have not saved the data you imported.

Select All Button

Selects all of the data elements.

Import Button

Imports the selected data and closes the window.

Related Information

For information on related tasks:

- How to Create and Use Domains

For information on related windows:

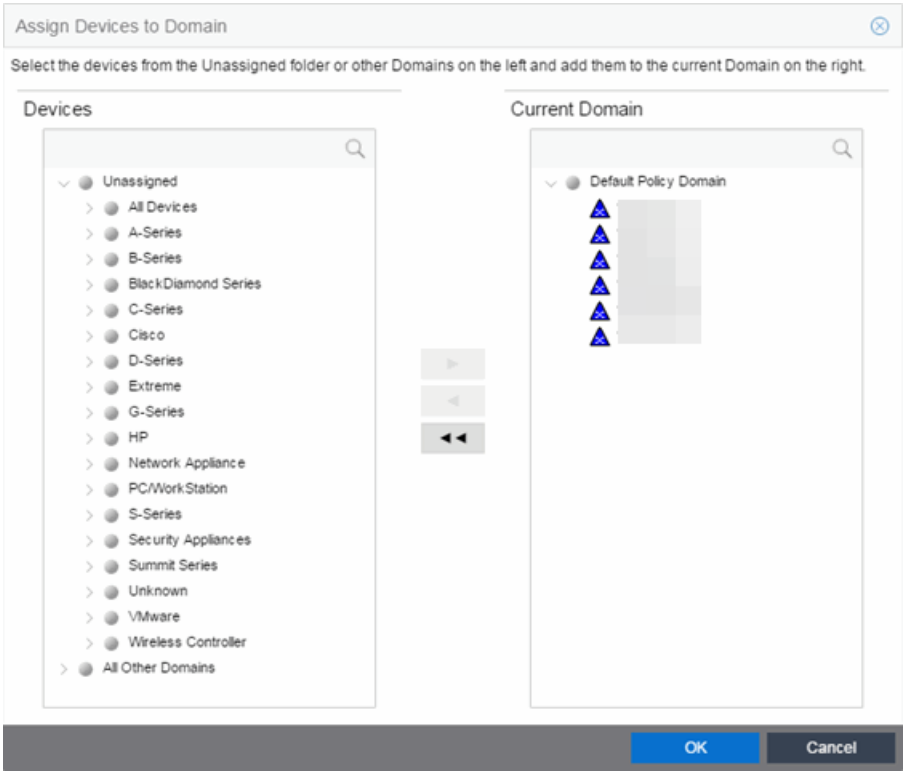
- Import From Domain Window

Assign Devices to Domain

This window lets you assign devices in the Extreme Management Center database to a Policy Domain or move devices from one domain to another. A Policy Domain contains any number of roles and a set of devices uniquely assigned to that particular domain. A device can exist in only one Policy Domain. For more information on domains, see How to Create and Use Domains.

Initially, you must add your devices to the Extreme Management Center database. Once your devices are in the database, use this window to assign the devices to a Policy Domain. As soon as the devices are assigned to a domain, they display automatically in the **Policy** tab **Devices** tab. Only devices that support policy are displayed in the **Devices** tab.

To access this window, open the domain to which you want to assign devices, and select **Open/Manage Domains > Assign Devices to Domain**.



Devices

The Devices list displays all the unassigned devices in the database (including devices that do not support policy) but are not assigned to a domain. The panel also displays any other domains and the devices assigned to that domain. Use the navigation trees to select a single domain or All Other Domains.

Current Domain

The Current Domain list displays the current domain and the devices assigned to that domain. To add a device to the current domain, select the device in the left panel and click the right arrow. You can also select and add multiple devices. To remove a device from the current domain, select the device and click the left arrow. This removes the device from the current domain and places it back in the device tree as either unassigned or as a member of the domain it came from. To remove all devices, click the double left arrow.

Device Domain Membership

This section is only displayed when more than one domain exists. It lists the domain assignment for whatever device or device group you have selected in the Devices panel. This is particularly useful when you have selected All Other Domains from the drop-down menu in the Devices panel, as it allows you to quickly see the domain assignment for each device.

Right Arrow Button

Adds the devices selected in the Devices list to the Current Domain list.

Remove Button

Removes the devices selected in the Current Domain list from the current domain and places it back in the Devices list as either unassigned or as a member of the domain from which it came.

NOTE: Removing a device from a domain does not delete the device from the Extreme Management Center database. To delete a device from the database, right-click on the device in the Network tab, and select Device > Delete Device from the menu. When a device is deleted from the database, it is automatically removed from the Network and Policy tabs.

Double Left Arrow Button

Removes all the devices from the current domain.

OK Button

Assigns the selected devices to the current domain and displays the devices in the Policy tab's Devices tab. Only devices that support policy are assigned to the domain and displayed in the Devices tab.

Related Information

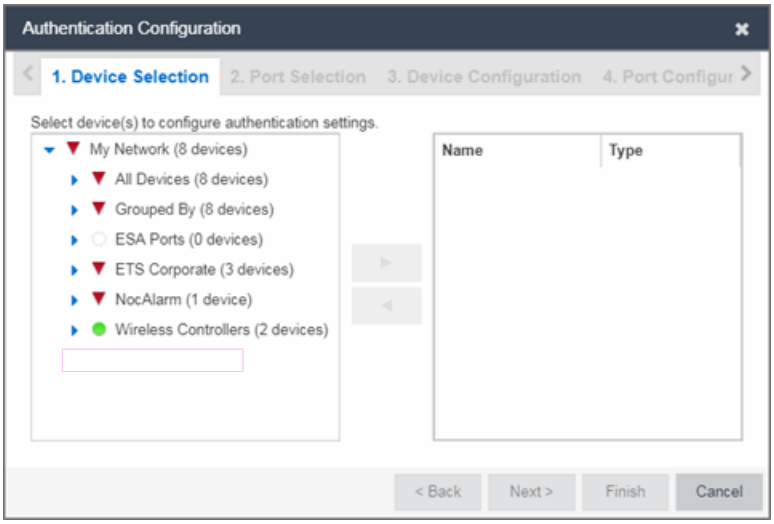
For information on related tasks:

- How to Add and Delete Devices
- How to Create and Use Domains

Extreme Management Center Authentication Configuration

The Authentication Configuration wizard enables you to configure and change the authentication settings on your devices. Authentication must be configured and enabled on a device in order for individual port authentication settings to take effect (see How to Configure Ports).

To access this tab, select Authentication Configuration from the Tools drop-down menu.



Device Selection

Use the Device Selection tab to select the devices on which you are configuring authentication settings.

Select a device from the available devices list in the left of the tab and click the right arrow icon to move the device to the selected devices list. Click Next> to proceed to the next tab.

Port Selection

Use the Port Selection tab to select the ports on which you are configuring authentication settings.

Select a port from the Available Ports list at the top of the tab and click Add Ports to move the port to the Selected Devices list. Click Next> to proceed to the next tab.

Device Configuration

The Device Configuration tab allows you to configure authentication for a device. Use the Port Configuration tab to configure authentication settings for individual ports on the device.

Save Device & Port Config Settings To Template

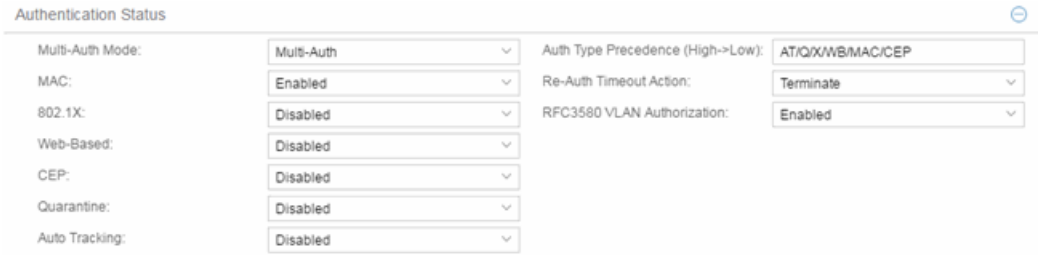
Click to save the settings you define on the Device Configuration and Port Configuration tabs to a template you can load for other devices.

Load Device & Port Config Settings From Template

Click to load a previously saved template of settings you previously defined on the Device Configuration and Port Configuration tabs.

Authentication Status

Use this section to select the authentication mode and types used on the device.



Use the fields on the left side of this section to select the appropriate single- or multi-user authentication types. Only options supported by the selected device are available for selection. Some devices support multiple authentication types and multiple users (Multi-User Authentication) per port, while others are restricted to only one or two authentication types and single users per port. Refer to the

Firmware Support tables for information on the authentication types supported by each device type.

WARNING: Switching Authentication Types, or changing the Authentication Status from Enabled to Disabled, logs off any currently authenticated users.

Auth Type Precedence (High->Low)

This displays the order in which the authentication types are attempted on the device, with the authentication type on the left having the highest precedence (attempted first). You can edit the precedence order by clicking the field. In the Edit Precedence window, select the authentication type you want to position, and use the Up and Down buttons to arrange the types in the desired order of precedence.

WARNING: Leave the default precedence, if possible. Changing the Quarantine precedence to be lower than any other type or changing the Auto Track precedence to be higher than any other type may cause problems.

Re-Auth Timeout Action

This setting defines the action for sessions that need to be re-authenticated if the RADIUS server re-authentication request times out. Select the Terminate option to terminate the session or the None option to allow the current session to continue without disruption.

Maximum Number of Users

This setting applies to devices with Multi-User as their configured authentication type. The maximum number of users that can be actively authenticated or have authentications in progress at one time on this device. You can specify the maximum number of users per port on the port's Port Properties Authentication Configuration tab.

RFC3580 VLAN Authorization

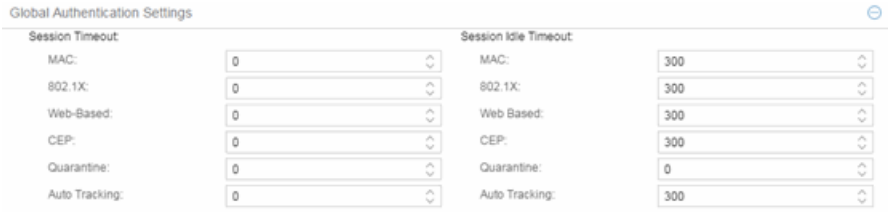
This allows you to enable and disable RFC 3580 VLAN Authorization for the selected device. RFC 3580 VLAN Authorization must be enabled on devices in networks where the RADIUS server is configured to return a VLAN ID when a user authenticates.

When RFC 3580 VLAN Authorization is enabled:

- devices that do not support policy tag packets with the VLAN ID.
- devices that support both policy and Authentication-Based VLAN to Role Mapping classify packets according to the role to which the VLAN ID maps.

Global Authentication Settings

This section lets you set session timeout and session idle timeout values for each authentication type.



Session Timeout

This setting represents the maximum number of seconds an authenticated session may last before automatic termination of the session. A value of zero indicates that no session timeout applies. This value may be superseded by a session timeout value provided by the authenticating server. For example, if a session is authenticated by a RADIUS server, that server may send a session timeout value in its authentication response.

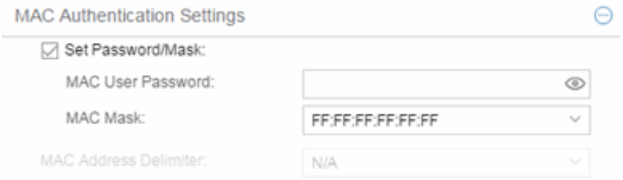
NOTE: Non-zero values are rounded to the nearest non-zero multiple of 10 by the device.

Session Idle Timeout

This displays the maximum number of consecutive seconds an authenticated session may be idle before Extreme Management Center automatically terminates the session. A value of zero indicates that no idle timeout applies. This value may be superseded by an idle timeout value provided by the authenticating server. For example, if a session is authenticated by a RADIUS server, that server may send an idle timeout value in its authentication response.

MAC Authentication Settings

This section enables you to set up the MAC password for MAC authentication. In order for MAC authentication to work, you must also configure the RADIUS server with the MAC password as well as the MAC addresses which are allowed to authenticate.



Set Password/Mask
Select this checkbox to set a password and mask for MAC authentication.

MAC User Password
The password passed to the RADIUS server for MAC authentication.

MAC Mask
You can select a mask to provide a way to authenticate end-systems based on a portion of their MAC address. For example, you could specify a mask that would base authentication on the manufacturers ID portion of the MAC address. The MAC Mask is passed to the RADIUS server for authentication after the primary attempt to authenticate using the full MAC address fails.

MAC Address Delimiter
The character used between octets in a MAC address:

- None — No delimiter is used in the MAC address (e.g. xxxxxxxxxxxx).
- Hyphen — A hyphen is used as a delimiter in the MAC address (e.g. xx-xx-xx-xx-xx-xx).

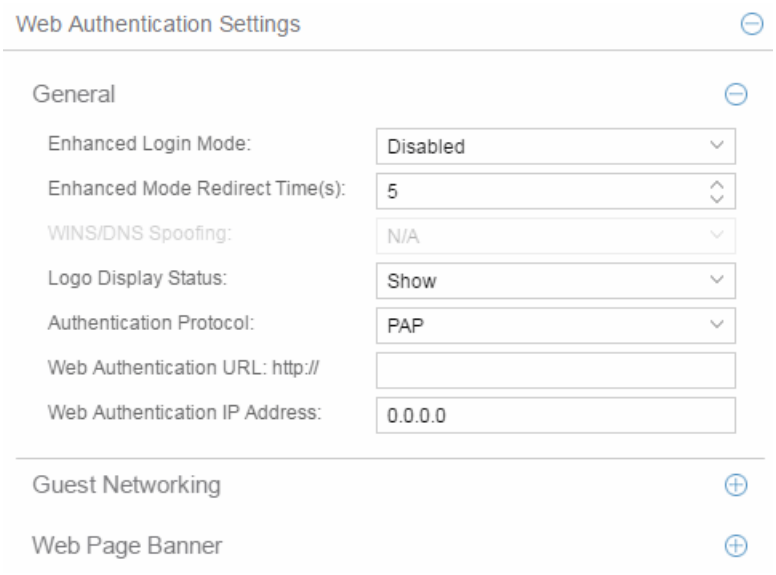
Web Authentication Settings

For users of web-based authentication, this tab lets you specify web authentication parameters using three sections:

- General
- Guest Networking
- Web Login

General

The General section lets you specify the URL of the authentication web page and the IP address of the system where it resides. It also lets you enable certain web authentication features, such as Enhanced Login Mode, on devices that support those features.



Enhanced Login Mode

Enabling the Enhanced Login Mode causes the authentication web page to be displayed regardless of whether the URL or IP address entered into the browser by the end user is the designated Web Authentication URL or IP address. This option is grayed out if the device does not support the mode.

Enhanced Mode Redirect Time(s)

This setting applies for devices with Enhanced Login Mode enabled. It specifies the amount of time (in seconds) before the end-user is redirected from the authentication web page to their requested URL.

An end-system using DHCP requires time to transition from the temporary IP address issued by the authentication process to the official IP address issued by the network. Enhanced Mode Redirect Time specifies the amount of time allowed for the end-system to complete this process and begin using its official IP address.

For example, if an end-user (in Enhanced Login Mode and a Redirect Time of 30 seconds) enters the URL of "http://ExtremeNetworks.com", the user is presented the authentication web page. When the user successfully authenticates into the network, the user sees a login success page that displays "Welcome to the Network. Completing network connections. You will be redirected to http://ExtremeNetworks.com in approximately 30 seconds."

WINS/DNS Spoofing

This setting allows you to enable and disable WINS/DNS spoofing for the selected device. Spoofing allows the end-user to resolve the Web Authentication URL name

to the IP address using WINS/DNS. The default is Disabled. This option is grayed out if not supported by the device.

Logo Display Status

Specifies whether the Extreme Networks logo is displayed or hidden on the authentication web page window. This option is grayed out if not supported by the device.

Authentication Protocol

This setting is the authentication protocol being used (PAP or CHAP). PAP (Password Authentication Protocol) provides an automated way for a PPP (Point-to Point Protocol) server to request the identity of user, and confirm it via a password. CHAP (Challenge Handshake Authentication Protocol), the more secure of the two protocols, provides a similar function, except that the confirmation is accomplished using a challenge and response authentication dialog.

Web Authentication URL

This is the URL for your authentication web page. Users wishing to receive network services access the web page from a browser using this URL. The http:// is supplied. Alphabetical characters, numerical characters and dashes are allowed as part of the URL, but dots are not. The URL needs to be mapped to the Web Authentication IP address in DNS or in the hosts file of each client. It must be resolvable via DNS/WINS, either on the device or at corporate, assuming the Web Authentication mapping has been set up on the corporate DNS/WINS service. This option is grayed out if not supported by the device.

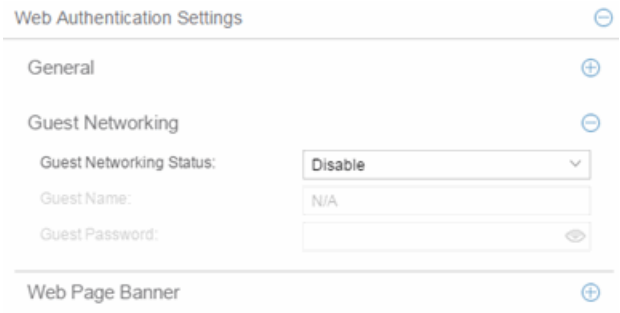
Web Authentication IP Address

This is the IP address of your authentication web page server. If you have specified a Web Authentication URL, the IP address needs to be mapped to the URL in DNS or in the host file of each client.

Guest Networking

The Guest Networking section lets you configure guest networking, a feature that allows any user to access the network and obtain a guest policy without having to know a username or password. The user accesses the authentication web page, where the username and password fields are automatically filled in, allowing them to log access as a guest. If the user does not want to log in as a guest, they can type in their valid username and password to log in.

NOTE: Guest networking is designed for networks using web-based authentication, with port mode set to Active/Discard.



Guest Networking Status

Use the drop-down list to specify guest networking status:

- Disable — Guest networking is unavailable.
- Local Auth — Guest Networking is enabled. The user accesses the authentication web page where the username field is automatically filled in with the specified Guest Name. Once the user submits the web page using this guest name, the default policy of that port becomes the active policy. The port mode must be set to Active/Discard mode.
- RADIUS Auth — Guest Networking is enabled. The user accesses the authentication web page, where the username field is automatically filled in with the specified Guest Name, and the password field is masked out with asterisks. Once the user submits the web page using these credentials, the value of the Guest Password is used for authentication. Following successful authentication from the RADIUS server, the port applies the policy (role) returned from the RADIUS server. The port mode must be set to Active/Discard mode.

Guest Name

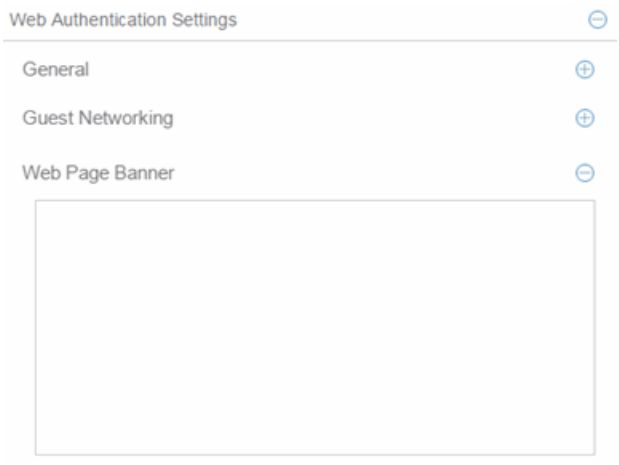
The username that Guest Networking uses to authenticate users. The guest name is displayed automatically on the authentication web page. If the user does not want to log in as a guest, they can type in their valid username to override the guest username.

Guest Password

The password that Guest Networking uses to authenticate users when RADIUS Auth is selected.

Web Page Banner

The Web Page Banner section allows you to customize the banner end users see at the top of the authentication web page and set a Redirect Time, if applicable.



Web Page Banner

Use this area to create a banner end users see at the top of the authentication web page. For example, you might include your company name and information on what to do if the user has questions or problems. Because this banner also appears in messages that occur during successful login and failed authentication, as well as on the "Radius Busy" screen, it is not appropriate to include "Welcome to [Your Company]" in the banner.

The Default button allows you to reset the banner to default text provided in a text file (pwa_banner.txt). Initially, the default banner text is the Extreme Networks contact information. However, you can customize the text for your network by editing the pwa_banner.txt file, located in the top level of the Policy Manager install directory. Then, when you click the Default button, the new text will be displayed in the Web Page Banner area.

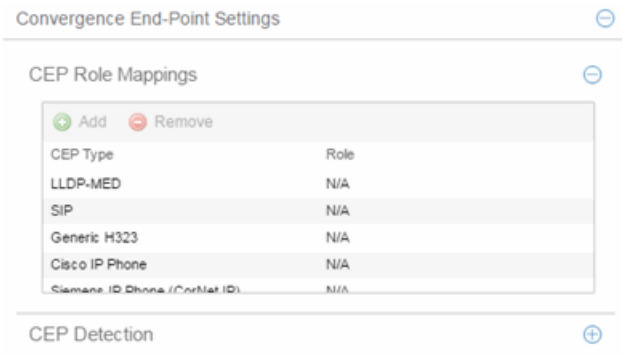
Convergence End-Point Settings

This section provides a way to identify Convergence End-Points (IP phones) connecting to the device, and apply a role to the end-point based on the type of end-point detected. The CEP Detection section lets you create detection rules for identifying the end-points, and the CEP Role Mappings section lets you map a role to each CEP product type.

In addition to configuring CEP on the device, you must also enable CEP protocols on each port using the CEP Access section in the Port Authentication Tab. Once you have configured CEP on the device and each port, you can monitor CEP usage on the Port Usage Tab (Port) or Port Usage Tab (Device).

CEP Role Mappings

This section lets you select the CEP product types supported on the device, and map a role for each type. Then, when a convergence end-point (such as an IP phone) connects to the network, the device identifies the type of end-point (using CEP detection rules) and applies the assigned role.



CEP Type
Lists the CEP types supported by the device.

Role
Lists the role mapped to each **CEP Type**.

Add
Select a CEP Type and click the **Add** button to open the Add Role Mapping window, where you can select a role for the selected **CEP Type**. Your selections are added to the CEP Role Mappings list.

Remove
Select the **CEP Type** and click **Remove** to remove the **CEP Type** in the CEP Role Mappings list.

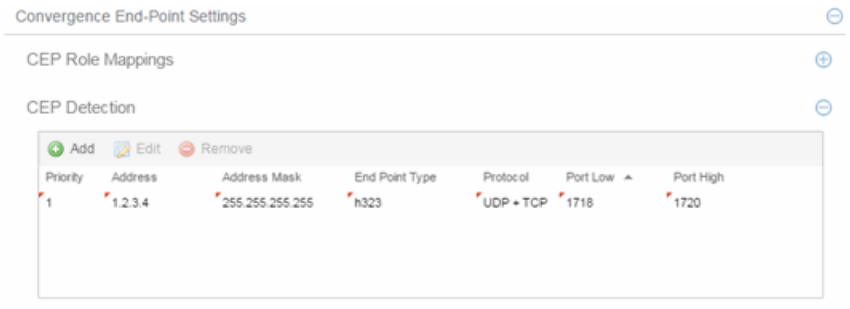
CEP Detection Tab

Use this section to create CEP detection rules used to determine if a connecting end-system is a CEP device and the type of CEP device. This allows Extreme Management Center to assign the appropriate role to the port based on the type of CEP device detected.

NOTE: CEP detection rules apply only to Siemens, H.323, and SIP (Session Initiation Protocol) phone detection. Cisco detection uses CiscoDP as its detection method.

CEP detection rules are based on two detection methods:

- TCP/UDP Port Number detection — Many CEP vendors use specific TCP/UDP port numbers for call setup on their IP phones. You can create detection rules that identify CEP devices based on specific TCP/UDP port numbers. By default, Siemens Hi-Path phones are detected on TCP/UDP port 4060.
- IP Address detection — H.323 phones use a reserved IP multicast address and UDP port number for call setup. You can create detection rules to detect an IP phone based on its IP address in combination with an IP address mask. By default, H.323 phones are detected using the multicast address 224.0.1.41 and the TCP/UDP ports 1718, 1719, and 1720. SIP phones are detected using the multicast address 224.0.1.75 and the TCP/UDP port 5060. H.323 and SIP phones are also detected using only their respective multicast addresses without the TCP/UDP ports.



Priority

The rule priority with one (1) being the highest priority. The rule with the highest priority is used first, so it is recommended the highest priority be given to the predominate protocol in the network to provide for greater efficiency.

Address

If the rule is based on IP address detection, this field displays the IP address that incoming packets matched against. By default, H.323 uses 224.0.1.41 as its IP address, SIP uses 224.0.1.75 as its IP address, and Siemens has no IP address configured.

Address Mask

If the rule is based on IP address detection, this field displays the IP address mask against which incoming packets are matched.

End Point Type

Specifies the end-point type assigned (H.323, Siemens, or SIP) if incoming packets match this rule.

Protocol

If the rule is based on TCP/UDP port detection, this field displays the protocol type used for matching, using a port range defined with the Port Low and Port High

values:

- UDP + TCP — Match the port number for both UDP and TCP frames.
- TCP — Match the port number only for TCP frames.
- UDP — Match the port number only for UDP frames.

Port Low
The low end of the port range defined for detection on UDP and/or TCP ports.

Port High
The high end of the port range defined for detection on UDP and/or TCP ports.

Add
Opens the Add/Edit CEP Detection Rule window where you can create CEP detection rules.

Remove
To remove a CEP detection rule, select the entry and click **Remove**.

Edit
To edit a CEP detection rule, select the rule and click **Edit**. The Add/Edit CEP Detection Rule window opens where you edit the rule's parameters. You can also double-click an entry in the table to open the edit window.

Port Configuration

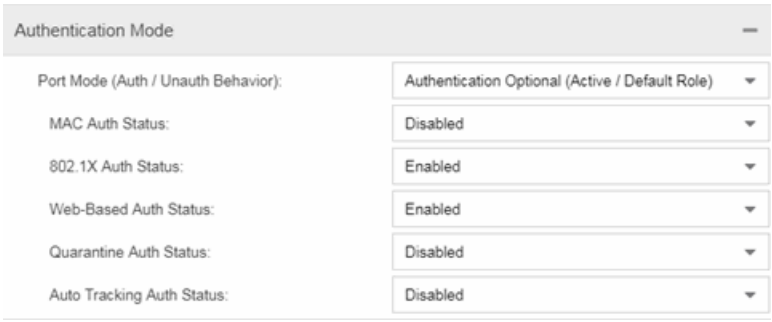
The **Port Configuration** tab allows you to configure authentication for the ports of a device.

The **Authentication Configuration** tab has six sections:

- Authentication Mode
- RFC3580 VLAN Authorization
- Login Settings
- Automatic Re-Authentication
- Authenticated User Counts
- CEP Access

Authentication Mode

This section displays general authentication and port mode information about the port.



Port Mode

This area displays the current port mode for the port, and allows you to change the settings if desired. Port mode defines whether or not a user is required to authenticate on a port, and how unauthenticated traffic will be handled. It is a combination of Authentication Behavior (whether or not authentication is enabled on the port), and Unauthenticated Behavior (whether unauthenticated traffic will be assigned to the port's default role or discarded). See Port Mode for a complete description of each port mode.

In addition, this section provides checkboxes that allow you to disable a specific authentication type at the port level.

Auth/Unauth Behavior

Select an option to specify how authenticated and unauthenticated traffic is handled on the port. (See Port Mode for more information.) If you set the port's Authentication Behavior to Active (i.e., you enable authentication for the port), it is recommended that you enable the Drop VLAN Tagged Frames feature.

NOTE: Authentication Behavior must be set to **Active** for authentication to be allowed using CEP Protocols.

Additionally, specify whether unauthenticated traffic is assigned to the port's default role or discarded. The current default role for the port is shown. For additional information, see Port Mode.

NOTE: For Single User 802.1X and 802.1X+MAC authentication types:

- Active/Default Role mode requires that a default role be set on the port
- Active/Discard mode requires that any default role set on the port is cleared

For Multi-User Web-based authentication Active/Discard mode is not supported.

MAC Auth Status

Select whether to enable or disable MAC authentication at the port level. If the device is only configured with MAC authentication, selecting this checkbox will result in the port Authentication Behavior being set to Inactive.

802.1X Auth Status

Select whether to enable or disable 802.1X authentication at the port level. If the device is only configured with 802.1X authentication, selecting this checkbox will result in the port Authentication Behavior being set to Inactive.

NOTE: For Single User 802.1X+MAC authentication with Active/Default Role as the selected port mode: Disabling 802.1X authentication also disables MAC authentication on the port. An end user connecting to the port will not be able to authenticate via 802.1X or MAC. The port will behave as if Inactive/Default Role is the selected port mode.

Web-Based Auth Status

Select whether to enable or disable web-based authentication at the port level. If the device is only configured with web-based authentication, selecting this checkbox will result in the port Authentication Behavior being set to Inactive.

NOTE: For Multi-User Web-Based authentication with Active/Discard as the selected port mode: This checkbox is automatically selected because multi-user web-based authentication does not support the Active/Discard port mode.

Quarantine Auth Status

Select whether to enable or disable Quarantine authentication at the port level. If the device is only configured with Quarantine authentication, selecting this checkbox will result in the port Authentication Behavior being set to Inactive.

Auto Tracking Auth Status

Select whether to enable or disable MAC authentication at the port level. If the device is only configured with Auto Tracking authentication, selecting this checkbox will result in the port Authentication Behavior being set to Inactive.

Apply Button

Applies any Port Mode changes to the port.

CEP protocols in the CEP Access tab

Use the CEP Access tab to disable CEP protocols at the port level.

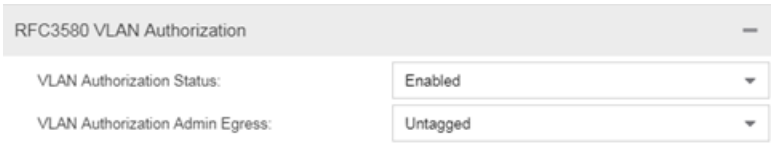
RFC3580 VLAN Authorization Tab

This tab lets you enable or disable RFC 3580 VLAN Authorization on the port and specify an egress state. RFC 3580 VLAN Authorization must be enabled in networks where the RADIUS server has been configured to return a VLAN ID when a user authenticates.

When RFC 3580 VLAN Authorization is enabled:

- ports on devices that do **not** support policy tag packets with the VLAN ID.
- ports on devices that do support policy and also support Authentication-Based VLAN to Role Mapping classify packets according to the role to which the VLAN ID maps.

You can also enable and disable VLAN Authorization at the device level using the device Authentication tab. If the device does not support RFC 3580, this tab is grayed out.



VLAN Authorization Status

Allows you to enable and disable RFC 3580 VLAN Authorization for the selected port. This option is grayed out if not supported by the device.

VLAN Authorization Admin Egress

Allows you to modify the VLAN egress list for the VLAN ID returned by the RADIUS server when a user authenticates on the port:

- None - No modification to the VLAN egress list will be made.
- Tagged - The port will be added to the list with the egress state set to Tagged (frames will be forwarded as tagged).
- Untagged - The port will be added to the list with the egress state set to Untagged (frames will be forwarded as untagged).

- Dynamic - The port will use information returned in the RADIUS response to modify the VLAN egress list. This value is supported only if the device supports a mechanism through which the egress state may be returned in the RADIUS response.

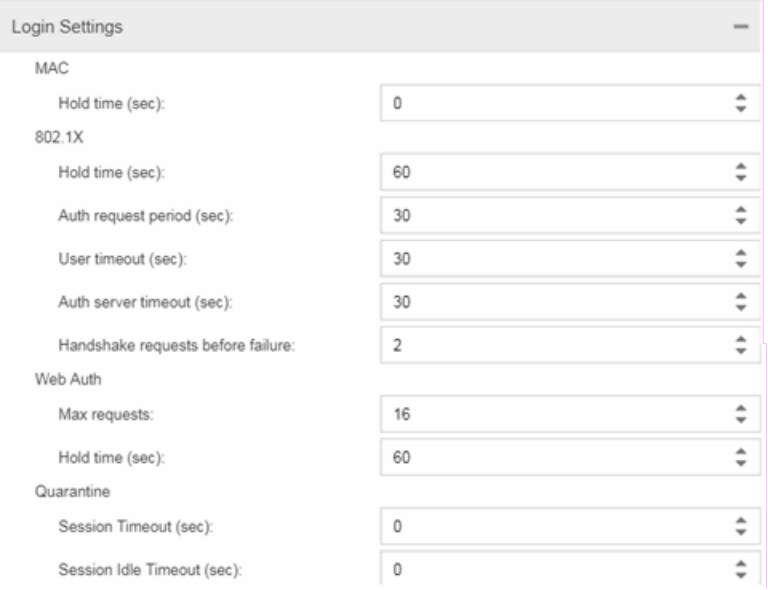
The current egress settings for the port are displayed in the VLAN Oper Egress column in the **User Sessions** tab. These options are grayed out if not supported by the device.

Apply Button

Saves any change you made to the VLAN Authorization settings.

Login Settings

This tab displays the current login settings for the port and allows you to change the settings if desired. The options available depend on what type(s) of authentication are enabled on the device.



Number of Attempts Before Timeout

Number of times a user can attempt to log in before authentication fails and login attempts are not allowed. For web-based authentication, valid values are 1-2147483647, zero is not allowed, and the default is 2. For 802.1X and MAC authentication, this value is permanently set to 1.

Hold Time (seconds)

Amount of time (in seconds) authentication will remain timed out after the specified Number of Attempts Before Timeout has been reached. Valid values are 0-65535. The default is 60. (Hold Time is also known as Quiet Period in web-based and MAC authentication.)

Authentication Request Period

For 802.1X authentication, how often (in seconds) the device queries the port to see if there is a new user on it. If a user is found, the device then attempts to authenticate the user. Valid values are 1-65535. The default is 30.

User Timeout

For 802.1X authentication, the amount of time (in seconds) the device waits for an answer when querying the port for the existence of a user. Valid values are 1-300. The default is 30.

Authentication Server Timeout

For 802.1X authentication, if a user is found on the port, the amount of time (in seconds) the device waits for a response from the authentication server before timing out. Valid values are 1-300. The default is 30.

Port Handshake Requests Before Failure

For 802.1X authentication, the number of times the device tries to finalize the authentication process with the user before the authentication request is considered invalid and authentication fails. Valid values are 1-10. The default is 2.

Quarantine Session Timeout (sec)

For Quarantine authentication, the maximum number of seconds an authenticated session may last before automatic termination of the session. A value of zero indicates that no session timeout will be applied.

Quarantine Session Idle Timeout (sec)

For Quarantine authentication, the maximum number of consecutive seconds an authenticated session may be idle before automatic termination of the session. A value of zero indicates that the device level setting is used.

Auto Tracking Session Timeout (sec)

For Auto Tracking sessions, the maximum number of seconds a session may last before automatic termination of the session. A value of zero indicates that the device level setting is used.

Auto Tracking Session Idle Timeout (sec)

For Auto Tracking sessions, the maximum number of consecutive seconds a session may be idle before automatic termination of the session. A value of zero indicates that the device level setting is used.

Apply Button

Applies the Login Settings changes to the port.

Automatic Re-Authentication

This tab is grayed out if only web-based authentication is enabled on the device. For 802.1X and MAC authentication, the Automatic Re-Authentication tab lets you set up the periodic automatic re-authentication of logged-in users on this port. Without disrupting the user's session, the device repeats the authentication process using the most recently obtained user login information to see if the same user is still logged in. Authenticated logged-in users are not required to log in again for re-authentication, as this occurs "behind the scenes."

802.1X Re-auth Status

If Active is selected, the re-authentication feature is enabled for 802.1X authentication. If Inactive is selected, the re-authentication feature is disabled.

802.1X Re-auth Frequency (sec)

How often (in seconds) the device checks the port to re-authenticate the logged-in user via 802.1X authentication. Valid values are 1-2147483647. The default is 3600.

MAC Re-auth Status

If Active is selected, the re-authentication feature is enabled for MAC authentication. If Inactive is selected, the re-authentication feature is disabled.

MAC Re-auth Frequency (sec)

How often (in seconds) the device checks the port to re-authenticate the logged in user via MAC authentication. Valid values are 1-2147483647. The default is 3600.

Authenticated User Counts

This tab provides authenticated user-count information for devices with Multi-User as their configured authentication type. See the device Authentication tab for information on setting the device authentication type.

Current Number of Users

The current number of users actively authenticated or have authentications in progress on this interface. If Multi-User authentication is disabled, this number is 0. Any unauthenticated traffic on the port is not included in this count.

Number of Users Allowed (up to 2048)

The number of users that can be actively authenticated or have authentications in progress at one time on this interface. If you set this value below the current number of users, end-user sessions exceeding that number are terminated.

NOTE: B2/C2 Devices. If you are configuring a single user and an IP phone per port, set this value to 2.

Number of MAC Users Allowed (up to 2048)

The number of users that can be actively authenticated via MAC authentication, or have MAC authentications in progress at one time on this interface. The number of MAC users allowed cannot exceed the number of users allowed. If you set this value below the current number of users, end user sessions exceeding that number are terminated. If MAC is not selected as a Multi-User authentication type on the device Authentication tab, this field will be grayed out.

Number of Quarantine Users Allowed (up to 2048)

The number of users that can be actively authenticated via Quarantine authentication, or have Quarantine authentications in progress at one time on this interface. The number of Quarantine users allowed cannot exceed the number of users allowed. If you set this value below the current number of users, end user sessions exceeding that number are terminated. If Quarantine

Auth is not enabled on the device Authentication tab, this field will be grayed out.

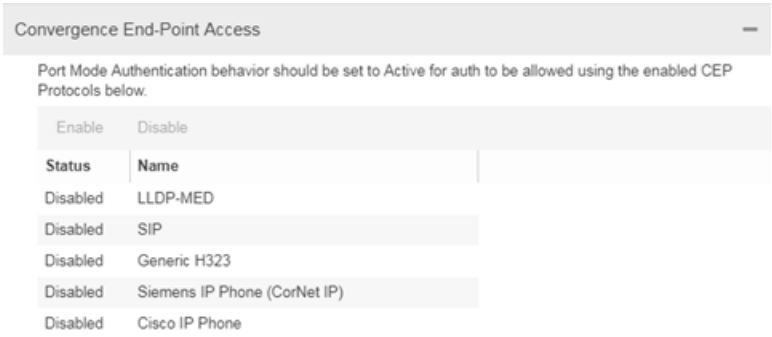
Number of Auto Tracking Users Allowed (up to 2048)
: The number of Auto Tracking users that can be actively authenticated or have authentications in progress at one time on this interface. The number of Auto Tracking users allowed cannot exceed the number of users allowed. If you set this value below the current number of users, end user sessions exceeding that number will be terminated. If Auto Tracking is not enabled on the device Authentication tab, this field is grayed out.

Convergence End-Point Access

This tab lists all the CEP (Convergence End-Point) protocols supported by the device on which the port resides, and lets you enable or disable them for that port. For devices that do not support CEP, the tab is blank.

NOTE: Port Mode Authentication Behavior must be set to Active (on the General sub-tab) for authentication to be allowed using these CEP Protocols.

Enable CEP protocols for multiple ports using the Port Configuration Wizard. In addition to enabling protocols on the port, you must also configure CEP for the device on which the port resides. Configure CEP for a single device using the device Authentication tab (CEP sub-tab) or for multiple devices using the Device Configuration Wizard.



CEP Access
: Lists all the CEP protocols supported by the device on which the port resides. Use the checkboxes to enable or disable CEP protocols on this port. If the device does not support the CEP feature, this area is blank.

Enable All Button
Selects all the checkboxes and enables all the CEP protocols for this port.

Disable All Button
Deselects all the checkboxes and disables all the CEP protocols for this port.

Apply Button
Applies CEP access changes to the port.

Related Information

For information on related windows:

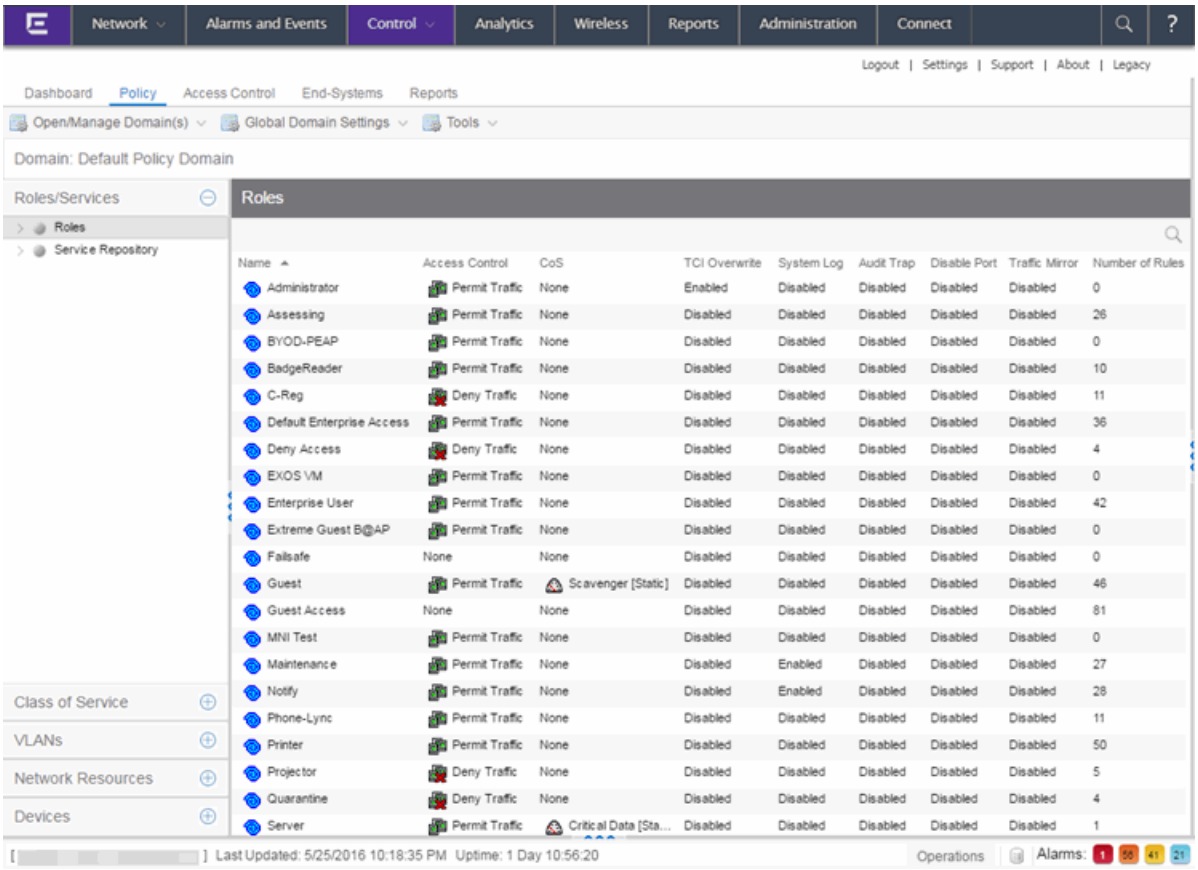
- Add/Edit CEP Detection Rule Window

Policy Main Window

The Control > Policy tab main window is the central point for all Policy tab tasks. It is divided into a left panel and a right panel. The tabs in the left panel display hierarchical trees that represent the roles, services, network elements, devices and port groups involved in managing policies for your network. There are five left-panel tabs: Roles/Services, Class of Service, VLANs, Network Resources, and Devices. The tabbed pages in the right panel display detailed information about the item selected in the left panel.

Information on Policy tab features:

- Dialog Boxes (Messages)
- Icons
- Left Panel



Dialog Boxes (Messages)

In the course of using the **Policy** tab, message dialog boxes appear confirming certain tasks are complete, or warning of the consequences of performing a certain action.

Icons

The icons used in the **Policy** tab and their meanings are as follows:

Icon	Definition	Icon	Definition
	Pre-Defined Groups		User-Defined Groups
	Device/Wireless Device		Port Group
	Port		Frozen Port
	Role		Quarantine Role
	Rule		Disabled Rule
	Device-specific Rule		Service Group

Icon	Definition	Icon	Definition
	Automated Service		Manual Service
	Network Resource Group		Slot/Logical Ports/Ports
	Contain VLAN		Deny VLAN
	VLAN or Network Resource Island		Island VLAN
	Warning		CoS (Class of Service)
	802.1p Priority		IP Type of Service Value
	CoS Port Group		Rate Limit
	Transmit Queue		Network Resource Topology

Open/Manage Domain Menu Icons

The following icons appear in the **Open/Manage Domains** drop-down menu:

Lock

Reminds you the current Policy Domain is locked for editing purposes. You can lock and unlock the domain from the Lock tool bar button.

Save

Reminds you that you've made changes, and you need to save the data to the Policy Domain. Clicking this icon initiates the save operation. Only users with the capability to Enforce are able to save the domain.

Enforce

Reminds you that you've made changes to roles that you need to enforce. Clicking this icon initiates the enforce operation.

Related Information

For information on related windows:

- Details View Tabs
- Left Panel

Policy Windows

The **Windows** Help section contains Help topics describing **Policy** tab windows and their field definitions.

Policy Concepts

This topic explains concepts used in the **Policy** tab.

Information on:

- Policy
- Role
    - What is a Role
    - Default Role
- Policy Domains
- Service
- Rule
    - What is a Rule
    - Disabling Rules
    - Conflict Checking
- Packet Tagging
- VLAN to Role Mapping
- Dynamic Egress
    - Setting Domain GVRP Status
- Policy VLAN Islands
- Traffic Mirroring
- Port Groups
- Network Resource Groups
    - Network Resource Topologies
- Verifying

- Enforcing
- Controlling Client Interactions with Locks

Policy

In the **Policy** tab, network access policies are called Roles. See Role, below, for a description.

Role

What is a Role

A role is a set of network access services that can be applied at various access points in a policy-enabled network. A port takes on a user's role when the user authenticates. Roles are usually named for a type of user such as Student or Engineering. Often, role names match the naming conventions that already exist in the organization. A role can contain any number of services in the **Policy** tab.

A role may also contain default access control (VLAN) and/or class of service (priority) characteristics that will be applied to traffic not identified specifically by the set of access services contained in the role. The set of services included in a role, along with any access control or class of service defaults, determine how all network traffic will be handled at any network access point configured to use that role.

Default Role

Once you have created a role, assign it as the default role for a port (see Assigning Default Roles to Ports).

Policy Domains

The **Policy** tab provides the ability to create multiple policy configurations by allowing you to group your roles and devices into Policy Domains. A Policy Domain contains any number of roles and a set of devices that are uniquely assigned to that particular domain. Policy Domains are centrally managed in the database and shared between the **Policy** tab clients.

In the **Policy** tab, you work in one current domain at a time. Each domain is identified by a unique name. The Domain menu lets you easily switch from one domain to another. There is no limit to the number of domains you can create, however, a device can exist in only one Policy Domain.

The first time you launch the Policy tab, you are in the Default Policy Domain. You can manage your entire network in the Default Policy Domain, or you can create multiple domains each with a different policy configuration, and assign your network devices to the appropriate domain. The roles, services, rules, VLAN membership, and class of service in this initial configuration define a suggested implementation of how network traffic can be handled. This is a starting point for a new policy deployment and often needs customization to fully leverage the power of a policy-enabled network.

The Policy tab ships with a set of domain configurations that provide ready-made workflows for common policy scenarios. Each domain configuration contains all the elements (roles, services, rules, VLAN membership, class of service) that define how network traffic is handled for each scenario. These domains are listed in the Open/Manage Domain menu.

You can import the data elements from one domain into another domain. You can also import a domain saved as a policy Database file (.pmd file) or data from a Database file into a domain, and you can export a domain or data from a domain to a .pmd file, (one file per domain) for backup and troubleshooting purposes. Verify and Enforce operations are performed only on the current domain.

In order for your network devices to be displayed on the left-panel Devices tab, they must be assigned to a Policy Domain. Initially, you must add your devices to the Extreme Management Center database. Once devices have been added to the Extreme Management Center database, you can assign the devices to a Policy Domain using the Policy tab. As soon as a device is assigned to a domain, it is automatically displayed on the left-panel Devices tab. Only devices that support policy are displayed in the Policy tab.

The Policy tab automatically locks the current Policy Domain when you begin to edit the domain configuration. Other users are notified that the domain is locked and they are not be able to save their own domain changes until the lock is released. For more information, see Controlling Client Interactions with Locks. After a Policy Domain has been changed, you must save the domain to notify all clients viewing that domain of the change and automatically update their view with the new configuration.

Service

Services are sets of rules that define how network traffic for a particular network service or application should be handled by a network access device. A service might consist of only one rule governing, for example, email priority, or it might consist of a complex set of rules combining class of service, filtering, rate limiting, and access control (VLAN) assignment. The **Policy** tab allows you to create Local Services (services that are unique to the current domain) and Global Services (services that are common to all domains). Global Services let you easily create and manage services shared between all your domains. A service can be included in any number of roles.

As an example, you might create a service called `High Priority Internet Web Access` that contains priority classification rules for traffic directed toward each of your organization's Internet proxy servers. This service would likely contain one traffic classification rule for each of your Internet proxy servers.

Services can be one of two types: Manual Service or Automated Service.

- **Manual Service** - This service consists of one or more traffic classification rules you create based on your requirements. Manual services are good for applying customized sets of rules to roles.
- **Automated Service** - This service automatically creates a rule with a specified action (class of service and/or access control), for each device in a particular network resource group. You create a network resource group using a list of IP addresses or an IP subnet, and then associate the group with the Automated service (see How to Create a Network Resource Group for more information). Automated rule types include Layer 3 IP Address and IP Socket rules, and Layer 4 IP UDP Port and IP TCP Port rules.

Services provide a common language that network engineers, information technology administrators, and business managers understand. See How to Create a Service for more information.

Rule

What is a Rule

Policy rules define one element of how traffic for a particular network service or application is handled by a network access device. For example, you might create a rule that assigns a certain priority to all email traffic, by adding an

802.1p, ToS, or DiffServ value to all SMTP traffic. A policy rule can be included in any number of services and you can select the types of devices to which the rule applies. You create rules by right-clicking a Service in the **Service Repository** tab and selecting **Create Rule**.

See Traffic Classification Rules for a detailed explanation of rules.

Disabling Rules

You can elect to disable a rule during or after its creation. If you disable a rule, it is temporarily unavailable for use by the current service, but it can still be copied to other services and enabled, or re-enabled at another time for the current service. Disabling a rule is a way to temporarily remove a rule from your service without having to delete and recreate it. You disable rules by right-clicking a Service in the **Service Repository** tab and selecting **Disable Rule**.

Conflict Checking

As you create your Policy view services and rules, you may define conflicting rules. A conflict exists when two rules in the same service or role define different actions for the same traffic description. For example, two rules might have the same traffic description, but forward traffic to different VLANs, or have different priorities. Extreme Management Center ensures that conflicting rules do not coexist in the same role or service by checking rule traffic descriptions and action values, providing a message if conflicts are found, and writing the conflict information to the Event Log. If a rule is disabled, conflicts between that rule and others are ignored.

The one exception to this conflict checking behavior, is when the conflicting rules coexist in the same role, but one rule exists in a Local service and the other exists in a Global service. In this case, the rule defined in the Local service takes precedence over the rule defined in the Global service because the Local service is specific to the current domain. Consider the following example:

In the North Campus domain you have a Local service "A" that assigns an Ethertype IP rule to the Red VLAN. The "A" service is assigned to the Student Role. In addition, a Global service "B" exists that assigns Ethertype IP rules to the Blue VLAN. The "B" service is also assigned to the Student Role. In this case, the Local service takes precedence over the Global service in the North Campus domain. Note that the precedence pertains to the rule's actions: class of service (priority) and access control (VLAN). For example, if a rule in a Local service and a rule in a Global service both have the same traffic description, and the Local

rule's actions apply CoS Priority 1 and no access control (no VLAN), while the Global rule's actions apply CoS Priority 2 and VLAN Blue(2), then the rule will be enforced using CoS Priority 1 and VLAN Blue(2). In addition, if *either* the Local or Global service has the Accounting or Security actions enabled, then they will be enforced to the devices.

Packet Tagging

Packet tagging in a Policy view environment occurs as follows:

Tagged packets and ingress filtering are processed first. Then, VLAN ID and priority are determined.

- *VLAN ID*: If the packet matches an active VLAN classification rule on the ingress port, the VID (VLAN ID) specified in the matching VLAN classification rule is assigned. Otherwise, if there is an active role on the ingress port and it specifies a default VLAN, the default VID from the active role on the ingress port is assigned. If there is no active role and no classification rule matches, the 802.1Q PVID for the ingress port is assigned.
- *Priority*: If the packet matches an active priority classification rule on the ingress port, the priority specified in the matching priority classification rule is assigned. Otherwise, if there is an active role on the ingress port and it specifies a default priority, the default priority from the active role on the ingress port is assigned. If there is no active role and no classification rule matches, the 802.1Q_PPRI for the ingress port is assigned.

The set of classification rules active on a port includes statically created rules that specify the ingress port on their port list, as well as any rules established as a result of a role being applied on that port. If the port has no active role and thus no default access control (VLAN) or class of service (priority), untagged packets that do not match any classification rules are assigned a VLAN and priority from the 802.1Q and 802.1p defaults for the ingress port.

For a graphical illustration of the packet tagging process in a Policy view scenario, see the Packet Flow Diagram. The packet passes through the decision-making process illustrated in the graphic twice — once for VLAN tagging and once for priority tagging.

VLAN to Role Mapping

VLAN to Role mapping lets you assign a role to an end user based on a VLAN ID. There are two kinds of VLAN to Role Mapping: Authentication-Based and Tagged Packet.

- Authentication-Based VLAN to Role Mapping (RFC 3580) — Provides a way to assign a role to a user during the authentication process, based on a VLAN Attribute. An end user connects to a policy-enabled device that supports 802.1X authentication using a RADIUS Server. During the authentication process, the RADIUS server returns a VLAN ID in its RADIUS VLAN Tunnel Attribute. The device uses the Authentication-Based VLAN to Role mapping list to determine what role to assign to the end user, based on the VLAN Tunnel Attribute. Authentication-Based VLAN to Role mappings are only configured at the device level (for all devices).

  NOTE: When configuring Authentication-Based VLAN to role mapping, you must enable RFC3580 VLAN Authorization on the device via the device Authentication tab. In addition, VLAN IDs must be configured on the RADIUS server for each user authorized to access the network. If a user does not have a configured VLAN ID, the default role (if there is one) or the 802.1Q PVID for the ingress port is assigned. For more information on configuring VLAN ID attributes on the RADIUS server, refer to your device firmware documentation, RFC 3580, and your RADIUS server documentation.

- Tagged Packet VLAN to Role Mapping - Provides a way to let policy-enabled devices assign a role to network traffic, based on a VLAN ID. When a device receives network traffic that has been tagged with a VLAN ID (tagged packet) it uses the Tagged Packet VLAN to Role mapping list to determine what role to assign the traffic based on the VLAN ID. Tagged Packet VLAN to Role mapping can be configured at the device level (all devices) and at the port level (for an individual port on a device). A VLAN can only be mapped to one role at the device level, but the same VLAN can be mapped to a different role at the port level. A mapping does not have to exist at the device level to be created at the port level, and port-level mappings will override any device-level mappings.

NOTE: TCI Overwrite Requirement
-- Tagged Packet VLAN to Role Mapping will apply the Role definition to incoming packets using a mapped VLAN. This definition will apply a COS and determine if the packet is discarded or permitted, and if TCI Overwrite is enabled will re-specify the VLAN ID defined by the Rule / Role Default. If TCI Overwrite is disabled, the packet will egress (if permitted by the Rule Hit) with the original VLAN ID it ingressed with.
-- If supported by the device, you can enable TCI Overwrite for an individual role in the role's General tab. The stackable devices support rewriting the CoS values but not the VLAN ID.

To configure VLAN to Role Mapping in the Policy view, use the role's Mappings tab and/or the VLAN's General tab.

Dynamic Egress

In the **VLANs** tab, you can enable Dynamic Egress for a VLAN by selecting the **Dynamic Egress** checkbox when you select a VLAN.

When Dynamic Egress is enabled for a VLAN, any time a device tags a packet with that VLAN ID, the ingress port is automatically added to the VLAN's egress list, enabling the reply packet to be forwarded back to the source. This means you do not need to add the ingress port to the VLAN's egress list manually. (See Example 1, below.)

Dynamic Egress affects only the egress lists for the source and destination ingress ports. However, GVRP (GARP VLAN Registration Protocol) automatically adds the interswitch ingress ports to the egress lists of VLANs. (See Example 2, below.) You can enable GVRP for the domain by selecting the **Global Domain Settings > GVRP > Enable** menu option.

NOTE: If you do not want GVRP enabled on your network, you can disable it by selecting the **Global Domain Settings > GVRP > Disable** menu option. If necessary, you can then manually configure the interswitch ports to do what GVRP does automatically, using local management to set up your interswitch links as Q trunks. The trunk ports will be automatically added to the egress lists of all the VLANs at the time of trunk configuration. For more information on using GVRP in the Policy view, see the section on Setting Domain GVRP Status below.

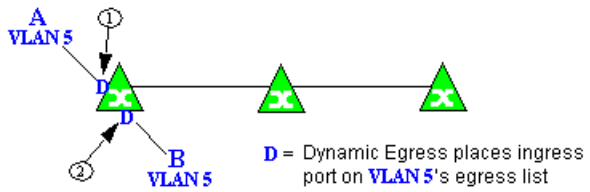
When you disable Dynamic Egress for a VLAN, the VLAN effectively becomes a discard VLAN. Since the destination port is not added to the egress list of the VLAN, the device discards the traffic. If you want a VLAN to act as a discard VLAN, disable Dynamic Egress for that VLAN. (See Example 3, below.)

If an endstation is talking to a "silent" endstation which does not send responses, like a printer, you need to add the silent endstation's ingress port to the VLAN's egress list manually using local management. Dynamic Egress and GVRP take care of adding the other ingress ports to the VLAN's egress list. (See Example 4, below.)

CAUTION: If no packets are tagged with the applicable VLAN on a port within five minutes, Dynamic Egress list entries time out. The result is that an endstation appears "silent" if the VLAN has not been used within that time period. For example, if there is a "telnet" rule and two users (A and B) are on ports whose role includes a service containing the "telnet" rule, if User B has not utilized the "telnet" rule within the five minute time frame, User A is not able to telnet to User B. For this reason, the best application of Dynamic Egress is for containing undirected traffic on "chatty" clients which utilize, for example, IPX, NetBIOS, AppleTalk, and/or broadcast/multicast protocols such as routing protocols.

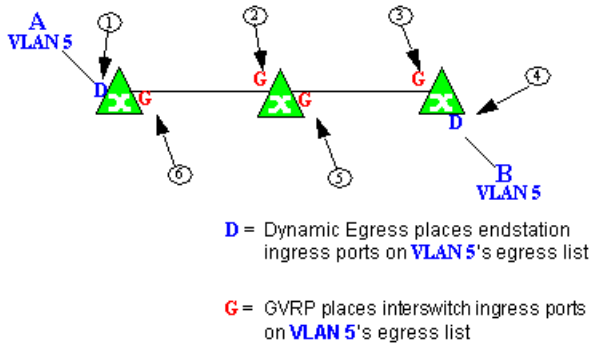
Example 1: Dynamic Egress Enabled

In this example, Dynamic Egress is enabled for VLAN 5. When source endstation A is tagged with VLAN 5, Dynamic Egress places A's ingress port (1) on VLAN 5's egress list. When destination endstation B's traffic is tagged with VLAN 5, Dynamic Egress places B's ingress port (2) on VLAN 5's egress list. The device can then forward traffic to both endstations.



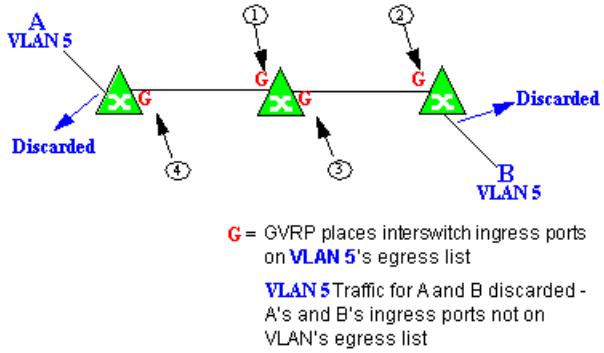
Example 2: Dynamic Egress + GVRP

In this example, Dynamic Egress is enabled for VLAN 5, and the destination endstation, B, is on a different device from the source endstation, A. When A is tagged with VLAN 5, Dynamic Egress places A's ingress port (1) on VLAN 5's egress list. GVRP then places interswitch ingress ports (2) and (3) on VLAN 5's egress list. When B's traffic is tagged with VLAN 5, Dynamic Egress places B's ingress port (4) on VLAN 5's egress list. GVRP then places interswitch ingress ports (5) and (6) on VLAN 5's egress list. The devices can then forward traffic to both endstations.



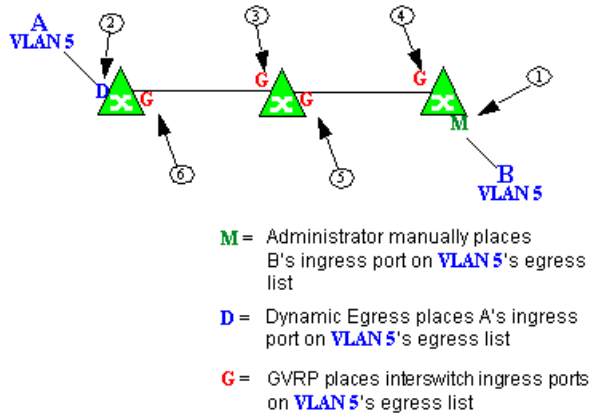
Example 3: Dynamic Egress Disabled

In this example, Dynamic Egress is disabled. When source endstation A is tagged with VLAN 5, A's ingress port is not placed on VLAN 5's egress list. GVRP places interswitch ingress ports (1) and (2) on VLAN 5's egress list. When B's traffic is tagged with VLAN 5, B's ingress port is not placed on VLAN5's egress list. GVRP places interswitch ingress ports (3) and (4) on VLAN 5's egress list. But VLAN 5 traffic for both A and B is discarded, because VLAN 5 is not aware of the ingress ports for A and B.



Example 4: Silent Endstation

In this example, Dynamic Egress is enabled for VLAN 5, but the destination endstation, B, is a "silent" endpoint, like a printer. Endstation B does not send responses, so the Administrator must place B's ingress port on VLAN 5's egress list manually (1). When A is tagged with VLAN 5, Dynamic Egress places A's ingress port (2) on VLAN 5's egress list. GVRP then places interswitch ingress ports (3) and (4), then (5) and (6) on VLAN 5's egress list. Endstation A is then able to communicate with the printer.



Setting Domain GVRP Status

The Policy view allows you to set the domain GVRP (GARP VLAN Registration Protocol) status via the Edit menu. There are three GVRP status options. To set the GVRP status for all the devices in the current domain, select a status and then enforce.

- Ignore — When this option is selected, Extreme Management Center ignores the GVRP configuration on a device during an Enforce operation. This allows you to configure some network switches with GVRP enabled and others with GVRP disabled, according to their configuration requirements.
- Enable — When this option is selected, GVRP is enabled for the devices in the current domain.
- Disable — Select this option if you do not want GVRP enabled on the devices in the current domain. Disabling GVRP may affect connectivity through ports with VLANs that rely on Dynamic Egress. If GVRP is disabled, rules using VLAN containment may not work properly unless the VLANs have been pre-configured on the devices outside of Extreme Management Center.

The following table shows how domain GVRP status affects device-level and port-level GVRP status when an Enforce operation is performed.

Domain GVRP Status	Device Set on Enforce
Domain GVRP status is set to Ignore.	No GVRP status is written to devices on Enforce.

Domain GVRP Status	Device Set on Enforce
Domain GVRP status is set to **Enable** and the device-level GVRP is enabled.	No GVRP status is written to the device on Enforce.
Domain GVRP status is set to **Enable** and the device-level GVRP is disabled.	Device-level GVRP status and port-level GVRP status is set to enabled on Enforce.
Domain GVRP status is set to **Disable** and the device-level GVRP is disabled.	No GVRP status is written to the device on Enforce.
Domain GVRP status is set to **Disable** and the device-level GVRP is enabled.	Device level GVRP status is set to disabled and no change is made to the port-level GVRP status on Enforce.

Policy VLAN Islands

The Policy view offers you the ability to set up Policy VLAN Islands which enable you to deploy a policy across your network, while restricting user access to only selected local devices. For example, if you want to have a guest VLAN but you do not want the guests in one facility to be able to communicate with guests in another facility, you can set up a VLAN island containing only selected devices in each facility, with access controlled by island VLANs.

- **Global VLAN** — Global VLANs are written to all selected devices with the same VID. They are referenced in the format <VID[name]>.
- **Island VLAN** — An Island VLAN is a conceptual VLAN and does not have an actual VID. The VID is assigned automatically based on the island it belongs to.

NOTE: The Policy view provides management of Global VLAN settings, but does not provide management of Island VLANs beyond setting the appropriate VIDs in the Role defaults and Rule access control actions. Also, you must manage separatly other related settings in the qBridgeMib such as name, and dynamic egress values.

See How to Create a Policy VLAN Island for more information.

Traffic Mirroring

The Policy view provides policy-based traffic mirroring functionality that allows network administrators to monitor traffic received at a particular port on the

network, by defining a class of traffic that will be duplicated (mirrored) to another port on that same device where the traffic can then be analyzed. Traffic mirroring can be configured for a rule (based on a traffic classification) or as a role default action. Only incoming traffic can be mirrored using policy-based traffic mirroring, and the traffic mirroring configuration takes precedence over regular port-based mirroring.

Traffic mirroring uses existing the Policy view port groups (created using the Port Groups tab) to specify the ports where the mirrored traffic will be sent for monitoring and analysis. When an end user connects to the device where the specified ports exist, and is assigned the role that has traffic mirroring configured, then there is a traffic mirror set up for the port the end user connected to. However, if the end user is assigned a role that does not have traffic mirroring configured, or if the end user connects to a device that doesn't have any ports in the specified port groups, then no traffic mirror will exist.

Examples of how traffic mirroring might be used include:

- Mirroring the traffic from suspicious users based on their MAC or IP address.
- Monitoring VoIP calls by IP address or port range.
- Mirroring traffic to optimized IDS systems, for example one system for all HTTP traffic (to look for suspicious websites) or one system for all emails (to look for spam).
- Mirroring traffic to Application Analytics appliances for use in Extreme Management Center application identification reports and analysis.

For information on configuring traffic mirroring, see the Role tab and the Rule General tab.

Port Groups

Extreme Management Center allows ports to be combined into groups, similar to the way services can be combined into service groups. Port groups enable you to configure multiple ports on the same device or on different devices simultaneously, or to retrieve port information from them. You can view port groups on the left-panel **Port Groups** tab.

The Policy view provides you with several commonly used port groups for your convenience, called Pre-Defined Port Groups. You can also create your own port groups, called User-Defined Port Groups.

User-Defined Port Groups

The Policy view also enables you to create your own port groups and select individual ports to add to the group.

Network Resource Groups

Network Resource Groups provide a quick and easy way to define traffic classification rules for groups of network resources such as routers, VoIP (Voice over IP) gateways, and servers. The default Policy domain configuration contains examples of network resource groups that you might want to create, such as Internet Proxy Servers and SAP Servers. Use the Network Resource Configuration window to view and define your network resource groups. See How to Create a Network Resource for more information.

Once a network resource group has been defined, you can associate it with an Automated service (see How to Create a Service for more information). The Automated service automatically creates a rule with a specified action (class of service and/or access control), for each resource in the network resource group. Automated rule types include Layer 2 MAC Address rules, Layer 3 IP Address and IP Socket rules, and Layer 4 IP UDP Port and IP TCP Port rules.

Network Resource Topologies

Network Resource Topologies are used to divide the devices in a domain into groups called islands. Each network resource group specifies a topology and can then define a unique resource list for each island within that topology, allowing user access to resources on the network based on the physical location at which they authenticate.

For example, you could create a topology called "Campus Printers" that could be used to restrict printer access to only the printers in the building where the end user is physically located. This topology might define islands such as "Library," "Admissions Office," or "Science Building." Each island would include the network devices for that location. Then, in the Network Resource Group that specifies this topology, there would be resource lists that define the printers for each of those islands.

In addition to defining topologies based on physical location (such as geographic region, corporate offices, or campus buildings) a topology could also be used to define resources based on the departments within a company (such as Sales, IT, or Human Resources).

When you create a topology, it contains a Default Island that includes all the devices in your domain. You can then create additional islands and distribute your devices between the different islands according to your needs. Each device in a domain must belong to one island in each topology. You can set any island as the Default island for new devices that are added to the domain.

Verifying

The Verify feature lets you verify that the roles in your current domain have been enforced. Verify operations are performed only on the current domain. The Verify operation compares the roles currently in effect (enforced) on your domain devices with the roles defined in the current Policy Domain.

NOTE: If you perform a Verify operation following an Import Policy Configuration from Device, the Verify may fail. This is because the import operation imports only roles and rules from the device, not the complete policy configuration. Also, when you import device-specific rules, these rules are converted to a Rule Type of "All Devices," and this will cause Verify to fail. If you want the rules to be device-specific, you will have to change their Rule Type via the Rule General tab after the import and prior to Enforce.

You can verify using the Open/Manage Domain > Verify Domain menu option, both of which verify the information on all the devices in the current domain. You can also selectively verify on individual devices or device groups in the domain by right-clicking the device or group in the left panel or in the right-panel Details View tab for the Devices folder or Device Group folder, and choosing **Verify** from the menu.

After verifying, you see a window that reports any discrepancies. The title bar of the window lets you know if the verify was done on all devices in the domain, or a subset of devices. From this window, you can select **Enforce Domain** to open the Enforce Preview window, where you can view the effects enforcing the current role set would have, prior to actually enforcing. You can also view the full results of the Verify operation in the event log, which displays any discrepancies and statistics of the operation itself.

Enforcing

In the **Policy** tab, enforcing means writing role information to a device or devices. Enforce operations are performed only on the current domain. Any time you add, make a change to, or delete a role or any part of it (any of its services and/or rules), the devices in your current domain need to be informed of the

change, otherwise the role will not take effect. To determine if the roles currently in effect on your domain devices match the set of roles you have defined in your current Policy Domain configuration, use the Verify feature.

NOTE: Setting up Profiles and Credentials for Enforce. All SNMP operations that are performed from the Policy view client use the SNMP credentials of the logged-in user. For example, when devices are identified, the credentials associated with the user's group are used to communicate with the devices. However, the Enforce operation occurs on the server and uses the Extreme Management Center Administrator profile to communicate with devices. Because of this, the Extreme Management Center Administrator profile must have write privileges on the devices that users can enforce.

When an Enforce is initiated, the Policy Domain is locked to prevent other clients from enforcing at the same time. Different Policy Domains can be enforced at the same time, but if another user attempts to enforce the same domain at the same time, that user will be notified that the domain is already locked.

To enforce, select the Open/Manage Domains > Enforce Domain menu option. You can also selectively enforce on individual devices by right-clicking the device in the Devices tab left panel or in the right-panel Devices tab and choosing Enforce from the menu. Only users that have been assigned the Enforce capability are allowed to perform an Enforce.

Controlling Client Interactions with Locks

Because the Policy view uses a Client/Server architecture, it is important to maintain a proper sequence of client interactions to ensure a consistent view of Policy Domains among all clients. To do this, the Policy view uses Server Locks to manage user interactions. When a user begins editing a Policy Domain (for example by assigning devices or adding a role), a lock is acquired for that domain at the server. That lock is not released until the same user saves the domain data. This guarantees a consistent view of that domain for all clients. Users are given the option of revoking locks held by other users. This protects against the possibility that users may forget they have locked a domain and keep that lock for an extended period of time.

A domain is locked automatically when a user begins to edit the domain data or a user can lock/unlock a domain by clicking the Lock toolbar button. When a domain is locked, the title bar states that the policy data is being edited and specifies the user who has locked the domain. Other Policy view clients are

notified that the domain is locked and they will not be able to save their own domain changes until the lock is released.

Here are some important things to remember about locks:

- Locks operate on individual Policy Domains. When a user edits a domain, a lock is acquired for that domain and it remains locked until the same user saves the domain data or the lock is revoked by another user. You cannot save a domain that is locked by another user.
- During Enforce, a lock is acquired on the domain which is being enforced. This ensures a consistent view of the domain while it is being used by the server.
- When devices are being assigned to a Policy Domain, multiple domains may be locked concurrently. This will happen if devices from one domain are being reassigned to another domain. In this case, locks for both domains are acquired.
- When a lock is revoked, the last domain save "wins." While consistency is always maintained by the server, the order of domain saves cannot be guaranteed when locks are revoked, and consequently work done by one user may be lost.

You can view server locks for all clients via the Options > Server Information tab.

Related Information

For information on related concepts:

- Traffic Classification Rules

For information on related tasks:

- Creating a Role
- How to Create a VLAN

For information on related windows:

- Create VLAN Window

Extreme Management Center Policy Tab Right-Panel

The Policy tab main window is divided into two panels: a left panel and a right panel. The Right-Panel Tabs Help section contains Help topics describing the tabs and their field definitions.

The right panel displays different tabs and information depending on the item selected in the left-panel tree. Help topics for right-panel tabs are named in a manner to reflect this. For example, the help topic named Details View Tab (Device Group), provides information on the right-panel Details View tab when a device group is selected in the left-panel tree.

Policy Left Panel

The left panel of the Policy tab contains tabs that display hierarchical trees representing the roles, services, classes of service, VLANs, network resources, devices, and port groups involved in managing policies for your network. What you select in the left panel determines what is displayed in the right panel. When you first open the Policy tab, the Roles tab is displayed in the left panel, by default.

Features of the left panel include:

- *Expanding and collapsing items in the hierarchy:* Double-click the item or its icon, or single-click the turner to the left of the icon.
- *Right-click menus:* Right-click a folder or other item in the left panel, and a menu of the options you can perform on your selection appears.

Information on the left-panel tabs:

- Roles/Services Tab
- Network Elements/Port Groups Tab
- Access Control Configuration
- Class of Service Configuration

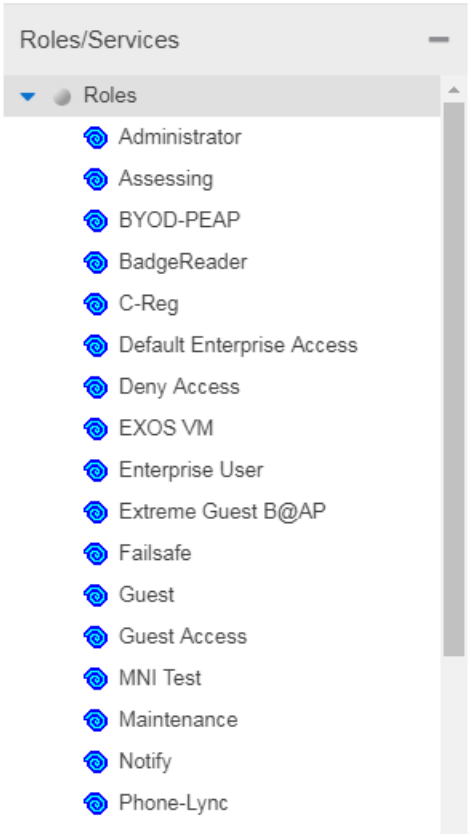
- Network Resources Configuration
- Devices/Port Groups

Roles/Services Tab

This tab displays the Roles and Service Repository trees.

Roles Tree

The Roles tree lists the roles defined for the current domain. A role is a set of network access services that can be applied at various access points in a policy-enabled network.



Roles Folder

This folder contains the roles defined for the current domain. See How to Create a Role for more information.

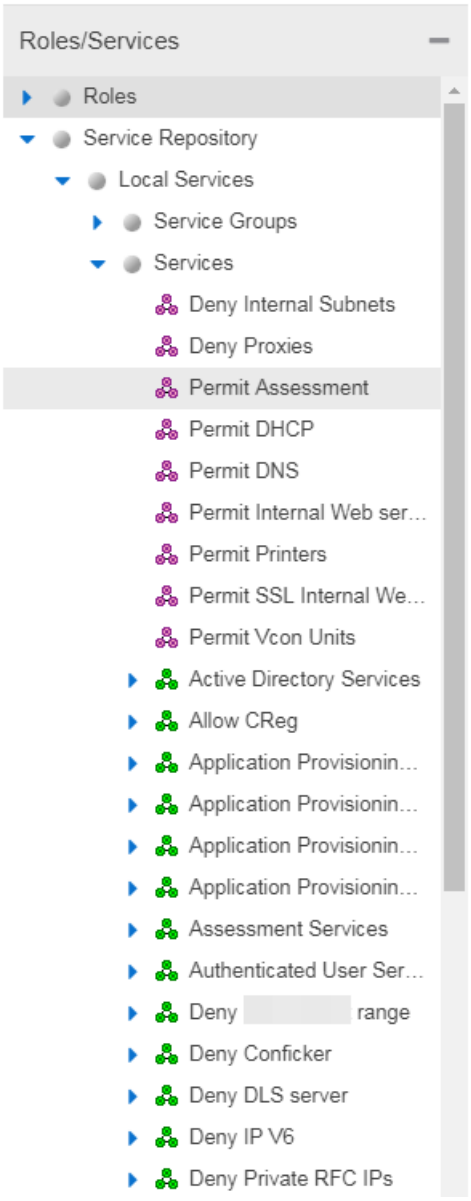
Role

Individual roles are listed by name. Select a role in the left panel, and view information about that role in the right-panel tabs. Only Quarantine roles are

displayed with a red icon .

Service Repository Tree

The Service Repository tree displays your Local and Global services and service groups. Services are sets of rules that define how network traffic for a particular network service or application is handled by a network access device. Local Services are services unique to the current domain. Global Services are services common to all domains. The tab also displays your network resource groups.



Local Services Folder

Local Services are services unique to the current domain. This folder contains the local service groups and services defined for the current domain. For more information, see How to Create a Service Group.

Global Services Folder

Global Services are services that are common across all domains. This folder contains the global service groups and services shared by all domains. For more information, see How to Create a Service Group.

Service Groups Folder

The Policy tab lets you create categories (service groups) into which you can group services. This folder contains the defined service groups. For more information, see How to Create a Service Group.

Service Group

Individual service groups are listed by name. Expand the service group to see the services and service groups included in that group.

Services Folder

This folder contains the automated and manual services that have been defined. For more information, see How to Create a Service.

Automated Service

Individual Automated services are listed under the Services Folder or within a service group in the Service Groups folder.

Manual Service

Individual Manual services are listed under the Services Folder. Expand the service to see the rules associated with it.

Rule

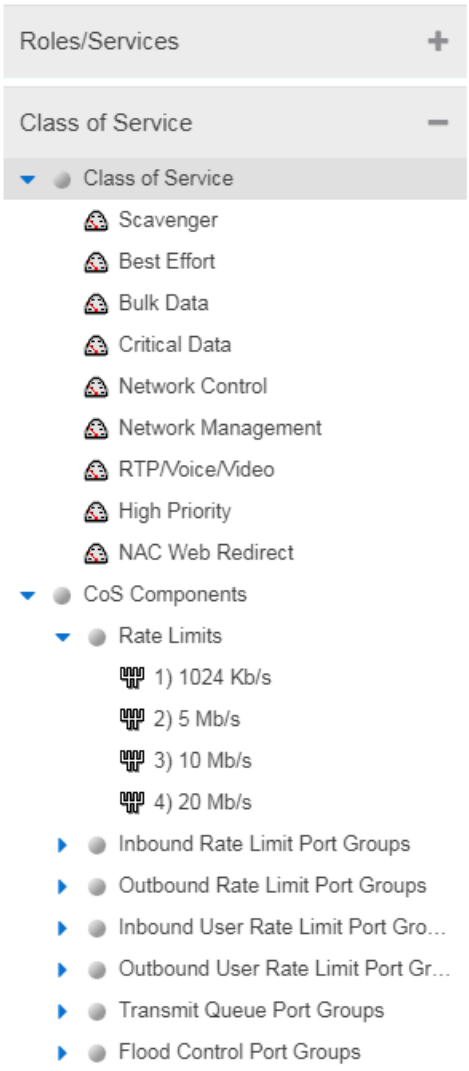
Individual rules are listed by name. If the rule is disabled, the rule icon displays a red X. If the rule is device-specific, the rule icon displays a small switch.

Class of Service Tab

The left panel Class of Service tab displays your Classes of Service defined for the current domain.

Classes of Service prioritize traffic with an 802.1p priority, and optionally an IP type of service (ToS/DSCP) value, rate limits, and transmit queue configuration.

You can then assign the class of service as a classification rule action, as part of the definition of an Automated service, or as a role default. For more information, see Getting Started with Class of Service.



Classes of Service Folder

When you first access the **Policy** tab, the left-panel Classes of Service tab is pre-populated with eight classes of service, each associated with one of the 802.1p priorities (0-7). These are static classes of service and cannot be deleted. You can use these classes of service as is, or configure them to include ToS/DSCP, rate limit, and/or transmit queue values. You can also rename them, if desired. In addition, you can also create your own classes of service. After you have created and defined your classes of service, they are then available when you make a class of service

selection for a rule action (Rule tab), a role default (General tab), or an automated service (General tab).

Class of Service

Select a Class of Service in the left panel, and view information about that service in the right-panel tabs. For more information, see How to Create a Class of Service.

CoS Components Folder

This folder contains subfolders of the possible components of a class of service (Rate Limits, Inbound Rate Limit Port Groups, Outbound Rate Limit Port Groups, and Transmit Queue Port Groups).

Rate Limits Folder

This folder contains the currently defined rate limits, listed in the order of precedence. For more information, see How to Define Rate Limits.

Inbound Rate Limit Port Groups

This folders contains the currently defined inbound rate limit port groups. Select a port group in the left panel and view information about that group in the right-panel tabs. For more information, see Creating Class of Service Port Groups.

Outbound Rate Limit Port Groups

These folders contain the currently defined outbound rate limit port groups. Select a port group in the left panel and view information about that group in the right-panel tabs. For more information, see Creating Class of Service Port Groups.

Transmit Queue Port Groups Folder

This folder contains the currently defined transmit queue port groups and the transmit queues defined for each group. For more information, see How to Configure Transmit Queues.

VLAN Tab

The left panel VLAN tab displays the Global VLANs for the current domain. If you have enabled Policy VLAN Islands, it also displays your Island VLANs and Policy VLAN Islands.

Global VLANs Folder

This folder contains your currently defined global VLANs for this domain.

VLAN

The VLAN icon indicates the access control for the VLAN-- if it is a Discard VLAN, the icon displays a red X. Otherwise, it is a Contain VLAN.

Island VLANs Folder

This folder appears only when the Policy VLAN Islands feature is enabled, and contains your currently defined Island VLANs for this domain.

Policy VLAN Islands Folder

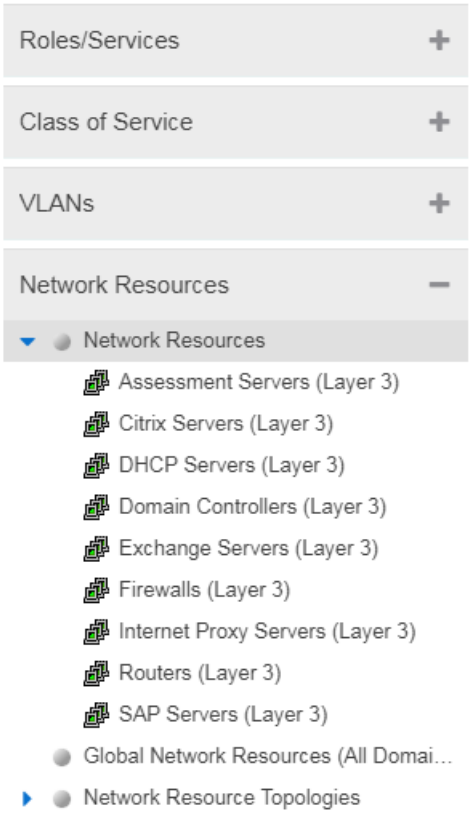
This folder appears only when the Policy VLAN Islands feature is enabled, and contains your currently defined VLAN islands and the devices that belong to them. When you enable Policy VLAN Islands, this folder is pre-populated with a Default Island containing all the devices in the domain.

VLAN Island

Click on a VLAN island to see the devices associated with it listed in the right-panel Details View tab. The Default Island is created by the Policy tab when you enable Policy VLAN Islands, and it cannot be deleted.

Network Resources Configuration

The Network Resources left-panel tab displays the network resources and network resource topologies for the current domain.



Network Resources Folder

This folder contains any network resource groups you have created. For more information, see How to Create a Network Resource.

Network Resource

Individual network resource groups are listed by name. Select a resource in the left panel, and view information about that resource in the right-panel tabs.

Global Network Resources Folder

Global Network Resources are network resources that are common across all domains. For more information, see How to Create a Network Resource.

Network Resource Topologies Folder

This folder contains the network resource topologies currently defined for this domain.

Network Resource Topology

A network resource topology can be used to divide the devices in a domain into groups called islands. You can then define a unique network resource list for each island within that topology, allowing user access to resources on the network based

on the physical location at which they authenticate. If you are not using custom topologies to group your devices, you will use the Domain Wide topology, which contains just one island for all your domain devices.

Topology Island

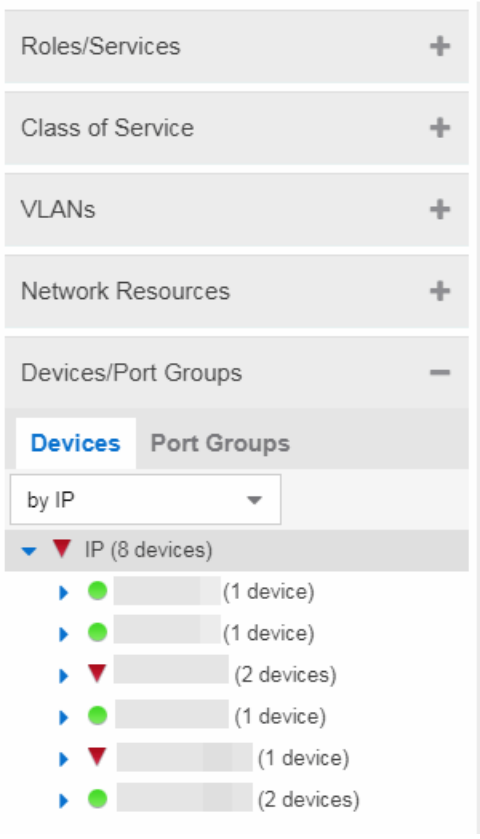
A topology island is a group of devices that have a unique network resource list, allowing you to set up network resource access based on the location where end users authenticate.

Devices/Port Groups Tab

This tab displays the Devices and Port Groups trees.

Devices Tree

The Devices tree displays the devices assigned to the current domain, organized into groups.



Devices

This tab contains all the devices assigned to the current domain. For information on adding devices to the domain, see How to Add and Delete Devices.

Port Groups

This tab contains the Pre-Defined and User-Defined Port Groups for the current domain. The Policy tab allows ports to be combined into groups, similar to the way devices are combined into device groups. Port groups enable you to configure multiple ports on the same device or on different devices simultaneously, or to retrieve port information from them. For more information, see How to Create a Port Group.

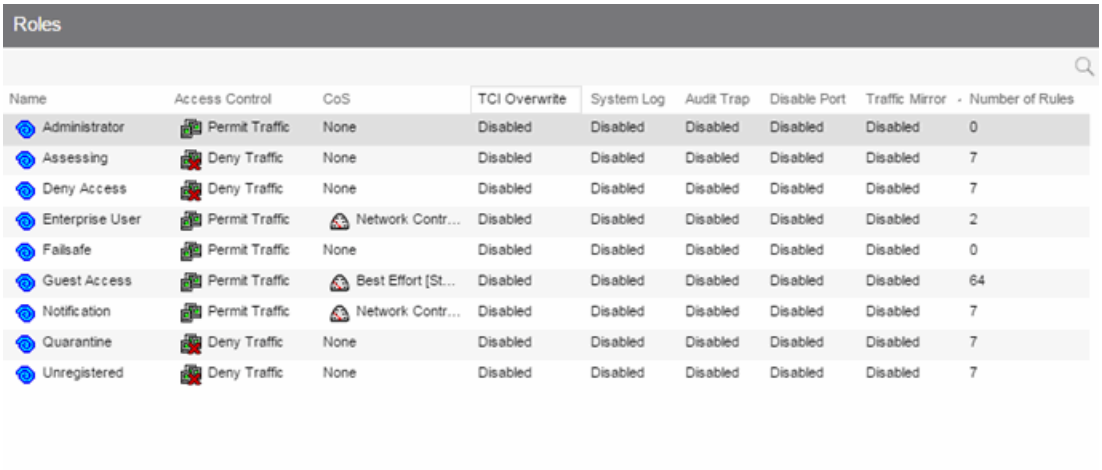
Related Information

For information on related windows:

- Main Window
- Right Panel

Extreme Management Center Summary (Roles)

This tab provides a summary view of the domain's roles. To access this tab, select the Roles left-panel tab in the Roles/Services tab. Right-click a role to add/remove services, rename the role, or delete the role.



Related Information

For information on related windows:

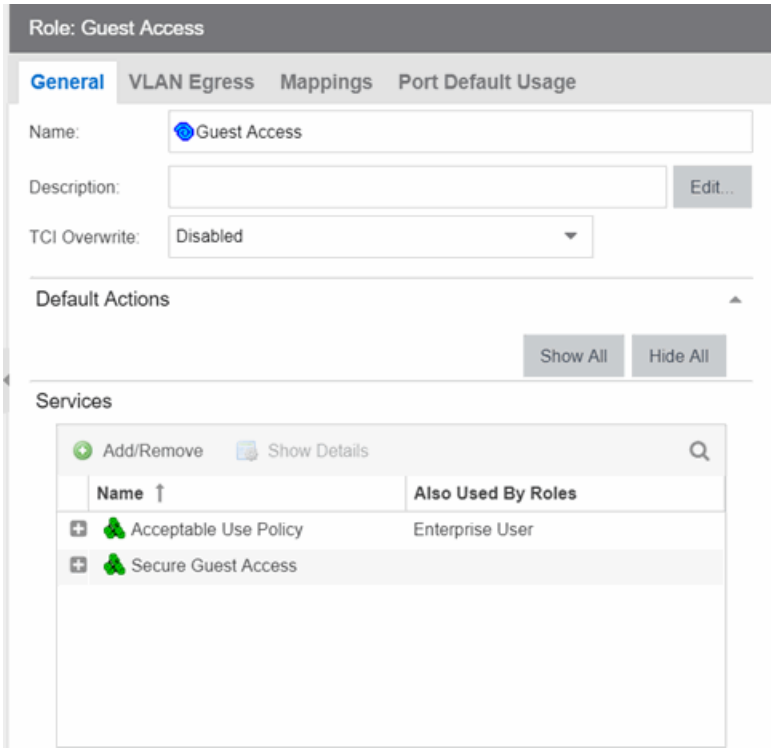
- General Tab (Roles)
- VLAN Egress Tab (Roles)
- Mappings Tab (Roles)

Extreme Management Center General (Role)

The role General tab lets you assign default actions for a role applied to traffic not identified specifically by the set of access services contained in the role. You can also use this tab to enable TCI Overwrite functionality for the role, and enter or edit the description of the role.

The Services section displays a list of the services and service groups associated with the selected role, and provides buttons for adding and removing services, creating a new service, viewing and editing a service or service group, and showing conflicting rules.

To access this tab, select a role in the left panel's Roles tab, then select the General tab in the right panel. Any additions or changes you make to this tab must be enforced in order to take effect.



Name

Name of the selected role.

Description

Use the Edit button to open a window where you can enter or modify a description of the role.

TCI Overwrite

Enable or disable TCI Overwrite functionality for the role. Enabling TCI Overwrite allows the VLAN (access control) and class of service characteristics defined in this role or any of its rules to overwrite the VLAN or class of service (CoS) tag in a received packet if that packet has already been tagged with VLAN or CoS information. If TCI Overwrite is not enabled, tagged packets will egress using the TCI data they already contain. You can also enable TCI Overwrite on a per-rule basis in the Rule Tab.

Default Actions

Default actions for a role are applied to traffic not identified specifically by the set of access services contained in the role.

Access Control

Use the drop-down menu to choose a default access control (VLAN) for the role. You can select:

- None - No default access control specified.
- Permit Traffic - Allows traffic to be forwarded with the port's assigned VID.
- Deny Traffic - Traffic will be automatically discarded.
- Contain To VLAN - This option contains traffic to the VLAN specified. Use the drop-down list to the right to select the desired VLAN. You can also select the NSI (Network Service Identifier) to extend the VLAN address space. The NSI is Extreme Management Center's implementation of a VXLAN, which increases the number of available VLANs.

Class of Service

Use the drop-down list to choose a default class of service (priority) for the role, create a new class of service, or select None if no class of service is desired. The drop-down list displays all of the classes of service for the current domain and also allows you to edit a class of service using the Edit button  .

System Log

When this option is enabled, a syslog message is generated as long as no matching rules specify that sending a syslog message is prohibited (that is, the rule's system log action is set to "Prohibited" on the Rule tab). When the option is disabled, the system log setting is ignored.

Audit Trap

When this option is enabled, an audit trap is generated as long no matching rules specify that sending an audit trap is prohibited (that is, the rule's audit trap action is set to "Prohibited" on the Rule tab). When the option is disabled, the audit trap setting is ignored.

Disable Port

When this option is enabled, the port is disabled as long no matching rules specify that disabling the port is prohibited (that is, the rule's disable port action is set to "Prohibited" on the Rule tab). Ports that have been disabled due to this option are displayed in the device Role/Rule tab. When the option is disabled, the disable port setting is ignored.

Traffic Mirror

Use the drop-down list to specify port groups where mirrored traffic is sent for monitoring and analysis. Select View/Modify Port Groups to open the Port Groups

tab where you can define user-defined port groups for selection.
To the right of the drop-down list is an option to mirror only the first (N) packets of a flow. This option is intended for use when mirroring traffic to an Application Analytics engine. The Application Analytics engine only needs the initial packets of a flow to properly identify the traffic, and setting this option will reduce network traffic overhead for the switch and engine. By default this number is set to 10, but can be changed by clicking on the Edit button  . Note that the value you set is used by all mirror actions in use in the current domain.

Services

Name

Lists the names of the services and service groups (local and global) associated with the selected role.

Also Used By Roles

List the other roles using this service. If the service is a global service, the domain name is also displayed if the role is in a different domain.

Add/Remove Services Button

Opens the role Add/Remove Services window, where you can add and remove services and service groups to and from any of the existing roles.

Show Details Button

Select a service or service group in the table and click this button to open the left-panel Services tab. The appropriate service or service group will be selected and you can access its right-panel tabs.

Show Conflicting Rules Button

If the rules in a Global service conflict with the rules in a Local service, the Name column will display a message indicating that the global rules will be overridden by the local rules. Click on the Show Conflicting Rules button to open a window that displays the rule conflicts and shows specifically which rules will be used and which will be overridden. For more information, see Conflict Checking.

Related Information

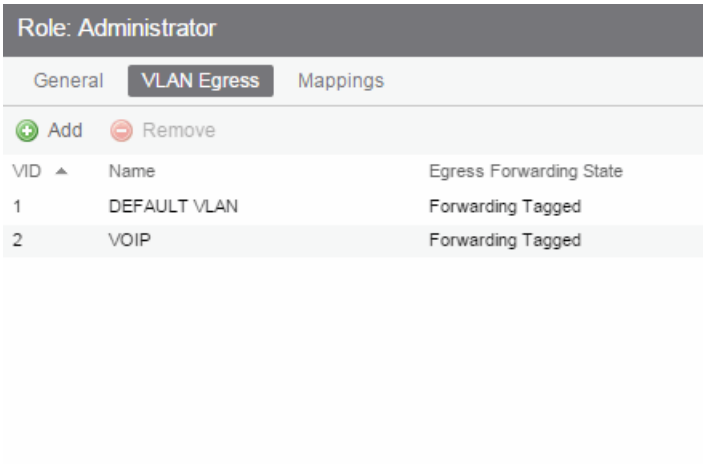
For information on related tasks:

- How to Create a Role
- How to Create a Class of Service

Extreme Management Center VLAN Egress (Role)

The role VLAN Egress tab displays the list of VLANs on the selected role's egress list, and allows you to add and remove VLANs and set their Egress Forwarding State. Ports that the selected role is active on forwards traffic belonging to the listed VLANs according to the specified forwarding state. Both the role's egress list and the VLAN egress list are checked for egress information. If the lists have duplications, the Forbid Forwarding state takes precedence.

To access this tab, select a role in the left panel's Roles/Services tab and click the VLAN Egress tab in the right panel. Any changes made on this tab need to be enforced.



VID

The VLAN ID.

Name

The VLAN Name.

Egress Forwarding State

Ports on which the selected role is active forward traffic belonging to this VLAN according to the egress forwarding state: Tagged (frames are forwarded as tagged), Untagged (frames are forwarded as untagged), or Forbid Forwarding (frames are not forwarded; they are discarded).

Add

Opens the Add Egress VLAN Window, where you can choose a VLAN for the role's egress list and specify the egress forwarding state.

Remove
Select a VLAN and click **Remove** to remove the VLAN from the list.

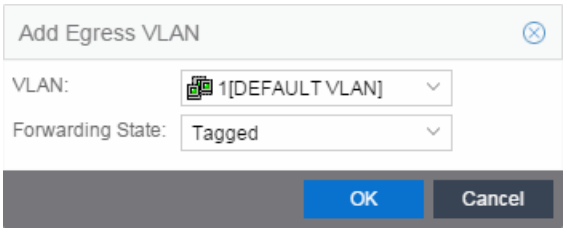
Related Information

For information on related windows:

- Add Egress VLAN Window

Add Egress VLAN Window

The Add Egress VLAN window appears when you click the **Add** button in the role's VLAN Egress tab. It allows you to add a VLAN to the Role's Egress list and specify the egress forwarding state.



VLAN
This is a drop-down menu of the available VLANs.

Forwarding State
Select the desired forwarding state: Tagged (frames are forwarded as tagged), Untagged (frames are forwarded as untagged), or Forbidden (frames are not forwarded; they are discarded).

Related Information

For information on related tasks:

- How to Create a VLAN

For information on related windows:

- Create VLAN Window
- VLAN Egress Tab (Role)

Extreme Management Center Mappings (Role)

This tab lets you view and configure four different mapping lists for the selected role:

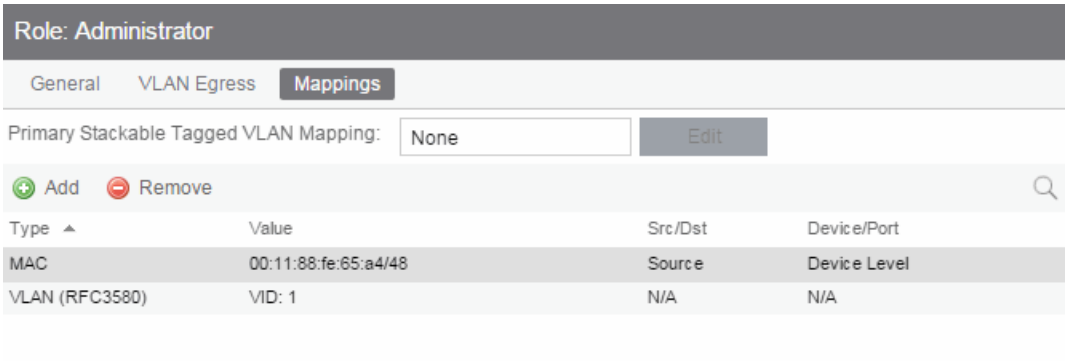
- MAC to Role Mapping — Lets you assign the role to an end user based on the user's MAC address.
- IP to Role Mapping — Lets you assign the role to an end user based on the user's IP address.
- Tagged Packet VLAN to Role Mapping — Lets you assign the role to network traffic based on the traffic's VLAN ID.
- Authentication-Based VLAN to Role Mapping — Lets you assign the role to an end user during the authentication process, based on a VLAN Attribute.

To access this tab, select a role in the left-panel **Roles** tab and click the **Mappings** tab in the right panel. Any additions or changes you make to this tab must be enforced in order to take effect.

NOTE: TCI Overwrite Requirement

-- Tagged Packet VLAN to Role Mapping applies the Role definition to incoming packets using a mapped VLAN. This definition applies a CoS and determine if the packet is discarded or permitted, and if TCI Overwrite is enabled re-specifies the VLAN ID defined by the Rule / Role Default. If TCI Overwrite is disabled, the packet egresses (if permitted by the Rule Hit) with the original VLAN ID with which it ingressed.

-- If supported by the device, you can enable TCI Overwrite for an individual role in the role's General tab. The stackable devices support rewriting the CoS values but not the VLAN ID.



Primary Stackable Tagged VLAN Mapping

Use this column to select the device-level VLAN to role mapping used for C2/C3/C5 and B2/B3/B5 devices (C2 firmware version 03.02.xx and higher/B2 firmware version 02.00.16 and higher), and D2, A4, and G3 devices (G3 firmware version 6.03.xx and higher). These devices only support one device-level VLAN to role mapping. If you do not make a selection, there will be no device-level mapping for these devices. Use the Mappings tab in the Enforce Preview window to quickly see which VLAN to role mapping is selected for these devices.

Type

This column indicates the type of mapping: MAC to Role, IP to Role, Tagged Packet VLAN to Role, and Authentication based VLAN to Role.

Value

The MAC addresses, IP addresses, or VLAN mapped to this role.

Src/Dst

Specifies whether the MAC address is a source or destination address.

Device/Port Level

This column indicates whether the mapping is a device-level mapping (all devices) or a port-level mapping (IP address and port description).

Add Button

Opens the Add Role Mapping window, where you can add a new Role mapping by entering the Mapping Type, Value, and Direction.

Remove Button

Remove the selected mapping from the list by clicking Remove.

MAC to Role Mapping

MAC to Role mapping provides a way to assign a role to an end station based on its MAC address. This allows you to create a specific role for a group of end stations (such as IP phones), and assign it to them based on their MAC address. When the end stations connect to the network, the policy-enabled device identifies the source MAC address and applies the mapped role.

IP to Role Mapping

IP to Role mapping provides a way to assign a role to an end station based on its IP address. For example, in networks that haven't deployed authentication, this

would allow you to map an individual IP address such as an administrator's laptop, to a specific role. When the end station connects to the network, the policy-enabled device identifies the IP address and applies the mapped role.

Tagged Packet VLAN to Role Mapping

Tagged Packet VLAN to Role mapping provides a way to let policy-enabled devices assign a role to network traffic, based on a VLAN ID. When a device receives network traffic that has been tagged with a VLAN ID (tagged packet) it uses the Tagged Packet VLAN to Role mapping list to determine what role to assign the traffic based on the VLAN ID. For more information, see VLAN to Role Mapping in the Concepts Help topic.

Authentication-Based VLAN to Role Mapping

Authentication-Based VLAN to Role mapping provides a way to assign a role to a user during the authentication process, based on a VLAN Attribute. An end user connects to a policy-enabled device that supports 802.1X authentication using a RADIUS Server. During the authentication process, the RADIUS server returns a VLAN ID in its RADIUS VLAN Tunnel Attribute. The device uses the Authentication-Based VLAN to Role mapping list to determine what role to assign to the end user, based on the VLAN Tunnel Attribute. Use this table to view and configure the VLANs that will map to the selected role. For more information, see VLAN to Role Mapping in the Concepts Help topic.

Related Information

For information on related concepts:

- VLAN to Role Mapping

Extreme Management Center Pre-configured Domains

To help you quickly achieve the best policy configuration for your network, the Policy tab provides pre-configured domains that include roles, services, and rules designed for specific network scenarios. You can use these pre-configured domains as templates, customizing them for your own network requirements.

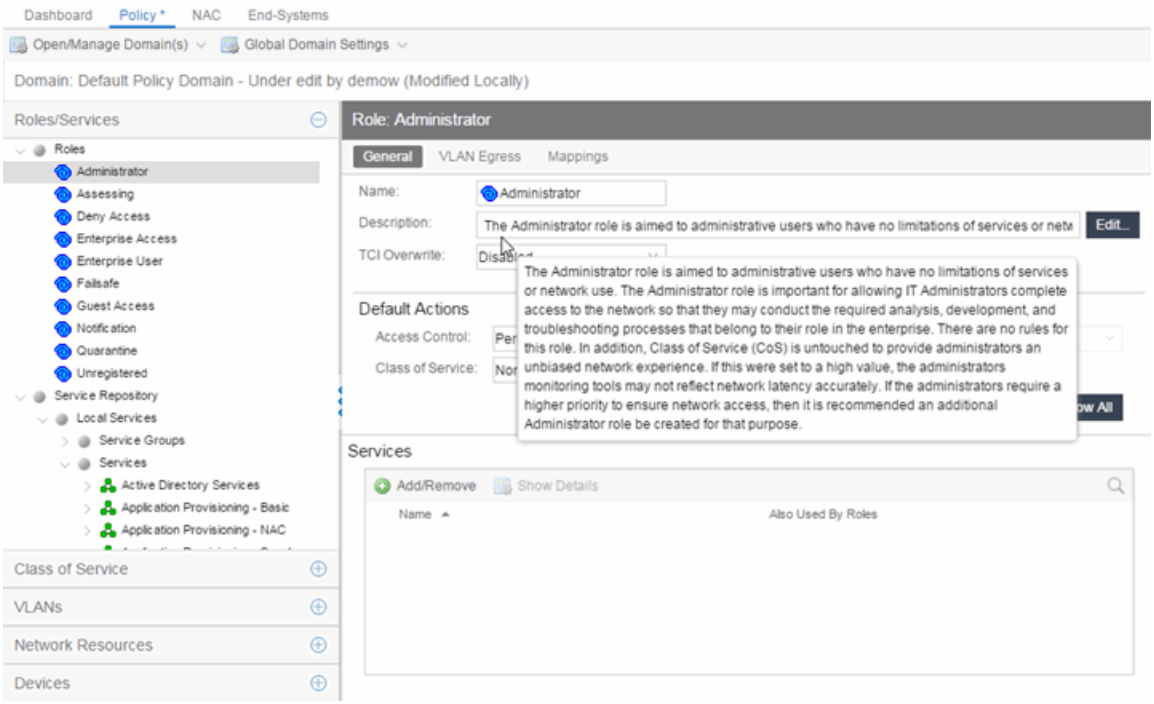
When you first access the **Policy** tab, it opens to the Default Domain. This domain can be deployed "as-is" for most networks, and provides a complete set of roles, services, and rules, as well as multiple switch platform support.

The **Policy** tab also provides additional pre-configured domains tailored to more specific network scenarios. These domains are named according to the policy configuration they provide, for example, HealthCare Services and Secure Guest. Below is a brief description of each domain along with some suggestions on how to use the domain in your network environment.

Access Pre-Configured Domains

Access the pre-configured domains from the **Open/Manage Domain** drop-down menu. At the top of the menu, the **Open Domain** menu displays all available domains from which you can select. To open a domain, select it in the menu. The domain opens in the **Policy** tab and you can look at the various roles, services, and rules that have been pre-configured in the domain.

As you look at a domain, use the extensive tool tips for the roles and services (as shown below) to view specific information on how to customize the domain to meet your requirements.



Pre-configured Domain Descriptions

The following sections describe the pre-configured domains available from the Domain menu.

Embedded NAC Domain

This domain can be used to configure the policy used by the Embedded Extreme Access Control engine. By default it will let traffic through unrestricted as you monitor your network.

Generic Services N-Series

This domain is designed to help networks that use Enterasys N-Series devices to increase security in their existing infrastructure. The roles defined in this domain leverage the capabilities supported on the N-Series. They are based on the best-practice of "least privilege" where all incoming traffic is denied access, and permit rules are used to allow only specific traffic onto the network. The rules also provide appropriate traffic classification.

Start with the roles, services, and rules defined in this domain for your N-Series devices and then expand and customize the domain to meet your own day-to-day business requirements.

Generic Services SecureStack

This domain is designed to help networks that use Enterasys SecureStack devices to increase security in their existing infrastructure. The roles defined in this domain leverage the capabilities supported on the SecureStack products, but will also work on N-Series devices. They are based on the best-practice of "least privilege" where all incoming traffic is denied access, and permit rules are used to allow only specific traffic onto the network. The rules also provide appropriate traffic classification.

Start with the roles, services, and rules defined in this domain for your Securestack devices and then expand and customize the domain to meet your own day-to-day business requirements.

HealthCare Services

The Healthcare Services domain provides a template of roles and services that can be utilized in healthcare industry networks. Roles correspond to the different business roles in health care settings, such as Physician, Nurse, Patient, IT, Hospital Administration, Management, and Guest. Services support a wide range of hospital departments, such as Cardiology, Emergency, Pediatrics, and Payroll/Benefits.

Quickstart

The Quickstart domain gets you up and running quickly with a set of roles, services, and rules that will increase security on your network. Most of the defined roles permit access to the network with certain rules designed to deny or prioritize applications, protocols, and communication traffic on the network. The services are bare minimum examples, and it is suggested that you modify or add roles, services, and rules to meet your day-to-day business requirements. HOW IS THIS DIFFERENT FROM THE DEFAULT DOMAIN?

Note: Before enforcing the policy configuration, set Class of Service mode for the device (select the device in the Policy Manager Network Elements tab, then click on the General tab) to "Role-Based Rate Limits / Transmit Queue Configuration". The default Class of Service mode can be specified in the Tools->Options view, and multiple devices can have their Class of Service mode changed using the Device Configuration Wizard in the Tools menu. THIS NOTE IS IN THE TAB DESCRIPTION, IS IT NEEDED?

Secure Guest

Secure Guest is a collection of sample services that you can use to increase security on edge ports where guest users connect.

There is one Secure Guest Access role that allows the end user basic guest services based on the principle of "least privilege" and will permit end users access to HTTP, HTTPS, and PPTP services. Apply this role to an Enterasys policy capable switch port.

The services are bare minimum examples, and it is suggested that you modify or add roles, services, and rules to meet your own business requirements.

ShoreTel

The ShoreTel domain provides a template for traffic prioritization of VoIP traffic on ShoreTel IP Phones that operate with the Media Gateway Control Protocol (MGCP) protocol. Class of Service is configured to provide higher priority to VoIP data, signaling and call control protocol, while lower priority is assigned to other required ShoreTel traffic such as DHCP and TFP.

The defined ShoreTel_IP_Phone role is based on the best practices methodology of "least privilege" where all incoming traffic is denied access, and permit rules are used to allow only specific traffic onto the network. Start by using the template for your N-Series devices, then add custom roles, services, and rules to meet your own network requirements.

VPN Termination Point

VPN Termination Point is a collection of Site-to-Site and Client-to-Site Roles that you can use to allow a VPN Concentrator to initiate, respond-to, and communicate to other VPN termination end points.

Related Information

Add/Remove Services (Roles)

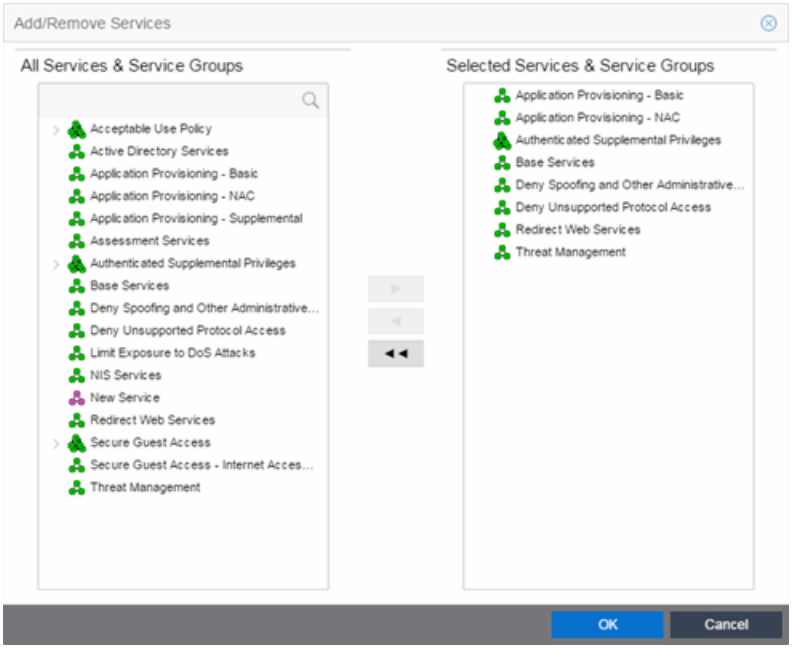
Add and remove services and service groups from roles using the Add/Remove Services window.

To access the Add/Remove Services window, you must have a role selected in the left-panel **Roles** tab. Click the **Add/Remove** button in the Services section of the Role window.

If you add a service to a role and any or all of the following conditions exist, you are in effect adding an "empty" service, and a warning message displays when you click **OK**:

- No traffic description exists for one or more of the classification rules.
- No access control or class of service has been defined for one or more of the classification rules.
- All of the classification rules are disabled.

When you add a service to a role which already has services associated with it, the **Policy** tab checks for rule conflicts. See Conflict Checking for more information.



All Services & Service Groups

This field displays all the services (local and global) and service groups in the current domain. Select the service groups or services you want to add to the role.

Selected Services & Service Groups

This field displays all the services currently defined for the selected role. Select the services you want to remove from the role.

Right Arrow

Click the **Right Arrow** to add the services or service groups selected in the All Services & Service Groups column to the Selected Services & Service Groups field.

Left Arrow

Click the **Left Arrow** to remove the services selected in the Selected Services & Service Groups field.

Double Left Arrow

Click the **Double Left Arrow** to remove all the services in the Selected Services & Service Groups field.

Related Information

For information on related tasks:

- Adding Services to a Role
- Removing Services from a Role

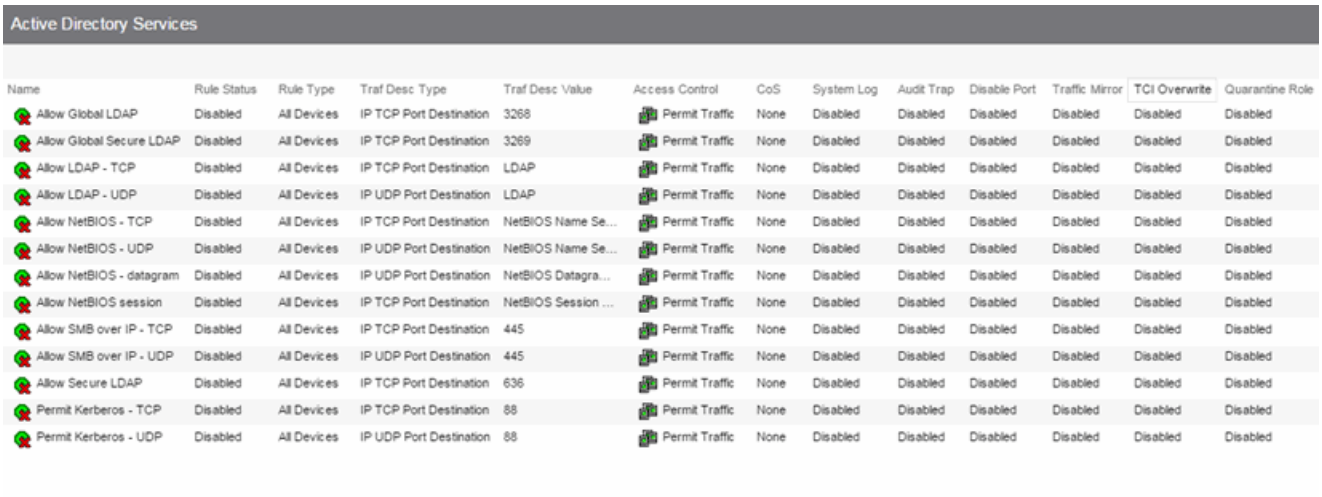
Extreme Management Center Details View (Service)

This tab displays information about the rules contained in a Manual service or an Automated service. To display this tab:

1. Select a service in the left-panel's **Roles/Services > Service Repository** tab.
2. Open either the **Local Services** tab or **Global Services** tab, depending on the type of service.
3. Select a service from within the **Services** left-panel tab.

The **Details View** tab opens in the right panel. Right-click a rule in the table to see a menu of available options.

For Manual services, you can double-click on any of the table columns opens the rule's General tab.



Name

Name of the rule. For rules contained in an Automated service, this column gives detailed information about the rule including the associated Network Resource (NR), if multiple resource groups are specified. You can rename a rule by right-clicking the rule and selecting Rename.

Rule Status

Indicates whether the rule is currently available for use by this service (Enabled), or not (Disabled), as set in the General tab for the rule. If the rule is disabled, the rule icon displays a red X  . You can enable or disable a rule by right-clicking and selecting Enable Rule or Disable Rule, respectively.

Rule Type

Indicates the device types to which the rule applies. (See Create Classification Rule Window for more information.)

Traf Desc Type

Traffic classification type for the rule. (See Classification Types and their Parameters for more information.)

Traf Desc Value

Values associated with the traffic classification type for the rule. (See Classification Types and their Parameters for more information.) Double-clicking on this column opens the Edit Rule window, where you can edit the parameters or values for the rule's classification type.

Access Control

VLAN action associated with the rule. Double-clicking on this column allows you change the setting. You can permit traffic to be forwarded, deny traffic altogether, or select a VLAN to contain traffic. Select None to disable access control for this rule.

CoS

Class of service action associated with the rule. Double-clicking on this column allows you change the setting.

System Log

Displays whether the syslog functionality (a syslog message is generated when the rule is used) is enabled, disabled, or prohibited for the rule. Double-clicking on this column allows you change the setting.

- Enabled - If this option is enabled, a syslog message is generated when the rule is used. This option must be enabled if you are configuring Policy Rule Hit Reporting on your devices.

- Disabled - If this option is disabled and this rule is hit, it does not generate a Syslog message, but lower-precedence rules and the role default actions may still specify a syslog message be sent for this data packet if there is a match.
- Prohibited - If this rule is hit, no syslog message is generated for this data packet, even when a lower-precedence rule or the role default actions has the System Log action set to enabled.

Audit Trap

Displays whether the audit trap functionality (an audit trap is generated when the rule is used) is enabled, disabled, or prohibited for the rule. Double-clicking on this column allows you change the setting.

- Enabled - If this option is enabled, an audit trap is generated when the rule is used.
- Disabled - If this option is disabled and this rule is hit, it does not generate an audit trap, but lower-precedence rules and the role default actions may still specify generating an audit trap for this data packet if there is a match.
- Prohibited - If this rule is hit, no audit trap is generated for this data packet, even when a lower-precedence rule or the role default actions has the Audit Trap action set to enabled.

Disable Port

Displays whether the disable port functionality (ports reported as using this rule will be disabled) is enabled, disabled, or prohibited for the rule. Double-clicking on this column allows you change the setting.

- Enabled - If this option is enabled, any port reported as using this rule are disabled.
- Disabled - If this option is disabled and this rule is hit, it does not disable the port, but lower-precedence rules and the role default actions may still specify disabling the port for this data packet if there is a match.
- Prohibited - If this rule is hit, the port is not disabled, even when a lower-precedence rule or the role default actions has the Disable Port action set to enabled.

Traffic Mirror

Displays whether the traffic mirror functionality is enabled, disabled, or prohibited for the rule. Double-clicking on this column allows you change the setting.

- Select port group(s) - Use the drop-down list to specify the port groups where

mirrored traffic will be sent for monitoring and analysis.

- Disabled - If this option is disabled and this rule is hit, traffic mirroring will not take place, but lower-precedence rules and the role default actions may still specify traffic mirroring for this data packet if there is a match.
- Prohibited - If this rule is hit, traffic mirroring is disabled, even when a lower-precedence rule or the role default actions has the Traffic Mirror action specified.

TCI Overwrite

Displays whether TCI Overwrite is enabled, disabled, or prohibited for the rule. Double-clicking on this column allows you change the setting.

- Enabled - Enabling TCI Overwrite allows the VLAN (access control) and class of service characteristics defined in this rule to overwrite the VLAN or class of service (CoS) tag in a received packet, if that packet has already been tagged with VLAN or CoS information.
- Disabled - If this option is disabled the TCI Overwrite option is ignored, but lower-precedence rules and the role default actions may still specify TCI Overwrite for the data packet if there is a match.
- Prohibited - Do not set TCI Overwrite for this data packet, even when a lower-precedence rule or the role default actions has the TCI Overwrite option set to enabled.

Quarantine Role

Displays whether a Quarantine role is enabled, disabled, or prohibited for the rule. Double-clicking on this column allows you change the setting.

- Select Role - Use the drop-down list to select the role that you want to assign as a Quarantine role.
- Disabled - If this option is disabled and this rule is hit, a Quarantine role will not be assigned, but lower-precedence rules may still specify a Quarantine role for this data packet if there is a match.
- Prohibited - If this rule is hit, a Quarantine role will not be assigned, even when a lower-precedence rule has a Quarantine role action specified.

Related Information

For information on related concepts:

- Traffic Classification Rules

For information on related windows:

- Rule Tab

Extreme Management Center Service Repository

Selecting Service Repository in the Roles/Services navigation panel in the left panel opens the Service Repository panel.

Double-click Local Services to display the service groups and services associated with the current domain or Global Services (All Domains) to display the service groups and services available to all domains.

Name
Displays the Local or Global service groups and services.

Related Information

For information on related tasks:

- How to Create a Service
- How to Create a Service Group

Extreme Management Center Local/Global Services

Selecting Local Services or Global Services (All Domains) in the Roles/Services > Service Repository navigation panel in the left panel opens the Local Services or Global Services (All Domains) panel, respectively.

Double-click Service Groups to display the services that are part of a service group or Services to view services not contained within a service group.

Name
Double-click one of the options to display the Service Groups or Services.

Related Information

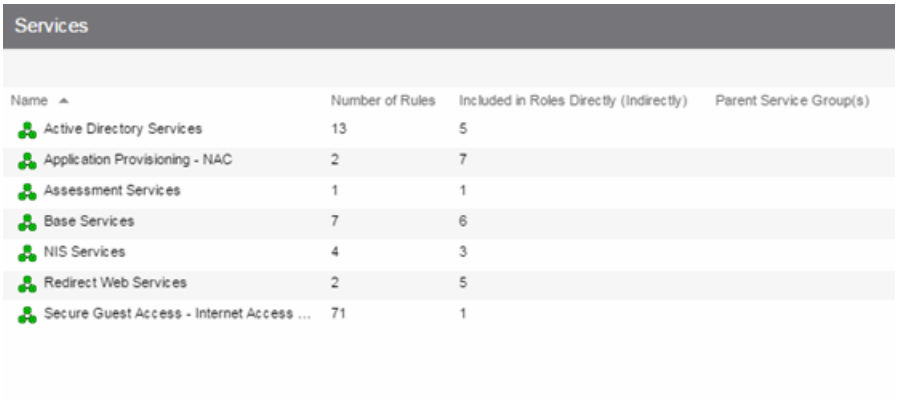
For information on related tasks:

- How to Create a Service
- How to Create a Service Group

Extreme Management Center Details View (Services)

This tab lists the Automated and Manual services you create in the **Policy** tab. To display the tab, expand the **Local Services** or **Global Services** left-panel tab in the **Roles/Services > Service Repository** tab, and select the **Services** tab. To see a menu of options available for a service, right-click the service.

For information on the differences between automated or manual services, and local or global services, see the Policy tab Concepts Help topic's section on Services.



Name
Name of the service.

Number of Rules
Number of rules associated with the service.

Included in Roles Directly (Indirectly)
Number of roles in which the service is included.

Parent Service Group
The service group in which the service is included.

Related Information

For information on related tasks:

- How to Create a Service

Extreme Management Center Details View (Service Group)

This tab lists information about the services or service groups contained in a Local or Global service group. To display this tab, select a service group in the left-panel Roles/Services > Service Repository tab.

Name

The name of the service or service group.

Number of Rules

The number of rules included in the service or service group.

Included in Roles Directly (Indirectly)

The number of roles where the service or service group exists directly in the role's Services list (as viewed on the role's General tab). If a service group also exists indirectly in other roles as part of another service group, that number of roles is displayed in parenthesis. In the example above, the service group called "Authenticated Supplemental Privileges" displays "1 (1)" in this column, showing that it is associated directly with one role (exists in that role's services list) and is also part of a service group associated with one other role.

Parent Service Group(s)

Displays all the "parent" service groups to which the service or service group belongs. This gives you an idea of the service group hierarchy without having to expand the left-panel tree.

Related Information

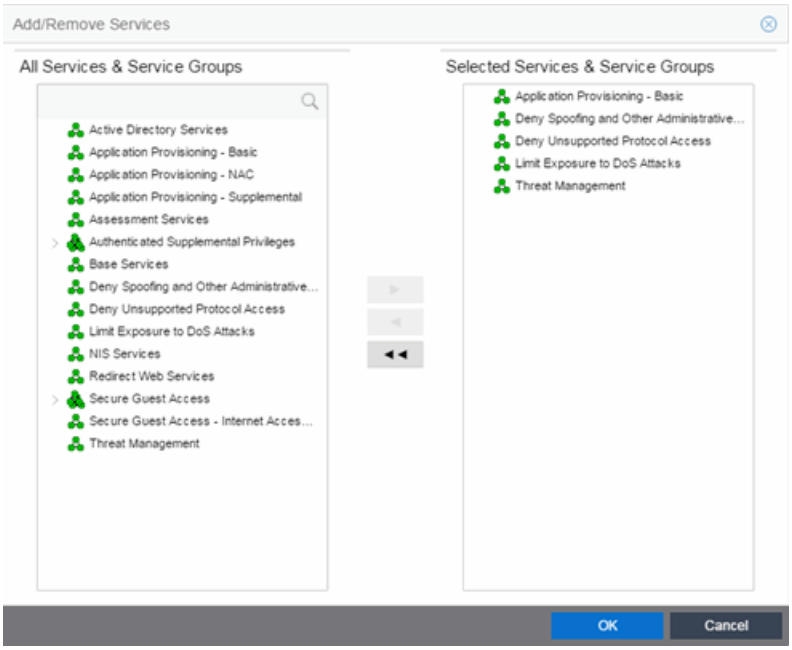
For information on related tasks:

- How to Create a Service

Add/Remove Services (Service Groups)

You can add and remove services from service groups using the Add/Remove Services window.

To access the Add/Remove Services window, either select the **Service Groups** tab in the **Local Services** or **Global Services** left-panel tab, right-click on a service group in the right panel and select **Add/Remove Services**. You can also right-click on a service group in the **Service Groups** left-panel tab and select **Add/Remove Services** from the menu.



All Services & Service Groups

This list displays all the local or global services and service groups in the current domain, depending whether you launched the window with a local or global service group selected. Select the services you want to add to the service group.

Selected Services & Service Groups

This list displays all the services currently defined for the selected service group. Select the services you want to remove from the service group.

Right Arrow Button

Click the **Right Arrow** button to add the services selected in the All Services & Service Groups list to the Selected Services & Service Groups list.

Left Arrow Button

Click the Left Arrow button to remove the services selected in the Selected Services & Service Groups list.

Double Left Arrow Button

Click the Double Left Arrow button to remove all the services from the Selected Services & Service Groups list.

Related Information

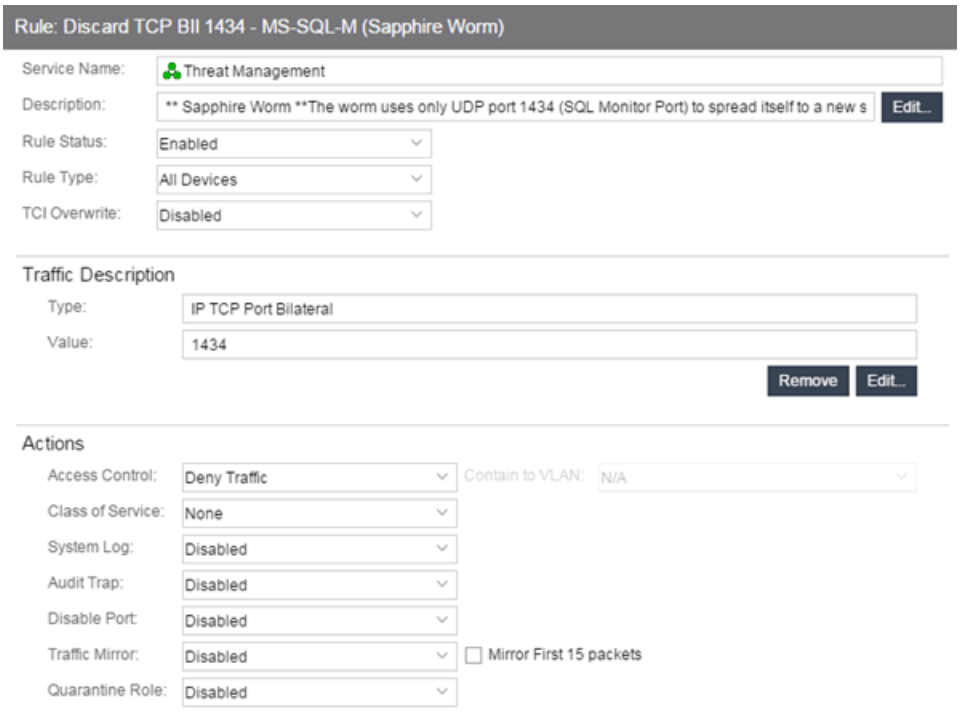
For information on related tasks:

- Adding Services to a Service Group
- Removing Services from a Service Group

Extreme Management Center Rule

The rule General tab displays general information about the rule selected for a Service in the left-panel Roles/Services > Service Repository > Local or Global Services tab and enables you to change it. In addition, you can view and change the Traffic Description and Actions associated with the rule. Traffic Description identifies the type of traffic to which the rule pertains. Actions apply class of service, access control, and/or accounting and security behavior to packets matching the rule.

Any additions or changes you make to this tab must be enforced in order to take effect. If you modify an enabled rule's actions, the Policy tab checks for conflicts with other rules in the services and roles with which the newly modified rule is associated. See Conflict Checking for more information.



General Area

Service Name

Displays the name of the rule.

Description

Use the Edit button to open a window where you can enter or modify a description of the rule.

Rule Status

Lets you disable the rule, or enable it if it's already disabled. If the rule is disabled, it is unavailable for use by the current service, but can still be copied to other services and enabled, or re-enabled at another time for the current service. Disabling a rule is an alternative to deleting and recreating it. The rule icon in the left panel displays a red X if the rule is disabled.

Rule Type

Use the drop-down list to select the types of devices to which you wish this rule to apply when enforced. The recommended selection is All Devices, unless there is a specific need for a device-specific rule. If this need arises, the Rule Type feature allows services to be customized to contain rules specific to a device's type when support for a traffic description and/or action may not be available on all managed

devices.

For device-specific rules, only those traffic descriptions supported on the device are available when you define the rule's traffic description on this tab. For All Devices rules, all traffic descriptions are available; however, you must be aware that you cannot enforce the rule to a device on which it is not supported.

TCI Overwrite

Specify the TCI Overwrite functionality for the rule:

- Enabled — Enabling TCI Overwrite allows the VLAN (access control) and class of service characteristics defined in this rule to overwrite the VLAN or class of service (CoS) tag in a received packet, if that packet has already been tagged with VLAN or CoS information.
- Disabled — If this option is disabled the TCI Overwrite option is ignored, but lower-precedence rules and the role default actions may still specify TCI Overwrite for the data packet if there is a match.
- Prohibited — Do not set TCI Overwrite for this data packet, even when a lower-precedence rule or the role default actions has the TCI Overwrite option set to enabled.

Traffic Description Area

The Traffic Description area allows you to view and change the traffic description associated with a rule. The Traffic Description identifies the traffic classification type for the rule. Rules allow you to assign access control (VLAN membership) and/or class of service to network traffic depending on the traffic's classification type.

Type

Displays the Classification Type selected for the rule.

Value

Displays the values/parameters selected for the rule's Classification Type. See Classification Types and their Parameters for parameter information.

Remove Button

Removes the traffic description from the rule.

Edit Button

If a Traffic Description Type has been defined for the rule, clicking Edit opens the Edit Rule window, where you can edit the parameters or values for the rule's classification type.

Actions Area

The Actions area allows you to view and change the actions associated with a rule. Actions apply access control, class of service, security, and/or accounting behavior to packets matching the rule.

Access Control

Use this drop-down list to select the appropriate access control for the rule. You can permit traffic to be forwarded, deny traffic altogether, or contain traffic to a VLAN. Select None to disable access control for this rule.

- Permit Traffic — allows traffic to be forwarded with the port's assigned VID.
- Deny Traffic — traffic will be automatically discarded.
- Contain to VLAN — contains traffic to a specific VLAN. Use the drop-down list to select the desired VLAN.

Class of Service

Use the drop-down list to select a class of service to associate with the rule. The Policy tab lets you define classes of service that each include an 802.1p priority, and optionally an IP type of service (ToS/DSCP) value, rate limits, and transmit queue configuration. You can then assign a class of service as a classification rule action. See Getting Started with Class of Service and How to Create a Class of Service for more information. Select None to disable class of service for this rule.

When rule accounting is enabled on a device, each rule keeps a list of the ports on which it has been used. Use the following three options to specify certain rule usage actions to take place when a "rule hit" is reported.

System Log

Specify System Log functionality for the rule. Syslog receivers are configured in the legacy Console java application. Refer to the Help topic in the Console User Guide for more information.

- Enabled — If this option is enabled, a syslog message is generated when the rule is used. This option must be enabled if you are configuring Policy Rule Hit Reporting on your devices.

- Disabled — If this option is disabled and this rule is hit, it does not generate a Syslog message, but lower-precedence rules and the role default actions may still specify a syslog message be sent for this data packet if there is a match.
- Prohibited — If this rule is hit, no syslog message is generated for this data packet, even when a lower-precedence rule or the role default actions has the System Log action set to enabled.

Audit Trap

Specify Audit Trap functionality for the rule:

- Enabled — If this option is enabled, an audit trap is generated when the rule is used.
- Disabled — If this option is disabled and this rule is hit, it does not generate an audit trap, but lower-precedence rules and the role default actions may still specify generating an audit trap for this data packet if there is a match.
- Prohibited — If this rule is hit, no audit trap is generated for this data packet, even when a lower-precedence rule or the role default actions has the Audit Trap action set to enabled.

Disable Port

Specify Disable Port functionality for the rule:

- Enabled — If this option is enabled, any port reported as using this rule will be disabled. Ports that have been disabled due to this option are displayed in the device Role/Rule tab.
- Disabled — If this option is disabled and this rule is hit, it does not disable the port, but lower-precedence rules and the role default actions may still specify disabling the port for this data packet if there is a match.
- Prohibited — If this rule is hit, the port is not disabled, even when a lower-precedence rule or the role default actions has the Disable Port action set to enabled.

Traffic Mirror

Specify traffic mirroring functionality for the rule:

- Select port group(s) — Use the drop-down list to specify the port groups where mirrored traffic will be sent for monitoring and analysis. Select View/Modify Port Groups to open the Port Groups tab where you can define user-defined port groups for selection.
  To the right of the drop-down list is an option to mirror only the first (N)

packets of a flow. This option is intended for use when mirroring traffic to an Application Analytics engine. The Application Analytics engine only needs the initial packets of a flow to properly identify the traffic, and setting this option will reduce network traffic overhead for the switch and engine. By default this number is set to 10, but can be changed by clicking on the Edit button  . Note that the value you set is used by all mirror actions in use in the current domain.

- Disabled — If this option is disabled and this rule is hit, traffic mirroring will not take place, but lower-precedence rules and the role default actions may still specify traffic mirroring for this data packet if there is a match.
- Prohibited — If this rule is hit, traffic mirroring is disabled, even when a lower-precedence rule or the role default actions has the Traffic Mirror action specified.

Quarantine Role

Specify the Quarantine Role functionality for the rule:

- Select Role — Use the drop-down list to select the role that you want to assign as a Quarantine role. Specifying a role as a Quarantine role turns the role's icon red, denoting its restrictive nature.
- Disabled — If this option is disabled and this rule is hit, a Quarantine role will not be assigned, but lower-precedence rules may still specify a Quarantine role for this data packet if there is a match.
- Prohibited — If this rule is hit, a Quarantine role will not be assigned, even when a lower-precedence rule has a Quarantine role action specified.

Related Information

For information on related concepts:

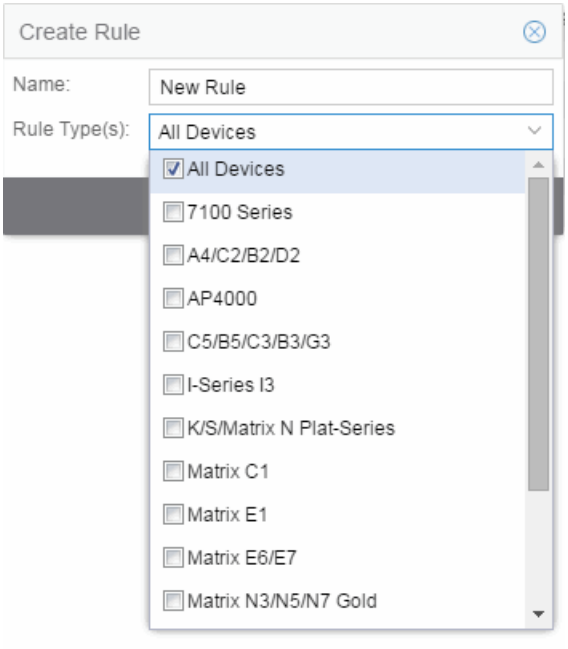
- Traffic Classification Rules

For information on related tasks:

- Using the Rule Tabs

Create Rule

This window appears when you right-click a service group or the **Services** tab in the left-panel and select **Create Rule**. If you use this window, traffic descriptions and actions can be added to the rule afterwards (see Using the Rule Tabs). In order for a rule to be applied to devices, you must enforce.



Name

Enter a name for the rule.

Type

Select the types of devices to which you wish this rule to apply when enforced. See Rule Type for more information on the consequences of your choice.

OK

Click **OK** to create the rule and close the **Create Rule** window.

Apply

Click **Apply** to create the rule and remain in the **Create Rule** window.

Cancel

Click **Cancel** to close the **Create Rule** window without saving your changes.

Related Information

For information on related concepts:

- Traffic Classification Rules

For information on related tasks:

- Using the Rule Tabs

For information on related windows:

- General Tab (Rule)

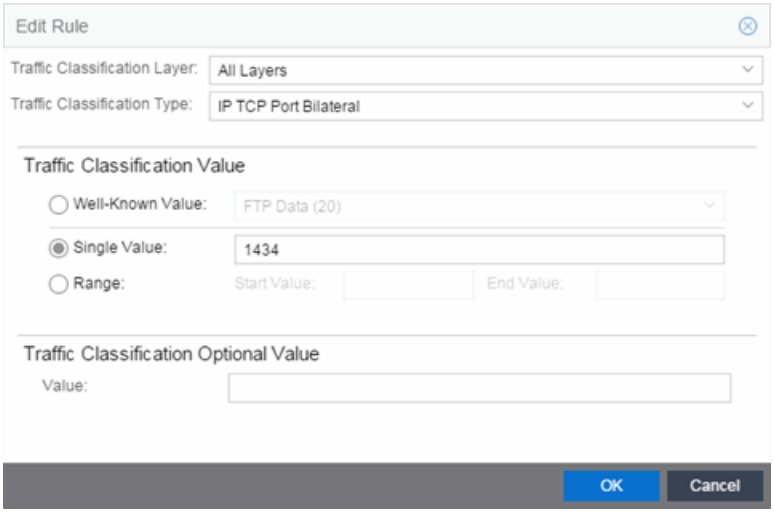
Edit Rule

The Edit Rule window allows you to change the traffic description associated with a rule. The Traffic Description, which includes the traffic classification layer, traffic classification type, and traffic value, was entered when the rule was created (see How to Create or Modify a Rule).

To display the Edit Rule window, select the rule in the left panel's **Services** tab. In the Traffic Description section, click **Edit** to bring up the Edit Rule window.

If you modify an enabled rule's traffic descriptions, the **Policy** tab checks for conflicts with other rules in the services and roles with which the newly modified rule is associated. See Conflict Checking for more information.

The contents of the Edit Rule window varies according to the selected rule and traffic description.



Layer Area

Traffic Classification Layer

The OSI model classification layer (or All Layers) currently associated with the rule. Each layer has multiple classification types from which you can select. If you change the layer, the Type and Value sections in the window change, and you must make new selections in those sections. See Classification Types and their Parameters for information.

Traffic Classification Type

The traffic classification type currently associated with the rule. Each classification type consists of certain parameters and/or values. If you change the type, the Value section of the window changes, and you must make new selections in that section. See Classification Types and their Parameters for information.

Value Area

This area displays the values currently selected for the traffic classification type, and allows you to change those values. Each traffic classification type requires certain parameters and/or values. See Classification Types and their Parameters for parameter information.

Related Information

For information on related concepts:

- Traffic Classification Rules

For information on related tasks:

- How to Create or Modify a Rule

For information on related windows:

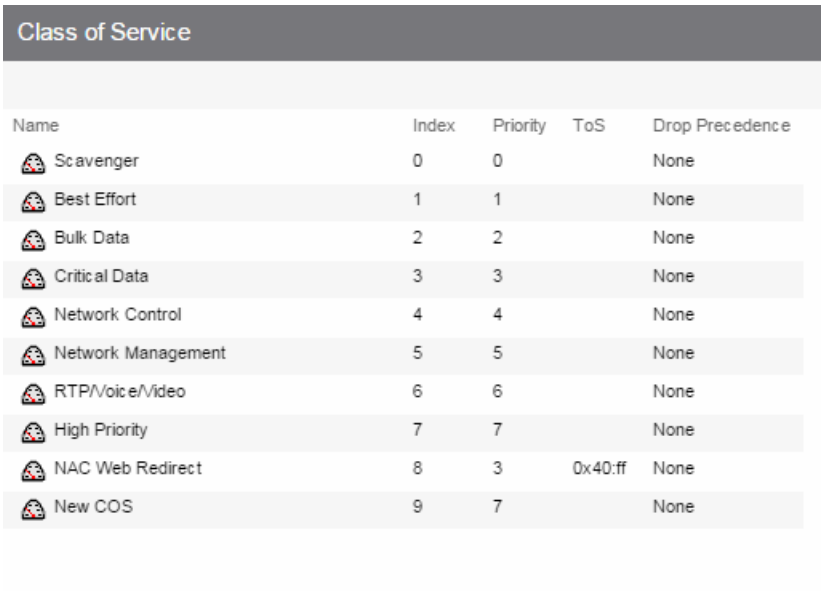
- General Tab (Rule)

Class of Service Overview

Use this tab to view the Class of Service (CoS) configuration for the current domain. To access this window, select the **Class of Service** left-panel tab from the **Policy** tab.

This window displays the eight pre-populated static classes of service, each associated with one of the 802.1p priorities (0-7). Use these predefined classes of service or create your own classes of service.

Expanding this tab in the left panel allows you to select individual classes of service in the right panel, which opens them in the Class of Service tab, where you can edit the configuration for the selected CoS.



Name

The name of the class of service.

Index

The index number automatically assigned to the class of service.

Priority
: The 802.1p priority associated with the class of service. The priority for the eight static classes of service provided by the Policy tab (Priority 0-7), cannot be disabled or changed.

ToS
: The IP type of service value associated with this class of service, if any. See IP Type of Service for more information.

Drop Precedence
: The drop precedence associated with this class of service. Double-click in the column to select a Drop Precedence value: Low, Medium, or High.

Related Information

For information on related concepts:

- Getting Started with Class of Service

For information on related tasks:

- How to Create a Class of Service
- How to Define Rate Limits

For information on related windows:

- General Tab (Class of Service)

Getting Started with Class of Service

This Help topic provides an overview of **Policy** tab's class of service (CoS) functionality, including information about defining rate limits and configuring transmit queues.

After you have read this topic, look at an example of how a network administrator might use CoS to configure VoIP traffic with appropriate priority, ToS, queue treatment, and flood control by clicking on the link: Class of Service Example.

This guide includes the following information:

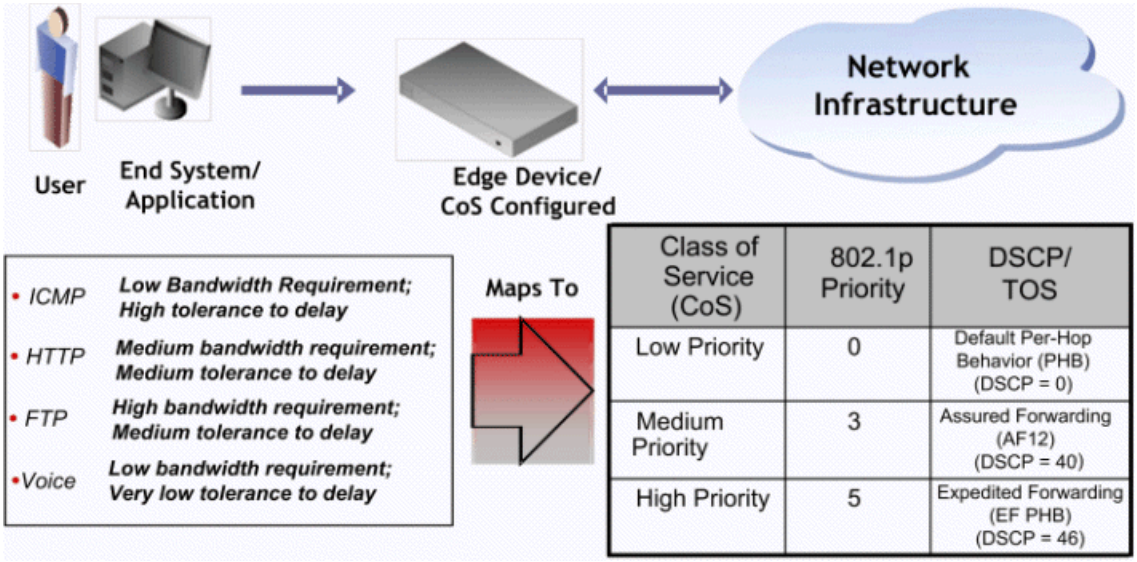
Class of Service Overview

Class of Service (CoS) provides the ability to give certain network traffic preferential treatment over other traffic. It classifies traffic into categories such as high, medium, and low, where high-priority traffic gets the best service while low-priority traffic is "drop eligible."

Class of Service helps you manage the bandwidth requirements of a given network flow with the available port resources on your network devices. (In a CoS context, a flow is a stream of packets classified with the same class of service as the packets transit the interface). Using CoS, you can:

- Assign different priority levels to different packet flows.
- Mark or re-mark the packet priority at port ingress with a Type of Service (ToS).
- Sort flows by transit queue. Higher priority queues get preferential access to bandwidth during packet forwarding.
- Limit the amount of bandwidth available to a given flow by either dropping (rate limiting) or buffering (rate shaping) packets in excess of configured limits.

The following figure shows how you can manage network bandwidth requirements by assigning different classes of service to different types of network traffic.



Class of Service (CoS)	802.1p Priority	DSCP/ TOS
Low Priority	0	Default Per-Hop Behavior (PHB) (DSCP = 0)
Medium Priority	3	Assured Forwarding (AF12) (DSCP = 40)
High Priority	5	Expedited Forwarding (EF PHB) (DSCP = 46)

The ICMP protocol, used for error messaging, has a low bandwidth requirement, with a high tolerance for delay and jitter, and is appropriate for a low priority setting. HTTP and FTP protocols, used respectively for browser-generated and file transfer traffic, have a medium to high bandwidth requirement, with a medium to high tolerance for delay and jitter, and are appropriate for a medium priority level. Voice (VoIP), used for voice calls, has a low bandwidth requirement, but is very sensitive to delay and jitter and is appropriate for a high priority level.

Implementing CoS

CoS determines how a given network flow is assigned bandwidth as it transits your network devices. As a preliminary step to using CoS, it is important that you understand the characteristics of the flows on your network and associate these flows with your policy roles. In this sense, CoS is the third step in a three step process:

1. Understand your network flows using NetFlow.
2. Associate your network flows with a Policy tab role.
3. Configure your classes of service and associate them with the rules contained in your roles.

Configuring CoS

The Policy tab lets you configure multiple classes of service that include one or more of the following components:

- 802.1p priority
- IP type of service (ToS) value
- drop precedence
- inbound and outbound rate limits
- outbound rate shaper per transmit queue.
- flood control rate limits

After you have created and defined your classes of service, they are then available when you make a class of service selection for a rule action (Rule tab), a role default (General tab), or an automated service (Automated Service tab).

To view and configure CoS, open the Class of Service Overview tab from the Policy tab. It is pre-populated with eight static classes of service, each associated with one of the 802.1p priorities (0-7). You can use these classes of service as is, or configure them to include ToS, drop precedence, rate limit, and/or transmit queue values. In addition, you can also create your own classes of service (user-defined CoS).

Rate Limits

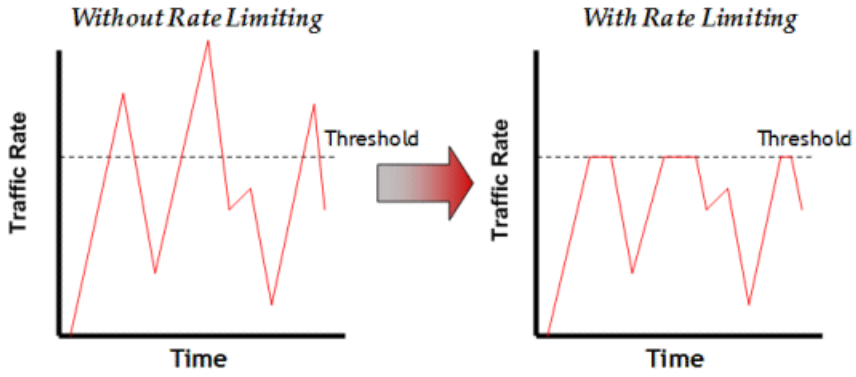
Rate limits are one component of a Policy tab class of service. They control the transmit rate at which traffic enters and exits ports in your network. All traffic mapped to a Class of Service on a given port share the bandwidth specified by the rate limit.

For instructions on how to configure rate limits, see How to Define Rate Limits.

Rate limits are tied directly to roles and rules, and are written to a device when the role/rule is enforced. When rate limits are implemented, all traffic on the port that matches the rule with the associated rate limit cannot exceed the configured limit. If the rate exceeds the configured limit, frames are dropped until the rate falls below the limit.

The rate limit remains on the port only as long as the role using the rate limit is active on the port either as the authenticated role or as the port's default role.

The following figure shows how bursty traffic is clipped above the assigned threshold when rate limiting is applied.



The CoS can be configured to perform one or all of the following actions when a rate limit is exceeded:

- Generate System Log on Rate Violation - a syslog message is generated when the rate limit is first exceeded.
- Generate Audit Trap on Rate Violation - an audit trap is generated when the rate limit is first exceeded.
- Disable Port on Rate Violation - the port is disabled when the rate limit is first exceeded.

The Policy tab class of service also provides the ability to create rate limit port groups. Port groups let you specify different rate limits within the same class of service. For example, you might create a port group for edge ports and a port group for core ports, and assign two different rate limits. For more information on rate limit port groups, see Creating Class of Service Port Groups.

Transmit Queues

Transmit queue configuration is defined within a class of service and associated with a specific role via a rule action or as a role default. It is implemented based on the role assigned to a port. All traffic received on a port and matching a rule with the associated class of service is forwarded using the defined transmit queue configuration.

For instructions on how to configure transmit queues, see How to Configure Transmit Queues.

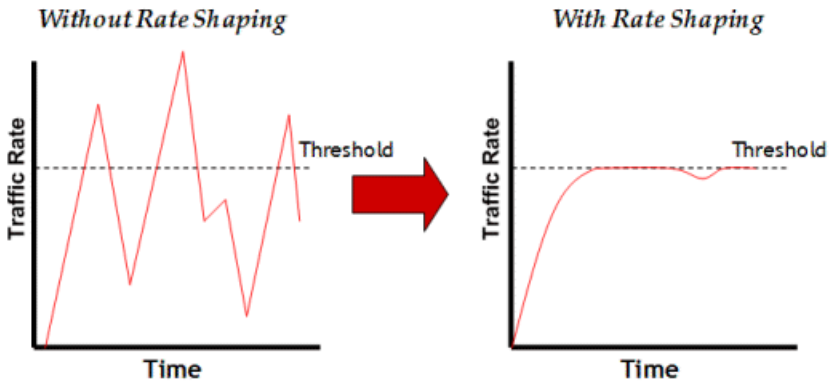
There are three components to transmit queue configuration:

- Transmit Queue Configuration allows you to set the transmit queue associated with the class of service.

- Transmit Queue Rate Shapers let you pace the rate at which traffic is transmitted out of that transmit queue.
- Bandwidth Configuration allows you to specify how the traffic in each transmit queue is serviced as it egresses the port.

The transmit queue configuration remains on the port only as long as the role using the configuration is active on the port either as the authenticated role or as the port's default role.

The following figure shows how bursty traffic is smoothed out when it goes above the assigned threshold when rate shaping is applied.



Rate shaping retains excess packets in a queue and then schedules these packets for later transmission over time. Therefore, the packet output rate is smoothed and bursts in transmission are not propagated as seen with rate limiting.

Rate shaping can be used for the following reasons:

- to control bandwidth
- to offer differing levels of service
- to avoid traffic congestion on other network links by removing the bursty property of traffic that can lead to discarded packets

The Policy tab class of service also provides the ability to create transmit queue shaper port groups that allow you to isolate certain kinds of sensitive network traffic so that you can vary the bandwidth of the shape for that single queue. For more information on transmit queue port groups, see Creating Class of Service Port Groups.

Flood Control

Flood control provides rate limiting capabilities to individual Class of Service to allow certain types of flooded traffic to be dropped. When enabled, incoming traffic is monitored over one second intervals. Traffic is identified using the following configuration types:

- unknown - unicast
- broadcast
- multicast

A traffic control rate sets the acceptable flow for each type, specified in packets per second. If, during a one second interval, the incoming traffic of a configured type reaches the traffic control rate on the port, the traffic is dropped until the interval ends. Packets are then allowed to flow again until the limit is reached.

By default, Flood Control is disabled for each CoS. Similar to CoS Port Groups, a different configuration can be assigned for each group. Since Flood Control is shared across all CoS, once Flood Control is enabled on at least one CoS, those rates apply to all ports that have Flood Control enabled.

For instructions on how to configure flood controls, see How to Configure Flood Control.

Related Information

For information on related tasks:

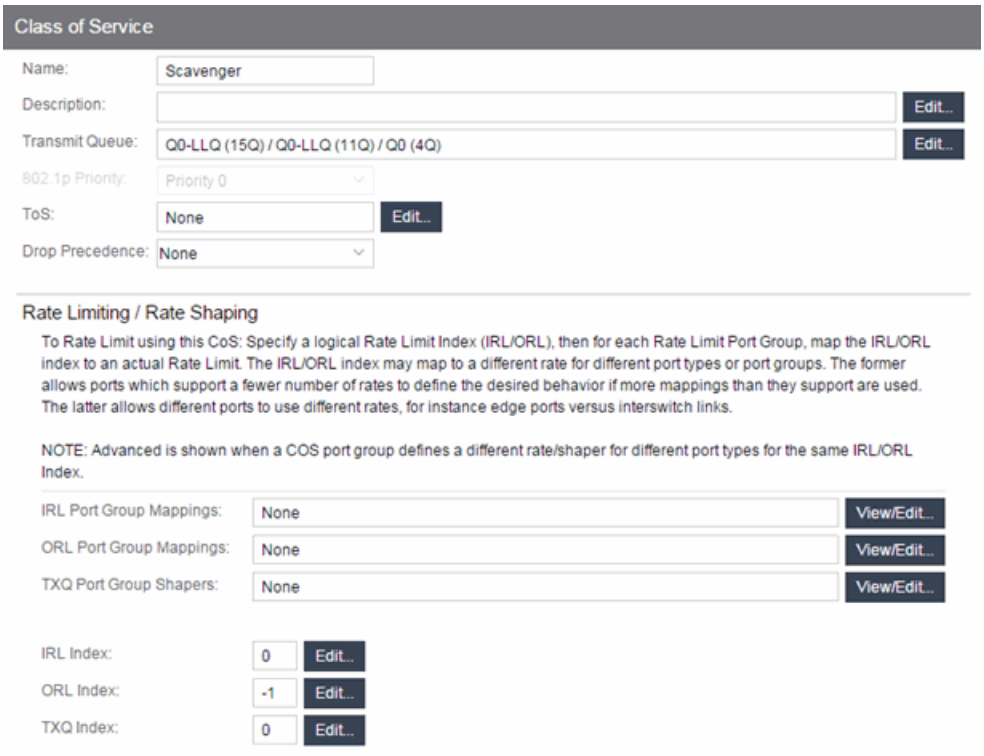
- How to Create a Class of Service
- How to Define Rate Limits
- How to Configure Transmit Queues

Extreme Management Center Class of Service

This tab lets you view and configure the components of a class of service (CoS). See below for a description of each section. For more information, see How to Create a Class of Service.

Once you have created and defined a class of service, you can then apply it as a classification rule action, as part of the definition of an automated service, or as a role default. For more information, see Getting Started with Class of Service.

To access this tab, select the **Class of Service** left-panel tab on the **Policy** tab. Select a class of service in the tree, and the information for the selected class of service displays in the right panel.



General

Name

Name of the selected class of service.

Description

Use the **Edit** button to open a window where you can add or modify a description for the class of service.

Transmit Queue

This field displays the transmit queue associated with the class of service for each port type. Use the **Edit** button to display a menu where you can select a new transmit queue, if desired.

802.1p Priority

This drop-down menu lets you select the 802.1p priority associated with the class of service, if desired. This field is grayed out for the eight static classes of service provided by the Policy tab (Priority 0-7), because the 802.1p priority cannot be disabled or changed.

ToS

Some IP rules allow a ToS value to be written to the ToS field in the IP header of incoming packets. Click the **Edit** button to open the Edit ToS window, where you can enter a ToS value. The value must be an 8-bit hexadecimal number between 0 and FF (see IP Type of Service for more information).

Drop Precedence

The Drop Precedence option is used in conjunction with the Flex-Edge feature available on K-Series and S-Series (Release 7.11 or higher) devices. Flex-Edge provides the unique capability to prioritize traffic in the MAC chip as it enters the switch. When the Class of Service is assigned to a policy role, and that role is applied to a port via a MAC source address mapping or the port default role, the drop precedence dictates the internal priority (within the MAC chip) used for packets received on the port. If congestion occurs, packets with a high drop precedence are discarded first. Therefore, if a packet is important, it should have a low drop precedence. Refer to the K-Series or S-Series Configuration Guide for more information on the Flex-Edge feature and drop precedence.

Rate Limiting/Rate Shaping

This section displays the inbound/outbound rate limits (IRL/ORL) and the outbound transmit queue (TxQ) rate shapers that are configured for the Default port groups associated with the class of service. If you have created additional port groups, the information displays for those groups as well.

With port rate limits, all traffic assigned to this class of service on a given port shares bandwidth specified by the rate limit. Rate shaping paces the rate at which traffic is transmitted out of the transmit queue. You can add or change a rate limit or a rate shaper by double-clicking on the area below a port group name.

If you have ExtremeWireless Controllers (Release 8.01.xx or higher) on your network, you also see the IRL and ORL user rate limits associated with the class of service. User rate limits specify the bandwidth given to each individual user on a port. Currently, user rate limits are only available on wireless controllers.

For more information, see Advanced Rate Limiting by Port Type and How to Configure Transmit Queues.

Index Numbers

At the bottom of the tab there is a section for configuring the rate limit and transmit queue index numbers associated with this class of service. These index numbers are used to map the class of service to the actual rate limits and transmit queue configuration on the device.

Typically, each class of service uses a different index number. The Policy tab automatically assigns these index numbers when you configure a class of services' rate limits and transmit queue shapers. An index number of "-1" indicates that no mappings are associated with the class of service.

All CoS using the same index will use the same rate limit and rate shaping assignments, and thus all traffic using those CoS will share the bandwidth.

IRL/ORL Index (Inbound/Outbound Rate Limits Index)

The inbound/outbound port rate limit index associated with the class of service. Index numbers map logical rate limit indexes to the actual physical rate limits you have created in the Policy tab. Click the button to open the Rate Limits selection view window, and select an index for the CoS. For convenience, existing index to rate limit mappings are displayed; if one of the existing indexes is selected, the displayed mappings will apply for this CoS. (Selecting an index highlights all the mappings configured for that index number within the selection view.)

TxQ Index (Transmit Queue Index)

The transmit queue index associated with the class of service. Index numbers map logical transmit queue indexes on the ports to the actual physical transmit queues you have configured in the Policy tab. If you have selected an 802.1p priority for this class of service, a default transmit queue index is automatically specified based on the selected priority. You can use the default index or change it according to your own transmit queue configuration. Click the button to open the Transmit Queues selection view window, which lists all the possible transmit queues, organized by index number for each existing port type and group. Selecting an index automatically includes all the transmit queues configured for that index number.

IUB/OUB Index (Inbound/Outbound User-Based Rates Index)

If you have ExtremeWireless Controllers (Release 8.01.xx or higher) on your network, you also see the inbound/outbound user rate limits associated with the class of service. User rate limits specify the bandwidth given to each individual user

on a port. Currently, user rate limits are only available for these wireless controllers. Click the button to open the Rate Limits selection view window, and select an index for the CoS. For convenience, existing index to rate limit mappings are displayed; if one of the existing indexes is selected, the displayed mappings apply for this CoS. (Selecting an index highlights all the mappings configured for that index number within the selection view.)

Flood Ctrl Port Groups

CoS-based flood control is a form of rate limiting that prevents configured ports from being disrupted by a traffic storm, by rate limiting specific types of packets through those ports. When flood control is enabled on a port, incoming traffic is monitored over one second intervals. During an interval, the incoming traffic rate for each configured traffic type (unknown-unicast, broadcast, or multicast) is compared with the configured traffic flood control rate, specified in packets per second. If, during a one second interval, the incoming traffic of a configured type reaches the traffic flood control rate configured on the port, CoS-based flood control drops the traffic until the interval ends. Packets are then allowed to flow again until the limit is again reached.

NOTE: By default, Flood Control is not managed by the Policy tab. To manage flood control configuration on devices in a domain, it can be enabled via the Domain Managed CoS Components drop-down menu by selecting All CoS Components or by selecting Flood Control.

Related Information

For information on related concepts:

- Getting Started with Class of Service

For information on related tasks:

- How to Create a Class of Service
- How to Define Rate Limits
- How to Configure Transmit Queues

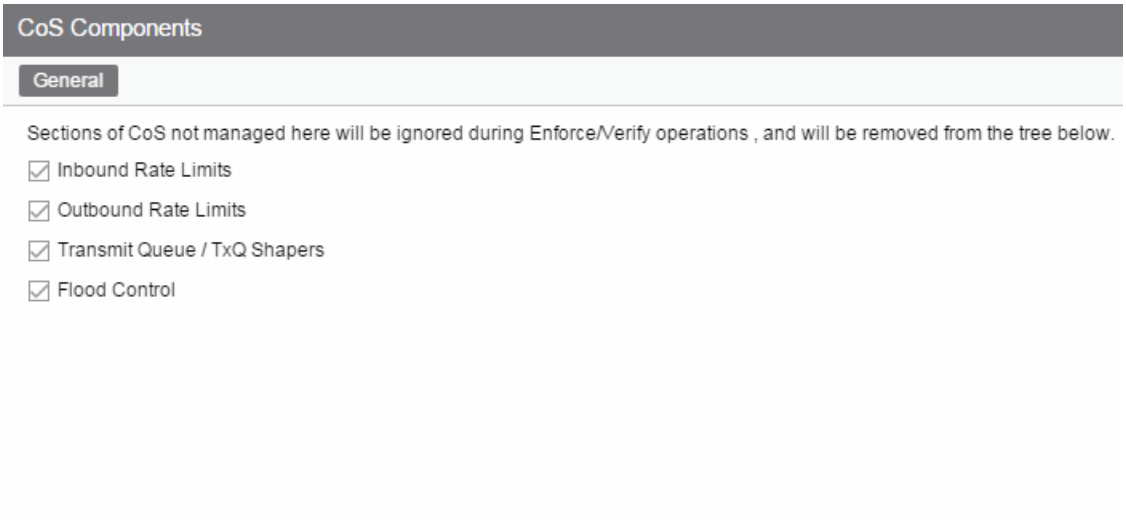
For information on related windows:

- General Tab (Rate Limit)

Extreme Management Center General (CoS Components Folder)

This tab lists the elements that comprise a class of service. It appears when you select the **CoS Components** tab in the **Class of Service** left-panel tab of the **Policy** tab.

See Getting Started with Class of Service for more information about these components.



Inbound Rate Limits

Select this checkbox to enable the Inbound Rate Limit Port Groups tab in the **CoS Components** left-panel tab.

Inbound Rate Limits

Select this checkbox to enable the Outbound Rate Limit Port Groups tab in the **CoS Components** left-panel tab.

Transmit Queue/TxQ Shapers

Select this checkbox to enable the Transmit Queue Port Groups tab in the **CoS Components** left-panel tab.

Flood Control Port Groups

Select this checkbox to enable the Flood Control Port Groups tab in the **CoS Components** left-panel tab.

Related Information

For information on related concepts:

- Getting Started with Class of Service

For information on related tasks:

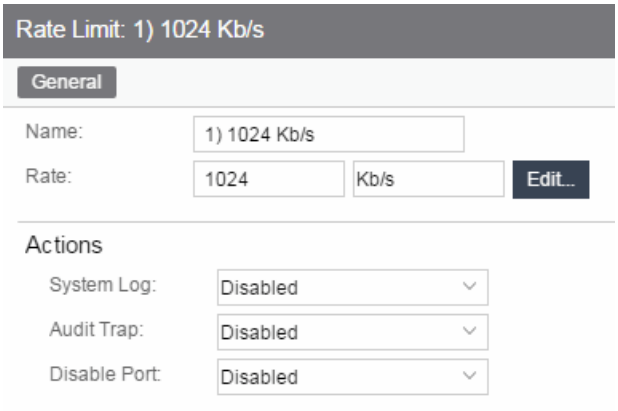
- How to Create a Class of Service
- How to Define Rate Limits
- How to Configure Transmit Queues
- How to Configure Flood Control

General (Rate Limits)

This tab allows you to create and define a rate limit. Rate limits are components of a class of service and are used to control the transmit rate at which traffic enters and exits ports in your network.

To access this window, open the **Control** tab, select the **Policy** tab > **Class of Service** left-panel tab > **CoS Components** left-panel tab > **Rate Limits** tab. Select an existing rate limit to view or modify a rate limit or right-click the **Rate Limits** left-panel tab and select the **Create Rate Limit** option to create a new rate limit.

To create the rate limit, fill out the window and click **OK** (to create a single rate limit) or **Apply** (to create more rate limits). After you create the rate limit, the General tab for the new rate limit appears, where you can configure additional rate limit parameters.



Name

Specify the name of the rate limit.

Rate Limit

Click the **Edit** button to specify the highest transmission rate at which traffic can enter or exit a port before packets are rate limited:

- % - A percentage of the total bandwidth available (not available for priority-based rate limits)
- PPS - Packets per second (not available for priority-based rate limits)
- Kb/s - Kilobits per second
- Mb/s - Megabits per second
- Gb/s - Gigabits per second

Actions

Select the action(s) you would like this rate limit to use:

- System Log - a syslog message is generated when the rate limit is first exceeded.
- Audit Trap - an audit trap is generated when the rate limit is first exceeded.
- Disable Port - the port is disabled when the rate limit is first exceeded.

NOTE: N-Series Gold devices do not support rate limit notification.

Related Information

For information on related concepts:

- Rate Limits

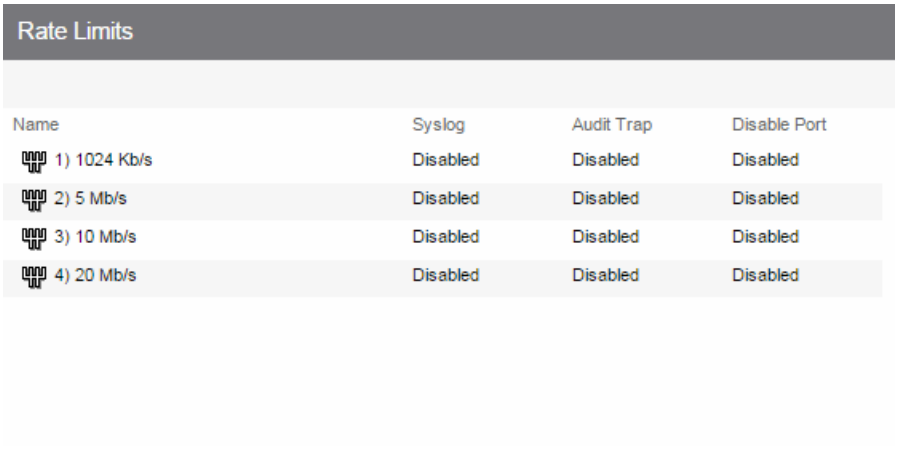
For information on related tasks:

- How to Define Rate Limits

Extreme Management Center Details View (Rate Limits Folder)

This tab lists information on any rate limits that have been defined in the Policy tab.

To access this tab, select the Class of Service > CoS Components > Rate Limits left-panel tab. See How to Define Rate Limits for more information.



Name
Name of the rate limit.

Syslog
Specifies whether a syslog message will be generated when the rate limit is first exceeded.

Audit Trap
Specifies whether an audit trap will be generated when the rate limit is first exceeded.

Disable Port
Specifies whether the port will be disabled when the rate limit is first exceeded.

Related Information

For information on related windows:

- General Tab (Rate Limits)

Extreme Management Center Priority-Based Rate Limits

Priority-based rate limits are used primarily by legacy devices. They are rate limits that are associated with one or more of the eight 802.1p priorities (0-7). When the associated priority is selected for a class of service, the rate limit becomes part of that class of service.

These rate limits are written directly to each port (unless the port is specified in the rate limit's exclusion list), and are implemented based on the 802.1p priority assigned to a data packet appearing on that port. While priority-based rate limits are not tied directly to roles or rules, they are displayed with the associated priority when you select a class of service while creating a rule, automated service, or role.

When priority-based rate limiting is implemented, the combined rate of all traffic on the port that matches the priorities associated with the rate limit cannot exceed the configured limit. If the rate exceeds the configured limit, frames are dropped until the rate falls below the limit.

Once a rate limit is associated with a priority, that priority includes rate limiting wherever and however it is used, until the rate limit is deleted from Extreme Management Center. Also, once a priority-based rate limit is applied to a port, it remains on the port even if the role that originally used the rate limit is no longer associated with the port. For example, if an untagged packet arrives on a port where there is no role or default priority, but the port's 802.1p priority includes a rate limit, that traffic is rate limited. As another example, if the priority of a tagged packet matches a priority-based rate limit on a port, the traffic is rate limited.

To configure a priority-based rate limit, you need to specify the following components:

- *Rate Limit* - The highest transmission rate at which traffic can enter or exit a port.
- *Direction* - The direction to which the limit applies (inbound or outbound traffic). In order to control traffic inbound and outbound on the same port, two rate limits must be configured (one inbound and one outbound). Inbound rate limiting takes place after a frame is classified into one of the eight priorities. Outbound rate limiting

takes place just before a frame is queued for transmission. A single frame may pass through inbound and outbound rate limits depending on the path it takes through the device and the rate limiting configuration on the device.

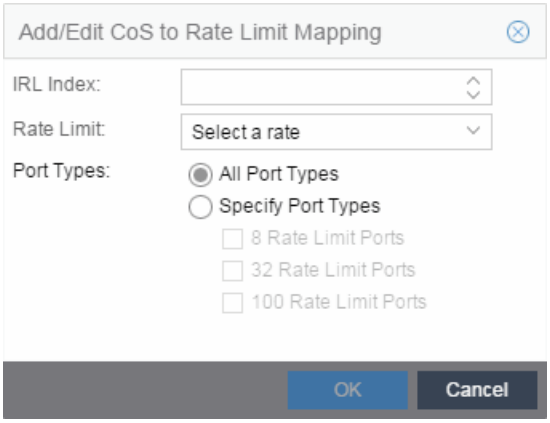
- *Priority* - The 802.1p priority or priorities with which the rate limit is associated.
- *Precedence* - The order in which the rate limit is written to supported devices. Extreme Management Center allows you to define as many rate limits as you wish; however, the number written to a device is restricted by the number of rate limits supported by the device. Each port on the device may utilize any or all of the defined rate limits up to the number of rate limits it supports.
- *Exclusion* - The devices/ports you wish to be excluded from the rate limit. For example, rate limiting is most often used for edge devices; therefore, you might want to exclude a device group or port group containing non-edge devices or ports.

Add/Edit CoS to Rate Limit Mapping

This window lets you configure the rate limit mappings for a rate limit port group. Rate limit mappings map a logical rate limit index to an actual physical rate limit you have created in Extreme Management Center.

For reference, the CoS IRL/ORL Index table (at the bottom of the window) displays classes of service that already have an IRL/ORL index specified, so that you can see which classes of service are affected by mapping an index to a rate limit.

To access this window, open the click on the **Add/Edit** button on the CoS - Rate Limit Mappings tab (**Control** tab > **Policy** tab > **Class of Service** left-panel tab > **CoS Components** left-panel tab and select a port group in either the **Inbound Rate Limit Port Groups** or **Outbound Rate Limit Port Groups** left-panel tab, depending on the type of rate limit.



IRL/ORL Index

Specify the IRL (Inbound Rate Limit) or ORL (Outbound Rate Limit) Index you are mapping.

Rate Limit

Use the drop-down menu to select a rate limit to map to the index. Rate limits are listed by the rate limit name followed by the precedence. For information on how to create a rate limit, see How to Define Rate Limits. Select None to remove an existing mapping for the specified port types.

Port Types

These options allow you to create a mapping for all port types at once, or create a mapping just for specific port types.

Related Information

For information on related concepts:

- Getting Started with Class of Service

For information on related tasks:

- Defining Rate Limits
- Advanced Rate Limiting by Port Type

For information on related windows:

- Ports Tab (Rate Limit Port Group)

Advanced Rate Limiting by Port Type

The **Policy** tab class of service feature provides the ability to create rate limit port groups that let you group together ports with similar rate limiting requirements. For instructions on creating a port group, see Creating Class of Service Port Groups.

This Help topic provides information about an advanced port group feature that lets you specify different rate limits for the different port types contained in a port group: 8-rate limit, 32-rate limit, 64-rate limit, and 100-rate limit port types.

After you have created your port groups, you can use the CoS to rate limit mappings tab to configure rate limit index mappings for each group. These mappings map a logical rate limit index to an actual physical rate limit created in the Policy tab. For each class of service, you can select one mapping index that gives you the desired physical rate limit for each port group (see the Index Numbers section of the CoS General tab for more information on CoS Index Numbers).

The **Policy** tab supports a maximum of 100 logical rate limit indexes and each rate limit port group lets you map all 100 indexes. For 8-rate limit, 32-rate limit, and 64-rate limit ports, this means that the number of logical indexes might be greater than the actual number of rate limits the port supports. The port group can map 100 logical rate limit indexes, but they can only be mapped to a maximum of 8, 32, or 64 different physical rate limits on those ports.

For example, you want to have 25 rate limits for 25 different CoS. You need to define the behavior for the 8-rate port type, since once you get to the 9th rate, you would have no more resources available for the remaining rates (9-25). You would either need to share some of the same resources, or not rate limit with the remaining rates.

The maximum supported indexes for a device is based on the largest number of rates supported for that device. On devices supporting a maximum of 8 rate limits, indexes 0-7 are supported. On devices supporting a maximum of 32 rate limits, indexes 0-31 are supported. On devices supporting 64 rate limits, IRL indexes 0-63 are supported. If a rate limit port group maps indexes greater than the supported value, they are ignored during Enforce (indicated in the Class of Service > Rate Limit Mappings tables of Enforce Preview)

Instructions on:

- Configuring Rate Limit Mappings
- Associating Rate Limits with a Class of Service

Configuring Rate Limit Mappings

Use the following instructions configure rate limit mappings for a port group.

1. Open the **Class of Service > CoS Components** left-panel tab.
2. Select either the **Inbound Rate Limit Port Groups** or **Outbound Rate Limit Port Groups** left-panel tab.
3. Select the right-panel **CoS - Rate Limit Mappings** tab.
4. Click **Add/Edit** to open the Add/Edit CoS to Rate Limit Mappings window.
5. In the window, specify the IRL (Inbound Rate Limit) or ORL (Outbound Rate Limit) Index you are mapping.
6. Use the drop-down list to select a rate limit to map to the index.
7. The port type options allow you to create a mapping for all port types at once, or create a mapping just for specific port types.
8. Click the **OK** button to map all your indexes and close the window. The Mappings tab displays your index to rate limit mapping configuration.

Associating Rate Limits with a Class of Service

After you have configured the rate limit mappings for a port group, you can associate a rate limit mapping index with a class of service.

1. Open the **Class of Service** left-panel tab.
2. Select the CoS in the left-panel tree. (If you have not created the class of service, see How to Create a Class of Service.)
3. At the bottom of the **Class of Service** tab in the right panel, click the **Edit** button next to the IRL or ORL index that you want to configure. The Edit Index window opens.
4. This window lists all the currently mapped rate limits, organized by index number for each existing port type and group. Selecting one index number automatically includes all the rate limits configured for that index number. To configure new mappings for the CoS, you can first select an index that is not currently mapped, then create the mappings as described in Configuring Rate Limit Mappings above. Click **OK**.

5. Once you have selected the mapping index, the table below displays the actual rate limits used by each rate limit port group for that class of service.
6. Click Open/Manage Domains > Save Domain.

Related Information

For information on related concepts:

- Getting Started with Class of Service

For information on related tasks:

- How to Create a Class of Service
- How to Define Rate Limits

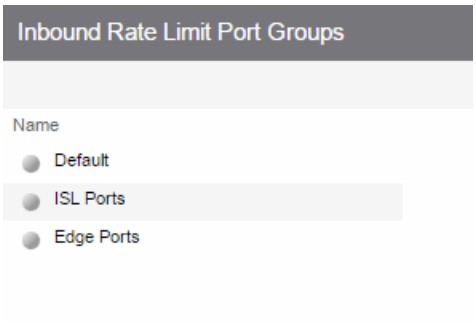
For information on related windows:

- Create Rate Limit Window
- General (Rate Limit)

Extreme Management Center Summary (Rate Limit Port Groups Folder)

This tab lists the name of all the inbound or outbound rate limit port groups (depending on the left-panel tab you select). Rate limit mappings map a logical rate limit index (IRL/ORL Index) to an actual physical rate limit. You can configure a port group's mappings on the port group Mappings tab.

To access this tab, open the Class of Service > CoS Components left-panel tab, then, select either the Inbound Rate Limit Port Groups left-panel tab or the Outbound Rate Limit Port Groups tab. The Summary tab displays in the right panel.



Name
The name of the port group

Related Information

For information on related concepts:

- Getting Started with Class of Service

For information on related tasks:

- Creating Class of Service Port Groups

Extreme Management Center CoS - Rate Limit Mappings (Rate Limit Port Group)

This tab lets you view and configure the rate limit mappings for a rate limit port group. Rate limit mappings map a logical rate limit index used by classes of service to an actual physical rate limit you create in Extreme Management Center.

Each port group has its own set of index mappings. Extreme Management Center automatically assigns these index numbers when you configure a class of services' rate limits and transmit queue shapers.

The rate limit mappings tab allows you to do two things:

- Map the index to a different rate for different port groups (edge ports versus inter-switch links). See Creating Class of Service Port Groups.

- Map the index to a different rate limit for each port type (8-rate limit, 32-rate limit, 64-rate limit, and 100-rate limit) in a port group. See Advanced Rate Limiting by Port Type.

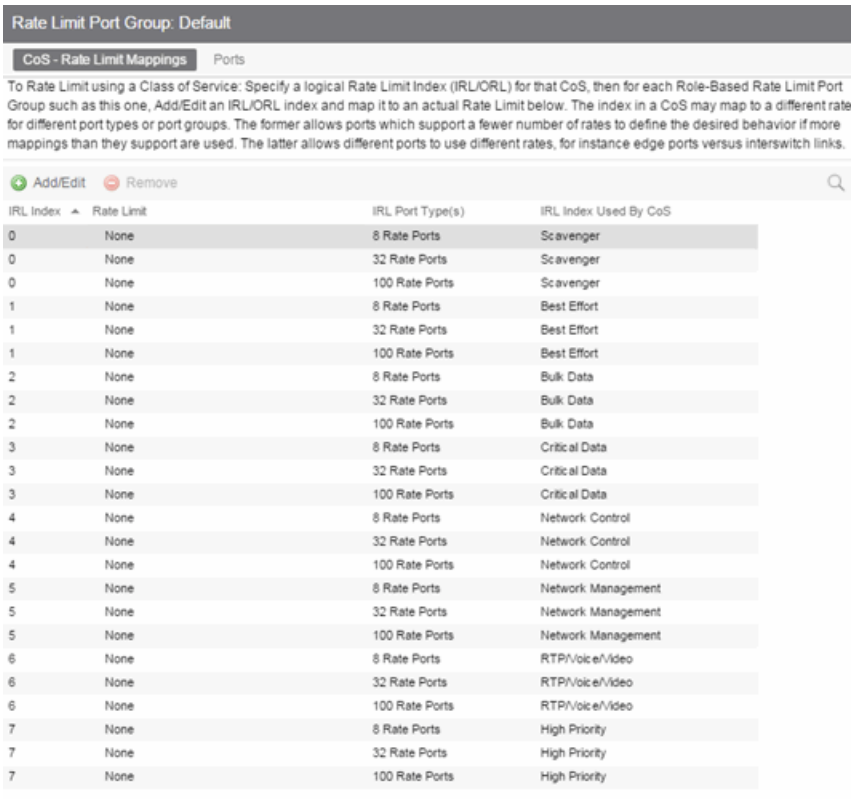
To access this tab:

1. Open the **Control** tab.
2. Open the **Policy** tab.
3. Open the **Class of Service** > **CoS Components** left-panel tab.
4. Select either the **Inbound Rate Limit Port Groups** or **Outbound Rate Limit Port Groups** left-panel tab, depending on whether the rate limit is inbound or outbound.
5. Select a existing port group in the left panel to open it in the **Rate Limit Port Group** tab.

NOTE: Create a new port group by right-clicking the **Inbound Rate Limit Port Groups** or **Outbound Rate Limit Port Groups** left-panel tab, selecting **Create Port Group**, entering a **Name** for the port group, and clicking **OK**.

---

6. Select the **CoS - Rate Limit Mappings** tab in the right panel.



IRL/ORL Index
The logical inbound rate limit (IRL) or outbound rate limit (ORL) index number. This index number is specified in a class of service and dictates the rate limiting behavior for incoming or outgoing packets. For each rate limit port group, use this tab to map the index number to an actual rate limit.

Rate Limit
The actual rate limit to which the IRL/ORL index is mapped.

IRL/ORL Port Type(s)
The type of ports included in the port group. Port type is based on the number of rate limits the ports support (for example, 8-rate limit ports and 32-rate limit ports).

IRL/ORL Index Used By CoS
The classes of service using this IRL/ORL index.

Add/Edit Button
Opens the Add/Edit CoS to Rate Limit Mappings window where you can add or edit rate limit mappings for the rate limit port group

Remove Button
Removes the mapping(s) selected in the table.

Related Information

For information on related concepts:

- Getting Started with Class of Service

For information on related tasks:

- How to Define Rate Limits
- Advanced Rate Limiting by Port Type

For information on related windows:

- Ports Tab (Rate Limit Port Group)

Extreme Management Center Ports (Rate Limit Port Group)

The rate limit port group Ports tab lets you view all the ports in the selected port group, as well as add and remove ports to and from the group. It provides information about each port, and lets you view and edit port information (via the port's General tab).

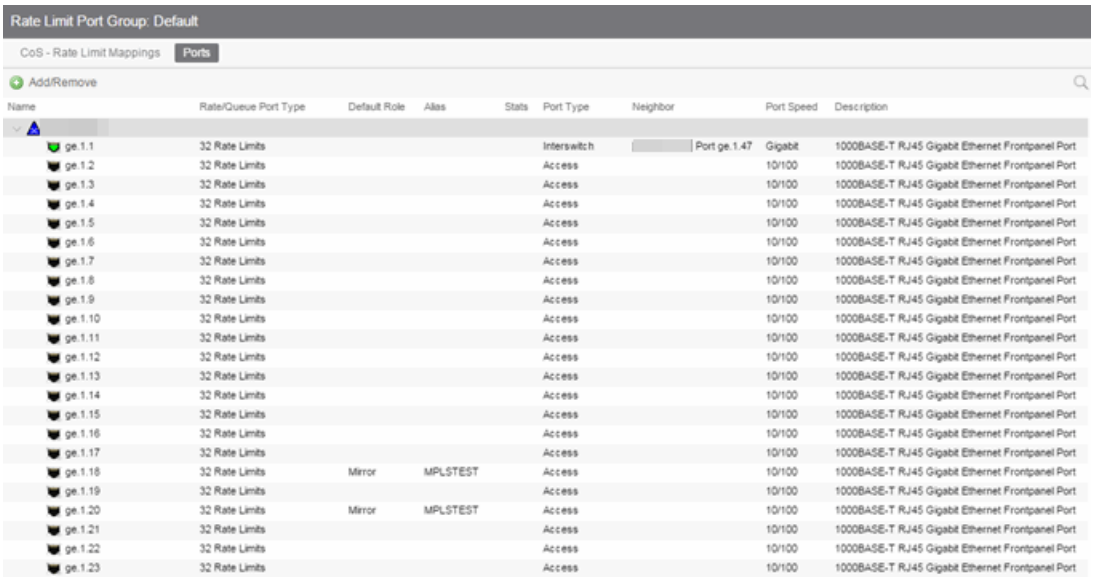
To access this tab:

1. Open the Control tab.
2. Open the Policy tab.
3. Open the Class of Service > CoS Components left-panel tab.
4. Select either the Inbound Rate Limit Port Groups or Outbound Rate Limit Port Groups left-panel tab, depending on whether the rate limit is inbound or outbound.
5. Select a existing port group in the left panel to open it in the Rate Limit Port Group tab.

   NOTE: Create a new port group by right-clicking the Inbound Rate Limit Port Groups or Outbound Rate Limit Port Groups left-panel tab, selecting Create Port Group, entering a Name for the port group, and clicking OK.

6. Select the Ports tab in the right panel.

Create a new port group by right-clicking the Inbound Rate Limit Port Groups or Outbound Rate Limit Port Groups left-panel tab, selecting Create Port Group, entering a Name for the port group, and clicking OK.



Name

Name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

Rate/Queue Port Type

The number of rate limits the port supports.

Default Role

The default role assigned to the port. See Default Role in the Concepts topic for information on default roles. For additional information, see Port Mode.

Alias

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

Stats

Shows statistics collected for a port, enabled via the Flow Collection & Interface setting in the PortView.

Port Type

Type of port. Possible values include: Access, Interswitch Backplane, Backplane, Interswitch, and Logical.

Neighbor

The port's neighbor port.

Port Speed

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

Description
A description of the port.

Add/Remove Ports Button
Opens the Add/Remove Ports window, where you can add and remove ports to and from the port group. When you create new port groups, you add ports from the Default group into your newly defined port groups.

Related Information

For information on related concepts:

- Getting Started with Class of Service

For information on related tasks:

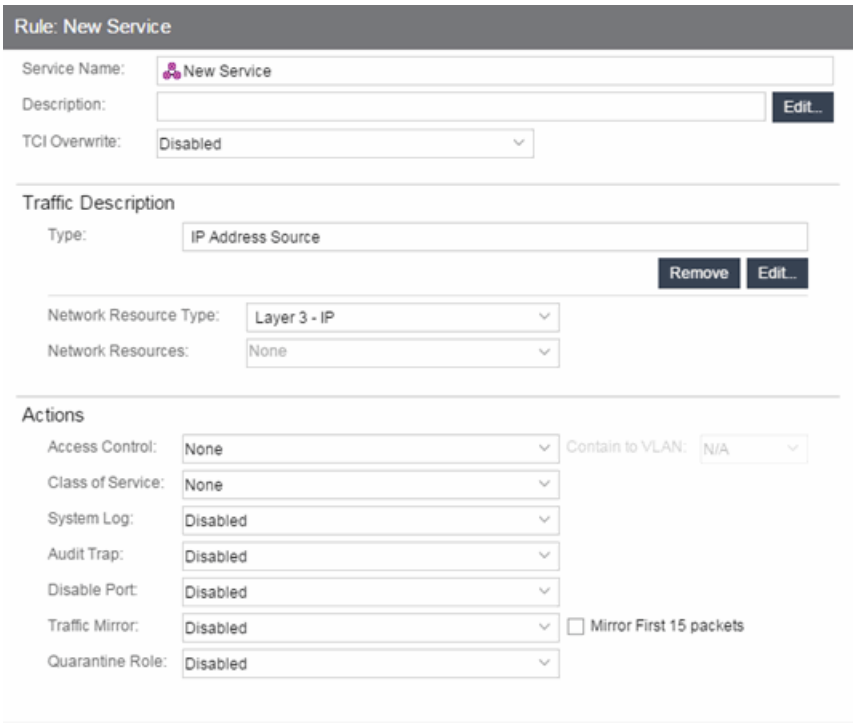
- How to Define Rate Limits
- Creating Class of Service Port Groups

For information on related windows:

- CoS - Rate Limits Mappings Tab (Rate Limit Port Group)

Extreme Management Center Automated Service

Selecting an Automated Service opens the **Automated Service** tab which allows you to define settings for the service. For more information on services, see How to Create a Service.



Service Name

Name of the selected service.

Description

Use the **Edit** button to open a window where you can enter or modify a description of the service.

TCI Overwrite

Specify the TCI Overwrite functionality for the service:

- **Enabled** - Enabling TCI Overwrite allows the VLAN (access control) and class of service characteristics defined in this service to overwrite the VLAN or class of service (CoS) tag in a received packet, if that packet has already been tagged with VLAN or CoS information.
- **Disabled** - If this option is disabled the TCI Overwrite option is ignored, but lower-precedence rules and the role default actions may still specify TCI Overwrite for the data packet if there is a match.
- **Prohibited** - Do not set TCI Overwrite for this data packet, even when a lower-precedence rule or the role default actions has the TCI Overwrite option set to enabled.

Traffic Description Area

Use this area to provide the specifications for an automated service. Specify the network resource type, the network resources for the service, and the rule type. Some rule types require that you enter certain parameters and/or values. This section is not displayed for a Manual service.

Type

Click the Edit button to select the type of rule you want to create for the network resources. Some rule types require you enter certain parameters and/or values. See Classification Types and their Parameters for parameter information. Select and/or enter the required parameters.

Network Resource Type

Select the network resource type (Layer 2 MAC or Layer 3 IP). This will determine the list of network resources available for selection for this service.

Network Resources

Use the drop-down list to select the network resources to associate with the automated service. Use the configuration menu button to the right of the list to add a network resource or view and edit your network resources. For more information, see How to Create a Network Resource.

Actions Area

Use this area to define the access control and/or a class of service for the Automated service rule. This section is not displayed for a Manual service.

Access Control

Use this drop-down list to select the appropriate access control for the rule. You can permit traffic to be forwarded, deny traffic altogether, or contain traffic to a VLAN. Select None to disable access control for this rule.

- Permit Traffic - allows traffic to be forwarded with the port's assigned VID.
- Deny Traffic - traffic will be automatically discarded.
- Contain to VLAN - contains traffic to a specific VLAN. Use the drop-down menu to select the desired VLAN. Use the Contain to VLAN drop-down menu to select a VLAN.

Class of Service

Use the drop-down menu to select a class of service to associate with the service. The Policy tab lets you define classes of service that each include an 802.1p priority, and optionally an IP type of service (ToS/DSCP) value, rate limits, and transmit queue configuration. You can then assign a class of service as a classification rule action. See Getting Started with Class of Service and How to Create a Class of Service for more information. Select None to disable class of service for this rule. Use the configuration menu button to the right of the drop-down list to add or edit a Class of Service.

When rule accounting is enabled on a device, each rule keeps a list of the ports on which it has been used. The next three options allow you to specify certain rule usage actions to take place when a "rule hit" is reported.

System Log

Specify System Log functionality for the rule:

- Enabled - If this option is enabled, a syslog message is generated when the rule is used. This option must be enabled if you are configuring Policy Rule Hit Reporting on your devices.
- Disabled - If this option is disabled and this rule is hit, it does not generate a Syslog message, but lower-precedence rules and the role default actions may still specify a syslog message be sent for this data packet if there is a match.
- Prohibited - If this rule is hit, no syslog message is generated for this data packet, even when a lower-precedence rule or the role default actions has the System Log action set to enabled.

Audit Trap

Specify Audit Trap functionality for the rule:

- Enabled - If this option is enabled, an audit trap is generated when the rule is used.
- Disabled - If this option is disabled and this rule is hit, it does not generate an audit trap, but lower-precedence rules and the role default actions may still specify generating an audit trap for this data packet if there is a match.
- Prohibited - If this rule is hit, no audit trap is generated for this data packet, even when a lower-precedence rule or the role default actions has the Audit Trap action set to enabled.

Disable Port

Specify Disable Port functionality for the rule:

- Enabled - If this option is enabled, any port reported as using this rule is disabled. Ports that have been disabled due to this option are displayed in the device Role/Rule tab.
- Disabled - If this option is disabled and this rule is hit, it does not disable the port, but lower-precedence rules and the role default actions may still specify disabling the port for this data packet if there is a match.
- Prohibited - If this rule is hit, the port is not disabled, even when a lower-precedence rule or the role default actions has the Disable Port action set to enabled.

Traffic Mirror

Specify traffic mirroring functionality for the rule:

- Select port group(s) - Use the drop-down list to select the port groups where mirrored traffic will be sent for monitoring and analysis. Use the configuration menu button to the right of the drop-down list and select View/Modify Port Groups to open the Port Groups tab where you can define user-defined port groups for selection.
- Disabled - If this option is disabled and this rule is hit, traffic mirroring will not take place, but lower-precedence rules and the role default actions may still specify traffic mirroring for this data packet if there is a match.
- Prohibited - If this rule is hit, traffic mirroring is disabled, even when a lower-precedence rule or the role default actions has the Traffic Mirror action specified.

Quarantine Role

Specify Quarantine role functionality for the rule:

- Enabled - If this option is enabled, any role reported as using this rule is quarantined.
- Disabled - If this option is disabled and this rule is hit, it does not quarantine the role, but lower-precedence rules and the role default actions may still specify quarantining the role for this data packet if there is a match.
- Prohibited - If this rule is hit, the role is not quarantined, even when a lower-precedence rule or the role default actions has the Quarantine Role action set to enabled.

Related Information

For information on related tasks:

- How to Create a Service
- How to Create a Network Resource

Traffic Classification Rules

Traffic Classification rules allow you to assign VLAN membership and/or class of service to your network traffic based on the traffic's classification type. Classification types are derived from Layers 2, 3, 4, and 7 of the OSI model, and all network traffic can be classified according to specific layer 2/3/4/7 information contained in each frame. In the Policy tab, rules are used to provide four key policy features: traffic containment, traffic filtering, traffic security, and traffic prioritization. Examples of how to design rules for each of these features are given below.

A Traffic Classification rule has two main parts: Traffic Description and Actions. The Traffic Description identifies the traffic classification type for the rule. The Actions specify whether traffic matching that classification type will be assigned VLAN membership, class of service, or both. When a frame arrives on a port, the switch checks to see if the frame's classification type matches the type specified in a rule. If it does, then the actions defined in that rule will apply to the frame.

In the Policy tab, rules are created and then grouped together into Services, which are then used to define roles. A role is assigned to each port either through end user authentication or as the port's default role. This means that there can be multiple rules active on a port. When a frame is received on a port, if the frame's classification type matches more than one rule, classification precedence rules are used to determine which rule to use.

The following information is discussed in this file:

- Traffic Descriptions
- Actions
    - VLAN Membership
    - Priority (Class of Service)

Traffic Descriptions

When you create a Traffic Classification rule in the **Policy** tab, you must define the rule's traffic description. The traffic description identifies the traffic classification type for that rule. You must select a classification type, and then select or enter certain parameters or values for each type.

Classification types are grouped according to Layers 2, 3, 4, and 7 of the OSI model and there are multiple classification types for each layer.

OSI Model
Layer 7 - Application
Layer 6 - Presentation
Layer 5 - Session
Layer 4 - Transport
Layer 3 - Network
Layer 2 - Data Link
Layer 1 - Physical

Specific Layer 2/3/4/7 information contained in each frame is used to identify the frame's classification type. Each layer uses different information to classify frames.

- **Layer 2 Data Link** -- classifies frames based on an exact match of the MAC address or specific protocol type of each frame.

- Layer 3 Network -- classifies IP or IPX frames based on specific information contained within the Layer 3 header.
- Layer 4 Transport -- classifies IP frames based on specific Layer 4 TCP or UDP port numbers contained in the header.
- Layer 7 Application -- classifies frames based on specific Layer 7 application types.

For a complete description of Layer 2, 3, 4, and 7 classifications, refer to Classification Types and Their Parameters.

Actions

When you create a Traffic Classification rule in the Policy tab, you must define the actions the rule performs. When a frame arrives on a port, the switch checks to see if the frame's classification type matches the type specified in a rule. If it does, then the actions defined in that rule will apply to the frame. Actions specify whether the frame will be assigned VLAN membership (access control) and/or priority (class of service).

VLAN Membership (Access Control)

In your network domains, you can create VLANs (Virtual Local Area Networks) that allow end-systems connected to separate ports to send and receive traffic as though they were all connected to the same network segment. Using traffic classification rules, you can classify a frame based on the frame's classification type to have membership in a specific VLAN, providing important traffic containment, filtering, and security for your network.

For example, a network administrator could use rules to separate end user traffic into VLANs according to protocol, subnet, or application. Rules could also be used to group geographically separate end-systems into job-specific workgroups.

Priority (Class of Service)

Traffic Classification rules allow you to assign a transmission priority to frames received on a port based on the frame's classification type. For example, a network administrator could use rules to assign priority to one network application over another.

Priority is a value between 0 and 7 assigned to each frame as it is received on a port, with 7 being the highest priority. Frames assigned a higher priority will be

transmitted before frames with a lower priority. Each of the priorities is mapped into a specific transmit queue by the switch or router. The insertion of the priority value (0-7) allows all 802.1Q devices in the network to make intelligent forwarding decisions based on its own level of support for prioritization.

The Policy tab enables you to utilize priority by creating classes of service that each include an 802.1p priority, and optionally an IP type of service (ToS/DSCP) value, rate limits, and transmit queue configuration. You can then assign the class of service as a classification rule action, as part of the definition of an automated service, or as a role default. See Getting Started with Class of Service for more information.

Classification Types and their Parameters

When you define a rule's traffic description, you select a classification type, and then select or enter certain parameters or values for each type. Classification types are grouped according to Layers 2, 3, 4, or 7 of the OSI model.

Layer 2 -- Data Link Classification Types

Layer 2 classification types allow you to define classification rules based on an exact match of the MAC address or specific protocol type of each frame.

MAC Address Source, MAC Address Destination, MAC Address Bilateral

These classification types are based on an exact match of the source, destination, or bilateral (either source or destination) MAC address contained in an Ethernet frame. Enter a valid MAC address or click Select to open a window where you can select a MAC address read from your network devices. You can specify a mask, however masking a MAC address is not supported on legacy devices.

Ethertype

This classification type is based on the specific protocol type of each frame defined in the two-byte Ethertype field. Select an Ethertype from the list of well-known values, or select Other and manually enter a single value in hexadecimal form. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

Well-known Ethertypes	Values
IP	0x0800

Well-known Ethertypes	Values
ARP	0x0806
Reverse ARP	0x8035
Novell IPX 1	0x8137
Novell IPX 2	0x8138
Banyan	0x0bad
AppleTalk	0x809b
AppleTalk ARP	0x80f3
IPv6	0x86dd
Decnet Phase 4	0x6003

DSAP/SSAP

This classification type is based on the specific protocol type of each frame defined in the DSAP and SSAP fields. Select a protocol from the list of well-known values, or select **Other** and manually enter a custom two-byte value in hexadecimal format (0xFFFF). The LSB of the DSAP address specifies Individual(0) or Group(1), while the LSB of the SSAP address specifies Command(0) or Response(1). For the SNAP frame type, you may enter Advanced DSAP/SSAP configurations. The advanced fields are not supported on legacy devices and are ignored.

Well-known DSAP/SSAP Types	Values
IP	0x0606
IPX	0xe0e0
NetBIOS	0xf0f0
Banyan Vines	0xbcbc
SNA	0x0404
SNAP	0xAAAA
Other	a two-byte value

VLAN ID

This classification type is based on an exact match of the VLAN tag contained within a frame. Select a VLAN ID (VID) from the list of VLANs defined in the Policy tab. If you select **Other**, you must enter a single VID or specify a range of VIDs in decimal form. Range rules are not supported on legacy devices.

Priority

This classification type is based on an exact match of the Priority tag contained within a frame. Select a Priority value 0 - 7 from the list of well-known values, or select Other and enter a value in decimal form.

Layer 3 -- Network Classification Types

Layer 3 Network classification types allow you to define classification rules based on specific information contained within the Layer 3 header of an IP or IPX frame.

IP Time to Live (TTL)

This classification type is based on an exact match of the TTL field contained in the IP header of a frame. The TTL field indicates the maximum number of router hops the packet can make before being discarded. The TTL field is set by the packet sender and reduced by every router on the route to its destination. If the TTL field reaches zero before the packet arrives at its destination, then the packet is discarded. IP Time to Live rules are only supported on K-Series and S-Series devices.

IPX Network Source, IPX Network Destination, IPX Network Bilateral

These classification types are based on specific information contained within the Layer 3 header of an IPX frame. It is a four-byte user-defined value that represents the IPX source, destination, or bilateral (either source or destination) network number. This value must be a valid IPX network address in hexadecimal form. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

IPX Socket Source, IPX Socket Destination, IPX Socket Bilateral

These classification types are based on specific information contained within the Layer 3 header of an IPX frame. It is a two-byte, user-defined value that represents the IPX source, destination, or bilateral (either source or destination) socket numbers. This value is used by higher layer protocols to target specific applications running among hosts. Select an IPX Socket type from the list of well-known values, or select Other and manually enter the value in decimal form. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

Well-known IPX Socket Types	Values
NCP	1105

Well-known IPX Socket Types	Values
SAP	1106
RIP	1107
NetBIOS	1109
Diagnostics	1110
NSLP	36865
IPX Wan	56868
Other	0-65535

IPX Class of Service

This classification type is based on specific information contained within the Layer 3 header of an IPX frame. This is a one-byte field used for transmission control (hop count) by IPX routers. Enter a valid IPX Class of Service in decimal form, 0-255. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

IPX Packet Type

This classification type is based on specific information contained within the Layer 3 header of an IPX frame. Select an IPX Packet type from the list of well-known values or select Other and manually enter the value in decimal form. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

Well-known IPX Packet Types	Values
Hello/SAP	0
RIP	1
Echo Packet	2
Error Packet	3
NetWare 386	4
SeqPackProt	5
NetWare 286	17
Other	0-31

IPv6 Address Source, IPv6 Address Destination, IPv6 Address Bilateral

These classification types are based on an exact match of the source, destination, or bilateral (either source or destination) IPv6 address information contained within

the IPv6 header of each frame. Enter a valid IPv6 address and optional mask ("/n") in the Value field.

IPv6 Socket Source, IPv6 Socket Destination, IPv6 Socket Bilateral

These classification types are based on an exact match of a specific source, destination, or bilateral (either source or destination) IPv6 address and a UDP/TCP port number (type) contained within the IPv6 header of each frame. Enter an IPv6 address in the Value field. Then, select a UDP/TCP type from the list of well-known values, or select **Other** and manually enter the value in form. (UDP/TCP port numbers are defined in RFC 1700.) If you select **Other**, you can enter a range of values.

Well-known UDP/TCP Types	Values
FTP Data	20
FTP	21
SSH	22
Telnet	23
SMTP	25
TACACS	49
DNS	53
BootP Server	67
BootP Client	68
TFTP	69
Finger	79
HTTP	80
POP3	110
Portmapper	111
NNTP	119
NTP	123
NetBIOS Name Service	137
NetBIOS Datagram Service	138
NetBIOS Session Service	139

Well-known UDP/TCP Types	Values
IMAP2/IMAP4	143
SNMP	161
IMAP3	220
LDAP	389
HTTPS	443
R-Exec	512
R-Login	513
R-Shell	514
LPR	515
RIP	520
SOCKS	1080
Citrix ICA	1494
RADIUS	1812
RADIUS Accounting	1813
NFS	2049
X11 (Range Start)	6000
X11 (Range End)	6063
Other	0-65535

IPv6 Flow Label

These classification types are based on the exact match of the value in the 20-bit Flow Label field in the IPv6 header. This field is used to identify packets belonging to particular traffic flow that needs special traffic handling. Enter a flow label value and sigbits mask.

IP Address Source, IP Address Destination, IP Address Bilateral

These classification types are based on an exact match of the source, destination, or bilateral (either source or destination) IP address information contained within the IP header of each frame. Enter a valid IP address and optional mask ("/n") in the Value field.

IP Socket Source, IP Socket Destination, IP Socket Bilateral

These classification types are based on an exact match of a specific source, destination, or bilateral (either source or destination) IP address and a UDP/TCP

port number (type) contained within the IP header of each frame. Enter an IP address in the Value field. Then, select a UDP/TCP type from the list of well-known values, or select **Other** and manually enter the value in decimal form. (UDP/TCP port numbers are defined in RFC 1700.) If you select **Other**, you can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

Well-known UDP/TCP Types	Values
FTP Data	20
FTP	21
SSH	22
Telnet	23
SMTP	25
TACACS	49
DNS	53
BootP Server	67
BootP Client	68
TFTP	69
Finger	79
HTTP	80
POP3	110
Portmapper	111
NNTP	119
NTP	123
NetBIOS Name Service	137
NetBIOS Datagram Service	138
NetBIOS Session Service	139
IMAP2/IMAP4	143
SNMP	161
IMAP3	220
LDAP	389

Well-known UDP/TCP Types	Values
HTTPS	443
R-Exec	512
R-Login	513
R-Shell	514
LPR	515
RIP	520
SOCKS	1080
Citrix ICA	1494
RADIUS	1812
RADIUS Accounting	1813
NFS	2049
X11 (Range Start)	6000
X11 (Range End)	6063
Other	0-65535

IP Fragment

This classification type is based on Layer 4 information in fragmented frames. IP supports frame fragmentation, where large frames are divided into smaller fragments and sent wrapped in the original Layer 3 (IP) header. When a frame is fragmented, information that is Layer 4 and above is only present in the first fragment. For example, the first fragment may be classified to Layer 4, while subsequent fragments will be classified only to Layer 3. The product line does not support Layer 4 classification for IP frames that have been fragmented, as the Layer 4 information is not present in these frames. Using the IP Fragment classification rule, any frame which is a fragment of a larger frame, is classified according to the information in the original frame. If the first fragment is classified to Layer 4, subsequent fragments will also be classified to Layer 4.

ICMP and ICMPv6

These classification types are based on an exact match of the ICMP (Internet Control Message Protocol) message contained in the ICMP tag within a frame. Select an ICMP well-known value type from the list of well-known values (some well-known value types also let you select a code), or select **Other** and manually enter the value in hexadecimal form. The format of the value is 0xXXYY, where "XX" is the ICMP

type, and "YY" is the associated code, if applicable. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

IP Type of Service

This classification type is based on an exact match of the one-byte ToS/DSCP field contained in the IP header of a frame. The ToS (Type of Service) or DSCP (Diffserve Codepoint) value is defined by an 8-bit hexadecimal number between 0 and FF. Enter a value or click Select to open a window where you can generate a hex value.

Type of Service can be used by applications to indicate priority and Quality of Service for each frame. The level of service is determined by a set of service parameters which provide a three way trade-off between low-delay, high-reliability, and high-throughput. The use of service parameters may increase the cost of service. In many networks, better performance for one of these parameters is coupled with worse performance on another. Except for very unusual cases, at most, two of the parameters should be set.

For a ToS value, the 8-bit hexadecimal number breaks down as follows:

Bits 0-2: Precedence
Bit 3: 0=Normal Delay, 1=Low Delay
Bit 4: 0=Normal Throughput, 1=High Throughput
Bit 5: 0=Normal Reliability, 1=High Reliability
Bits 6-7: Explicit Congestion Notification

The precedence bits (bits 0-2) break down as follows:

111 - Network Control
110 - Internetwork Control
101 - CRITIC/ECP
100 - Flash Override
011 - Flash
010 - Immediate
001 - Priority
000 - Routine

The Network Control precedence designation is intended to be used within a network only. The actual use and control of that designation is up to each network. The Internetwork Control designation is intended for use by gateway originators only.

For a DSCP value, the value represents codepoints for two Differentiated Services (DS) Per-Hop-Behavior (PHB) groups called Expedited Forwarding (EF) and Assured Forwarding (AF). For more information on these PHB groups, refer to RFC 2597 and RFC 2598.

IP Protocol Type

This classification type is based on the specific protocol type defined in a field contained in the IP header of each frame. Select a protocol from the list of well-known values, or select Other and manually enter the value in decimal form. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

Well-known IP Protocol Types	Values
ICMP	1
IGMP	2
TCP	6
EGP	8
UDP	17
IPv6 (encapsulated in IPv4 packets)	41
RSVP	46
GRE	47
ESP	50
AH	51
ICMPv6	58
EIGRP	88
OSPF	89
PIM	103
VRRP	112
L2TP	115
Other	0-255

Layer 4 -- Application Transport Classification Types

Layer 4 IP classification types allow you to define classification rules based on specific Layer 4 TCP or UDP port numbers contained in the header of an IP frame. You can specify a specific port number or a range of port numbers.

Note: Certain devices do not support Layer 4 classification for IP frames that have been fragmented, as the Layer 4 information is not present in these frames. If a device has an FDDI HSIM installed, Layer 4 classification will not be supported for any frames larger than 1500 bytes. Frames larger than 1500 bytes are fragmented internally in the switch. When creating classification rules based on specific Layer 4 information, using the IP Fragment classification rule will allow fragmented frames to be classified according to the Layer 4 information contained in the original frame.

IP UDP Port Source, IP UDP Port Destination, IP UDP Port Bilateral

These classification types are based on specific Layer 4 UDP port numbers contained within the header of an IP frame. Select a UDP type from the list of well-known values, or select Other and manually enter the value in decimal form. (UDP port numbers are defined in RFC 1700.) You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold. Enter a valid IPv4 or IPv6 address and optional mask ("/n"), if desired. The IP address is an optional field and does not have to be specified. It is only valid for non-range port values.

Well-known UDP Types	Values
FTP Data	20
FTP	21
SSH	22
Telnet	23
SMTP	25
TACACS	49
DNS	53
BootP Server	67
BootP Client	68
TFTP	69

Well-known UDP Types	Values
Finger	79
HTTP	80
POP3	110
Portmapper	111
NNTP	119
NTP	123
NetBIOS Name Service	137
NetBIOS Datagram Service	138
NetBIOS Session Service	139
IMAP2/IMAP4	143
SNMP	161
IMAP3	220
LDAP	389
HTTPS	443
R-Exec	512
R-Login	513
R-Shell	514
LPR	515
RIP	520
SOCKS	1080
Citrix ICA	1494
RADIUS	1812
RADIUS Accounting	1813
NFS	2049
X11 (Range Start)	6000
X11 (Range End)	6063
Other	0-65535

IP TCP Port Source, IP TCP Port Destination, IP TCP Port Bilateral

These classification types are based on specific Layer 4 TCP port numbers contained within the header of an IP frame. Select a TCP type from the list of well-known values, or select **Other** and manually enter the value in decimal form. (TCP port numbers are defined in RFC 1700.) You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold. Enter a valid IPv4 or IPv6 address and optional mask ("/n"), if desired. The IP address is an optional field and does not have to be specified. It is only valid for non-range port values.

Well-known TCP Types	Values
FTP Data	20
FTP	21
SSH	22
Telnet	23
SMTP	25
TACACS	49
DNS	53
BootP Server	67
BootP Client	68
TFTP	69
Finger	79
HTTP	80
POP3	110
Portmapper	111
NNTP	119
NTP	123
NetBIOS Name Service	137
NetBIOS Datagram Service	138
NetBIOS Session Service	139
IMAP2/IMAP4	143
SNMP	161

Well-known TCP Types	Values
IMAP3	220
LDAP	389
HTTPS	443
R-Exec	512
R-Login	513
R-Shell	514
LPR	515
RIP	520
SOCKS	1080
Citrix ICA	1494
RADIUS	1812
RADIUS Accounting	1813
NFS	2049
X11 (Range Start)	6000
X11 (Range End)	6063
Other	0-65535

IP UDP Port Source Range, IP UDP Port Destination Range, IP UDP Port Bilateral Range

These classification types are based on Layer 4 UDP port numbers contained within the header of an IP frame. When you select this type, you enter a range of UDP port numbers that the port number in the header will be matched against. Enter the start and end range values in decimal form. UDP port numbers are defined in RFC 1700.

IP TCP Port Source Range, IP TCP Port Destination Range, IP TCP Port Bilateral Range

These classification types are based on Layer 4 TCP port numbers contained within the header of an IP frame. When you select this type, you enter a range of TCP port numbers that the port number in the header will be matched against. Enter the start and end range values in decimal form. TCP port numbers are defined in RFC 1700.

Layer 7 -- Application Classification Types

Layer 7 IP classification types allow you to define classification rules based on specific Layer 7 application types.

Application

This rule type allows management of traffic for a specific application type, for example Apple traffic (Bonjour) using mDNS-SD. The following application types are supported:

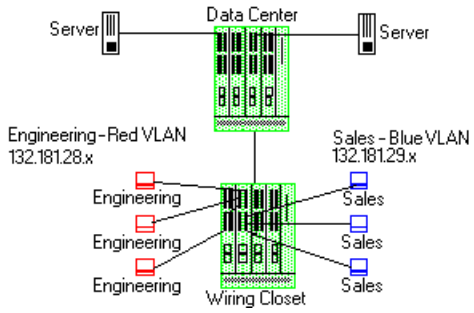
- LLMNR - (Link Local Multicast Name Resolution) Query/Response
  This protocol is based on the Domain Name System (DNS) packet format. It allows hosts to perform name resolution for hosts on the same local link.
- SSDP - (Simple Service Discovery Protocol) Query/Response
  SSDP is a Universal Plug-and-Play (UPnP) based protocol. SSDP uses the NOTIFY and MSEARCH HTTP methods to discover and advertise services on the network.
- mDNS-SD - (Multicast Domain Name System – Service Discovery) Query/Response
  DNS-SD is a service discovery protocol that utilizes the Domain Name System. Multicast DNS is a protocol that is mostly compatible with normal DNS but uses link local multicast addressing, allowing for zero configuration networking (zeroconf) functionality.

Examples of How Rules are Used

Traffic Classification rules are used to provide four key policy features: Traffic Containment, Traffic Filtering, Traffic Security, and Traffic Priority.

Traffic Containment

Using classification rules, network administrators can group together users of a given protocol, subnet, or application, and control where their traffic can logically go on the network.



The figure above shows a configuration where the network administrator wants to separate end-user traffic into VLANs based on the assigned IP subnet of each

department. This can easily be accomplished by creating two Layer 3 classification rules based on the IP subnet range of the respective departments.

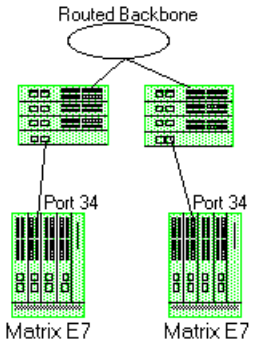
Rule 1 - Engineering, which uses the 132.181.28.x subnet, will be assigned to the Red VLAN.

Rule 2 - Sales, which uses the 132.181.29.x subnet, will be assigned to the Blue VLAN.

Based on these two Layer 3 classification rules, the traffic from the Engineering VLAN will be isolated from the Sales VLAN. Since these rules are based on Layer 3 information, an Engineering user could enter the network from a connection in the Sales department, and that user would still be contained in the Engineering VLAN.

Traffic Filtering

Classification rules can also be used to filter out (discard) specific unwanted traffic. Filter criteria can include things such as broadcast routing protocols, specific IP addresses, or even applications such as HTTP or SMTP.



The figure above shows a common configuration in which a routed backbone is using both RIP and OSPF for its routing protocols. The network administrator does not want the multicast OSPF and broadcast RIP frames propagated to the end stations. The network is designed so that only end users are attached to the E7 devices.

To implement filtering in this scenario, a Layer 3 rule and a Layer 4 rule will be created.

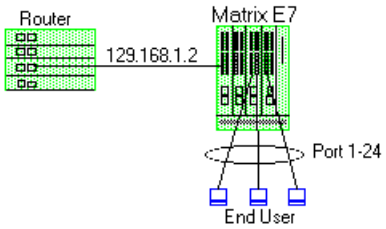
Rule 1 (Layer 3) - Any frame received with an IP Protocol Type of 89 (OSPF) will be discarded.

Rule 2 (Layer 4) - Any frame received with a Bilateral UDP port number of 520 (RIP) will be discarded.

Based on this configuration, all RIP and OSPF frames will be filtered from the end users.

Traffic Security

Traffic Security uses the same concepts as Traffic Filtering. Imagine a scenario where network access is provided to a group of unknown users. There have been problems with these unknown users "hacking" into the router and altering the configuration. A simple classification rule can be put in place that will prevent these types of occurrences.



In the figure above, the network components include a router and an E7 device. In this configuration end-users connect to the ports of the E7 device.

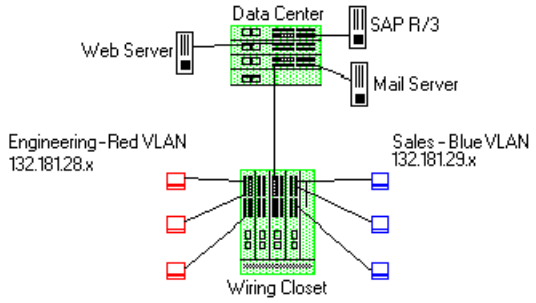
Since the end-users would never need to communicate directly to the router using the router's IP address, a Layer 3 IP classification rule will be used.

Rule - Any frames received by the switch with a destination IP address of the router (129.168.1.2) will be discarded.

The end result is that any frames from a user trying to "hack" into the router will be discarded before ever reaching the router.

Traffic Prioritization

Classification rules can be used to specify that certain network applications receive the highest transmission priority. For example, a network administrator wants to assign priority to three network applications, SAP R/3, web traffic, and email, in that order.



To accomplish the prioritization goals in this example, there are two main steps required: creating the classification rules, and then configuring the priority-to-transmit queue mapping for the switch, if needed.

First, create one Layer 3 and two Layer 4 classification rules.

> Rule 1, Layer 3 (SAP R/3) - All frames to or from the IP address of the SAP R/3 server will be tagged with a priority indicator of 7 (highest).
>
> Rule 2, Layer 4 (Web) - All frames with a TCP port number of 80 (HTTP) will be tagged with a priority indicator of 5.
>
> Rule 3, Layer 4 (email) - All frames with a TCP port number of 25 (SMTP) will be tagged with a priority indicator of 3.

Note: An IP address classification was selected for Rule 1 because it has been observed that SAP R/3 dynamically negotiates the TCP/UDP port used, so the port number selections vary from session to session. If this was not the case, a Layer 4 UDP classification could be used.

Then, configure the priority-to-transmit queue mappings. Each switch has default priority-to-transmit queue mappings. You can use these defaults or change the mappings using local management or the legacy Console java application. In addition, the Policy tab provides the ability to configure transmit queues as part of the Role-Based Rate Limits and Transmit Queue Configuration class of service mode. This functionality is available only on certain devices such as the S-Series and N-Series Gold and Platinum devices (refer to the Extreme Management Center Firmware Support tables for specific device/firmware rate limit support).

Based on the default priority-to-traffic queue mapping for an E7 device, the priorities assigned above will work out so that each frame classification type will be mapped to the desired traffic queue. This means that no user configuration of the priority-to-transmit queue mapping would be required.

With the classification rules described above, the network traffic would be prioritized as shown in the table below:

Application	Classification Type	Desired Priority	Priority Value	E7 Traffic Queue
SAP R/3	Bilateral IP	High	7	3
Web	TCP Port Number	Medium	5	2
Email	TCP Port Number	Low	3	1

Related Information

For information on related tasks:

- How to Create or Modify a Rule
- How to Define Traffic Descriptions

Extreme Management Center Ports (Transmit Queue Port Group)

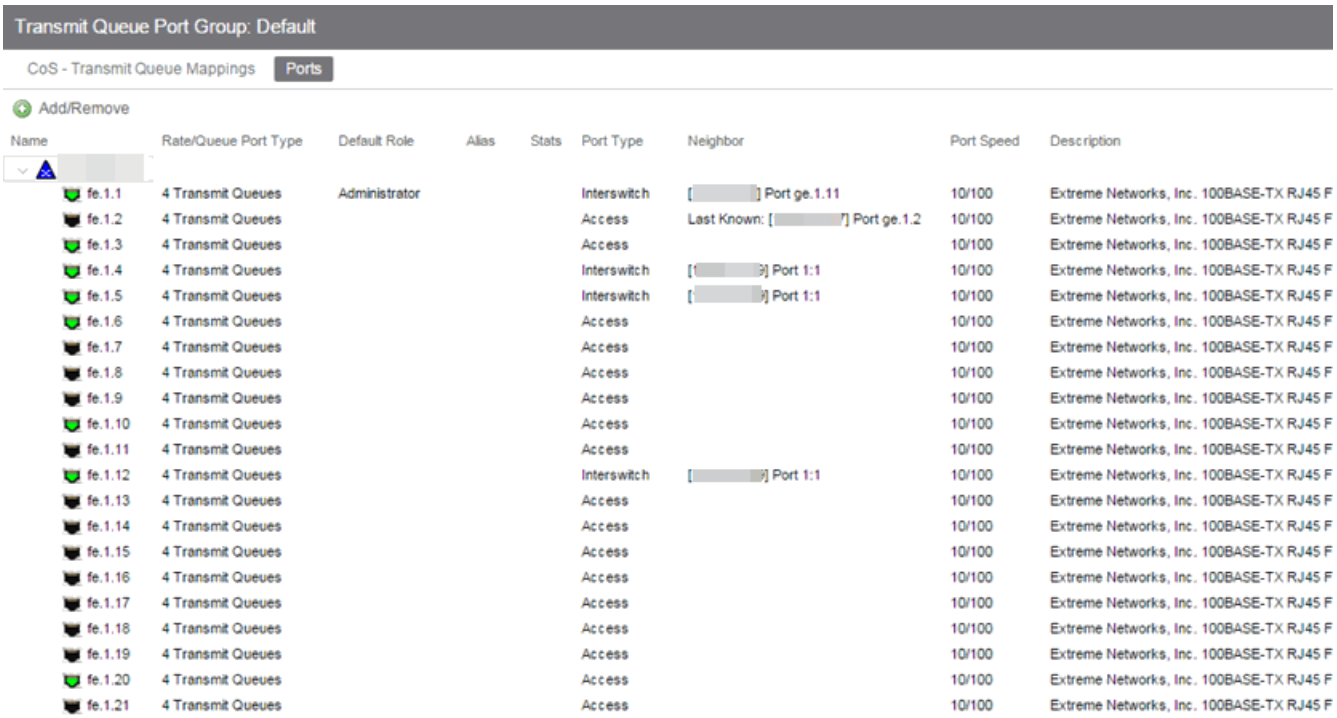
The **Ports** tab lets you view all the ports in the selected transmit queue port group, as well as add and remove ports to and from the group. It provides information about each port, and lets you view and edit port information.

To access this tab:

1. Open the **Control** tab.
2. Open the **Policy** tab.
3. Open the **Class of Service** > **CoS Components** left-panel tab.
4. Select either the **Transmit Queue Port Groups** left-panel tab.
5. Select a existing port group in the left panel to open it in the **Transmit Queue Port Group** tab.

   NOTE: Create a new port group by right-clicking the **Transmit Queue Port Groups** left-panel tab, selecting **Create Port Group**, entering a **Name** for the port group, and clicking **OK**.

6. Select the **Ports** tab in the right panel.



Name
: Name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

Rate/Queue Port Type
: The number of rate limits the port supports.

Default Role
: The default role assigned to the port. See Default Role in the Concepts topic for information on default roles. For additional information, see Port Mode.

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

Stats
: Shows statistics collected for a port, enabled via the Flow Collection & Interface setting in the PortView.

Port Type
: Type of port. Possible values include: Access, Interswitch Backplane, Backplane, Interswitch, and Logical.

Neighbor
: The port's neighbor port.

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

Description
A description of the port.

Add/Remove Ports Button
Opens the Add/Remove Ports window, where you can add and remove ports to and from the port group. When you create new port groups, you add ports from the Default group into your newly defined port groups.

Related Information

For information on related concepts:

- Getting Started with Class of Service

For information on related tasks:

- How to Configure Transmit Queues

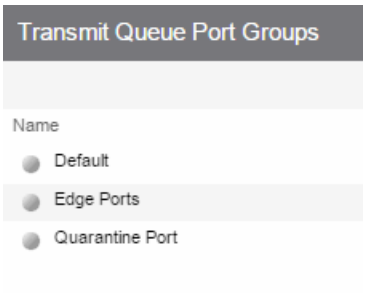
For information on related windows:

- CoS - Transmit Queue Mappings Tab (Transmit Queue Port Group)

Extreme Management Center Summary (Transmit Queue Port Groups)

This tab displays the transmit queue port groups. Transmit queue mapping maps a logical transmit queue index (used by a class of service) to an actual physical transmit queue you have configured in the **Policy** tab. You can configure transmit queue mappings for a port group using the CoS - Transmit Queue Mappings tab.

To access this tab, open the **Class of Service > CoS Components** tab. Then, select the select the **Transmit Queue Port Groups** tab in the left panel. The Summary tab displays in the right panel.



Name
The name of the transmit queue port group.

Related Information

For information on related concepts:

- Getting Started with Class of Service

For information on related tasks:

- How to Configure Transmit Queues

For information on related windows:

- CoS - Transmit Queue Mappings Tab (Transmit Queue Port Group)
- Ports Tab (Transmit Queue Port Group)

Extreme Management Center CoS - Transmit Queue Mappings (Transmit Queue Port Group)

This tab lets you view and configure the transmit queue mappings for a port group. Transmit queue mappings map a logical rate limit index used by classes of service to an actual physical rate limit you have created in Extreme Management Center.

Each port group has its own set of index mappings. Extreme Management Center automatically assigns these index numbers when you configure a class of services' rate limits and transmit queue shapers.

The Transmit Queue Mappings tab allows you to do two things:

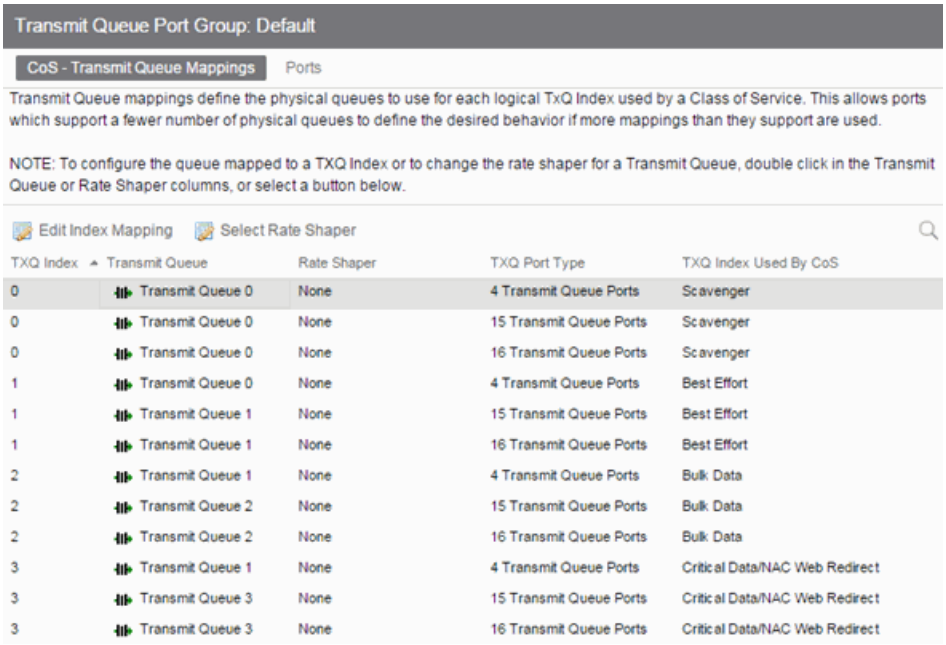
- Map the index to a different rate for different port groups (edge ports versus inter-switch links). See Creating Class of Service Port Groups
- Map the index to a different rate limit for each port type (8-rate limit, 32-rate limit, 64-rate limit, and 100-rate limit) in a port group. See Advanced Rate Limiting by Port Type.

To access this tab:

1. Open the **Control** tab.
2. Open the **Policy** tab.
3. Open the **Class of Service** > **CoS Components** left-panel tab.
4. Select either the **Transmit Queue Port Groups** left-panel tab.
5. Select a existing port group in the left panel to open it in the **Transmit Queue Port Group** tab.

NOTE: Create a new port group by right-clicking the **Transmit Queue Port Groups** left-panel tab, selecting **Create Port Group**, entering a **Name** for the port group, and clicking **OK**.

6. Select the **CoS - Transmit Queue Mappings** tab in the right panel.



TXQ Index

The logical transmit queue index. This index number is specified in a class of service and dictates the queue and shaping behavior for incoming packets.

Transmit Queue
Displays the physical transmit queue used to map to each transmit queue index. To change this value, click the Edit Index Mapping button to open the Edit Transmit Queue Mapping window and select a value in the Transmit Queue drop-down menu.

Rate Shaper
The transmit queue's associated rate shaper. To change this value, click the Select Rate Shaper button to open the Select Transmit Queue Rate Shaper window and select a value in the Rate Limit field.

TXQ Port Type
The Port Type is based on the number of transmit queues the port supports: 4 transmit queues or 16 transmit queues.

TXQ Index Used By CoS
The Class of Service using this TXQ index.

Related Information

For information on related concepts:

- Getting Started with Class of Service

For information on related tasks:

- How to Configure Transmit Queues

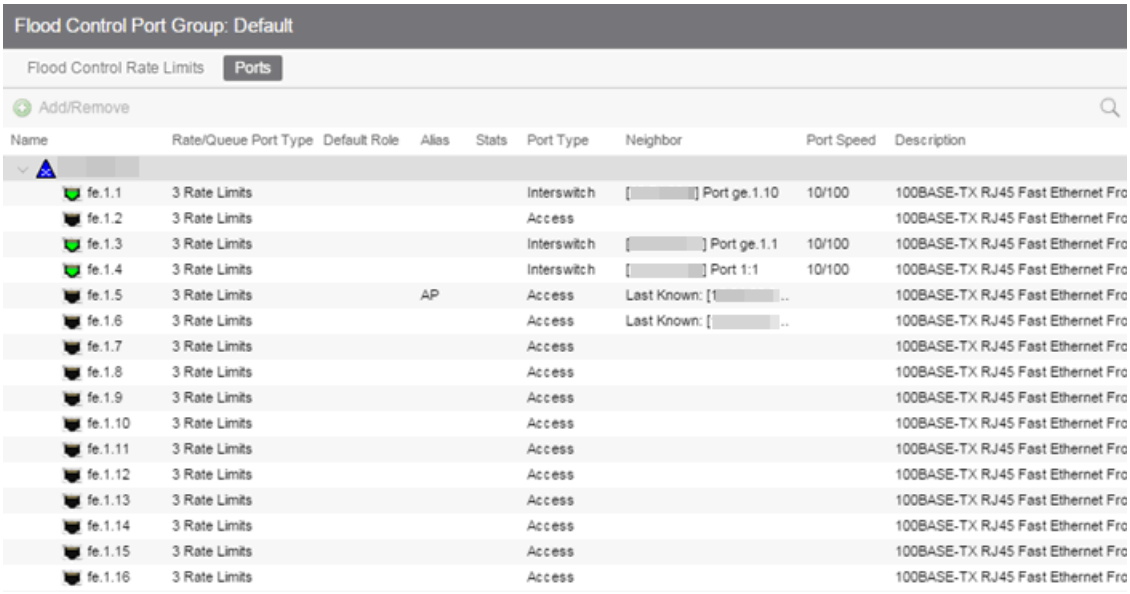
For information on related windows:

- Ports Tab (Transmit Queue Port Group)

Extreme Management Center Ports (Flood Control Port Groups)

The Flood Control Port Group Ports tab provides a table of information about the ports in the selected port group. It also includes buttons that enable you to retrieve the latest information about the ports and to add and remove ports. To access this tab, select a port group in the left-panel Flood Control Port Groups tab, then select the Ports tab in the right panel.

NOTE: The Ports tab is only available when a Flood Control port group is selected, and when advanced mode is enabled on the CoS Components tab.



Name
: Name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

Rate/Queue Port Type
: Shows the selected port type rate/queue.

Default Role
: Shows the default role for the port. See Default Role in the Concepts topic for information on default roles. For additional information, see Port Mode.

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

Stats
: Shows that statistics are being collected for a port, enabled via the PortView.

Port Type
: Type of port. Possible values include: Access, Interswitch Backplane, Backplane, Interswitch, and Logical.

Neighbor
: Port to which the port is connected.

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

Description
A description of the port.

Add/Remove Button
Selecting a port in the table and clicking this button opens the Add/Remove Ports window, which enables you to add and remove ports to and from the port group. This option is available for user-defined port groups only.

Related Information

For information on related concepts:

- Getting Started with Class of Service

For information on related tasks:

- How to Create a Class of Service
- How to Configure Flood Control

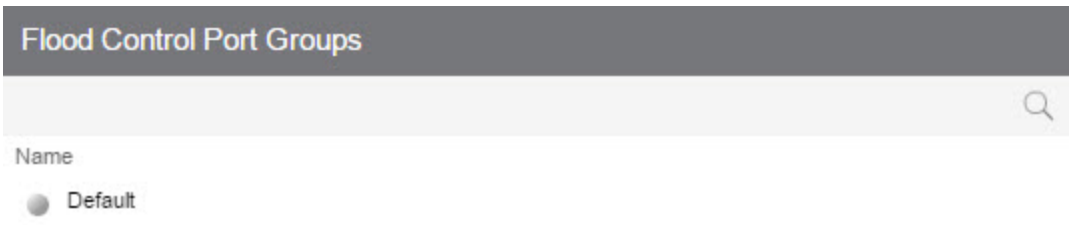
For information on related windows:

- General Tab (Rate Limit)

Extreme Management Center Flood Control Port Groups

This panel lists port groups on which you can configure flood control. Each port group supports rate limits for three separate configured traffic types (Unicast, Multicast, and Broadcast).

To access this tab, open Class of Service > CoS Components left panel of the Policy tab and select Flood Control Port Groups.



Name
The name of the port group.

Related Information

For information on related concepts:

- Getting Started with Class of Service

For information on related tasks:

- How to Create a Class of Service
- How to Configure Flood Control

Extreme Management Center Flood Control Rate Limits (Flood Control Port Groups)

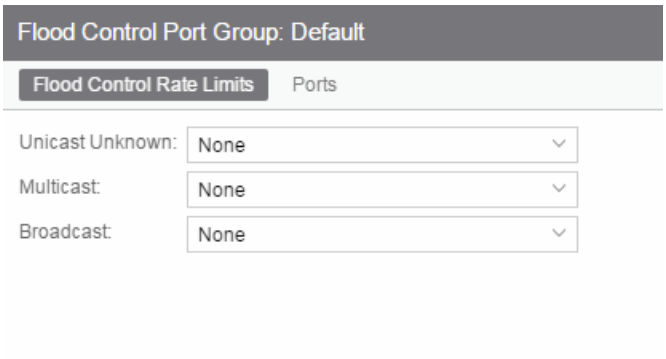
This tab allows you to set individual flood control rates for each traffic type (Unicast, Multicast, and Broadcast).

Choices include:

- None
- Rate limits created in the **Rate Limit** tab. For additional information, see Create Rate Limit/Shaper.

As flood control is enabled/disabled for a Class of Service, when enabled, each column displays a rate limit, or **None**, if no rate has been defined for that portion of flood control.

To access this tab, open the **Class of Service** > **CoS Components** left-panel tab. Then, select the **Flood Control** checkbox from the **General** tab in the left-panel to display the **Flood Control Port Groups** tab in the left panel. Expand the **Flood Control Port Groups** tab, and select a flood control port group in the tree. The **Flood Control Port Groups** tab is displayed in the right panel.



Unicast Unknown

Select a rate, create a new rate, or edit an existing flood control rate limit for Unicast traffic.

Multicast

Select a rate, create a new rate, or edit an existing flood control rate limit for Multicast traffic.

Broadcast

Select a rate, create a new rate, or edit an existing flood control rate limit for Broadcast traffic.

Related Information

For information on related concepts:

- Getting Started with Class of Service

For information on related tasks:

- How to Create a Class of Service
- How to Configure Flood Control
- How to Create a Rate Limit

For information on related windows:

- General Tab (Rate Limit)

Class of Service Example

This Help topic provides an example of how class of service (CoS) can be configured on a network to manage bandwidth requirements of network traffic. Before you look at this example, read Getting Started with Class of Service.

In this example, an organization's network administrator needs to assure that VoIP traffic, both originating in and transiting a network of edge switches and a core router, is configured with appropriate priority, ToS, and queue treatment. We also rate limit the VoIP traffic at the edge to 1 Mb/s to guard against DOS attacks, VoIP traffic into the core at 25 Mb/s, and H.323 call setup at 5 PPS. Data traffic retains the default configuration.

This example assumes CEP authentication using H.323 for VoIP. For networks that do not authenticate VoIP end point with CEP H.323 authentication, the VoIP policy needs to be adjusted accordingly. For instance, SIP uses UDP port 5060, not the TCP port 1720.

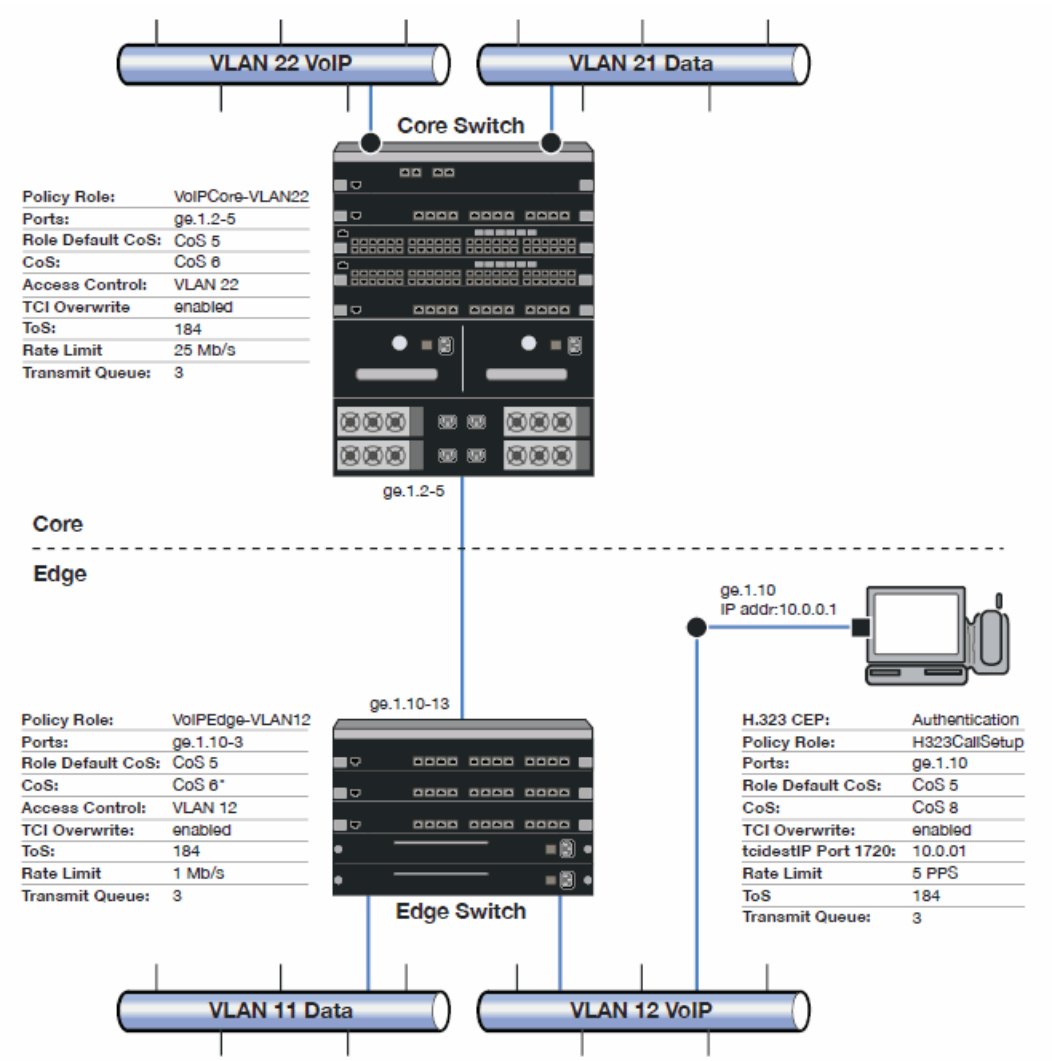
To simplify the discussion of the configuration process, this example is limited to the VoIP configuration context. The following table provides a set of sample values for priority, inbound rate limit (IRL), and transmit queue across a number

of real world traffic types. This table can be used as an aid in thinking about how you might want to apply CoS across your network. Note that Scavenger class is traffic that should be treated as less than best effort: external web traffic, for instance.

CoS Name	CoS Index	Priority	IRL		Transmit Queue					
					Queue #		Shaping		Bandwidth	
			Edge	Core	Edge	Core	Edge	Core	Edge	Core
Scavenger (Static)	0	0	15 Mb/s		0	0	10%		5%	5%
Best Effort (Static)	1	1			1	1	80%		45%	45%
Bulk Data (Static)	2	2								
Critical Data (Static)	3	3								
Network Control (Static)	4	4	40 PPS	1 Mb/s	2	2	1 Mb/s		25%	25%
Network Mgmt (Static)	5	5	2 Mb/s							
RTP/Voice/Video (Static)	6	6	1 Mb/s	25 Mb/s	3	3			25%	25%
High Priority (Static)	7	7								
VoIP Call Setup	8	7	5 PPS		3	3			25%	25%

The following figure displays the network setup for this example configuration, with the desired Profile/CoS summary for each network device. Each device is configured with VoIP and Data VLANs. Each VoIP VLAN contains four 1 -gigabit interfaces for each device.

CoS VoIP Configuration Example



Edge and Core port groups in the RTP/Voice/Video (Static) CoS provide for the difference in rate limiting needs between the end user and aggregation devices. A VoIP Call Setup CoS provides rate limiting for the setup aspect of the VoIP call.

The Edge, Core, and H.323 Call Setup roles are configured with TCI Overwrite, default CoS 5 (best default priority for voice and video), and default access control that contains traffic to the appropriate VLAN.

Use the Policy tab to configure the policy roles and related services using the following instructions. For more information, see How to Create a Class of Service and How to Define Rate Limits.

Configure the Classes of Service

Use the Class of Service tab to configure the static RTP/Voice/Video CoS with the appropriate edge and core rate limits, and create a new CoS for the call setup rate limits.

1. For the static RTP/Voice/Video CoS (CoS Index 6):
    a. Set the ToS to B8.
    b. Create two new Inbound RL port groups called Edge and Core.
    c. Set the Edge port group rate limit to 1 Mb/s and the Core port group rate limit to 25 Mb/s. (You may need to first create these rate limits.)
    d. Add the appropriate ports to each port group.
2. Create a new class of service and name it VoIP Call Setup (CoS Index 8).
    a. Set the rate limit to 5 PPS for all port groups. (You may need to first create this rate limit.)
    b. Set the ToS to B8.

Create the VoIP Core Role

For the core router, create a policy role for VoIP Core. VoIP Core policy deals with packets transiting the core network using VoIP VLAN 22.

1. Name the role VoIPCore-VLAN22.
2. Enable TCI overwrite so that ToS is rewritten for this role.
3. Set the default access control action to Contain to VLAN 22.
4. Set default Class of Service to CoS Index 5.

Create a VoIP Core Service

1. Name the service VoIPCore.
2. Add the service to the VoIPCore-VLAN22 role.

Create a Rule

1. Create a Layer 2 traffic classification rule for VLAN ID 22 within the VoIPCore service.
2. Assign the static RTP/Voice/Video CoS (CoS Index 6) as the Class of Service action for the rule.

Creating the VoIP Edge Role

For the edge switches, create a policy role for VoIP Edge. VoIP Edge policy deals with packets transiting the edge network using VoIP VLAN 12.

1. Name the role VoIPEdge_VLAN12.
2. Enable TCI overwrite so that ToS is rewritten for this role.
3. Set the default access control action to Contain to VLAN 12.
4. Set default Class of Service to CoS Index 5.

Create a VoIP Edge Service

1. Name the service VoIPEdge.
2. Add the service to the VoIPEdge_VLAN12 role.

Create a Rule

1. Create a Layer 2 traffic classification rule for VLAN ID 12 within the VoIPEdge service.
2. Assign the static RTP/Voice/Video CoS (CoS Index 6) as the Class of Service action for the rule.

Creating the H.323 Call Setup Role

The H.323 Call Setup role deals with the call setup traffic for VoIP H.323 authenticated users directly attached to the switch using link ge.1.10.

1. Name the role H323CallSetup.
2. Enable TCI overwrite so that ToS is rewritten for this policy.
3. Set default Class of Service to CoS Index 5.

Create a H.323 Call Setup Service

1. Name the service H323CallSetup.
2. Add the service to the H323CallSetup role.

Create a Rule

Create a Layer 4 traffic classification rule as follows:

1. Traffic Classification Type: IP TCP Port Destination
2. Enter in Single Value field: 1720 (TCP Port ID).
3. For IP TCP Port Destination value: 10.0.0.1 with a mask of 255.255.255.255.
4. Assign the new VoIP Call Setup CoS (CoS Index 8) as the Class of Service action for the rule.

Apply the Roles to Network Devices

Once you have created your roles, you must apply them to the network devices as follows:

Core Router

Apply the VoIPCore VLAN22 role to ports ge.1.2 5.

Edge Switch

Apply the VoIPEdge VLAN12 role to ports ge.1.10 13.

Apply the H323CallSetup role to port ge.1.10

ToS/DSCP Value Definition Chart

Use this chart to compare ToS and DSCP values.

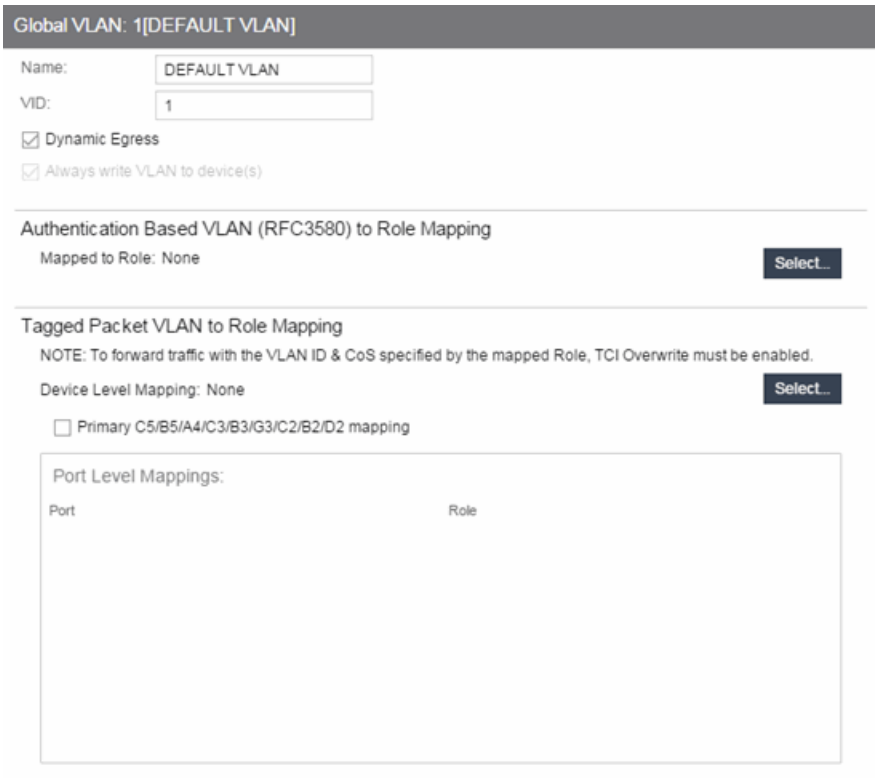
ToS (Dec)	ToS (Hex)	ToS (Binary)	ToS Precedence (Binary)	ToS Precedence (Decimal)	ToS Precedence Name	ToS Delay Flag	ToS Throughput Flag	ToS Reliability Flag	DSCP (Binary)	DSCP (Hex)	DSCP (Decimal)	DSCP Class
0	0x00	00000000	000	0	Routine	0	0	0	000000	0x00	0	none
32	0x20	00100000	001	1	Priority	0	0	0	001000	0x08	8	cs1
40	0x28	00101000	001	1	Priority	0	1	0	001010	0x0A	10	af11
48	0x30	00110000	001	1	Priority	1	0	0	001100	0x0C	12	af12
56	0x38	00111000	001	1	Priority	1	1	0	001110	0x0E	14	af13
64	0x40	01000000	010	2	Immediate	0	0	0	010000	0x10	16	cs2
72	0x48	01001000	010	2	Immediate	0	1	0	010010	0x12	18	af21
80	0x50	01010000	010	2	Immediate	1	0	0	010100	0x14	20	af22
88	0x58	01011000	010	2	Immediate	1	1	0	010110	0x16	22	af23
96	0x60	01100000	011	3	Flash	0	0	0	011000	0x18	24	cs3
104	0x68	01101000	011	3	Flash	0	1	0	011010	0x1A	26	af31
112	0x70	01110000	011	3	Flash	1	0	0	011100	0x1C	28	af32

ToS (Dec)	ToS (Hex)	ToS (Binary)	ToS Precedence (Binary)	ToS Precedence (Decimal)	ToS Precedence Name	ToS Delay Flag	ToS Throughput Flag	ToS Reliability Flag	DSCP (Binary)	DSCP (Hex)	DSCP (Decimal)	DSCP Class
120	0x78	01111000	011	3	Flash	1	1	0	011110	0x1E	30	af33
128	0x80	10000000	100	4	FlashOverride	0	0	0	100000	0x20	32	cs4
136	0x88	10001000	100	4	FlashOverride	0	1	0	100010	0x22	34	af41
144	0x90	10010000	100	4	FlashOverride	1	0	0	100100	0x24	36	af42
152	0x98	10011000	100	4	FlashOverride	1	1	0	100110	0x26	38	af43
160	0xA0	10100000	101	5	Critical	0	0	0	101000	0x28	40	cs5
184	0xB8	10111000	101	5	Critical	1	1	0	101110	0x2E	46	ef
192	0xC0	11000000	110	6	InterNetwork Control	0	0	0	110000	0x30	48	cs6
224	0xE0	11100000	111	7	Network Control	0	0	0	111000	0x38	56	cs7

Policy VLAN Tab Overview

The VLAN tab displays information about the VLAN selected in the left panel and lets you configure certain VLAN parameters. If you are using VLAN to Role mapping in your network, you can also use this tab to map the VLAN to a specific role. If you make a change on this tab, you need to enforce it.

To view this tab, select Control > Policy > VLANs and select a VLAN from the drop down.



General

This area provides general information about the VLAN and allows you to configure the VLAN.

Name

Name of the VLAN selected in the left panel.

VID

Unique number assigned to the VLAN, also called VID (for VLAN ID). This ID was either assigned by an administrator or assigned automatically by the system when the VLAN was created. The value can be anywhere between 1 and 4094, with VID 1 being reserved for the DEFAULT VLAN (a name for a particular VLAN, not to be confused with a role's assigned default VLAN).

Dynamic Egress

Dynamically add all ports which use this VLAN to this VLAN's egress list. Dynamic Egress is enabled by default in Policy Manager. Leave disabled for discard VLANs. See Dynamic Egress for more information.

Always write VLAN to device(s)

If the box is checked, the VLAN is written to the device whether the VLAN is being used in a rule or role, or not. If it is not checked, the VLAN is not written to the device unless it is being used in a rule or role. Enabling this option is a way of ensuring that the device is aware of a VLAN that is being used for something other than policy configuration, and it allows you to configure that VLAN for Dynamic Egress. If the Default VLAN (VID=1) is selected in the left panel, this option is checked and cannot be edited, as the default VLAN is always on the device.

Authentication-Based VLAN to Role Mapping

Authentication-Based VLAN to Role Mapping provides a way to assign a role to a user during the authentication process, based on a VLAN Attribute. (For more information, see VLAN to Role Mapping in the Concepts help topic.) This area displays what role (if any) the VLAN is mapped to (at the device-level) and lets you configure a mapping, if desired.

Mapped to Role

The role to which the VLAN is mapped. To select a role, click **Select**, click the **Assign RFC3580 VLAN -> Role Mapping** radio button, choose a role in the drop-down menu, and click **OK**.

Select

Opens the role Selection View, where you can choose a role to associate with the VLAN.

Tagged Packet VLAN to Role Mapping

Tagged Packet VLAN to Role Mapping provides a way to let policy-enabled devices assign a role to network traffic, based on a VLAN ID. (For more information, see VLAN to Role Mapping in the Concepts help topic.) This area displays what role (if any) the VLAN is mapped to at both the device-level and port-level, and lets you configure mappings, if desired.

NOTE: TCI Overwrite Requirement

Tagged Packet VLAN to Role Mapping will apply the Role definition to incoming packets using a mapped VLAN. This definition will apply a CoS and determine if the packet is discarded or permitted, and if TCI Overwrite is enabled will re-specify the VLAN ID defined by the Rule / Role Default. If TCI Overwrite is disabled, the packet will egress (if permitted by the Rule Hit) with the original VLAN ID it ingressed with.

If supported by the device, you can enable TCI Overwrite for an individual role in the role's General tab. The stackable devices support rewriting the CoS values but not the VLAN ID.

Device Level Mapping

The role the VLAN is mapped to at the device level (all devices). To select a role, click Select, choose a role, and click OK.

Select

Opens the role Selection View, where you can choose a role to associate with the VLAN at the device level.

Primary C2/B2/D2/C3/B3/G3/C5/B5/A4 mapping

Use this checkbox to specify that this VLAN to role mapping will be the primary mapping for C2/C3/C5 and B2/B3/B5 devices (C2 firmware version 03.02.xx and higher/B2 firmware version 02.00.16 and higher), and D2, A4, and G3 devices (G3 firmware version 6.03.xx and higher). These devices only support one device-level VLAN to role mapping. If you do not make this selection, there will be no device-level mapping for these devices.

Port Level Mappings

This table lists any port-level Tagged Packet VLAN to Role Mappings configured for this VLAN. Port-level mappings override any device-level mapping.

NOTE: This functionality is not yet enabled.

Related Information

For information on related concepts:

- Dynamic Egress
- Policy VLAN Islands

For information on related tasks:

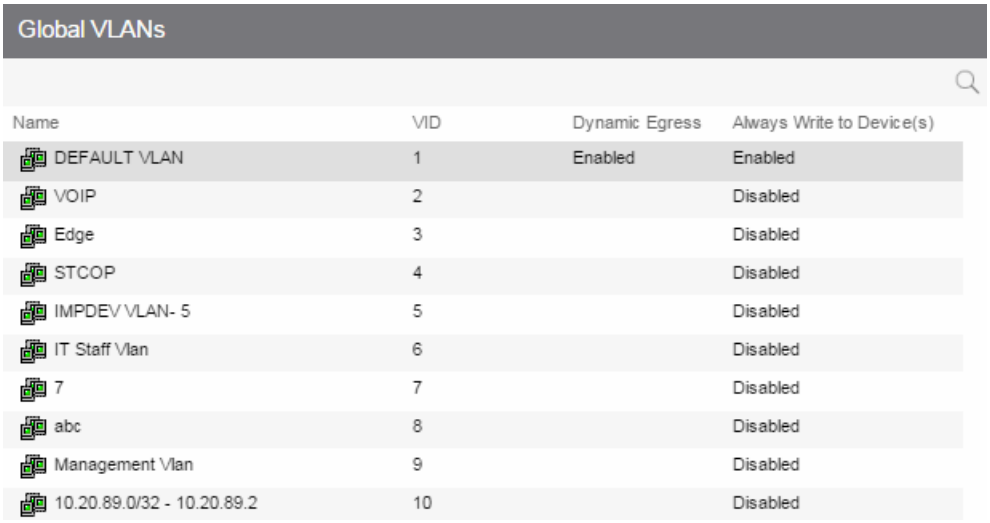
- How to Create a VLAN
- How to Create a Policy VLAN Island

Global VLANs

This tab appears when you select the **Global VLANs** tab in the **VLANs** left-panel tab. It displays a table of information about the existing VLANs.

Right-clicking the **Global VLANs** tab allows you to create a new VLAN by selecting the **Create VLAN** option, while selecting **Reload VLANs** updates the list of VLANs with the latest information.

If you right-click a VLAN in the left-panel tab or in the right-panel table, you have the option to rename and delete the selected VLAN.



Name

Name of the VLAN.

VID

Unique number assigned to the VLAN, also called VID (for VLAN ID). For Global VLANs, this ID was either assigned by an administrator or assigned automatically by the system when the VLAN is created. The value can be anywhere between 1 and 4094, with VID 1 being reserved for the DEFAULT VLAN (a name for a particular VLAN, not to be confused with a role's assigned default VLAN).

Dynamic Egress

Indicates whether the Dynamic Egress feature is on (**Enabled**) or off (**Disabled**) for the VLAN. The default is **Enabled**; therefore, this column displays **Enabled** unless a user has turned it off for a particular VLAN.

Always Write to Device(s)

If enabled, the VLAN is written to the device whether or not it is being used in a rule or role.

Related Information

For information on related tasks:

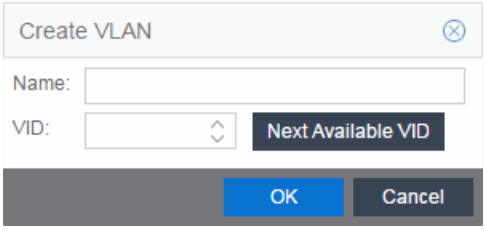
- How to Create a VLAN

For information on related windows:

- VLAN Tab
- VLAN Egress Tab (Role)

Create VLAN

This window appears when you right-click the **Global VLANs** left-panel tab and select **Create VLAN**. See How to Create a VLAN, How to Create a Policy VLAN Island, and Roles for additional information.



Name

The name for the VLAN you want to create. VLAN names can be up to 32 characters in length, including spaces. Do not create a VLAN name that uses any letters with diacritical marks. Diacritical marked letters are not supported by SNMP. VLAN names are case sensitive. For example, "Sales" and "sales" would be considered two different VLAN names. You can have multiple VLANs with the same name but with different VLAN IDs in the Policy tab.

VID

Unique numerical identifier for the VLAN, also known as VLAN ID. Can be a value between 1 and 4094, with VID1 being reserved for the DEFAULT VLAN (a name for a particular VLAN, not to be confused with a default VLAN you assign to a role). To select the next VID in sequence, click Next Available VID.

Next Available VID Button

Enters the next unassigned VID in the VLAN ID field.

Editing an existing VLAN/Class of Service

OK Button

Creates the VLAN.

Related Information

For information on related concepts:

- Dynamic Egress
- Policy VLAN Islands

For information on related tasks:

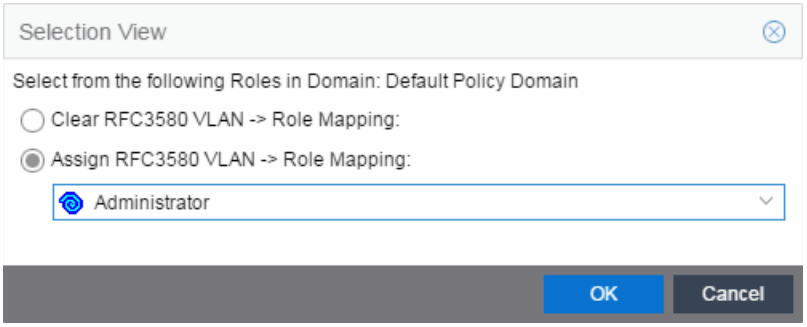
- How to Create a VLAN
- How to Create a Policy VLAN Island

For information on related windows:

- General Tab (Role)

Selection View (Roles)

The Roles Selection View appears when you are selecting a role for VLAN to role mapping. It also lets you clear the current VLAN to role mapping. To access this view, click the desired VLAN in the VLANs > Global VLANs left-panel tab, then click the Select button in the VLAN to Role Mapping section on the VLAN tab.



Clear RFC3580 VLAN -> Role Mapping

Select this option to clear the current role selection.

Assign RFC3580 -> Role Mapping

Select this option to assign a new role and make a selection from the list of available roles.

Related Information

For information on related tasks:

- Creating a Role

For information on related windows:

- General Tab (VLAN)

Policy VLAN Islands

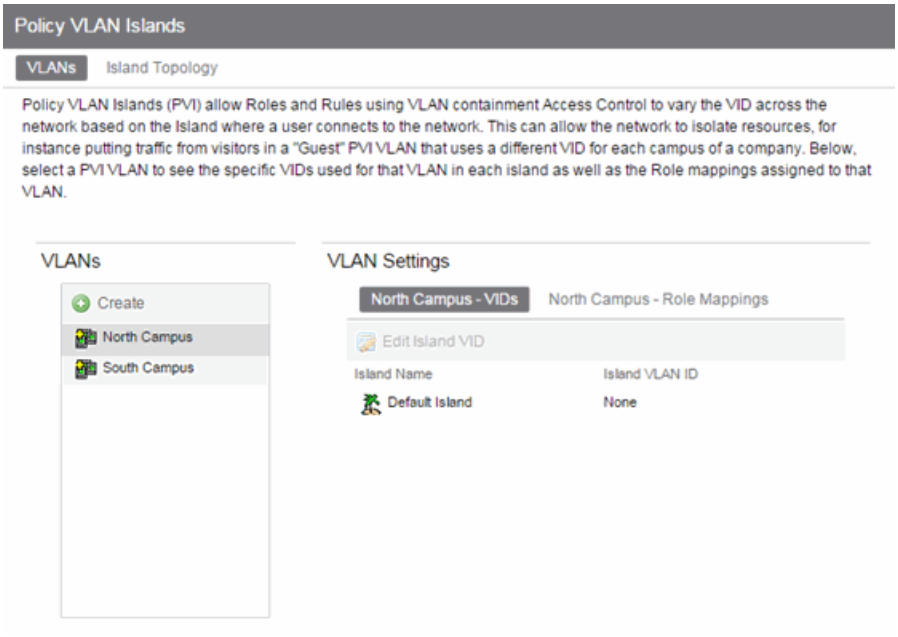
This tab displays a table of the Island VLANs being used in the Policy VLAN Island, and the names created on the devices in the island. To display this tab, select Control > Policy > VLANs > Policy VLANs Islands.

The VLANs Tab provides two sub-tabs:

- (VLAN) - VIDs Tab
- (VLAN) - Role Mappings Tab

(VLANs) - VIDs Tab

This tab provides information on VIDs assigned to specific islands. When an island is selected, the VIDs tab shows all VIDs for the defined PVI VLANs used for that island.



VLANs

Name of all defined VLANs. Select a VLAN to see the policy VLAN islands in the VLAN Settings section of the window and the VIDs with which that island is associated.

Create

Opens the Create VLAN window from which you can create a PVI VLAN. Unlike global VLANs, PVI VLANs are not created by the Policy tab during enforce. It is left to the user to configure these on the device(s) externally. The Policy tab only associates the appropriate VIDs to the rules during enforce.

Island Name

Shows the names of all VLAN Islands for the PVI VLAN selected in the VLANs section of the window.

Island VLAN ID

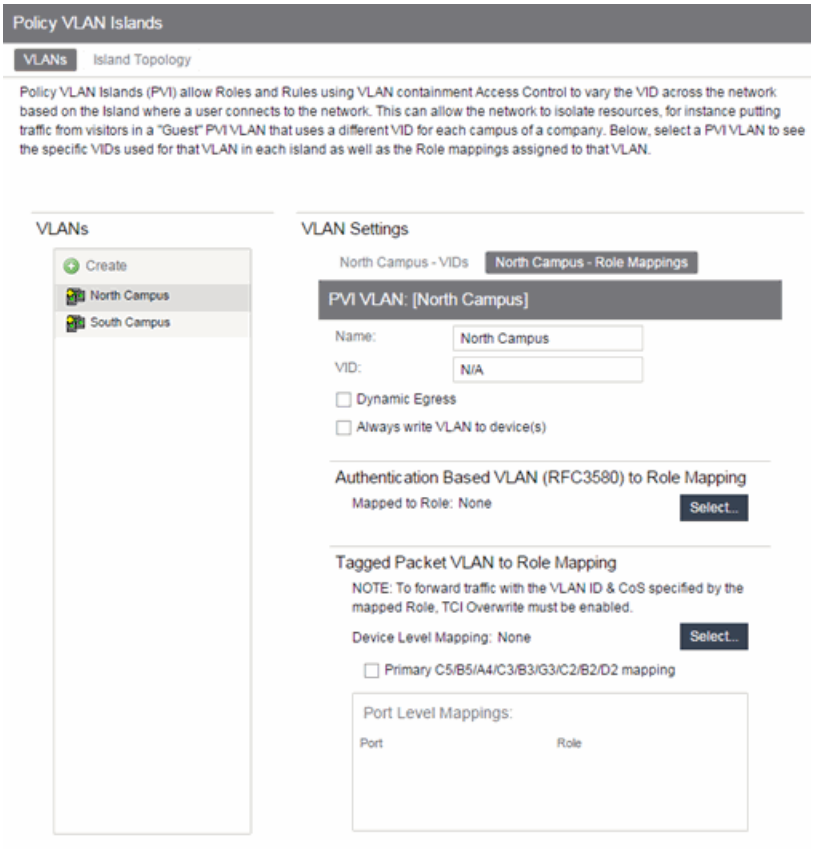
Shows the VID used for this PVI VLAN in this Island.

Edit Island VLAN ID

Selecting an island in the table and clicking this button opens the Edit Island VLAN ID window, where you can change the VID for the Island VLAN.

(VLANs) - Role Mappings Tab

This tab displays the role mappings for the Policy VLAN Island.



General

This area provides general information about the VLAN and allows you to configure the VLAN.

Name

Name of the VLAN selected in the left panel.

VID

Unique number assigned to the VLAN, also called VID (for VLAN ID). This ID was either assigned by an administrator or assigned automatically by the system when

the VLAN was created. The value can be anywhere between 1 and 4094, with VID 1 being reserved for the DEFAULT VLAN (a name for a particular VLAN, not to be confused with a role's assigned default VLAN).

Dynamic Egress

Dynamically add all ports which use this VLAN to this VLAN's egress list. Dynamic Egress is enabled by default in Policy Manager. Leave disabled for discard VLANs. See Dynamic Egress for more information.

Always write VLAN to device(s)

If the box is checked, the VLAN is written to the device whether the VLAN is being used in a rule or role, or not. If it is not checked, the VLAN is not written to the device unless it is being used in a rule or role. Enabling this option is a way of ensuring that the device is aware of a VLAN that is being used for something other than policy configuration, and it allows you to configure that VLAN for Dynamic Egress. If the Default VLAN (VID=1) is selected in the left panel, this option is checked and cannot be edited, as the default VLAN is always on the device.

Authentication-Based VLAN to Role Mapping

Authentication-Based VLAN to Role Mapping provides a way to assign a role to a user during the authentication process, based on a VLAN Attribute. (For more information, see VLAN to Role Mapping in the Concepts help topic.) This area displays what role (if any) the VLAN is mapped to (at the device-level) and lets you configure a mapping, if desired.

Mapped to Role

The role to which the VLAN is mapped. To select a role, click Select, click the Assign RFC3580 VLAN -> Role Mapping radio button, choose a role in the drop-down menu, and click OK.

Select

Opens the role Selection View, where you can choose a role to associate with the VLAN.

Tagged Packet VLAN to Role Mapping

Tagged Packet VLAN to Role Mapping provides a way to let policy-enabled devices assign a role to network traffic, based on a VLAN ID. (For more information, see VLAN to Role Mapping in the Concepts help topic.) This area displays what role (if any) the VLAN is mapped to at both the device-level and port-level, and lets you configure mappings, if desired.

NOTE: TCI Overwrite Requirement

Tagged Packet VLAN to Role Mapping will apply the Role definition to incoming packets using a mapped VLAN. This definition will apply a CoS and determine if the packet is discarded or permitted, and if TCI Overwrite is enabled will re-specify the VLAN ID defined by the Rule / Role Default. If TCI Overwrite is disabled, the packet will egress (if permitted by the Rule Hit) with the original VLAN ID it ingressed with.

If supported by the device, you can enable TCI Overwrite for an individual role in the role's General tab. The stackable devices support rewriting the CoS values but not the VLAN ID.

Device Level Mapping

The role the VLAN is mapped to at the device level (all devices). To select a role, click **Select**, choose a role, and click **OK**.

Select

Opens the role Selection View, where you can choose a role to associate with the VLAN at the device level.

Primary C2/B2/D2/C3/B3/G3/C5/B5/A4 mapping

Use this checkbox to specify that this VLAN to role mapping will be the primary mapping for C2/C3/C5 and B2/B3/B5 devices (C2 firmware version 03.02.xx and higher/B2 firmware version 02.00.16 and higher), and D2, A4, and G3 devices (G3 firmware version 6.03.xx and higher). These devices only support one device-level VLAN to role mapping. If you do not make this selection, there will be no device-level mapping for these devices.

Port Level Mappings

This table lists any port-level Tagged Packet VLAN to Role Mappings configured for this VLAN. Port-level mappings override any device-level mapping.

NOTE: This functionality is not yet enabled.

Related Information

For information on related concepts:

- Policy VLAN Islands
- VLAN to Role mapping

For information on related tasks:

- How to Create a Policy VLAN Island

Add Devices (VLAN Islands)

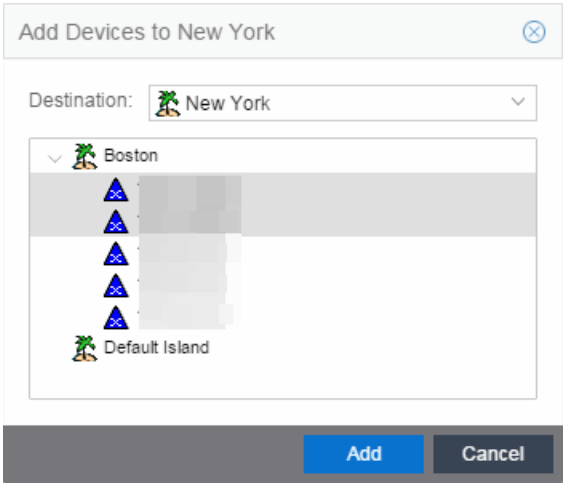
This window enables you to add devices to VLAN islands.

To access the window:

1. Click the **VLANs > Policy VLAN Islands** tab in the left panel.
2. Select the **Island Topology** tab in the Policy VLAN Islands right panel.
3. Select the Default Island - Devices tab in the Island Settings section of the window.
4. Click the **Add Devices** button.

Devices contained in an island are assigned a VID for each Island VLAN unique to the island, allowing roles and rules which use the Island VLANs to isolate users to that island. A device must always belong to an island, and shares a common VID assignment for the Island VLANs with all other devices contained in that island.

To add a device to an island, select the Island to which the device is to be added in the **Destination** drop-down menu, select the device in the Devices section, and click **Add**. You can also select and add multiple devices.



Destination

Select the VLAN Island to which the device is to be added.

Devices Section

Expand the Island folder from which the VLAN Island is being selected to add the device or devices.

Add Button

Adds the device(s) selected in the Devices panel to the island selected in the Islands panel.

Related Information

For information on related concepts:

- Policy VLAN Islands

For information on related tasks:

- How to Create a Policy VLAN Island

Extreme Management Center Island Topology (Policy VLAN Islands)

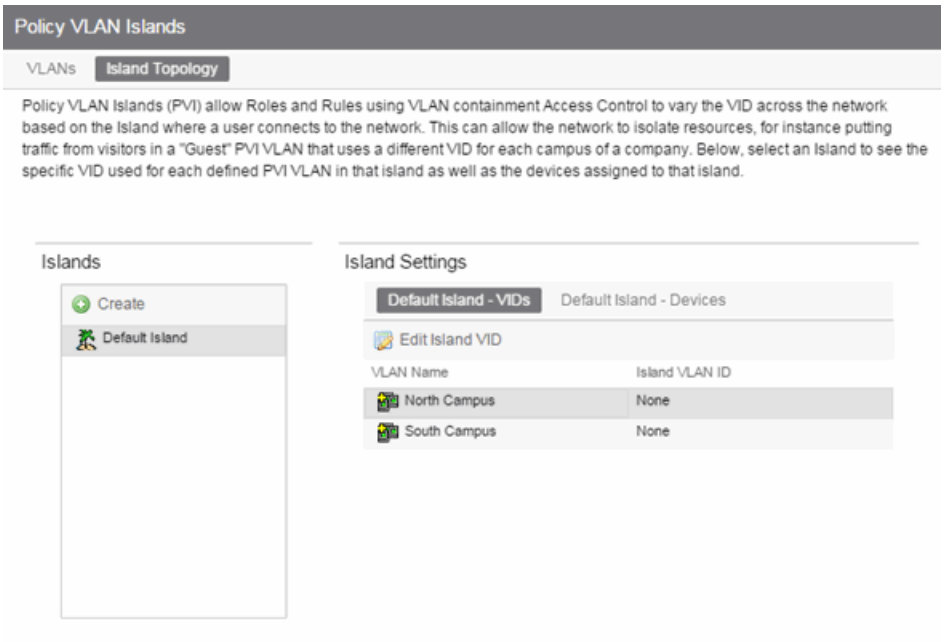
This tab displays a table of information about the Policy VLAN Islands, which shows the VIDs used in the selected island for all defined PVI VLANs. To access this tab, select the Policy VLAN Islands node in the tree of the Access Control Configuration view, and select the Island Topology tab on the right panel.

The Island Topology tab provides two sub-tabs:

- (Island) - VIDs Tab
- (Island) - Devices Tab

(Island) - VIDs Tab

This tab provides information on VIDs assigned to specific islands. When an island is selected, the VIDs tab shows all VIDs for the defined PVI VLANs that will be used for that island.



Islands

Name of all defined PVI islands. Select an island to see the VIDs and devices associated with that Island.of the VLAN island in which the Island VLAN is being used.

VLAN Name

Shows the defined PVI VLANs in the Domain. Unlike global VLANs, PVI VLANs are not created by the Policy tab during enforce. It is left to the user to configure these on the device(s) externally. The Policy tab only associates the appropriate VIDs to the rules during enforce.

Island VLAN ID

Shows the VID used for this PVI VLAN in this Island.

Edit Island VLAN ID

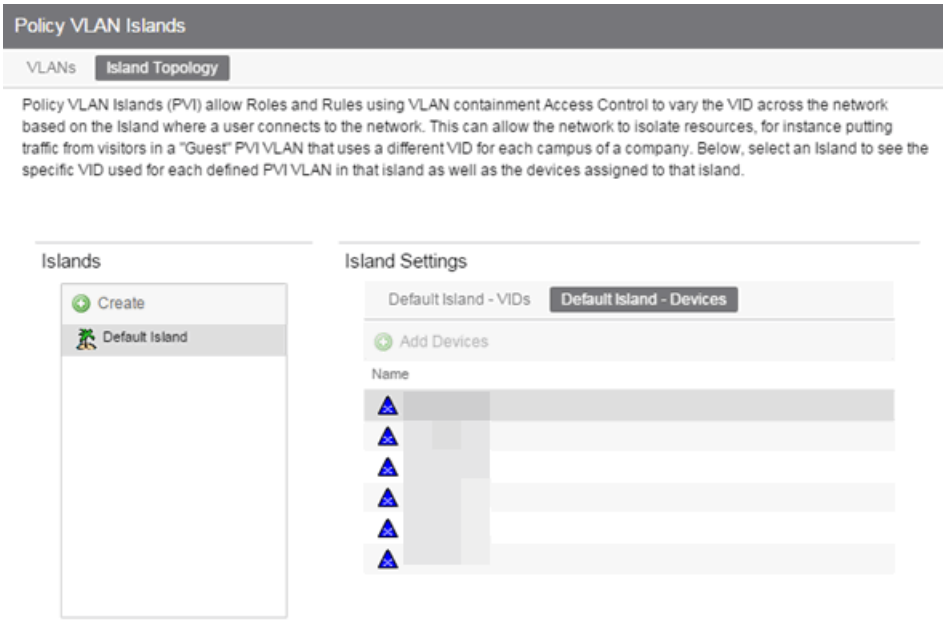
Selecting an island in the table and clicking this button opens the Edit Island VLAN ID window, where you can change the VID for the Island VLAN.

Create

Opens the Create VLAN Island dialog. For more information, see Creating a VLAN Island.

(Island) - Devices Tab

This tab displays the devices that are part of a Policy VLAN Island. To see a menu of options for a device in the table, right-click the device.



Create

Opens the Create VLAN Island dialog. For more information, see Creating a VLAN Island.

Name

The device's IP address.

Add Devices

Opens a separate dialog to add devices to specific Islands. For more information, see Add/Remove Devices window.

Related Information

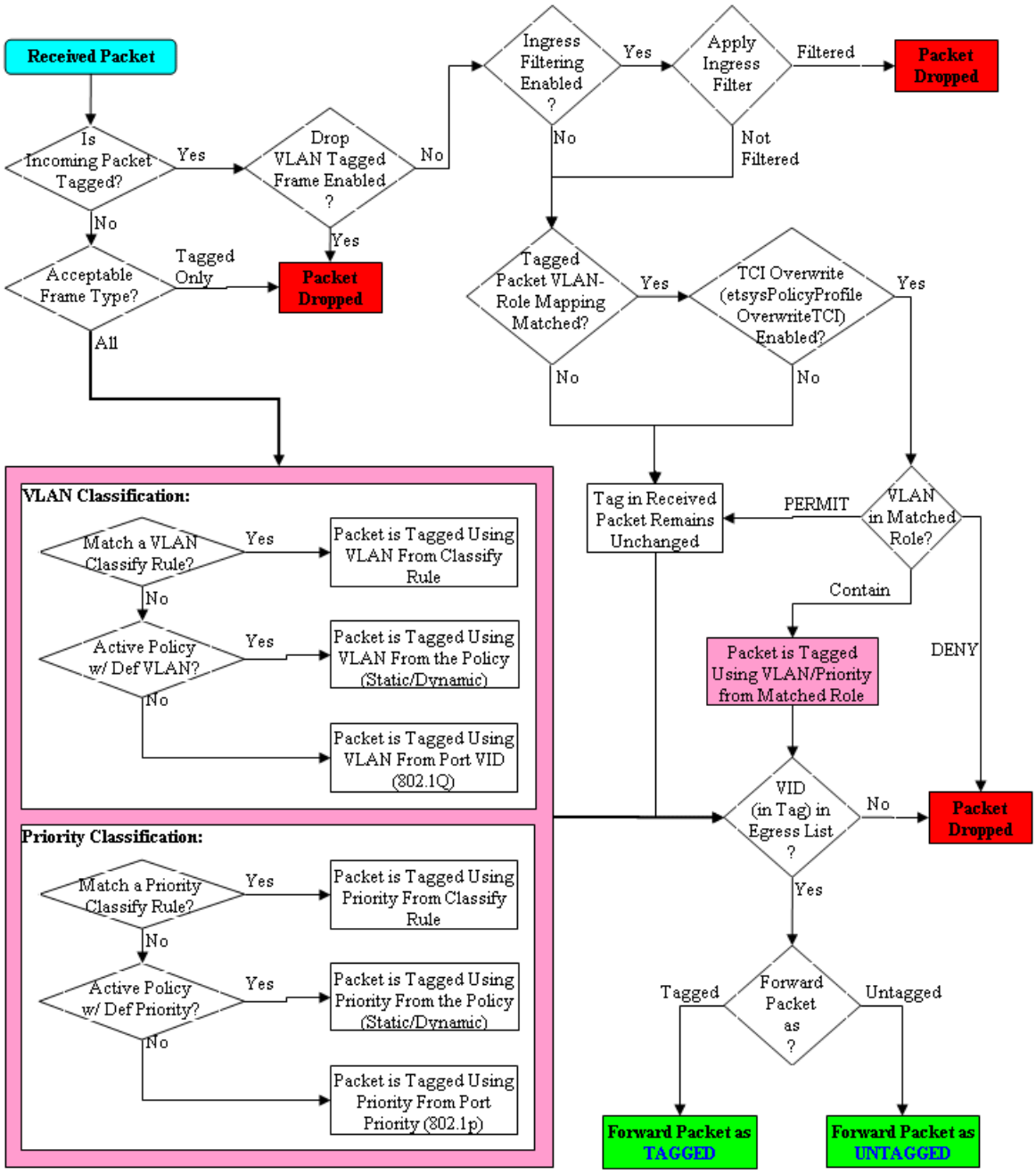
For information on related concepts:

- Policy VLAN Islands
- Network Resource Groups

For information on related tasks:

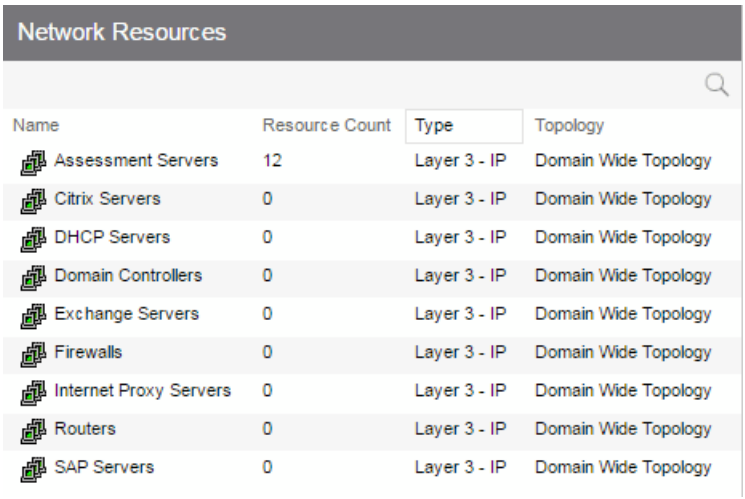
- How to Create a Policy VLAN Island
- How to Create a Network Resource Group

Extreme Management Center Packet Flow Diagram



Extreme Management Center Network Resources Tab Overview

The **Network Resources** tab displays a table of information about all the network resources in the current domain. To access this tab, select the **Network Resources > Network Resources** left-panel tab on the **Policy** tab. The Details View is displayed in the right panel. Right-click a network resource to rename or delete it. See How to Create a Network Resource for more information on topologies and islands.



Name

Name of the network resource group.

Resource Count

The number of addresses added to the network resource.

Type

The network resource type:

- Layer 2 MAC - Define a group of network resource MAC addresses.
- Layer 3 IP - Define a group of network resource IP addresses.

Topology

The network resource topology for this group.

Related Information

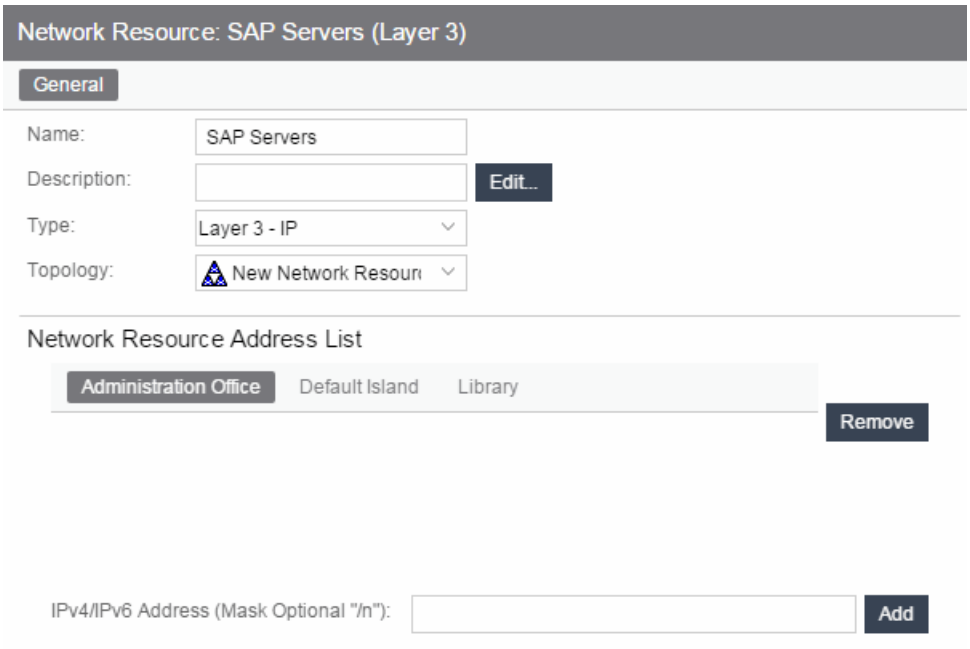
For information on related windows:

- General Tab (Network Resources)
- How to Create a Network Resource

Extreme Management Center Network Resource Group General Tab

This tab lets you configure a network resource group, which is a group of network resource devices associated with an Automated service. You configure the group by selecting a network resource type (MAC or IP) and typology, and then creating a list of MAC or IP addresses for the resources that are part of the group. Once a network resource group is defined, you can associate it with the desired Automated service (see How to Create a Service for more information).

To access this tab, select a network resource group in the Network Resources left-panel tab of the Policy tab.



Name
Name of the network resource group selected in the left panel.

Description
Use the Edit button to open a window where you can add or modify a description for the network resource group.

Type
Select the network resource type:

- Layer 2 MAC - Define a group of network resource MAC addresses.
- Layer 3 IP - Define a group of network resource IP addresses.

Topology
Use this drop-down menu to select a network resource topology for this group. Use the configuration menu button on the right to add a new topology or edit an existing topology.

Network Resource Address List
Lists the addresses included in the selected network resource. Use the address field (IPv4 or IPv6, depending on the selected type) and click the Add button to add a new resource to the list.

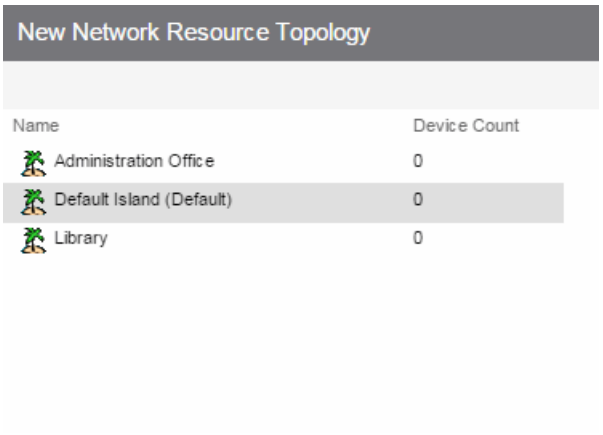
Related Information

For information on related tasks:

- How to Create a Network Resource Group
- How to Create a Service

Extreme Management Center Network Resource Topology Tab

This tab appears when you select a Network Resource Topology in the left panel of the Network Resources tab. It displays a list of the islands defined for the topology and the number of devices assigned to each island. See How to Create a Network Resource for more information on topologies and islands.



Name
Name of the topology island.

Device Count
The number of devices included in that island.

Related Information

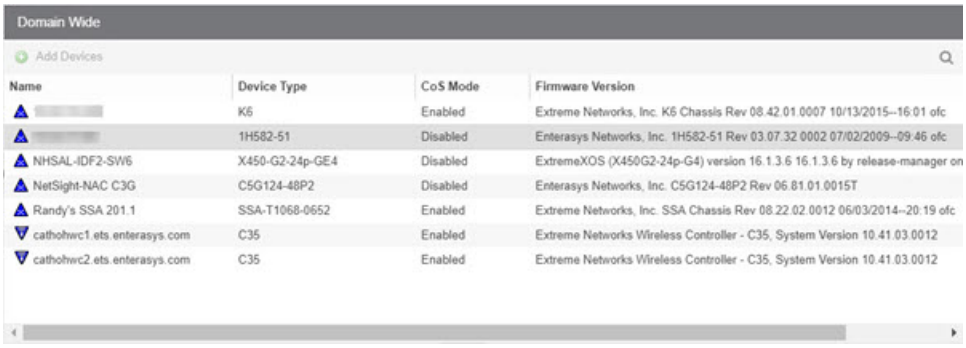
For information on related windows:

- General Tab (Network Resource Group)
- How to Create a Network Resource

Extreme Management Center Network Resource Topology Island Domain Wide

---

The Domain Wide tab displays a table of information about all the devices in an island within the network resource topology selected in the left panel. To access this tab, select a network resource island in a network resource topology on the Network Resources > Network Resource Topologies left-panel tab on the Policy tab. The Domain Wide view is displayed in the right panel. To see a menu of options available for a device, right-click the device.



Name

Name of the device, or its IP address if it does not have a display name.

Device Type

Indicates the type of device. Certain devices may be listed as "Authentication Only" (supports 802.1X and RFC 3580 only; does not support Policy).

CoS Mode

Shows whether the Class of Service mode has been enabled or disabled on the device.

Firmware Version

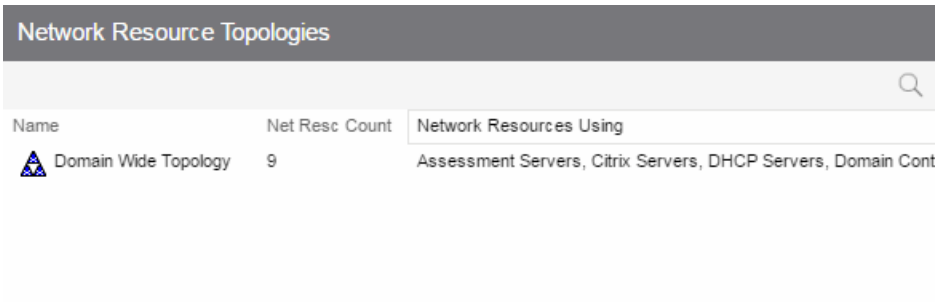
Shows the current firmware revision for this device.

Add Devices Button

Click the Add Devices button to add devices to the network resource topology.

Extreme Management Center Details View (Network Resource Topologies Folder)

This tab appears when you select Network Resources > Network Resource Topologies in the left panel of the **Policy** tab. It displays a table of information about the network resource topologies configured in the current domain. See How to Create a Network Resource for more information on topologies.



Name
Name of the network resource topology.

Net Resc Count
The number of network resource groups using this topology.

Network Resources Using
The names of the network resource groups using this topology.

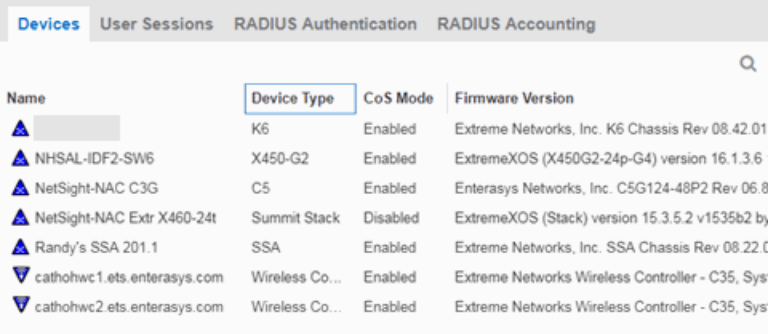
Related Information

For information on related windows:

- General Tab (Network Resource Group)
- How to Create a Network Resource

Extreme Management Center Devices (Devices)

The Devices tab displays a table of information about all the devices in the current domain. To access this tab, select the Devices/Port Groups > Devices left-panel tab on the Policy tab. The Details View is displayed in the right panel. To see a menu of options available for a device, right-click the device.



Name
Name of the device, or its IP address if it does not have a display name.

Device Type
Indicates the type of device. Certain devices may be listed as "Authentication Only" (supports 802.1X and RFC 3580 only; does not support Policy).

CoS Mode
Indicates whether Class of Service is enabled or disabled on the device.

Firmware Version
Shows the current firmware revision for this device.

Related Information

For information on related windows:

- Details View Tabs

Extreme Management Center User Sessions (Devices)

The device User Sessions panel displays information related to end user login sessions for a device.

This tab can be accessed in a variety of ways:

1. Select a device in the left-panel Devices tab, then click the User Sessions tab in the right panel.
2. Select the My Network navigation tree in the left panel, select a device in the Devices list, and right-click the device or open the tools menu and select View > User Sessions.
3. Open the Control > Policy tab, select Devices in the left panel, and select the User Sessions tab in the right panel.

User Sessions Tab

This tab displays information about each login session for the ports on the device, including the current values being collected for a session still in progress, or the final values for the last valid session when there is no session currently active.

Checking the Show Only Active Sessions checkbox displays only your active sessions. Deselect the checkbox to display all entries. Active sessions applied to traffic are listed in blue text. Active sessions not being applied are listed in green text.

Some devices support multiple authentication sessions simultaneously per interface. This allows a single user to authenticate via 802.1X, Web-Based, MAC, and CEP all at the same time. However, only one authentication type per interface can be *applied* at a single time. The multi-user authentication type precedence (configured on the device Authentication tab) determines which type is applied. The applied session is the one that provides the role and traffic classification information. The remaining non-applied sessions will only be used if the currently applied session is terminated. For example, if a user authenticates on a port that has multi-user authentication enabled (802.1X, Web-Based, and MAC) the active/applied session will be displayed in blue text and the other two

sessions will be in green text. Another example would be if the user authenticates using the MAC authentication type but MAC authentication is disabled on the port, the session would be listed in green text. For devices that do not support multi-authentication, by definition the active session is also applied.

NOTE: Devices configured for multi-user authentication always list *only* active sessions even if the Show Only Active Session checkbox is deselected.

Session entries are collected up to the maximum allowed. When the maximum is reached, the oldest session entries are replaced with newer ones. The exception to this is the RoamAbout R2, where older session data is not kept.

For devices that support one authenticated user per port, only one user/current role per port appears in the table. For devices that support multiple authenticated users per port, all users authenticated on its ports are listed in the table, along with the roles under which they are authenticated.

Session Status
The status of the device.

Switch IP
The IP address or name of the device.

Switch Port
A description of the port.

Switch Alias
The alias (ifAlias) for the interface, is one is assigned.

Type
The authentication type of this login session: Web-Based, 802.1X, MAC, CEP, Quarantine, Auto Tracking, or Role Override. If Role Override is displayed, it signifies that a rule has been applied to the port, overriding the user's current role with a different role.

- Role Override (MAC) signifies that a MAC address rule has been applied to the port, overriding the Default role or any authenticated role assigned to the end user.
- Role Override (IP) signifies that an IP address rule has been applied to the port, overriding the Default role or any authenticated role assigned to an end user

authenticated with Single User 802.1X. An IP Address rule will not override the authenticated role for any authentication type other than Single User 802.1X.

MAC Address

The MAC address of the remote user of this login session.

IP Address

For web-based authentication sessions, this column displays the IP address of the remote user of this login session.

Hostname

The hostname of the remote user of this login session. To determine the hostname, the Policy tab takes the IP address (when available) and uses the hostname cache on the Extreme Management Center server. The hostname cache must be explicitly enabled by selecting the Enable Name Resolution checkbox in the Administration > Options > tab (by default, this option is disabled).

Role

The role under which the user authenticated on the port. If the user authenticated via RFC 3580 VLAN Authorization, this column displays the role the VLAN is mapped to (configured through Authentication-based VLAN to Role Mapping). If VLAN to Role mapping has not been configured, the port's Default role is displayed (if there is one); otherwise, the column displays "N/A."

Default VID Source

When traffic received on a port doesn't match any rules, it is assigned the default VLAN ID. This column indicates the source for the default VLAN ID:

- Policy Default Access Control - The role assigned to the session defines the default VLAN ID via its Default Access Control.
- PVID - If the role assigned to the session has no Default Access Control specified, then the 802.1Q PVID for the port is assigned to the traffic.

Default VID

Displays the VLAN ID that comes from the source listed in the Default VLAN ID Source column: Permit (4095), Deny (VLAN ID #), or Contain (VLAN ID #).

RFC3580 VID

If the user authenticated via RFC 3580 VLAN Authorization, this is the VLAN ID that was returned from the RADIUS server. A VLAN ID value of 0 indicates that no VLAN was assigned. If VLAN authentication is not supported on the device, this column will display "N/A."

VLAN Oper Egress

The modification that will be made to the VLAN egress list for the VLAN ID returned by the RADIUS server, if the user authenticated via RFC 3580 VLAN Authorization.

- None - No modification to the VLAN egress list will be made.
- Tagged - The port will be added to the list with the egress state set to Tagged (frames will be forwarded as tagged).
- Untagged - The port will be added to the list with the egress state set to Untagged (frames will be forwarded as untagged).
- Dynamic - The port will use information returned in the RADIUS response to modify the VLAN egress list.

If VLAN authentication is not supported on the device, this column will display "N/A."

Start Time

The time and date when the login session started.

Duration

The duration of the user's login session, in the format D + HH:MM:SS.

Auth Status

The authentication status of the login session. Possible values are:

- Authentication Successful
- Authentication Failed
- Authentication in Progress
- Authentication Server Timeout
- Authentication Terminated

Terminate Cause

The reason the login session terminated. For web-based authentication, the possible values are:

- Administratively Terminated
- Authorization Revoked
- Link Down
- Not Applicable
- Port Disabled

- Unknown Termination Cause
- User Logged Out

For 802.1X authentication, the possible values are:

- Authorization Revoked
- Client Restarted
- Link Down (or Lost Carrier)
- Not Applicable
- Port Disabled
- Port Reinitialized
- Reauthentication Failed
- Unknown Termination Cause
- User Logged Out

Authentication Server

The RADIUS server that authenticated the session.

Related Information

For information on related concepts:

- MAC Locking
- Getting Started with Class of Service

For information on related tasks:

- Defining Rate Limits

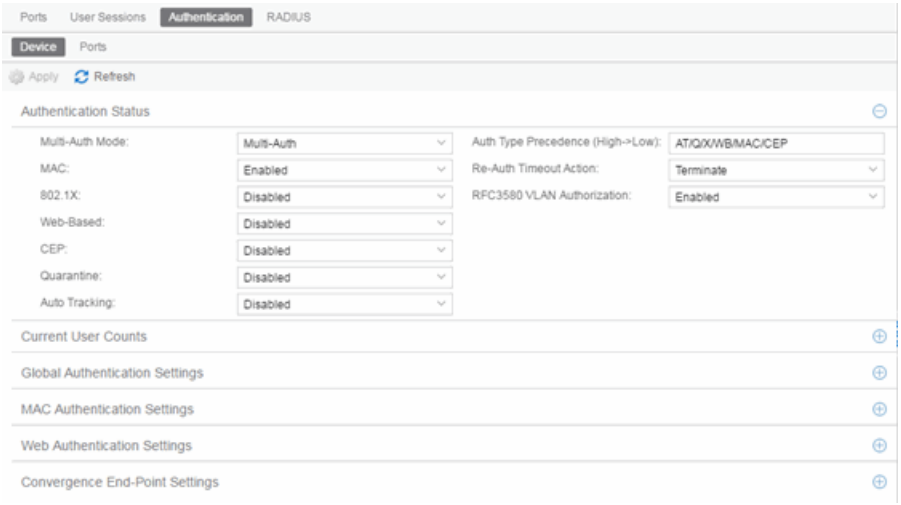
For information on related windows:

- General Tab (Rate Limit)

Extreme Management Center Authentication (Device)

The device **Authentication** tab enables you to configure and change the authentication settings on the selected device. Authentication must be configured and enabled on the device in order for individual port authentication settings to take effect (see How to Configure Ports).

To access this tab, select a device in the left panel under Devices > Devices, then click the **Authentication** tab in the right panel.



Apply

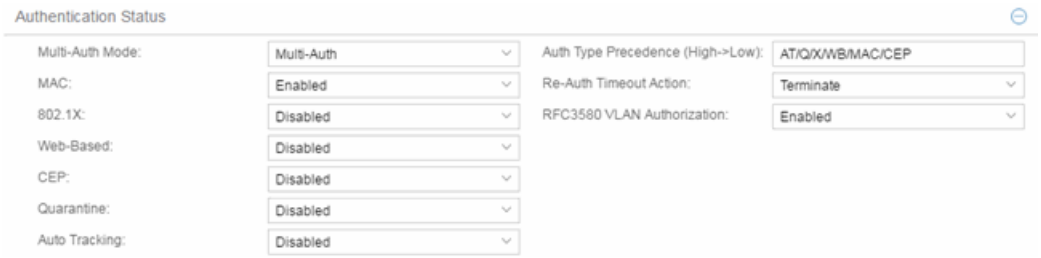
Click this button to save any changes you made to the **Authentication** tab.

Refresh

Click this button to update the tab with your changes.

Authentication Status

Use this section to select the authentication mode and types used on the device.



Use the fields on the left side of this section to select the appropriate single- or multi-user authentication types. Only options supported by the selected device are available for selection. Some devices support multiple authentication types and multiple users (Multi-User Authentication) per port, while others are restricted to only one or two authentication types and single users per port. Refer to the Firmware Support tables for information on the authentication types supported by each device type.

WARNING: Switching Authentication Types, or changing the Authentication Status from Enabled to Disabled, logs off any currently authenticated users.

Auth Type Precedence (High->Low)

This displays the order in which the authentication types are attempted on the device, with the authentication type on the left having the highest precedence (attempted first). You can edit the precedence order by clicking the field. In the Edit Precedence window, select the authentication type you want to position, and use the Up and Down buttons to arrange the types in the desired order of precedence.

WARNING: Leave the default precedence, if possible. Changing the Quarantine precedence to be lower than any other type or changing the Auto Track precedence to be higher than any other type may cause problems.

Re-Auth Timeout Action

This setting defines the action for sessions that need to be re-authenticated if the RADIUS server re-authentication request times out. Select the Terminate option to terminate the session or the None option to allow the current session to continue without disruption.

Maximum Number of Users

This setting applies to devices with Multi-User as their configured authentication type. The maximum number of users that can be actively authenticated or have authentications in progress at one time on this device. You can specify the

maximum number of users per port on the port's Port Properties Authentication Configuration tab.

RFC3580 VLAN Authorization

This allows you to enable and disable RFC 3580 VLAN Authorization for the selected device. RFC 3580 VLAN Authorization must be enabled on devices in networks where the RADIUS server is configured to return a VLAN ID when a user authenticates.

When RFC 3580 VLAN Authorization is enabled:

- devices that do **not** support policy tag packets with the VLAN ID.
- devices that support both policy and Authentication-Based VLAN to Role Mapping classify packets according to the role to which the VLAN ID maps.

Current User Counts

This section allows you to specify the maximum number of users on the device and per authentication type.

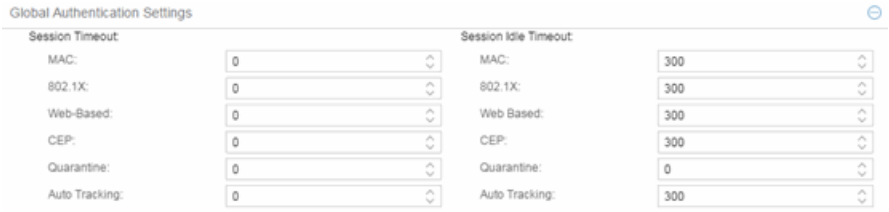
Current Number of Users

For devices with Multi-User as their configured authentication type. The current number of users that are actively authenticated or have authentications in progress, or that the device is keeping authentication termination information for. Any unauthenticated traffic on the port is not included in this count.

NOTE: On E1 and E6/E7 devices, if both 802.1X and MAC authentication are enabled, it is possible for the device to receive a start or response 802.1X packet while a MAC authentication is in progress. If this happens, the device immediately terminates the MAC authentication, and the 802.1X authentication proceeds to completion. Regardless of the success of the 802.1X login attempt, no new MAC authentication logins may occur on the port until 1) the link is toggled; 2) the user executes an 802.1X logout; or 3) the 802.1X session is terminated administratively.

Global Authentication Settings

This section lets you set session timeout and session idle timeout values for each authentication type.



Session Timeout

This setting represents the maximum number of seconds an authenticated session may last before automatic termination of the session. A value of zero indicates that no session timeout applies. This value may be superseded by a session timeout value provided by the authenticating server. For example, if a session is authenticated by a RADIUS server, that server may send a session timeout value in its authentication response.

NOTE: Non-zero values are rounded to the nearest non-zero multiple of 10 by the device.

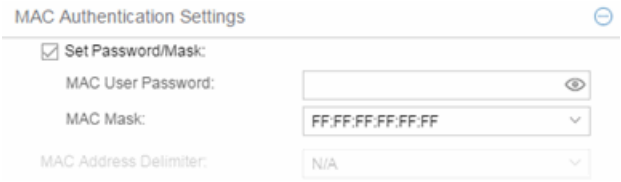
Session Idle Timeout

This displays the maximum number of consecutive seconds an authenticated session may be idle before Extreme Management Center automatically terminates the session. A value of zero indicates that no idle timeout applies. This value may be superseded by an idle timeout value provided by the authenticating server. For example, if a session is authenticated by a RADIUS server, that server may send an idle timeout value in its authentication response.

MAC Authentication Settings

This section enables you to set up the MAC password for MAC authentication. In order for MAC authentication to work, you must also configure the RADIUS

server with the MAC password as well as the MAC addresses which are allowed to authenticate.



Set Password/Mask

Select this checkbox to set a password and mask for MAC authentication.

MAC User Password

The password passed to the RADIUS server for MAC authentication.

MAC Mask

You can select a mask to provide a way to authenticate end-systems based on a portion of their MAC address. For example, you could specify a mask that would base authentication on the manufacturers ID portion of the MAC address. The MAC Mask is passed to the RADIUS server for authentication after the primary attempt to authenticate using the full MAC address fails.

MAC Address Delimiter

The character used between octets in a MAC address:

- None — No delimiter is used in the MAC address (e.g. xxxxxxxxxxxx).
- Hyphen — A hyphen is used as a delimiter in the MAC address (e.g. xx-xx-xx-xx-xx-xx).

Web Authentication Settings

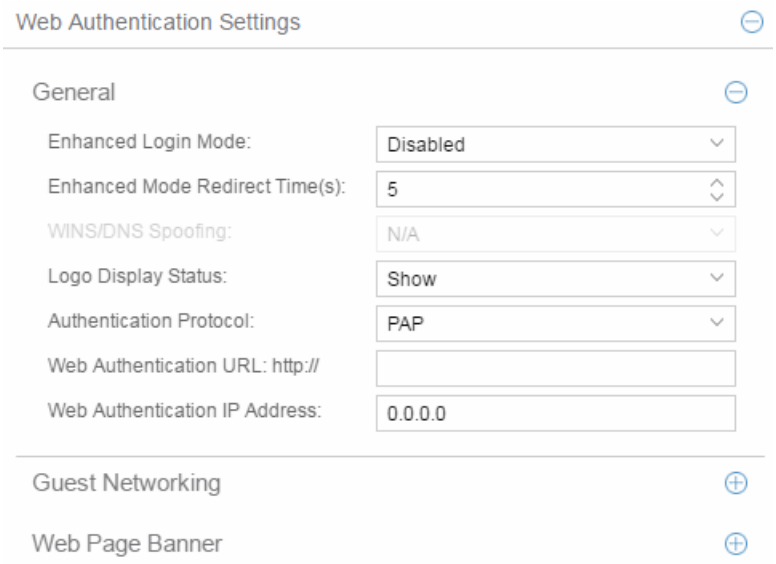
For users of web-based authentication, this tab lets you specify web authentication parameters using three sections:

- General
- Guest Networking
- Web Login

General

The General section lets you specify the URL of the authentication web page and the IP address of the system where it resides. It also lets you enable certain

web authentication features, such as Enhanced Login Mode, on devices that support those features.



Enhanced Login Mode

Enabling the Enhanced Login Mode causes the authentication web page to be displayed regardless of whether the URL or IP address entered into the browser by the end user is the designated Web Authentication URL or IP address. This option is grayed out if the device does not support the mode.

Enhanced Mode Redirect Time(s)

This setting applies for devices with Enhanced Login Mode enabled. It specifies the amount of time (in seconds) before the end-user is redirected from the authentication web page to their requested URL.

An end-system using DHCP requires time to transition from the temporary IP address issued by the authentication process to the official IP address issued by the network. Enhanced Mode Redirect Time specifies the amount of time allowed for the end-system to complete this process and begin using its official IP address.

For example, if an end-user (in Enhanced Login Mode and a Redirect Time of 30 seconds) enters the URL of "http://ExtremeNetworks.com", the user is presented the authentication web page. When the user successfully authenticates into the network, the user sees a login success page that displays "Welcome to the Network. Completing network connections. You will be redirected to http://ExtremeNetworks.com in approximately 30 seconds."

WINS/DNS Spoofing

This setting allows you to enable and disable WINS/DNS spoofing for the selected device. Spoofing allows the end-user to resolve the Web Authentication URL name to the IP address using WINS/DNS. The default is Disabled. This option is grayed out if not supported by the device.

Logo Display Status

Specifies whether the Extreme Networks logo is displayed or hidden on the authentication web page window. This option is grayed out if not supported by the device.

Authentication Protocol

This setting is the authentication protocol being used (PAP or CHAP). PAP (Password Authentication Protocol) provides an automated way for a PPP (Point-to Point Protocol) server to request the identity of user, and confirm it via a password. CHAP (Challenge Handshake Authentication Protocol), the more secure of the two protocols, provides a similar function, except that the confirmation is accomplished using a challenge and response authentication dialog.

Web Authentication URL

This is the URL for your authentication web page. Users wishing to receive network services access the web page from a browser using this URL. The http:// is supplied. Alphabetical characters, numerical characters and dashes are allowed as part of the URL, but dots are not. The URL needs to be mapped to the Web Authentication IP address in DNS or in the hosts file of each client. It must be resolvable via DNS/WINS, either on the device or at corporate, assuming the Web Authentication mapping has been set up on the corporate DNS/WINS service. This option is grayed out if not supported by the device.

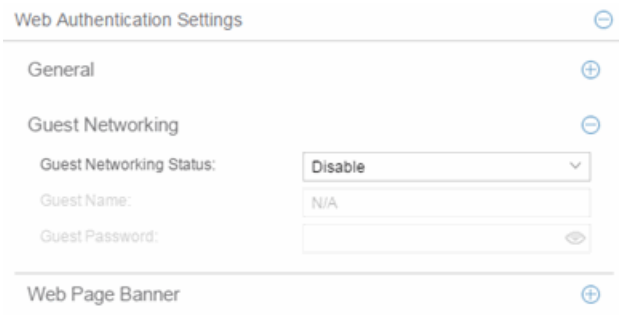
Web Authentication IP Address

This is the IP address of your authentication web page server. If you have specified a Web Authentication URL, the IP address needs to be mapped to the URL in DNS or in the host file of each client.

Guest Networking

The Guest Networking section lets you configure guest networking, a feature that allows any user to access the network and obtain a guest policy without having to know a username or password. The user accesses the authentication web page, where the username and password fields are automatically filled in, allowing them to log access as a guest. If the user does not want to log in as a guest, they can type in their valid username and password to log in.

NOTE: Guest networking is designed for networks using web-based authentication, with port mode set to Active/Discard.



Guest Networking Status

Use the drop-down list to specify guest networking status:

- Disable — Guest networking is unavailable.
- Local Auth — Guest Networking is enabled. The user accesses the authentication web page where the username field is automatically filled in with the specified Guest Name. Once the user submits the web page using this guest name, the default policy of that port becomes the active policy. The port mode must be set to Active/Discard mode.
- RADIUS Auth — Guest Networking is enabled. The user accesses the authentication web page, where the username field is automatically filled in with the specified Guest Name, and the password field is masked out with asterisks. Once the user submits the web page using these credentials, the value of the Guest Password is used for authentication. Following successful authentication from the RADIUS server, the port applies the policy (role) returned from the RADIUS server. The port mode must be set to Active/Discard mode.

Guest Name

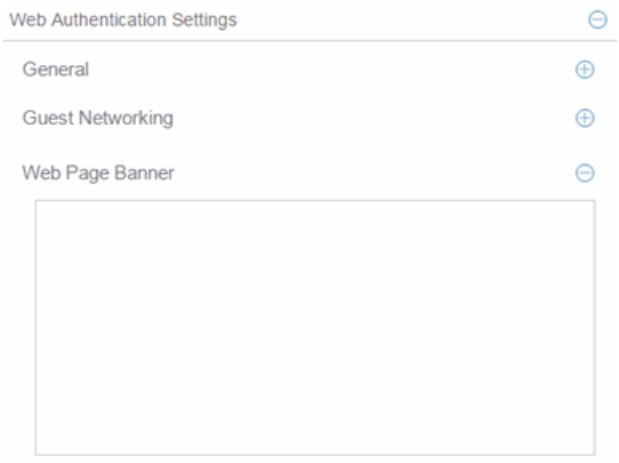
The username that Guest Networking uses to authenticate users. The guest name is displayed automatically on the authentication web page. If the user does not want to log in as a guest, they can type in their valid username to override the guest username.

Guest Password

The password that Guest Networking uses to authenticate users when RADIUS Auth is selected.

Web Page Banner

The Web Page Banner section allows you to customize the banner end users see at the top of the authentication web page and set a Redirect Time, if applicable.



Web Page Banner

Use this area to create a banner end users see at the top of the authentication web page. For example, you might include your company name and information on what to do if the user has questions or problems. Because this banner also appears in messages that occur during successful login and failed authentication, as well as on the "Radius Busy" screen, it is not appropriate to include "Welcome to [Your Company]" in the banner.

The Default button allows you to reset the banner to default text provided in a text file (pwa_banner.txt). Initially, the default banner text is the Extreme Networks contact information. However, you can customize the text for your network by editing the pwa_banner.txt file, located in the top level of the Policy Manager install directory. Then, when you click the Default button, the new text will be displayed in the Web Page Banner area.

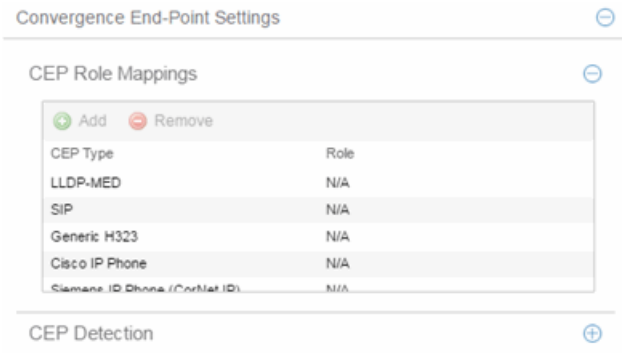
Convergence End-Point Settings

This section provides a way to identify Convergence End-Points (IP phones) connecting to the device, and apply a role to the end-point based on the type of end-point detected. The CEP Detection section lets you create detection rules for identifying the end-points, and the CEP Role Mappings section lets you map a role to each CEP product type.

In addition to configuring CEP on the device, you must also enable CEP protocols on each port using the CEP Access section in the Port Authentication Tab. Once you have configured CEP on the device and each port, you can monitor CEP usage on the Port Usage Tab (Port) or Port Usage Tab (Device).

CEP Role Mappings

This section lets you select the CEP product types supported on the device, and map a role for each type. Then, when a convergence end-point (such as an IP phone) connects to the network, the device identifies the type of end-point (using CEP detection rules) and applies the assigned role.



CEP Type

Lists the CEP types supported by the device.

Role

Lists the role mapped to each **CEP Type**.

Add

Select a CEP Type and click the **Add** button to open the Add Role Mapping window, where you can select a role for the selected **CEP Type**. Your selections are added to the CEP Role Mappings list.

Remove

Select the **CEP Type** and click **Remove** to remove the **CEP Type** in the CEP Role Mappings list.

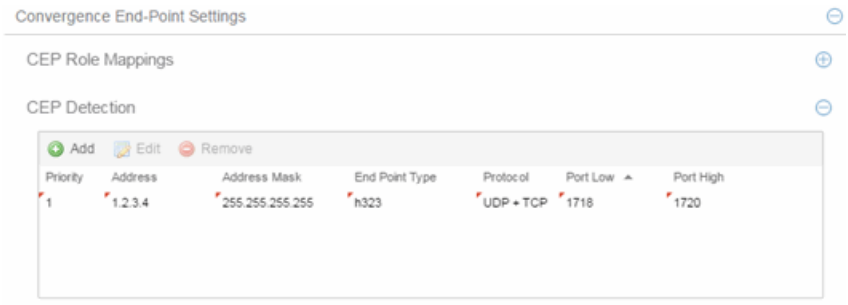
CEP Detection Tab

Use this section to create CEP detection rules used to determine if a connecting end-system is a CEP device and the type of CEP device. This allows Extreme Management Center to assign the appropriate role to the port based on the type of CEP device detected.

NOTE: CEP detection rules apply only to Siemens, H.323, and SIP (Session Initiation Protocol) phone detection. Cisco detection uses CiscoDP as its detection method.

CEP detection rules are based on two detection methods:

- TCP/UDP Port Number detection — Many CEP vendors use specific TCP/UDP port numbers for call setup on their IP phones. You can create detection rules that identify CEP devices based on specific TCP/UDP port numbers. By default, Siemens Hi-Path phones are detected on TCP/UDP port 4060.
- IP Address detection — H.323 phones use a reserved IP multicast address and UDP port number for call setup. You can create detection rules to detect an IP phone based on its IP address in combination with an IP address mask. By default, H.323 phones are detected using the multicast address 224.0.1.41 and the TCP/UDP ports 1718, 1719, and 1720. SIP phones are detected using the multicast address 224.0.1.75 and the TCP/UDP port 5060. H.323 and SIP phones are also detected using only their respective multicast addresses without the TCP/UDP ports.



Priority

The rule priority with one (1) being the highest priority. The rule with the highest priority is used first, so it is recommended the highest priority be given to the predominate protocol in the network to provide for greater efficiency.

Address

If the rule is based on IP address detection, this field displays the IP address that incoming packets matched against. By default, H.323 uses 224.0.1.41 as its IP address, SIP uses 224.0.1.75 as its IP address, and Siemens has no IP address configured.

Address Mask

If the rule is based on IP address detection, this field displays the IP address mask against which incoming packets are matched.

End Point Type
Specifies the end-point type assigned (H.323, Siemens, or SIP) if incoming packets match this rule.

Protocol
If the rule is based on TCP/UDP port detection, this field displays the protocol type used for matching, using a port range defined with the Port Low and Port High values:

- UDP + TCP — Match the port number for both UDP and TCP frames.
- TCP — Match the port number only for TCP frames.
- UDP — Match the port number only for UDP frames.

Port Low
The low end of the port range defined for detection on UDP and/or TCP ports.

Port High
The high end of the port range defined for detection on UDP and/or TCP ports.

Add
Opens the Add/Edit CEP Detection Rule window where you can create CEP detection rules.

Remove
To remove a CEP detection rule, select the entry and click Remove.

Edit
To edit a CEP detection rule, select the rule and click Edit. The Add/Edit CEP Detection Rule window opens where you edit the rule's parameters. You can also double-click an entry in the table to open the edit window.

Related Information

For information on related windows:

- Add/Edit CEP Detection Rule Window

Extreme Management Center Add/Edit CEP Detection Rule

Use this window to add or edit CEP detection rules that are used to determine if a connecting end-system is a CEP device, and what type of CEP device it is. This allows Policy Manager to assign the appropriate role to the port based on the type of CEP device detected. Access the window from the CEP Detection sub-tab in the right-panel Device Authentication tab.

NOTE: CEP detection rules apply only to Siemens, H.323, and SIP (Session Initiation Protocol) phone detection. Cisco detection uses CiscoDP as its detection method.

CEP detection rules are based on two detection methods:

- TCP/UDP Port Number detection — Many CEP vendors use specific TCP/UDP port numbers for call setup on their IP phones. You can create detection rules that identify CEP devices based on specific TCP/UDP port numbers. By default, Siemens Hi-Path phones are detected on TCP/UDP port 4060.
- IP Address detection — H.323 phones use a reserved IP multicast address and UDP port number for call setup. You can create detection rules detect an IP phone based on its IP address in combination with an IP address mask. By default, H.323 phones are detected using the multicast address 224.0.1.41 and the TCP/UDP ports 1718, 1719, and 1720. SIP phones are detected using the multicast address 224.0.1.75 and the TCP/UDP port 5060. H.323 and SIP phones are also detected using only their respective multicast addresses without the TCP/UDP ports.

CEP Detection Settings

Priority

Enter the rule priority with one (1) being the highest priority. The rule with the highest priority is used first, so it is recommended the highest priority be given to the predominate protocol in the network to provide for greater efficiency.

IP Address

If the rule is based on IP address detection, enter the IP address against which incoming packets are matched. By default, H.323 uses 224.0.1.41 as its IP address, SIP uses 224.0.1.75 as its IP address, and Siemens has no IP address configured.

Address Mask

If the rule is based on IP address detection, enter the IP address mask against which incoming packets are matched.

End Point Type

Select the endpoint type (H.323, Siemens, or SIP) assigned to incoming packets that match this rule.

Protocol

If the rule is based on TCP/UDP port detection, select the UDP and/or TCP checkbox and define a port range with Port Low and Port High values:

- UDP and TCP — Match the port number for both UDP and TCP frames.
- TCP — Match the port number only for TCP frames.
- UDP — Match the port number only for UDP frames.

Port Low

Define the low end of the port range for detection on UDP and/or TCP ports.

Port High

Define the high end of the port range for detection on UDP and/or TCP ports.

Related Information

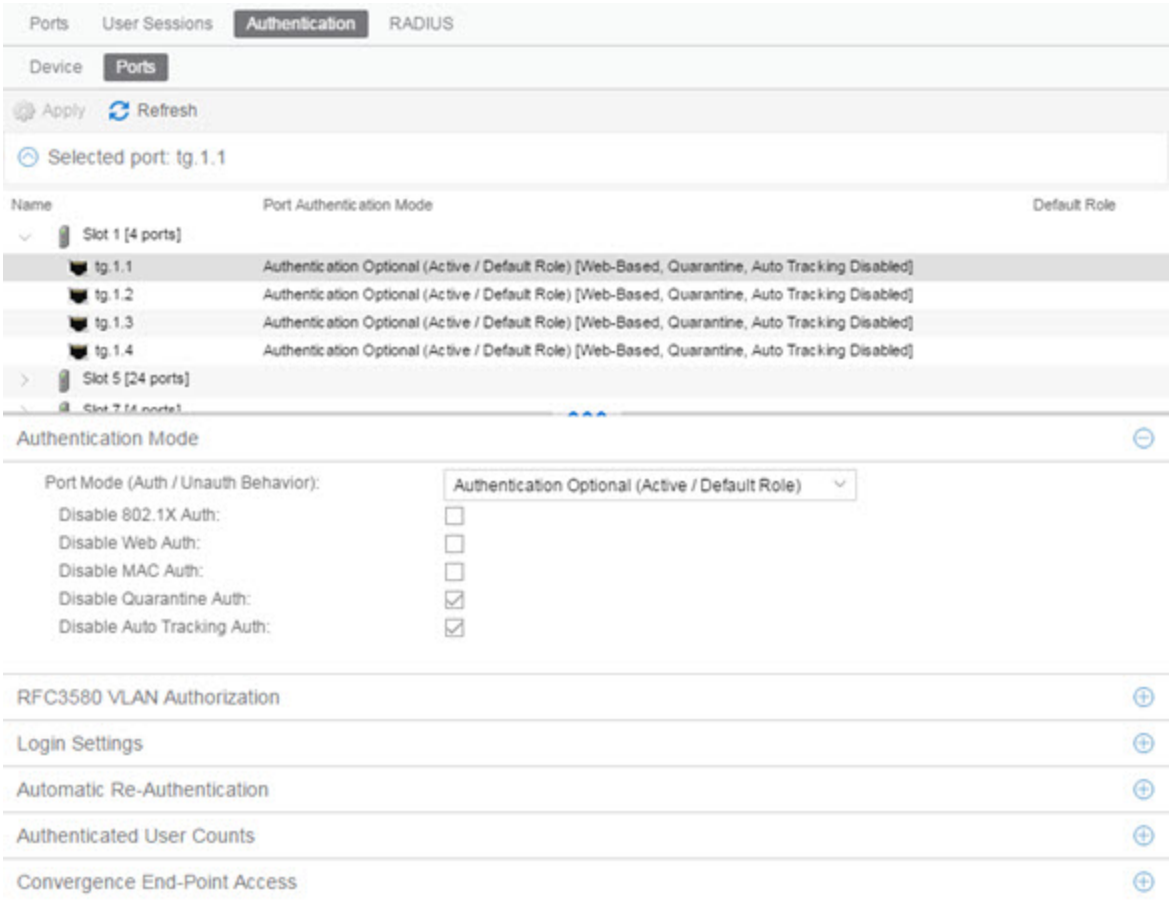
For information on related windows:

- Device Authentication Tab

Extreme Management Center Ports (Authentication)

The Ports (Authentication) tab allows you to configure and change the authentication settings for a port. Authentication must be configured and enabled on the device in order for individual port authentication settings to take effect. Only those areas of the tab that relate to the authentication type configured on the device are available for editing.

To access the Ports (Authentication) tab, select a device in the left-panel Devices > Devices tab, then select Authentication > Ports in the right panel.



Select a port in the top section to display and configure the authentication settings for that port in the bottom of the window.

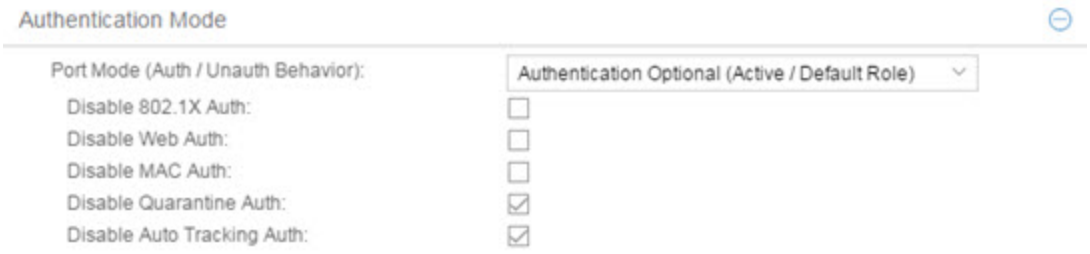
Click the Apply button at the top of the window to save changes to this tab.

The Authentication Configuration tab has six sections:

- Authentication Mode
- RFC3580 VLAN Authorization
- Login Settings
- Automatic Re-Authentication
- Authenticated User Counts
- Convergence End-Point Access

Authentication Mode

This tab displays general authentication and port mode information about the port.



This area displays the current port mode for the port, and allows you to change the settings if desired. Port mode defines whether or not a user is required to authenticate on a port, and how unauthenticated traffic is handled. It is a combination of Authentication Behavior (whether or not authentication is enabled on the port), and Unauthenticated Behavior (whether unauthenticated traffic is assigned to the port's default role or discarded). See Port Mode for a complete description of each port mode.

In addition, this section provides checkboxes that allow you to disable a specific authentication type at the port level.

Port Mode (Auth/Unauth Behavior)

Select an option to specify whether or not authentication is enabled on the port. (See Port Mode for more information.)

NOTE: Authentication Behavior must be set to **Active** for authentication to be allowed using CEP Protocols.

Disable 802.1X Auth

Select this checkbox to disable 802.1X authentication at the port level. If the device is only configured with 802.1X authentication, selecting this checkbox results in the port Authentication Behavior being set to Inactive.

NOTE: For Single User 802.1X+MAC authentication with Active/Default Role as the selected port mode: Disabling 802.1X authentication also disables MAC authentication on the port. An end user connecting to the port is not able to authenticate via 802.1X or MAC. The port behaves as if Inactive/Default Role is the selected port mode.

Disable Web-Based Auth

Select this checkbox to disable web-based authentication at the port level. If the device is only configured with web-based authentication, selecting this checkbox results in the port Authentication Behavior being set to Inactive.

NOTE: For Multi-User Web-Based authentication with Active/Discard as the selected port mode: This checkbox is automatically selected because multi-user web-based authentication does not support the Active/Discard port mode.

Disable MAC Auth

Select this checkbox to disable MAC authentication at the port level. If the device is only configured with MAC authentication, selecting this checkbox results in the port Authentication Behavior being set to Inactive.

Disable Quarantine Auth

Select this checkbox to disable Quarantine authentication at the port level. If the device is only configured with Quarantine authentication, selecting this checkbox results in the port Authentication Behavior being set to Inactive.

Disable Auto Tracking Auth

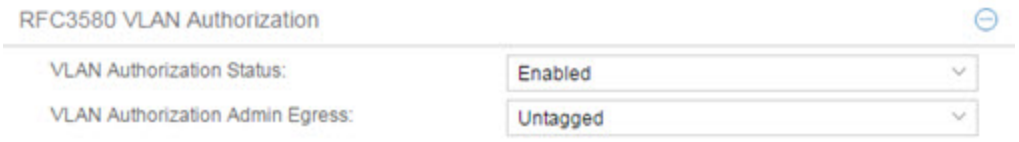
Select this checkbox to disable MAC authentication at the port level. If the device is only configured with Auto Tracking authentication, selecting this checkbox results in the port Authentication Behavior being set to Inactive.

RFC3580 VLAN Authorization

This section lets you enable or disable RFC 3580 VLAN Authorization on the port and specify an egress state. RFC 3580 VLAN Authorization must be enabled in networks where the RADIUS server has been configured to return a VLAN ID when a user authenticates. When RFC 3580 VLAN Authorization is enabled:

- ports on devices that do **not** support policy, will tag packets with the VLAN ID.
- ports on devices that do support policy and also support Authentication-Based VLAN to Role Mapping, will classify packets according to the role that the VLAN ID maps to.

You can also enable and disable VLAN Authorization at the device level using the device Authentication tab. If the device does not support RFC 3580, this tab will be grayed out.



VLAN Authorization Status

Allows you to enable and disable RFC 3580 VLAN Authorization for the selected port. This option is grayed out if not supported by the device.

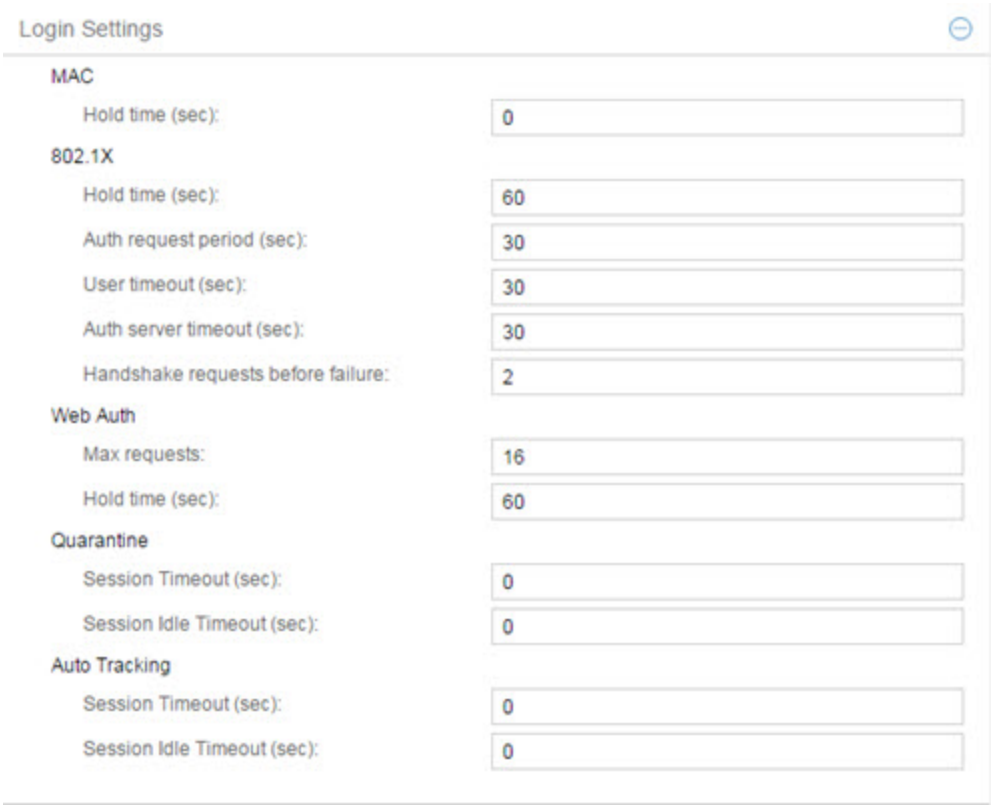
VLAN Authorization Admin Egress

Allows you to modify the VLAN egress list for the VLAN ID returned by the RADIUS server when a user authenticates on the port:

- None — No modification to the VLAN egress list is made.
- Tagged — The port is added to the list with the egress state set to Tagged (frames are forwarded as tagged).
- Untagged — The port is added to the list with the egress state set to Untagged (frames are forwarded as untagged).
- Dynamic — The port uses information returned in the RADIUS response to modify the VLAN egress list. This value is supported only if the device supports a mechanism through which the egress state may be returned in the RADIUS response.

Login Settings

This tab displays the current login settings for the port and allows you to change the settings if desired. The options available depend on what type(s) of authentication are enabled on the device.



MAC

Hold Time (sec)

Amount of time (in seconds) authentication remains timed out after the user fails to login. Valid values are 0-65535. The default is 60. (Hold Time is also known as Quiet Period in web-based and MAC authentication.)

802.1X

Hold Time (sec)

Amount of time (in seconds) authentication remains timed out after the user fails to login. Valid values are 0-65535. The default is 60.

Auth request period (sec)

For 802.1X authentication, how often (in seconds) the device queries the port to see if there is a new user on it. If a user is found, the device then attempts to authenticate the user. Valid values are 1-65535. The default is 30.

User timeout (sec)

For 802.1X authentication, the amount of time (in seconds) the device waits for an answer when querying the port for the existence of a user. Valid values are 1-300. The default is 30.

Auth server timeout (sec)

For 802.1X authentication, if a user is found on the port, the amount of time (in seconds) the device waits for a response from the authentication server before timing out. Valid values are 1-300. The default is 30.

Handshake requests before failure

For 802.1X authentication, the number of times the device tries to finalize the authentication process with the user, before the authentication request is considered invalid and authentication fails. Valid values are 1-10. The default is 2.

Web Auth

Max Requests

Number of times a user can attempt to log in before authentication fails and login attempts are not allowed. For web-based authentication, valid values are 1-2147483647, zero is not allowed, and the default is 2.

Hold Time (sec)

Amount of time (in seconds) authentication remains timed out after the specified Max Requests is reached. Valid values are 0-65535. The default is 60.

Quarantine

Session Timeout (sec)

For Quarantine authentication, the maximum number of seconds an authenticated session may last before automatic termination of the session. A value of zero indicates that no session timeout applies.

Session Idle Timeout (sec)

For Quarantine authentication, the maximum number of consecutive seconds an authenticated session may be idle before automatic termination of the session. A value of zero indicates that the device level setting is used.

Auto Tracking

Session Timeout (sec)

For Auto Tracking sessions, the maximum number of seconds a session may last before automatic termination of the session. A value of zero indicates that the device level setting is used.

Session Idle Timeout (sec)

For Auto Tracking sessions, the maximum number of consecutive seconds a session may be idle before automatic termination of the session. A value of zero indicates that the device level setting is used.

Automatic Re-Authentication

This tab is grayed-out if only web-based authentication is enabled on the device. For 802.1X and MAC authentication, the Automatic Re-Authentication tab lets you set up the periodic automatic re-authentication of logged-in users on this port. Without disrupting the user's session, the device repeats the authentication process using the most recently obtained user login information, to see if the same user is still logged in. Authenticated logged-in users are not required to log in again for re-authentication, as this occurs "behind the scenes."

802.1X Re-auth Status

If Enabled is selected, the re-authentication feature is enabled. If Disabled is selected, the re-authentication feature is disabled.

802.1X Re-auth Frequency (sec)

The length of time (in seconds) the device checks the port to re-authenticate the logged in user. Valid values are 1-2147483647. The default is 3600.

MAC Re-auth Status

If Enabled is selected, the re-authentication feature is enabled. If Disabled is selected, the re-authentication feature is disabled.

MAC Re-auth Frequency (sec)

The length of time (in seconds) the device checks the port to re-authenticate the logged in user. Valid values are 1-2147483647. The default is 3600.

Authenticated User Counts

This section provides authenticated user count information for devices with Multi-User as their configured authentication type. See the device Authentication tab for information on setting the device authentication type.

Current Number of Users

The current number of users actively authenticated or are in the process of authenticating on this interface. If multi-user authentication is disabled, this number is 0 (zero). Any unauthenticated traffic on the port is not included in this count.

Number of Users Allowed

The maximum number of users that can actively authenticate or be in the process of authenticating at one time on this interface. If you set this value below the current number of users, end user sessions exceeding that number are terminated.

NOTE: B2/C2 Devices. If you are configuring a single user and an IP phone per port, set this value to 2.

Number of MAC Users Allowed

The number of users that can actively authenticate via MAC authentication, or be in the process of authenticating via MAC authentication at one time on this interface. The number of MAC users allowed cannot exceed the number of users allowed. If you set this value below the current number of users, end user sessions exceeding that number are terminated. If MAC is not selected as a Multi-User authentication type on the device Authentication tab, this field is grayed out.

Number of Quarantine Users Allowed

The number of users that can be actively authenticated via Quarantine authentication, or have Quarantine authentications in progress at one time on this interface. The number of Quarantine users allowed cannot exceed the number of users allowed. If you set this value below the current number of users, end user sessions exceeding that number are terminated. If Quarantine Auth is not enabled on the device Authentication tab, this field is grayed out.

Number of Auto Tracking Users Allowed

The number of Auto Tracking users that can be actively authenticated or have authentications in progress at one time on this interface. The number of Auto Tracking users allowed cannot exceed the number of users allowed. If you set this value below the current number of users, end user sessions exceeding that number are terminated. If Auto Tracking is not enabled on the device Authentication tab, this field is grayed out.

Convergence End-Point Access

This section lists all the Convergence End-Point (CEP) protocols supported by the device that the port resides on, and lets you enable or disable them for that port. For devices that do not support CEP, the section is blank.

Enable Button

Selects all the checkboxes and enables all the CEP protocols for this port.

Disable All Button

Deselects all the checkboxes and disables all the CEP protocols for this port.

CEP Protocols List

Lists all the CEP protocols supported by the device on which the port resides. Highlight a CEP protocol and click the Enable or Disable button to enable or disable

CEP protocols, respectively. If the device does not support the CEP feature, this area is blank.

Related Information

For information on related tasks:

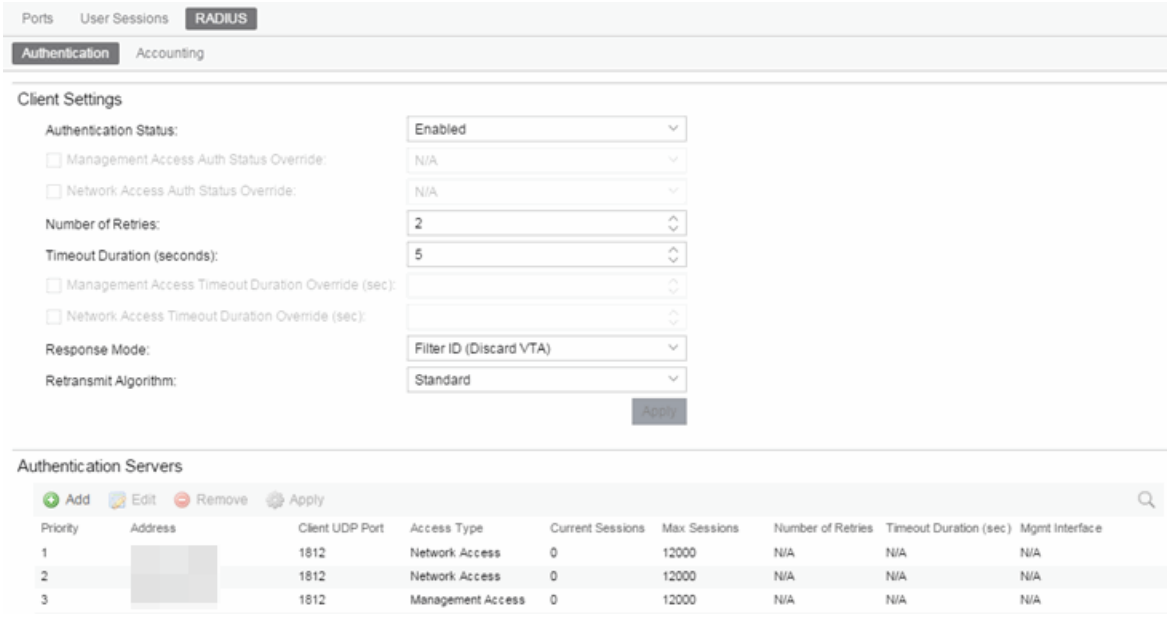
- How to Configure Ports

Extreme Management Center RADIUS (Device)

The device RADIUS tab allows you to configure and enable communication between the selected device (the RADIUS client), a RADIUS server or servers, and Extreme Management Center, for the purposes of authentication and accounting.

RADIUS accounting collects various data and statistics, such as the length of time a user has been logged on, and makes that data available to an administrator. It is used by a device to save accounting data on a RADIUS server. The device sends accounting requests to the server. The server acknowledges these requests, and data is passed to the server via accounting updates. For more information on accounting functionality, refer to your RADIUS server documentation.

To display the device RADIUS tab, select a device in the left-panel Devices tab, then click the RADIUS tab in the right panel.



Authentication Tab

Use this tab to view and configure the RADIUS authentication servers with which the device (the RADIUS client) can communicate.

RADIUS Authentication Client Settings

This section lets you enable or disable communication between the selected device (the RADIUS client) and the RADIUS authentication servers, and specify connection attempt information.

Authentication Status

Allows you to enable and disable communication between this device and the RADIUS authentication server(s). If enabled, the device becomes a RADIUS client and communicates with a RADIUS authentication server whenever a user logs on to a port on the device, as long as the port itself is enabled for authentication and the device is set up as a client on the RADIUS authentication server. The default is Disabled. For ExtremeWireless devices, the Client Status is automatically set to Enabled when a RADIUS server exists and Disabled when it does not.

Management Access Auth Status Override

Allows you to override the Authentication Status for users accessing the RADIUS authentication server(s) that have requested management access via the console, Telnet, SSH, or HTTP, etc.

Network Access Auth Status Override

Allows you to override the Authentication Status for users accessing the network via 802.1X, MAC, or Web-Based authentication.

Number of Retries

The number of attempts the device will make in contacting each RADIUS authentication server before giving up and trying the next RADIUS authentication server on the list. Valid values are 1-65535. For ExtremeWireless devices, this value is entered when the RADIUS server is added.

Timeout Duration

The total number of seconds the device will wait for the RADIUS authentication server to respond, before trying again. Valid values are 1-65535. For ExtremeWireless devices, this value is entered when the RADIUS server is added.

Management Access Timeout Duration Override (sec)

The total number of seconds the device waits for the RADIUS authentication server to respond before trying again for users accessing the RADIUS authentication server (s) that have requested management access via the console, Telnet, SSH, or HTTP, etc.

Network Access Timeout Duration Override (sec)

The total number of seconds the device waits for the RADIUS authentication server to respond before trying again for users accessing the network via 802.1X, MAC, or Web-Based authentication.

Response Mode

Select the RADIUS response attribute that the device should use for authentication:

- Filter ID — The Filter ID (role) is used. If a VLAN Tunnel Attribute (VTA) is returned, it will be ignored.
- VLAN Tunnel Attribute — The VLAN Tunnel Attribute is used and the Authentication-Based VLAN to Role Mappings are applied, if present. If a Filter ID is returned, it will be ignored.
- Filter ID With VLAN Tunnel Attribute — Both attributes are applied in the following manner: the role is applied to the user, except that the VLAN Tunnel Attribute replaces the role's Default Access Control VLAN (if present). In this case, the Authentication-Based VLAN to Role mappings are ignored (as the role was explicitly assigned). VLAN classification rules are still applied, as defined by the assigned role.

Retransmit Algorithm

Select the authentication retransmission algorithm for this device to use with your RADIUS servers. Devices that do not support this functionality will have the option grayed out.

- Standard — Specifies that the primary RADIUS server should always be used for authentication, if it is available. The standard RADIUS authentication algorithm focuses on using RADIUS servers for redundancy rather than for scale provisioning. The only time secondary RADIUS servers are used, is when the primary server is unreachable due to a network outage or because server capacity is exceeded.
- Round-Robin — The round-robin RADIUS authentication algorithm spreads RADIUS server usage evenly between available RADIUS servers, allowing the load balancing of a large number of authentications across all RADIUS servers. This allows for a maximum authentication throughput for the number of servers configured.

Additionally, if a single server is down, only a portion of the authenticating sessions will be affected by the outage.

- Sticky Round-Robin — This algorithm uses round-robin when assigning a RADIUS server to each unique authentication session, but specifies that the same RADIUS server should be used for any given authentication session once a session is initiated. In large-scale NAC deployments, this algorithm is used for switches that are authenticating more users than a NAC appliance supports. For example, a NAC deployment might have an S-Series device that supports 9000 users deployed at the distribution level and authenticating users to three NAC appliances that support 3000 users each. In this scenario, the sticky round-robin algorithm allows the S-Series device to spread the load across all three NAC appliances while using the same NAC appliance for all RADIUS transactions for a given session (MAC address).

Apply Button

Applies the changes you made in the RADIUS Authentication Client Settings section.

Authentication RADIUS Server(s) Table

This table lists the RADIUS authentication servers with which the device (the RADIUS client) can communicate. Use the buttons to add or remove servers, and edit server parameters. You can also edit a server's parameters by double-clicking the server entry in the list.

Priority

Order in which the RADIUS authentication server is checked, as compared to the other RADIUS authentication servers listed here. The lower the number, the higher the priority.

RADIUS Server IP

IP address of the RADIUS authentication server.

Client UDP Port

UDP port number (1-65535) on the RADIUS authentication server that the device will send authentication requests to; 1812 is the default port number.

Access Type

The type of authentication access allowed for this RADIUS server:

- Any access — the server can authenticate users originating from any access type.

- Management access — the server can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- Network access — the server can only authenticate users that are accessing the network via 802.1X, MAC, or Web-Based authentication.

Devices that do not support this feature will display N/A in this column.

Current Sessions

The current number of sessions associated with this server when the device is using the sticky round-robin RADIUS authentication algorithm. This value is not used when other algorithms are being used.

Max Sessions

The maximum number of sticky round-robin authentication sessions allowed on the server when the sticky round-robin RADIUS authentication algorithm is configured for the device. This value is not used when other algorithms are being used. In sticky round-robin, if a MAC address needs to re-authenticate, the request is sent to the same RADIUS server as the initial authentication request, unless the current number of authentication sessions for the server has reached the specified Max Sessions value. When this value is reached, re-authentication requests will instead default to the standard round-robin behavior to determine which RADIUS server to send the request to.

Number of Retries

The number of times the device will resend an authentication request if the RADIUS authentication server does not respond. For ExtremeWireless devices, this value is configured per RADIUS server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the RADIUS Authentication Client Settings section.

Timeout Duration

The amount of time in seconds the device will wait for the RADIUS authentication server to respond to an authentication request. For ExtremeWireless devices, this value is configured per RADIUS server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the RADIUS Authentication Client Settings section.

Management Interface

The IP address and VRName used when the switch is communicating with a configured RADIUS server.

Apply Button

Applies any changes you made in the RADIUS Authentication Server(s) tab.

Add Button

Opens the Add RADIUS Authentication Server window, where you can enter the parameters for a server you want to add to the list. When you click OK on this window, the new server is added.

Remove Button

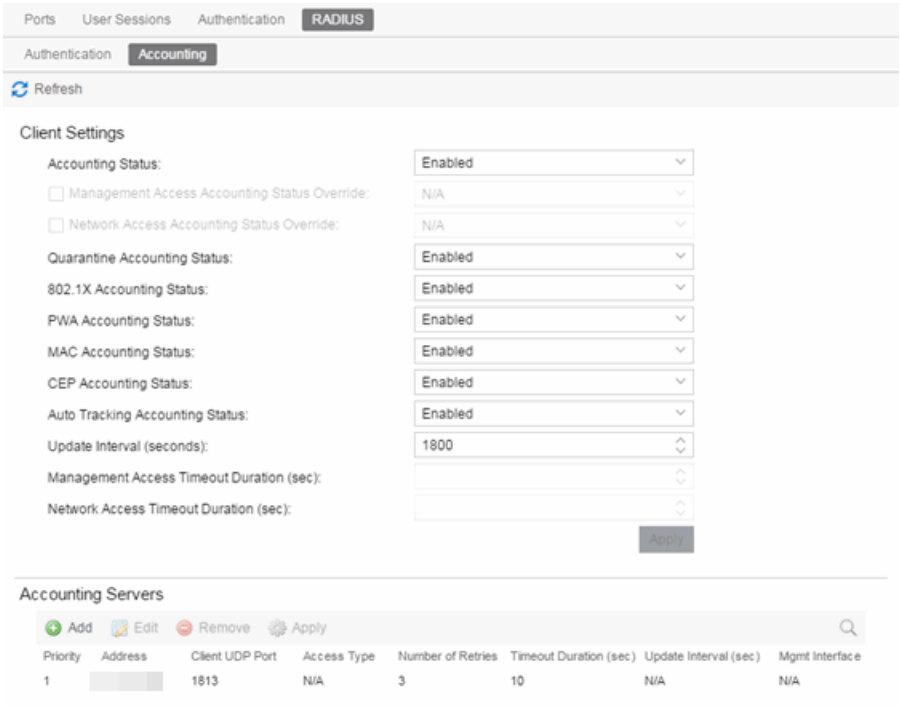
Select a RADIUS authentication server in the list and use this button to remove the server.

Edit Button

Select a RADIUS authentication server in the list and use this button to edit the server's parameters. You can also edit the server parameters by double-clicking the server entry in the list.

Accounting Tab

Use this tab to view and configure the RADIUS accounting servers with which the device (the RADIUS client) can communicate.



RADIUS Accounting Client Settings

This section lets you enable or disable communication between the selected device (the RADIUS client) and the RADIUS accounting servers, and specify the update interval.

Accounting Status

Allows you to enable or disable RADIUS accounting. RADIUS accounting is used by a device to save accounting data on a RADIUS accounting server. If accounting is enabled, an accounting session starts after the user is successfully authenticated by a RADIUS authentication server. The default is Disabled. For ExtremeWireless devices, the status is automatically set to Enabled when a RADIUS server exists and Disabled when it does not. Devices that do not support RADIUS accounting will have this field grayed out.

Management Access Auth Status Override

Allows you to override the Accounting Status for users accessing the RADIUS accounting server(s) that have requested management access via the console, Telnet, SSH, or HTTP, etc.

Network Access Auth Status Override

Allows you to override the Accounting Status for users accessing the network via 802.1X, MAC, or Web-Based authentication.

Per Authentication Type Accounting Status

Allows you to enable/disable RADIUS accounting for individual authentication types. Some authentication types do not have RADIUS accounting enabled by default (when global RADIUS accounting is enabled). Enabling these authentication types will give both NAC and other RADIUS servers more complete information regarding authentication sessions. These options also allow you to disable accounting messages from certain authentication types, for example, Auto-Tracking, which does not actually authenticate end users. Note that the global Accounting Status option controls accounting on a global basis for all authentication types. Devices that do not support this functionality will have these fields grayed out.

Update Interval (minutes)

Collected accounting data is sent from the device to the RADIUS accounting server via accounting updates. The Accounting Update Interval is the amount of time in minutes between accounting updates. Valid values are 1-65535. It is recommended that the value be greater than 10 minutes, and careful consideration should be given to its impact on network traffic. Devices that do not support RADIUS accounting

have this field grayed out (with the exception of an SNMPv1 R2 device, which display accounting values but will not allow you to set them.) For ExtremeWireless devices, this value is entered when the RADIUS server is added.

Management Access Timeout Duration Override (sec)
: The total number of seconds the device waits for the RADIUS accounting server to respond before trying again for users accessing the RADIUS accounting server(s) that have requested management access via the console, Telnet, SSH, or HTTP, etc.

Network Access Timeout Duration Override (sec)
: The total number of seconds the device waits for the RADIUS accounting server to respond before trying again for users accessing the network via 802.1X, MAC, or Web-Based authentication.

Apply Button
: Applies the changes you made in the RADIUS Accounting Client Settings section.

Accounting RADIUS Servers Table

This tab lists the RADIUS accounting servers with which the device (the RADIUS client) can communicate. Use the buttons to add or remove servers, and edit server parameters. You can also edit a server's parameters by double-clicking the server entry in the list.

Priority
: Order in which the RADIUS accounting server is checked, as compared to the other RADIUS accounting servers listed here. The lower the number, the higher the priority.

RADIUS Server IP
: IP address of the RADIUS accounting server.

Client UDP Port
: UDP port number (1-65535) on the RADIUS accounting server that the device will send accounting requests to; 1813 is the default port number. Devices that do not support RADIUS accounting will display N/A in this column (with the exception of an SNMPv1 R2 device, which will display accounting values but will not allow you to set them.)

Access Type

The type of authentication access allowed for this RADIUS server:

- Any access — the server can authenticate users originating from any access type.
- Management access — the server can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- Network access — the server can only authenticate users that are accessing the network via 802.1X, MAC, or Web-Based authentication.

Devices that do not support this feature will display N/A in this column.

Number of Retries

The number of times the device will resend an accounting request if the RADIUS accounting server does not respond. Valid values are 0-20. Devices that do not support RADIUS accounting will display N/A in this column (with the exception of an SNMPv1 R2 device, which display accounting values but does not allow you to set them.)

Timeout Duration

The amount of time in seconds the device will wait for the RADIUS accounting server to respond to an accounting request. Valid values are 2-10 seconds. Devices that do not support RADIUS accounting will display N/A in this column (with the exception of an SNMPv1 R2 device, which display accounting values but does not allow you to set them.)

Update Interval

The amount of time in minutes between accounting updates. For ExtremeWireless devices, this value is configured per RADIUS server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the RADIUS Accounting Client Settings section.

Management Interface

The IP address and VRName used when the switch is communicating with a configured RADIUS server.

Apply Button

Applies any changes you made in the RADIUS Accounting Server(s) tab.

Add Button

Opens the Add RADIUS Accounting Server window, where you can enter the parameters for a server you want to add to the list. When you click OK on this window, the new server is added.

Remove Button

Select a RADIUS accounting server in the list and use this button to remove the server.

Edit Button

Select a RADIUS accounting server in the list and use this button to edit the server's parameters. You can also edit the server parameters by double-clicking the server entry in the list.

Related Information

For information on related concepts:

- Authentication

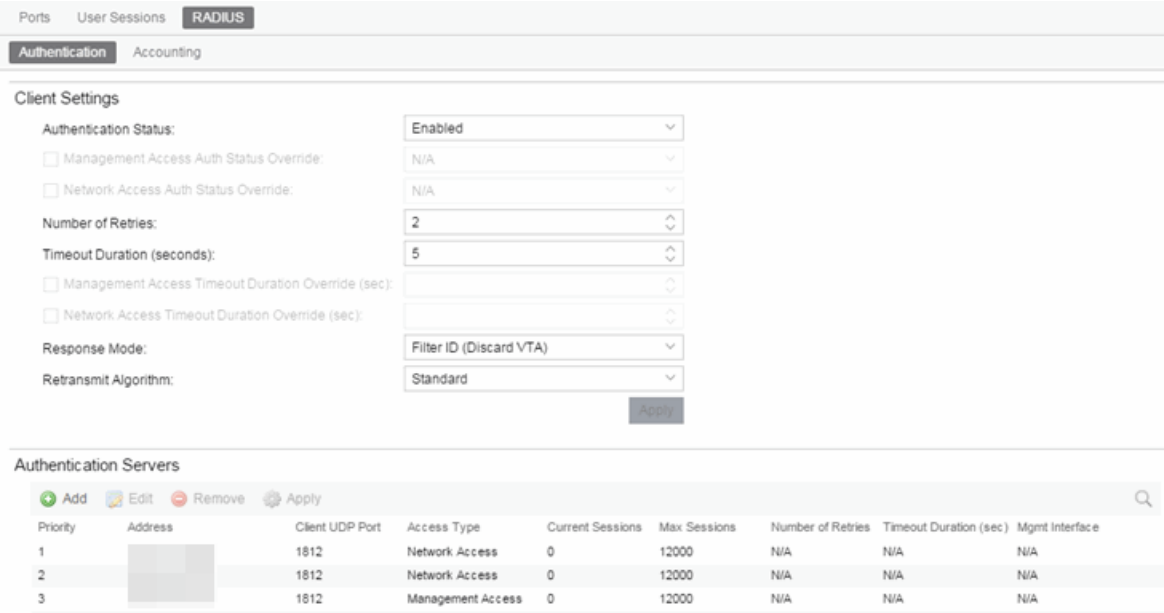
For information on related windows:

- Ports Tab (Device)
- Add RADIUS Authentication Server Window
- Add RADIUS Accounting Server Window

RADIUS Authentication (Device)

The device RADIUS **Authentication** tab allows you to configure and enable communication between the selected device (the RADIUS client), a RADIUS server or servers, and Extreme Management Center, for the purposes of authentication and accounting (for your SNMPv3 devices that support it).

Use this tab to view and configure the RADIUS authentication servers with which the device (the RADIUS client) can communicate.



RADIUS Authentication Client Settings

This section lets you enable or disable communication between the selected device (the RADIUS client) and the RADIUS authentication servers, and specify connection attempt information.

Authentication Status

Allows you to enable and disable communication between this device and the RADIUS authentication server(s). If enabled, the device becomes a RADIUS client and communicates with a RADIUS authentication server whenever a user logs on to a port on the device, as long as the port itself is enabled for authentication and the device is set up as a client on the RADIUS authentication server. For

ExtremeWireless devices, the Client Status is automatically set to Enabled when a RADIUS server exists and Disabled when it does not.

Management Access Auth Status Override

Allows you to override the Authentication Status for users accessing the RADIUS authentication server(s) that requested management access via the console, Telnet, SSH, or HTTP, etc.

Network Access Auth Status Override

Allows you to override the Authentication Status for users accessing the network via 802.1X, MAC, or Web-Based authentication.

Number of Retries

The number of attempts the device makes in contacting each RADIUS authentication server before giving up and trying the next RADIUS authentication server on the list. For ExtremeWireless devices, this value is entered when the RADIUS server is added.

Timeout Duration (seconds)

The total number of seconds the device waits for the RADIUS authentication server to respond, before trying again. For ExtremeWireless devices, this value is entered when the RADIUS server is added.

Management Access Timeout Duration Override (sec)

The total number of seconds the device waits for the RADIUS authentication server to respond before trying again for users accessing the RADIUS authentication server (s) that requested management access via the console, Telnet, SSH, or HTTP, etc.

Network Access Timeout Duration Override (sec)

The total number of seconds the device waits for the RADIUS authentication server to respond before trying again for users accessing the network via 802.1X, MAC, or Web-Based authentication.

Response Mode

Select the RADIUS response attribute the device uses for authentication:

- Filter ID (Discard VTA) — The Filter ID (role) is used. If a VLAN Tunnel Attribute (VTA) is returned, it is ignored.
- VLAN Tunnel Attribute (Discard Tunnel Attribute) — The VLAN Tunnel Attribute is used and the Authentication-Based VLAN to Role Mappings are applied, if present. If a Filter ID is returned, it is ignored.
- Filter ID With VLAN Tunnel Attribute — Both attributes are applied in the following manner: the role is applied to the user, except that the VLAN Tunnel Attribute

replaces the role's Default Access Control VLAN (if present). In this case, the Authentication-Based VLAN to Role mappings are ignored (as the role was explicitly assigned). VLAN classification rules are still applied, as defined by the assigned role.

Retransmit Algorithm

Select the authentication retransmission algorithm for this device to use with your RADIUS servers. Devices that do not support this functionality have the option grayed out.

- Standard — Specifies that the primary RADIUS server should always be used for authentication, if it is available. The standard RADIUS authentication algorithm focuses on using RADIUS servers for redundancy rather than for scale provisioning. The only time secondary RADIUS servers are used, is when the primary server is unreachable due to a network outage or because server capacity is exceeded.
- Round-Robin — The round-robin RADIUS authentication algorithm spreads RADIUS server usage evenly between available RADIUS servers, allowing the load balancing of a large number of authentications across all RADIUS servers. This allows for a maximum authentication throughput for the number of servers configured. Additionally, if a single server is down, only a portion of the authenticating sessions are affected by the outage.
- Sticky Round-Robin — This algorithm uses round-robin when assigning a RADIUS server to each unique authentication session, but specifies that the same RADIUS server is used for any given authentication session once a session is initiated. In large-scale Extreme Access Control deployments, this algorithm is used for switches authenticating more users than an Extreme Access Control appliance supports. For example, an Extreme Access Control deployment might have an S-Series device that supports 9000 users deployed at the distribution level and authenticating users to three Extreme Access Control appliances that support 3000 users each. In this scenario, the sticky round-robin algorithm allows the S-Series device to spread the load across all three Extreme Access Control appliances while using the same Extreme Access Control appliance for all RADIUS transactions for a given session (MAC address).

Apply Button

Applies the changes you made in the RADIUS Authentication Client Settings section.

Authentication RADIUS Server(s) Table

This table lists the RADIUS authentication servers with which the device (the RADIUS client) can communicate. Use the buttons to add or remove servers, and

edit server parameters. You can also edit a server's parameters by double-clicking the server entry in the list.

Priority

Order in which the RADIUS authentication server is checked, as compared to the other RADIUS authentication servers listed here. The lower the number, the higher the priority with 1 being the highest priority.

Address

IP address of the RADIUS authentication server.

Client UDP Port

UDP port number (1-65535) on the RADIUS authentication server to which the device sends authentication requests; 1812 is the default port number.

Access Type

The type of authentication access allowed for this RADIUS server:

- Any access — the server can authenticate users originating from any access type.
- Management access — the server can only authenticate users that requested management access via the console, Telnet, SSH, or HTTP, etc.
- Network access — the server can only authenticate users accessing the network via 802.1X, MAC, or Web-Based authentication.

Devices that do not support this feature display N/A in this column.

Current Sessions

The current number of sessions associated with this server when the device is using the sticky round-robin RADIUS authentication algorithm. This value is not used when other algorithms are being used.

Max Sessions

The maximum number of sticky round-robin authentication sessions allowed on the server when the sticky round-robin RADIUS authentication algorithm is configured for the device. This value is not used when other algorithms are selected. In sticky round-robin, if a MAC address needs to re-authenticate, the request is sent to the same RADIUS server as the initial authentication request, unless the current number of authentication sessions for the server has reached the specified Max Sessions value. When this value is reached, re-authentication requests instead default to the standard round-robin behavior to determine the RADIUS server to which to send the request.

Number of Retries

The number of times the device resends an authentication request if the RADIUS authentication server does not respond. For ExtremeWireless devices, this value is configured per RADIUS server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the RADIUS Authentication Client Settings section.

Timeout Duration (sec)

The amount of time in seconds the device waits for the RADIUS authentication server to respond to an authentication request. For ExtremeWireless devices, this value is configured per RADIUS server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the RADIUS Authentication Client Settings section.

Management Interface

The IP address and VRName used when the switch is communicating with a configured RADIUS server.

Add Button

Opens the Add/Edit RADIUS Authentication Server window, where you can enter the parameters for a server you want to add to the list. When you click OK on this window, the new server is added.

Edit Button

Select a RADIUS authentication server in the list and use this button to edit the server's parameters. You can also edit the server parameters by double-clicking the server entry in the list.

Remove Button

Select a RADIUS authentication server in the list and use this button to remove the server.

Apply Button

Applies any changes you made in the RADIUS Authentication Server(s) tab.

Related Information

For information on related concepts:

- Authentication

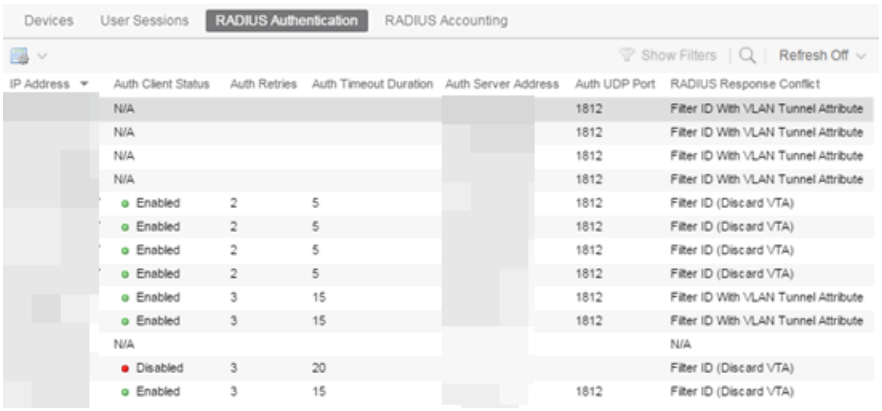
For information on related windows:

- Port Properties - Authentication Configuration Tab
- Add RADIUS Authentication Server Window
- Add RADIUS Accounting Server Window

Extreme Management Center RADIUS Authentication (Devices)

The RADIUS Authentication tab displays authentication RADIUS server information for all the devices in the current domain. You can configure RADIUS server information for an individual device using the device's RADIUS Tab.

To access this tab, selectDevices/Port Groups>Devicesin the left-panel of thePolicy tab, then click the RADIUS Authentication tab in the right panel.



IP Address

IP address of the device.

Auth Client Status

Informs you whether or not the device is enabled as a RADIUS client. If Enabled, the device is a RADIUS client and communicates with a RADIUS authentication server whenever a user logs on to a port on the device, as long as the port itself is enabled for authentication. If Disabled, the device is currently not enabled as a RADIUS client.

Auth Retries

Number of attempts the device (RADIUS client) makes to connect to the RADIUS authentication server before giving up and trying the next RADIUS server on the list.

Auth Timeout Duration

Total number of seconds the device (RADIUS client) waits for the RADIUS authentication server to respond before trying again.

Auth Server Address
The IP addresses of the RADIUS servers the client device attempts to contact.

Auth UDP Port
The UDP port number used to send authentication requests.

RADIUS Response Conflict
Indicates the RADIUS response attribute that the device uses for authentication. You can configure the Response Mode in the RADIUS tab for the device.

Related Information

For information on related concepts:

- Authentication

For information on related windows:

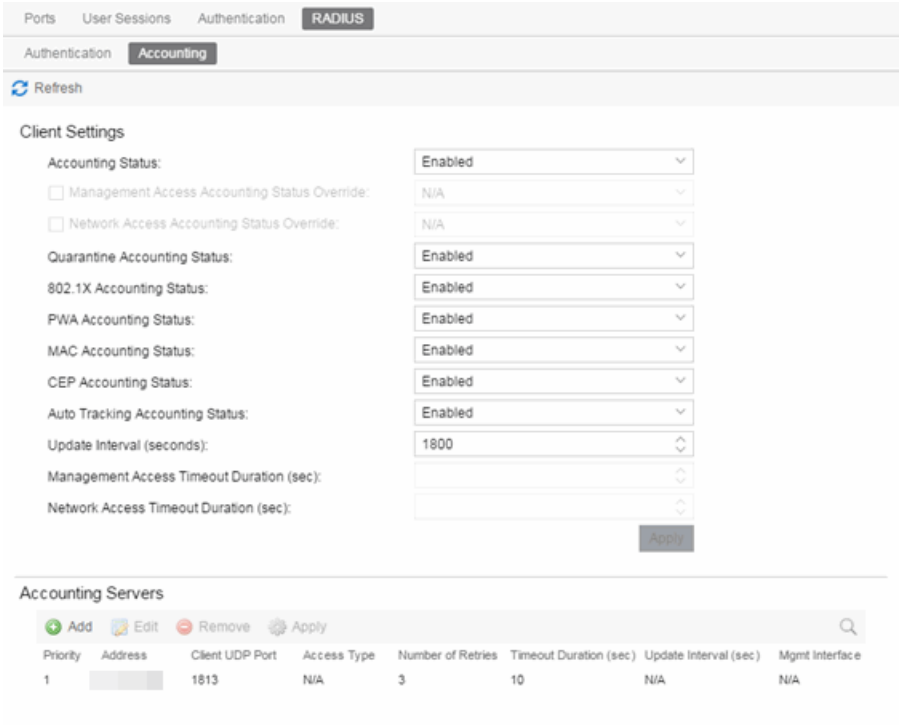
- Add RADIUS Authentication Server Window
- Add RADIUS Accounting Server Window

Extreme Management Center RADIUS Accounting (Device)

The device RADIUS Accounting tab allows you to configure and enable communication between the selected device (the RADIUS client), a RADIUS server or servers, and Extreme Management Center, for the purposes of accounting (for your SNMPv3 devices that support it).

RADIUS accounting collects various data and statistics, such as the length of time a user has been logged on, and makes that data available to an administrator. It is used by a device to save accounting data on a RADIUS server. Accounting requests are sent from the device to the server. The server acknowledges these requests, and data is passed to the server via accounting updates. For more information on accounting functionality, refer to your RADIUS server documentation.

To display the device RADIUS Accounting tab, select a device in the left panel Devices > Devices tree, then click RADIUS > Accounting in the right panel.



RADIUS Accounting Client Settings

This section lets you enable or disable communication between the selected device (the RADIUS client) and the RADIUS accounting servers, and specify the update interval.

Accounting Status

Allows you to enable or disable RADIUS accounting on SNMPv3 devices that support it. RADIUS accounting is used by a device to save accounting data on a RADIUS accounting server. If accounting is enabled, an accounting session starts after the user is successfully authenticated by a RADIUS authentication server. The default is Disabled. For ExtremeWireless devices, the status is automatically set to Enabled when a RADIUS server exists and Disabled when it does not. Devices that do not support RADIUS accounting have this field grayed out.

Management Access Auth Status Override

Allows you to override the Accounting Status for users accessing the RADIUS accounting server(s) that have requested management access via the console, Telnet, SSH, or HTTP, etc.

Network Access Auth Status Override

Allows you to override the Accounting Status for users accessing the network via 802.1X, MAC, or Web-Based authentication.

Per Authentication Type Accounting Status

Allows you to enable/disable RADIUS accounting for individual authentication types (Quarantine, 802.1X, PWA, MAC, CEP, and Auto Tracking). Some authentication types do not have RADIUS accounting enabled by default (when global RADIUS accounting is enabled). Enabling these authentication types gives both Extreme Access Control and other RADIUS servers more complete information regarding authentication sessions. These options also allow you to disable accounting messages from certain authentication types, for example, Auto-Tracking, which does not actually authenticate end users. Note that the global Accounting Status option controls accounting on a global basis for all authentication types. Devices that do not support this functionality have these fields grayed out.

Update Interval (seconds)

Collected accounting data is sent from the device to the RADIUS accounting server via accounting updates. The Accounting Update Interval is the amount of time in seconds between accounting updates. This field is greyed out for devices that do not support RADIUS accounting (with the exception of an SNMPv1 R2 device, which

displays accounting values but does not allow you to set them.) For ExtremeWireless devices, this value is entered when the RADIUS server is added.

Management Access Timeout Duration Override (sec)
: The total number of seconds the device waits for the RADIUS accounting server to respond before trying again for users accessing the RADIUS accounting server(s) that have requested management access via the console, Telnet, SSH, or HTTP, etc.

Network Access Timeout Duration Override (sec)
: The total number of seconds the device waits for the RADIUS accounting server to respond before trying again for users accessing the network via 802.1X, MAC, or Web-Based authentication.

Apply Button
: Applies the changes you made in the RADIUS Accounting Client Settings section.

Accounting RADIUS Servers Table

This table lists the RADIUS accounting servers with which the device (the RADIUS client) can communicate. Use the buttons to add or remove servers, and edit server parameters. You can also edit a server's parameters by double-clicking the server entry in the list.

Priority
: Order in which the RADIUS accounting server is checked, as compared to the other RADIUS accounting servers listed here. The lower the number, the higher the priority with 1 being the highest priority.

Address
: IP address of the RADIUS accounting server.

Client UDP Port
: UDP port number (1-65535) on the RADIUS accounting server to which the device sends accounting requests; 1813 is the default port number. Devices that do not support RADIUS accounting display N/A in this column (with the exception of an SNMPv1 R2 device, which displays accounting values, but does not allow you to set them.)

Access Type
: The type of authentication access allowed for this RADIUS server:

- Any access — the server can authenticate users originating from any access type.

- Management access — the server can only authenticate users accessing the network via the console, Telnet, SSH, or HTTP, etc.
- Network access — the server can only authenticate users accessing the network via 802.1X, MAC, or Web-Based authentication.

Devices that do not support this feature display N/A in this column.

Number of Retries

The number of times the device resends an accounting request if the RADIUS accounting server does not respond. Valid values are 0-20. Devices that do not support RADIUS accounting display N/A in this column (with the exception of an SNMPv1 R2 device, which displays accounting values, but does not allow you to set them.)

Timeout Duration (sec)

The amount of time in seconds the device waits for the RADIUS accounting server to respond to an accounting request. Valid values are 2-10 seconds. Devices that do not support RADIUS accounting display N/A in this column (with the exception of an SNMPv1 R2 device, which displays accounting values, but does not allow you to set them.)

Update Interval (sec)

The amount of time in seconds between accounting updates. For ExtremeWireless devices, this value is configured per RADIUS server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the RADIUS Accounting Client Settings section.

Management Interface

The IP address and VRName used when the switch is communicating with a configured RADIUS server.

Apply Button

Applies any changes you made in the RADIUS Accounting Server(s) tab.

Add Button

Opens the Add RADIUS Accounting Server window, where you can enter the parameters for a server you want to add to the list. When you click OK on this window, the new server is added.

Remove Button

Select a RADIUS accounting server in the list and use this button to remove the server.

Edit Button

Select a RADIUS accounting server in the list and use this button to edit the server's parameters. You can also edit the server parameters by double-clicking the server entry in the list.

Related Information

For information on related concepts:

- Authentication

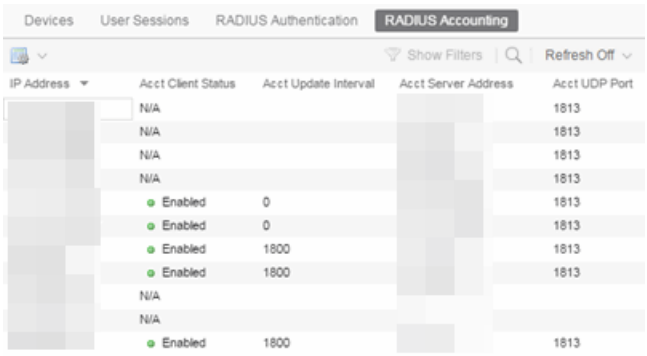
For information on related windows:

- Port Properties - Authentication Configuration Tab
- Add RADIUS Authentication Server Window
- Add RADIUS Accounting Server Window

Extreme Management Center RADIUS Accounting (Devices)

The RADIUS Accounting tab displays accounting RADIUS server information for all the devices in the current domain. You can configure RADIUS server information for an individual device using the device's RADIUS Tab.

To access this tab, select Devices/Port Groups>Devices in the left-panel of the Policy tab, then click the RADIUS Accounting tab in the right panel.



IP Address

IP address of the device.

Acct. Client Status

Informs you whether or not RADIUS accounting is enabled on the device (the RADIUS client). RADIUS accounting is supported on certain SNMPv3 devices, and is used by the device to save accounting data on a RADIUS server. If accounting is enabled, an accounting session starts after the user is successfully authenticated by a RADIUS server. Devices that do not support RADIUS accounting display N/A in this column (with the exception of an SNMPv1 R2 device, which displays a status.)

Acct. Update Interval

Collected accounting data is sent from the device (RADIUS client) to the RADIUS server via accounting updates. The Accounting Update Interval is the amount of time in minutes between accounting updates. Devices that do not support RADIUS accounting display N/A in this column (with the exception of an SNMPv1 R2 device, which displays a value.)

Acct Server Address

The IP addresses of the RADIUS servers the client device attempts to contact.

Auth UDP Port

The UDP port number used to send accounting requests.

Related Information

For information on related concepts:

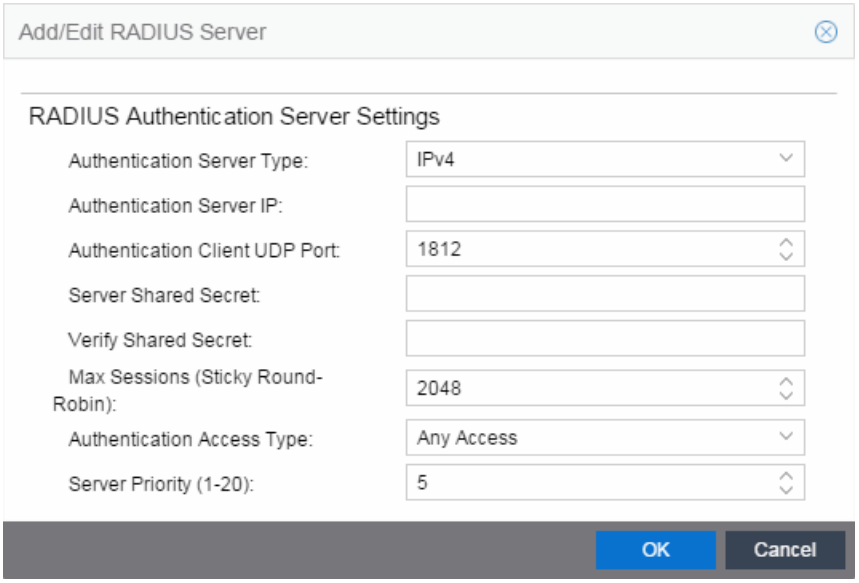
- Authentication

For information on related windows:

- Add RADIUS Authentication Server Window
- Add RADIUS Accounting Server Window

Extreme Management Center Add/Edit RADIUS Server

This window lets you add a RADIUS server to Extreme Management Center for the purpose of authentication. Access this window by clicking **Add** in the RADIUS Server(s) Authentication sub-tab in the RADIUS tab for a device.



Authentication Server Type

Select the authentication type used on the RADIUS server.

NOTE: DNS servers (on supported devices) may only be added when there is a valid DNS server configured on the Device which allows the DNS name to resolve to an IP address at the time of configuration.

Authentication Server IP

Enter the IP or IPv6 address, or the hostname of the RADIUS authentication server. Not all devices support IPv6 address types.

Authentication Client UDP Port

Enter the UDP port number (1-65535) the device (RADIUS client) uses to send authentication requests to the RADIUS authentication server; 1812 is the default port number.

Server Shared Secret

A string of characters used to encrypt and decrypt communications between the device (RADIUS client) and the RADIUS authentication server. This string must match the shared secret entered when you added the client device on the RADIUS server. Without the shared secret, the server and client are unable to communicate, and authentication attempts fail. The shared secret must be at least 6 characters long; 16 characters is recommended. Dashes are allowed in the string, but spaces are not.

NOTES: If you are configuring multiple RADIUS servers, the same server shared secret must be used for each RADIUS server. This is because most devices (RADIUS clients) only support one shared secret. Matrix N-Series devices with firmware version 5.0 or above are an exception to this, as these devices do support a unique shared secret for each server.

This Server Shared Secret is not to be confused with the Application Shared Secret that encrypts communication between the RADIUS client and Extreme Management Center, entered in the Application Shared Secret area of the RADIUS tab for a device.

Verify Shared Secret

Re-enter the Server Shared Secret you entered above.

Max Sessions (Sticky Round-Robin)

Specifies the maximum number of sticky round-robin authentication sessions allowed on the server when the sticky round-robin RADIUS authentication algorithm is configured for a device. In sticky round-robin, if a MAC address needs to re-authenticate, the request is sent to the same RADIUS server as the initial authentication request, unless the current number of authentication sessions for the server has reached the specified Max Sessions value. When this value is reached, re-authentication requests will instead default to the standard round-robin behavior to determine which RADIUS server to send the request to. Devices that do not support this functionality will have the option grayed out.

Number of Retries

The number of times the device will resend an authentication request if the RADIUS authentication server does not respond. For ExtremeWireless devices, this value is configured for each server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the RADIUS Authentication Client Settings section of the RADIUS tab.

Timeout Duration

The amount of time in seconds the device will wait for the RADIUS authentication server to respond to an authentication request. For ExtremeWireless devices, this value is configured for each server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the RADIUS Authentication Client Settings section of the RADIUS tab.

Authentication Access Type

Use the drop-down list to select the type of authentication access allowed for this RADIUS server:

- Any access - the server can authenticate users originating from any access type.
- Management access - the server can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- Network access - the server can only authenticate users that are accessing the network via 802.1X, MAC, or Web-Based authentication.

This feature allows you to have one set of servers for authenticating management access requests and a different set for authenticating network access requests. Devices that do not support this feature will have this field grayed out.

Server Priority

Order in which the RADIUS authentication server will be checked, as compared to the other RADIUS authentication servers on the device. The lower the number, the higher the priority.

Management Interface

Select the IP address and VRName to use when the switch is communicating with a configured RADIUS server.

NOTE: ExtremeXOS devices must define a Management Interface.

Related Information

For information on related concepts:

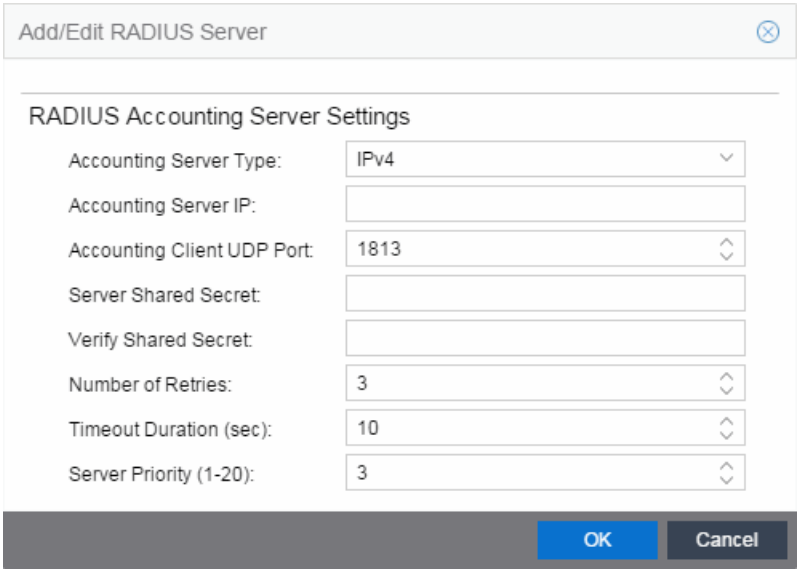
- Authentication

For information on related windows:

- RADIUS Tab

Extreme Management Center Add RADIUS Accounting Server

This window lets you add a RADIUS server to Extreme Management Center for the purpose of RADIUS accounting. Access this window by clicking **Add** in the RADIUS Server(s) Accounting sub-tab in the RADIUS tab for a device.



Accounting Server Type

Select the accounting type used on the RADIUS server.

NOTE: DNS servers (on supported devices) may only be added when there is a valid DNS server configured on the Device which allows the DNS name to resolve to an IP address at the time of configuration.

Accounting Server IP

Enter the IP or IPv6 address, or the hostname of the RADIUS accounting server. Not all devices support IPv6 address types.

Accounting Client UDP Port

Enter the UDP port number (1-65535) the device (RADIUS client) uses to send accounting requests to the RADIUS server; 1813 is the default port number. Devices that do not support RADIUS accounting will have this field grayed out (with the exception of an SNMPv1 R2 device, which will display accounting values but will not allow you to set them.)

Server Shared Secret

A string of characters used to encrypt and decrypt communications between the device (RADIUS client) and the RADIUS accounting server. This string must match the shared secret entered when you added the client device on the RADIUS server. Without the shared secret, the server and client will be unable to communicate. The shared secret must be at least 6 characters long; 16 characters is recommended. Dashes are allowed in the string, but spaces are not.

NOTES: If you are configuring multiple RADIUS servers, the same server shared secret must be used for each RADIUS server. This is because most devices (RADIUS clients) only support one shared secret. Matrix N-Series devices with firmware version 5.0 or above are an exception to this, as these devices **do** support a unique shared secret for each server.

This Server Shared Secret is different than the Application Shared Secret that encrypts communication between the RADIUS client and Extreme Management Center, entered in the Application Shared Secret area of the RADIUS tab for a device.

Verify Shared Secret

Re-enter the Server Shared Secret you entered above.

Number of Retries (0-20)

The number of times the device will resend an accounting request if the RADIUS server does not respond. Valid values are 0-20. Devices that do not support RADIUS accounting will have this field grayed out (with the exception of an SNMPv1 R2 device, which will display accounting values but will not allow you to set them.)

Timeout Duration (2 -10 sec)

The amount of time in seconds the device will wait for the RADIUS server to respond to an accounting request. Valid values are 2-10 seconds. Devices that do not support RADIUS accounting will have this field grayed out (with the exception of an SNMPv1 R2 device, which will display accounting values but will not allow you to set them.)

Update Interval (minutes)

The Accounting Update Interval is the amount of time in minutes between accounting updates. For ExtremeWireless Wireless devices, this value is configured per RADIUS server. For all other devices, this value is global to all RADIUS servers, and is specified per device (Client Default) in the RADIUS Accounting Client Settings section of the RADIUS tab. Devices that do not support RADIUS accounting will have this field grayed out.

Accounting Access Type

Use the drop-down menu to select the type of accounting access allowed for this RADIUS server:

- Any access - the server can send an accounting request for users originating from any access type.
- Management access - the server can only send an accounting request for users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- Network access - the server can only send an accounting request users that are accessing the network via 802.1X, MAC, or Web-Based accounting.

This feature allows you to have one set of servers for accounting management access requests and a different set for accounting network access requests. Devices that do not support this feature have this field grayed out.

Server Priority (1-20)

Order in which the RADIUS accounting server will be checked, as compared to the other RADIUS accounting servers on the device. The lower the number, the higher the priority.

Management Interface

Select the IP address and VRName to use when the switch is communicating with a configured RADIUS server.

NOTE: ExtremeXOS devices must define a Management Interface.

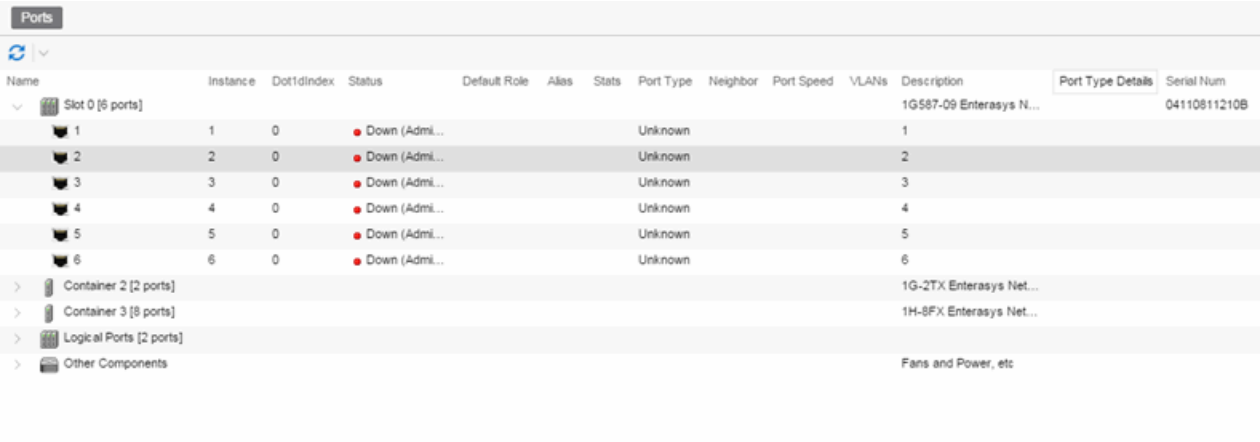
Related Information

For information on related windows:

- RADIUS Tab

Extreme Management Center Ports (Device)

The device Port Groups tab displays a table of information about the selected device's ports. To access this tab, select a port group from the left panel'sDevices/Port Groups>Port Groups tab.



Name

Name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

Instance

Shows the instance for the port.

Dot1dIndex

The index value assigned to the port interface.

Status

Shows the status (Up, Down, or Unknown) of the port.

Default Role

Displays the default role for the port. To set the default role, select a port, right-click and select Set Default Role. The Roles Selection view appears where you can select the desired default role. See Default Role in the Concepts topic for information on default roles.

NOTE: Setting a default role on an ExtremeWireless Controller port that is not yet a VNS, creates a new VNS on the HWC.

Alias

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

Stats

Displays information about the port, if configured in PortView.

Port Type

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

Neighbor
The port to which the port is connected.

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

VLANs
The VLANs to which the port is associated.

Description
A description of the port and the device.

Port Type Details
Additional information about the type of port.

Serial Number
The serial number of the device.

Retrieve Button
Retrieves the most recent information about the ports on the device.

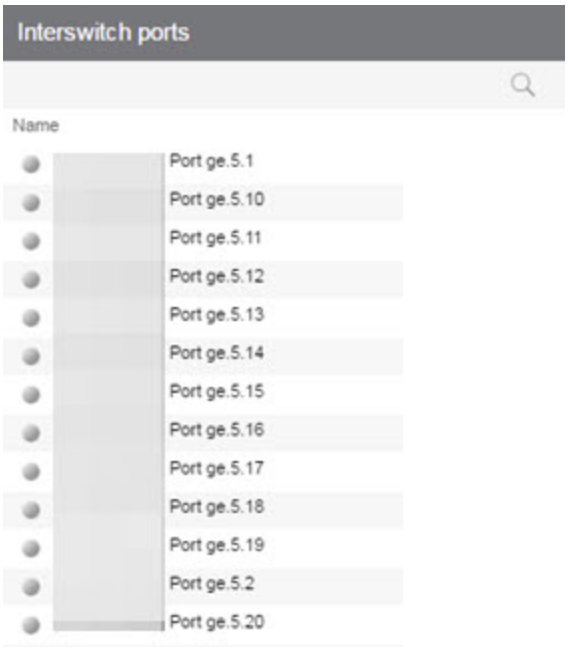
Related Information

For information on related tasks:

- How to Create a Port Group

Extreme Management Center Ports (Port Group)

The Ports panel in the Port Groups navigation tree lists the ports in the selected port group. You can also add and remove ports (user-defined port groups only) by right-clicking the Port Group in the left-hand navigation tree. To access this panel, select a port group in the left-panel Devices/Port Groups > Port Groups navigation tree.



Name

Name of the port, constructed of the name or IP address of the device and either the port index number or the port interface name.

Default Role

See Default Role in the Concepts topic for information on default roles. For additional information, see Port Mode.

Alias

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

Port Type

Type of port. Possible values include: Access, Interswitch Backplane, Backplane, Interswitch, and Logical.

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

Related Information

For information on related tasks:

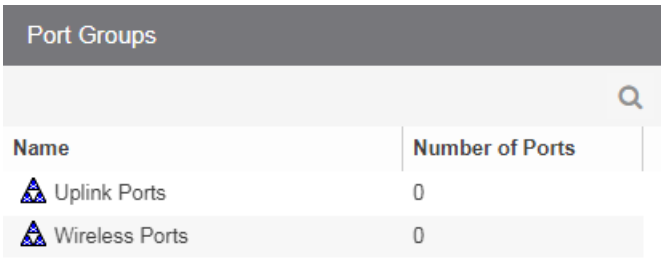
- How to Configure Ports

For information on related windows:

- Add/Remove Ports Window
- Port (Authentication) Tab

Extreme Management Center Details View (Port Groups)

This tab appears when you select the Devices/Port Groups > Port Groups left-panel tab. It displays a table of information about the existing port groups.



Name
Name of the port group.

Number of Ports
Number of ports in the port group.

Related Information

For information on related windows:

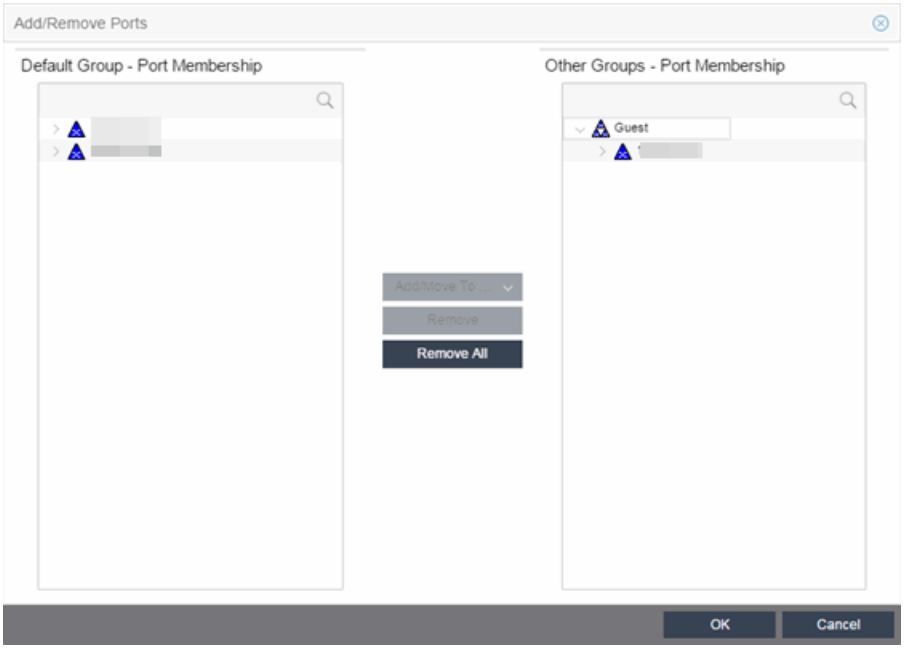
- Details View Tabs

Extreme Management Center Add/Remove Ports (User-Defined Port Groups)

Use the Add/Remove Ports window to add and remove ports from user-defined port groups.

To access this window, select the left-panel Port Groups tab. Expand the User-Defined Port Groups folder and select a port group. From this window you can:

- Click the Add/Remove Ports button in the right-panel Ports tab.
- Right-click a Port Group in the left-panel and select Add/Remove Ports.



Default Group — Port Membership

This list displays all the device groups, devices, and port groups in the current domain. Select the ports you want to add to the port group. You can select individual ports, devices, or groups of ports.

Other Groups — Port Membership

This field displays all the ports currently defined for the port group. Select the port you want to remove from the port group.

Add/Move To Button

Click Add/Move To and select the port group to add the ports selected in the Default Group — Port Membership list to the Other Groups — Port Membership list.

Remove Button

Click Remove to remove the ports selected in the Other Groups — Port Membership list from the port group.

Remove All Button

Click Remove All to remove all the ports in the Other Groups — Port Membership list.

Related Information

For information on related tasks:

- Adding Ports to a Port Group
- Removing Ports from a Port Group

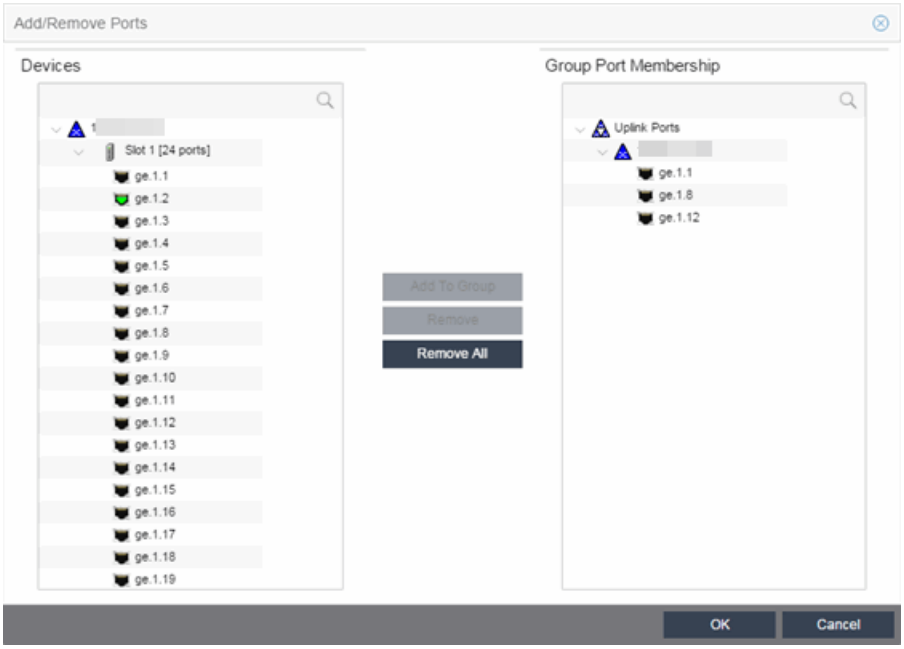
Add/Remove Ports

In this window, you can add and remove ports to and from port groups. Initially, all ports are grouped into a Default port group. When you create new port groups, you add ports from the Default group into your newly defined port groups using this window.

To access this window, open the Devices > Port Groups tab. Then, right-click on the port group to which the ports are being added and select Add/Remove Ports. The Add/Remove Ports window opens with the ports in the Default port group displayed in the left panel.

Add ports to the port group by selecting the ports in the left-panel, then selecting the port group in the right panel and clicking Add To Group.

NOTE: User based ports are not listed because user based port groups can only be one default.



Devices

This field displays the Devices assigned to the Policy Domain. Ports grouped in the Devices list are not members of the Port Group.

Group Port Membership

This field displays any port groups you have created and their currently defined ports.

Add To Group Button

Adds the ports selected under the Devices list to the port group selected on the right.

Remove Button

Select the ports you want to remove from a port group and click Remove to return the ports to the Devices list.

Remove All Button

Select a port group and click Remove All to remove all ports from the port group and return them to the Devices list.

Related Information

For information on related concepts:

- Getting Started with Class of Service

For information on related tasks:

- How to Define Rate Limits
- Creating Class of Service Port Groups
- How to Configure Transmit Queues

Extreme Management Center Port Authentication Configuration

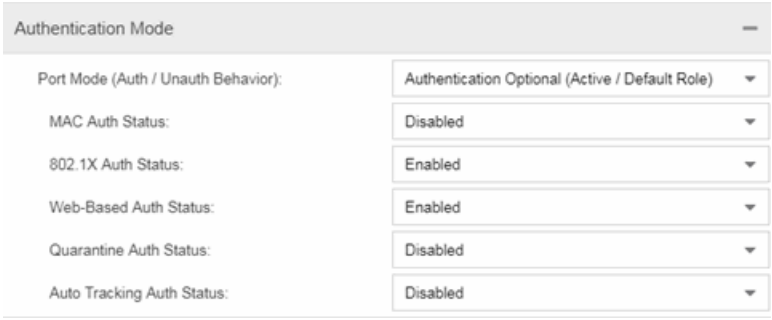
The Port Configuration tab allows you to configure and change the authentication settings for a port. Authentication must be configured and enabled on the device in order for individual port authentication settings to take effect. Only those areas of the tab that relate to the authentication type configured on the device are available for editing.

The Authentication Configuration tab has six sections:

- Authentication Mode
- RFC3580 VLAN Authorization
- Login Settings
- Automatic Re-Authentication
- Authenticated User Counts
- CEP Access

Authentication Mode

This section displays general authentication and port mode information about the port.



Port Mode

This area displays the current port mode for the port, and allows you to change the settings if desired. Port mode defines whether or not a user is required to authenticate on a port, and how unauthenticated traffic will be handled. It is a

combination of Authentication Behavior (whether or not authentication is enabled on the port), and Unauthenticated Behavior (whether unauthenticated traffic will be assigned to the port's default role or discarded). See Port Mode for a complete description of each port mode.

In addition, this section provides checkboxes that allow you to disable a specific authentication type at the port level.

Auth/Unauth Behavior

Select an option to specify how authenticated and unauthenticated traffic is handled on the port. (See Port Mode for more information.) If you set the port's Authentication Behavior to Active (i.e., you enable authentication for the port), it is recommended that you enable the Drop VLAN Tagged Frames feature.

NOTE: Authentication Behavior must be set to **Active** for authentication to be allowed using CEP Protocols.

Additionally, specify whether unauthenticated traffic is assigned to the port's default role or discarded. The current default role for the port is shown. For additional information, see Port Mode.

NOTE: For Single User 802.1X and 802.1X+MAC authentication types:

- Active/Default Role mode requires that a default role be set on the port
- Active/Discard mode requires that any default role set on the port is cleared

For Multi-User Web-based authentication Active/Discard mode is not supported.

MAC Auth Status

Select whether to enable or disable MAC authentication at the port level. If the device is only configured with MAC authentication, selecting this checkbox will result in the port Authentication Behavior being set to Inactive.

802.1X Auth Status

Select whether to enable or disable 802.1X authentication at the port level. If the device is only configured with 802.1X authentication, selecting this checkbox will result in the port Authentication Behavior being set to Inactive.

NOTE: For Single User 802.1X+MAC authentication with Active/Default Role as the selected port mode: Disabling 802.1X authentication also disables MAC authentication on the port. An end user connecting to the port will not be able to authenticate via 802.1X or MAC. The port will behave as if Inactive/Default Role is the selected port mode.

Web-Based Auth Status

Select whether to enable or disable web-based authentication at the port level. If the device is only configured with web-based authentication, selecting this checkbox will result in the port Authentication Behavior being set to Inactive.

NOTE: For Multi-User Web-Based authentication with Active/Discard as the selected port mode: This checkbox is automatically selected because multi-user web-based authentication does not support the Active/Discard port mode.

Quarantine Auth Status

Select whether to enable or disable Quarantine authentication at the port level. If the device is only configured with Quarantine authentication, selecting this checkbox will result in the port Authentication Behavior being set to Inactive.

Auto Tracking Auth Status

Select whether to enable or disable MAC authentication at the port level. If the device is only configured with Auto Tracking authentication, selecting this checkbox will result in the port Authentication Behavior being set to Inactive.

Apply Button

Applies any Port Mode changes to the port.

CEP protocols in the CEP Access tab

Use the CEP Access tab to disable CEP protocols at the port level.

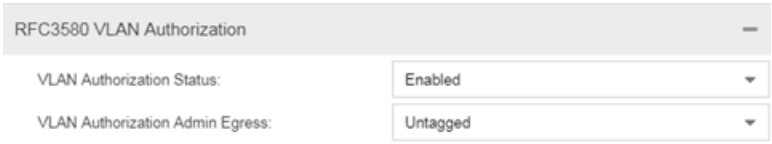
RFC3580 VLAN Authorization Tab

This tab lets you enable or disable RFC 3580 VLAN Authorization on the port and specify an egress state. RFC 3580 VLAN Authorization must be enabled in networks where the RADIUS server has been configured to return a VLAN ID when a user authenticates.

When RFC 3580 VLAN Authorization is enabled:

- ports on devices that do **not** support policy tag packets with the VLAN ID.
- ports on devices that do support policy and also support Authentication-Based VLAN to Role Mapping classify packets according to the role to which the VLAN ID maps.

You can also enable and disable VLAN Authorization at the device level using the device Authentication tab. If the device does not support RFC 3580, this tab is grayed out.



VLAN Authorization Status

Allows you to enable and disable RFC 3580 VLAN Authorization for the selected port. This option is grayed out if not supported by the device.

VLAN Authorization Admin Egress

Allows you to modify the VLAN egress list for the VLAN ID returned by the RADIUS server when a user authenticates on the port:

- None - No modification to the VLAN egress list will be made.
- Tagged - The port will be added to the list with the egress state set to Tagged (frames will be forwarded as tagged).
- Untagged - The port will be added to the list with the egress state set to Untagged (frames will be forwarded as untagged).
- Dynamic - The port will use information returned in the RADIUS response to modify the VLAN egress list. This value is supported only if the device supports a mechanism through which the egress state may be returned in the RADIUS response.

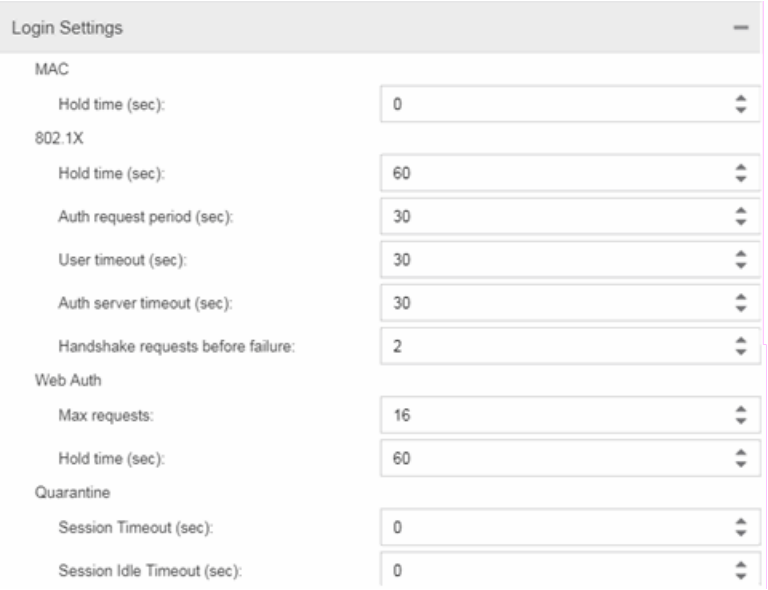
The current egress settings for the port are displayed in the VLAN Oper Egress column in the User Sessions tab. These options are grayed out if not supported by the device.

Apply Button

Saves any change you made to the VLAN Authorization settings.

Login Settings

This tab displays the current login settings for the port and allows you to change the settings if desired. The options available depend on what type(s) of authentication are enabled on the device.



Number of Attempts Before Timeout

Number of times a user can attempt to log in before authentication fails and login attempts are not allowed. For web-based authentication, valid values are 1-2147483647, zero is not allowed, and the default is 2. For 802.1X and MAC authentication, this value is permanently set to 1.

Hold Time (seconds)

Amount of time (in seconds) authentication will remain timed out after the specified Number of Attempts Before Timeout has been reached. Valid values are 0-65535. The default is 60. (Hold Time is also known as Quiet Period in web-based and MAC authentication.)

Authentication Request Period

For 802.1X authentication, how often (in seconds) the device queries the port to see if there is a new user on it. If a user is found, the device then attempts to authenticate the user. Valid values are 1-65535. The default is 30.

User Timeout

For 802.1X authentication, the amount of time (in seconds) the device waits for an answer when querying the port for the existence of a user. Valid values are 1-300. The default is 30.

Authentication Server Timeout

For 802.1X authentication, if a user is found on the port, the amount of time (in seconds) the device waits for a response from the authentication server before timing out. Valid values are 1-300. The default is 30.

Port Handshake Requests Before Failure

For 802.1X authentication, the number of times the device tries to finalize the authentication process with the user before the authentication request is considered invalid and authentication fails. Valid values are 1-10. The default is 2.

Quarantine Session Timeout (sec)

For Quarantine authentication, the maximum number of seconds an authenticated session may last before automatic termination of the session. A value of zero indicates that no session timeout will be applied.

Quarantine Session Idle Timeout (sec)

For Quarantine authentication, the maximum number of consecutive seconds an authenticated session may be idle before automatic termination of the session. A value of zero indicates that the device level setting is used.

Auto Tracking Session Timeout (sec)

For Auto Tracking sessions, the maximum number of seconds a session may last before automatic termination of the session. A value of zero indicates that the device level setting is used.

Auto Tracking Session Idle Timeout (sec)

For Auto Tracking sessions, the maximum number of consecutive seconds a session may be idle before automatic termination of the session. A value of zero indicates that the device level setting is used.

Apply Button

Applies the Login Settings changes to the port.

Automatic Re-Authentication

This tab is grayed out if only web-based authentication is enabled on the device. For 802.1X and MAC authentication, the Automatic Re-Authentication tab lets you set up the periodic automatic re-authentication of logged-in users on this port. Without disrupting the user's session, the device repeats the authentication process using the most recently obtained user login information to see if the same user is still logged in. Authenticated logged-in users are not required to log in again for re-authentication, as this occurs "behind the scenes."

802.1X Re-auth Status

If Active is selected, the re-authentication feature is enabled for 802.1X authentication. If Inactive is selected, the re-authentication feature is disabled.

802.1X Re-auth Frequency (sec)

How often (in seconds) the device checks the port to re-authenticate the logged-in user via 802.1X authentication. Valid values are 1-2147483647. The default is 3600.

MAC Re-auth Status

If Active is selected, the re-authentication feature is enabled for MAC authentication. If Inactive is selected, the re-authentication feature is disabled.

MAC Re-auth Frequency (sec)

How often (in seconds) the device checks the port to re-authenticate the logged in user via MAC authentication. Valid values are 1-2147483647. The default is 3600.

Authenticated User Counts

This tab provides authenticated user-count information for devices with Multi-User as their configured authentication type. See the device Authentication tab for information on setting the device authentication type.

Current Number of Users

The current number of users actively authenticated or have authentications in progress on this interface. If Multi-User authentication is disabled, this number is 0. Any unauthenticated traffic on the port is not included in this count.

Number of Users Allowed (up to 2048)

The number of users that can be actively authenticated or have authentications in progress at one time on this interface. If you set this value below the current number of users, end-user sessions exceeding that number are terminated.

NOTE: B2/C2 Devices. If you are configuring a single user and an IP phone per port, set this value to 2.

Number of MAC Users Allowed (up to 2048)

The number of users that can be actively authenticated via MAC authentication, or have MAC authentications in progress at one time on this interface. The number of MAC users allowed cannot exceed the number of users allowed. If you set this value below the current number of users, end user sessions exceeding that number are terminated. If MAC is not selected as a **Multi-User** authentication type on the device Authentication tab, this field will be grayed out.

Number of Quarantine Users Allowed (up to 2048)

The number of users that can be actively authenticated via Quarantine authentication, or have Quarantine authentications in progress at one time on this interface. The number of Quarantine users allowed cannot exceed the number of users allowed. If you set this value below the current number of users, end user sessions exceeding that number are terminated. If Quarantine Auth is not enabled on the device Authentication tab, this field will be grayed out.

Number of Auto Tracking Users Allowed (up to 2048)

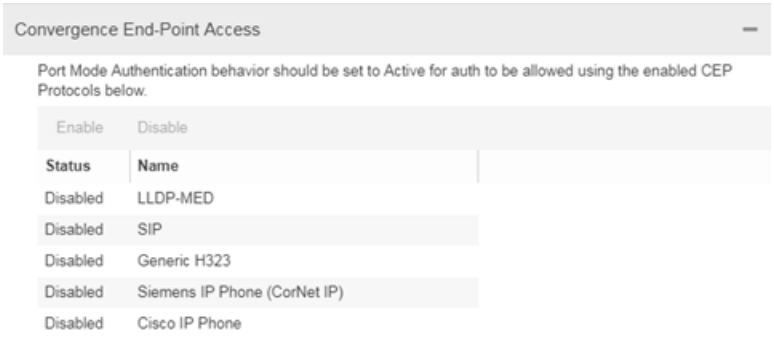
The number of Auto Tracking users that can be actively authenticated or have authentications in progress at one time on this interface. The number of Auto Tracking users allowed cannot exceed the number of users allowed. If you set this value below the current number of users, end user sessions exceeding that number will be terminated. If Auto Tracking is not enabled on the device Authentication tab, this field is grayed out.

Convergence End-Point Access

This tab lists all the CEP (Convergence End-Point) protocols supported by the device on which the port resides, and lets you enable or disable them for that port. For devices that do not support CEP, the tab is blank.

NOTE: Port Mode Authentication Behavior must be set to **Active** (on the General sub-tab) for authentication to be allowed using these CEP Protocols.

Enable CEP protocols for multiple ports using the Port Configuration Wizard. In addition to enabling protocols on the port, you must also configure CEP for the device on which the port resides. Configure CEP for a single device using the device Authentication tab (CEP sub-tab) or for multiple devices using the Device Configuration Wizard.



CEP Access

Lists all the CEP protocols supported by the device on which the port resides. Use the checkboxes to enable or disable CEP protocols on this port. If the device does not support the CEP feature, this area is blank.

Enable All Button

Selects all the checkboxes and enables all the CEP protocols for this port.

Disable All Button

Deselects all the checkboxes and disables all the CEP protocols for this port.

Apply Button

Applies CEP access changes to the port.

Related Information

For information on related tasks:

- How to Configure Ports
- Authentication Configuration Guide

For information on related tabs:

- Port Properties - Port Usage Tab
- Port Properties - General Tab

How To Use Extreme Management Center Policy

The **How To** section contains Help topics that give you instructions for performing tasks in the **Policy** tab.

How to Select on Add/Remove Windows

The **Policy** tab includes several Add/Remove windows in which you can add items from a left panel to a right panel, and remove items from the right panel. The following procedures explain how to make single and multiple selections in the panels and move the selections to the opposite panel.

Instructions on:

- Selecting single items
- Selecting multiple sequential items
- Selecting multiple non-sequential items

Selecting single items

To select one item from the left panel and add it to the right panel, click the item, then click the **Right Arrow** button.

To remove one item from the right panel, click the item, then click the **Left Arrow** button.

Selecting multiple sequential items

To select a sequence of items in the left panel and add them to the right panel:

1. Hold down the **Shift** key and click the first and last (or last and first) items in the sequence.
2. Click the **Right Arrow** button.

To remove a sequence of items from the right panel:

1. Hold down the **Shift** key and click the first and last (or last and first) items in the sequence.
2. Click the **Left Arrow** button.

Selecting multiple non-sequential items

To select multiple non-sequential items in the left panel and add them to the right panel:

1. Hold down the **Ctrl** key and click each item you want to add.
2. Click the **Right Arrow** button.

To remove multiple non-sequential items from the right panel:

1. Hold down the **Ctrl** key and click each item you want to remove.
2. Click the **Left Arrow** button.

How to Create and Use Domains

Extreme Management Center provides the ability to create multiple policy configurations by allowing you to group your roles and devices into Policy Domains. A Policy Domain contains any number of roles and a set of devices that are uniquely assigned to that particular domain. For example, a university may have a Dormitory domain with a policy configuration created for students, and an Administration domain with a policy configuration for staff members.

You can create multiple domains and easily switch from one domain to another. You can also export policy domain configuration data to a .pmd file, (one file per domain) for backup and troubleshooting purposes, and you can import data from a .pmd file into a policy domain.

In order for your network devices to be displayed in the **Policy** tab's left-panel **Devices** tab, they must be assigned to a Policy Domain. Initially, you must use a device Discover to add your devices to the Extreme Management Center database. Once your devices are in the database, you can assign the devices to a Policy Domain. As soon as the devices are assigned to a domain, they are automatically displayed in the **Policy** tab's left-panel **Devices** tab. Only devices that support policy are displayed.

Extreme Management Center automatically locks the current Policy Domain when you begin to edit the domain configuration. Other users are notified that the domain is locked and they are not be able to save their own domain changes until the lock is released. For more information, see Controlling Client Interactions with Locks. After a modification is made, you must save the domain

to notify all clients that are viewing that domain of the change, and automatically update their view with the new configuration.

Instructions on:

- Creating a New Domain
- Opening a Domain
- Assigning Devices to a Domain
- Removing Devices From a Domain
- Importing a File into a Domain
- Exporting a Domain to a File
- Importing Data from a Domain
- Saving a Domain
- Reading a Domain
- Renaming a Domain
- Deleting a Domain

Creating a New Domain

Use these steps to create a new Policy Domain.

1. Select **Open/Manage Domain > Create Domain**.
2. Enter the name for the new domain. Click **OK**.
3. A new (blank) Domain opens.
4. Select the **Global Domain Settings > Do Not Use Global Services** checkbox if you don't want the domain to include and display services common to all domains.
5. Proceed with assigning devices to the domain and then configuring the desired policies.

Opening a Domain

In Extreme Management Center, you work in one current domain at a time. To change to a different domain, use the **Open/Manage Domain > Open Domain** menu to select the desired domain. If you have made changes to the current domain, you are prompted to update the database with the current domain configuration prior to opening the new domain.

Assigning Devices to a Domain

Initially, you must perform a device Discover to add a device to the Extreme Management Center database. Once your devices have been added to the database, you must assign the devices to a Policy Domain. A device can exist in only one Policy Domain. As soon as the devices are assigned to a domain, they are automatically displayed in the **Policy** tab's left-panel **Devices** tab. Only devices assigned to the Policy Domain you are currently viewing are displayed in the tab.

Use these steps to assign devices to a Policy Domain.

1. If necessary, open the domain to which you want to assign devices.
2. Select **Open/Manage Domain > Assign Devices to Domain**. The Assign Devices to Domain window opens.
3. Devices in the database but not assigned to a domain are listed in the left-panel Unassigned folder (including devices that do not support policy). The left panel also displays any other domains and the devices assigned to those domains. Use the drop-down list to select a single domain or All Other Domains. If you select All Other Domains, use the bottom panel to view the domain to which each device is assigned.

   Note: Select the search icon to search for a device. A search box is available to filter through the visible device tree.
4. The right panel displays the current domain and the devices assigned to that domain. To add a device to the current domain, select the device in the left panel and click **Add**. You can also select and add multiple devices.
5. To remove a device from the current domain, select the device and click **Remove**. This removes the device from the current domain and places it back in the device tree as either unassigned or as a member of the domain from which it came. It does not delete the device from the Extreme Management Center database.
6. Click **OK**.
7. The selected devices are assigned to the current domain and displayed in the **Policy** tab left-panel **Devices** tab. (Only devices that support policy are assigned to the domain and displayed.)

Removing Devices From a Domain

Removing a device from a domain, removes the device from the **Devices** tab and places it in the Unassigned folder in the Assign Devices to Domain window.

NOTE: Removing a device from a domain does not delete the device from the Extreme Management Center database. To delete a device from the database, right-click on the device in the left-panel **Devices** tab, and select **Delete** from the menu. When a device is deleted from the database, it is automatically removed from Extreme Management Center and the **Devices** tab.

1. If necessary, open the domain from which you want to remove devices.
2. Select **Open/Manage Domain > Assign Devices to Domain**. The Assign Devices to Domain window opens.
3. The right panel displays the current domain and the devices assigned to that domain. To remove a device from the current domain, select the device from the Current Domain right-panel and click the left arrow. This removes the device from the current domain and places it back in the device tree as either unassigned or as a member of the domain from which it came. It does not delete the device from the Extreme Management Center database.
4. Click **OK**.

Importing a File into a Domain

You can import policy data from a PMD file into a Policy Domain.

1. Make sure that the domain you want to import a file into is your current domain.
2. Select **Open/Manage Domain > Import/Export > Import From File**. The Import from File window opens.
3. Enter the name and path for the data file (PMD) you want to import, or browse to the file. Clicking **Select File**, opens a dialog box from which you can select a data file by searching your local drive or a network drive.
4. Select the specific data elements you want to import or click **Select All** to select all the data import options at once. See Data Elements to Import for important information on each element and how they are imported.
5. To append, update, or overwrite the global rules with the PMD file you are importing, select the **Global Services & Rules** checkbox.
6. Select how you want the imported data applied to your current domain. Click on the links below for detailed information on how each specific action affects the import of certain data elements.
    - Append data to existing elements
    - Update existing data with elements from domain
    - Overwrite existing elements

7. Click **OK**. The data elements are imported and see a message regarding import status.

Exporting a Domain to a File

You can export policy data from a Policy Domain to a PMD file.

1. Select **Open/Manage Domain > Import/Export > Export to File**.
2. Select the **Domain** to save as a PMD file.
3. Click **Export**.
4. The Policy Domain is downloaded to the default file download location.

Importing Data from a Domain

You can import policy configuration data from one policy domain into another.

1. Ensure your current domain is the domain into which you want to import data.
2. Select **Open/Manage Domain > Import/Export > Import From Domain**. (This menu option is not available if only one domain exists, as there are no other domains from which to import data.) The Import from Domain window opens.
3. Use the drop-down list to select the domain whose data you want to import.
4. Select the specific data elements you want to import or click **Select All** to select all the data import options at once. See Data Elements to Import for important information on each element and how they are imported.
5. Select how you want the imported data applied to your current domain. Click on the links below for detailed information on how each specific action affects the import of certain data elements.
    - Append data to existing elements
    - Update existing data with elements from domain
    - Overwrite existing elements
6. Click **Import**. The data elements are imported and you see a message regarding import status.

Saving a Domain

After a Policy Domain has been changed, you must save the domain to notify all clients using that domain of the change and automatically update their tab with the new configuration. An asterisk (*) is displayed beside the Policy tab title

when you have made changes to the domain that need to be saved. You can save a Policy Domain by selecting **Open/Manage Domain > Save Domain**. To discard unsaved changes you made to a domain, open the **Open/Manage Domains > Open Domain** menu and select the domain in which you are currently working.

Renaming a Domain

You can rename the current Policy Domain by selecting **Open/Manage Domain > Rename Domain** and entering a new name.

Deleting a Domain

You can delete one or more Policy Domains by selecting **Open/Manage Domain > Delete Domain**.

Related Information

For information on related tasks:

- How to Add and Delete Devices

For information on related windows:

- Assign Devices to Domain Window
- Import from Domain Window
- Import from File Window

How to Create a Role

A role is a policy profile consisting of a set of network access services that you can apply at various access points in a policy-enabled network. A port takes on a user's role when the user authenticates.

Creating a role using the role tabs consists of creating a name for the role with the **Create Role** menu option, then defining its characteristics (default class of service, default access control, and/or services) using the role's right-panel tabs. You might also use this method if you are creating a role for which there is default class of service and/or access control, but no services.

If you want to change the characteristics of a role, you can select the role in the left panel and use the right panel to modify it.

Instructions on:

- Using the **Role** Tabs
- Modifying a Role
- Deleting a Role

Using the Role Tabs

Creating a role using the **Role** tab consists of creating a name for the role, then using the right panel to specify the characteristics of the role (default class of service, default access control, and/or services).

1. In the **Policy** tab left panel, select the **Roles/Services > Roles** tab.
2. Right-click the **Roles** tab, and select **Create Role**.
   The Create window opens.
3. Type the role name in the highlighted box. The name can be up to 64 characters in length, and special characters are allowed, with the exception of colons (:) and semicolons (;). Duplicate names are not allowed, regardless of case. For example, if you already have a role `Faculty` and you attempt to name the new role `Faculty` or `faculty`, the **Policy** tab creates the role, but with the name `New Role`, or `New Role`*n* (where *n* is the sequence number, if there is more than one `New Role`). You can then rename the new role. Press **Enter** after you've entered the name. (If you don't press **Enter**, the name remains `New Role`.)
4. Select the role in the left panel, and the role opens in the right panel. Use the right panel to add a role description, enable TCI Overwrite, and set the role's default actions (including access control and class of service).
5. In the Services section in the right panel, click the **Add/Remove Services** button to add services to the role. This opens the role Add/Remove Services window.

   NOTE: The **Policy** tab checks for rule conflicts when more than one service is added. See Conflict Checking for more information.

6. To add a VLAN to the Role's Egress list, select the role and use the VLAN Egress tab in the right panel.

7. To configure MAC, IP, and VLAN to role mapping lists for the role, select the role and use the **Mappings** tab in the right panel.
8. Now that you have created the role, you can:
    - Assign the role as the default role for a port
    - Modify the role's characteristics
9. Enforce to write the new information to the devices.

Modifying a Role

Once you've created a role, you can change its characteristics by selecting the role in the Policy tab's left panel and using the associated tabs in the right panel.

Instructions on:

- Adding Services to Roles
- Modifying a Role's Default Class of Service
- Modifying a Role's Default Access Control
- Modifying a Role's Description
- Modifying a Role's Ports
- Removing Services from Roles

Adding Services to Roles

To add services to roles:

1. Select the left panel **Roles/Services > Roles** tab and expand the **Roles** tab. Select the role to which you want to add services in the left panel, then select the **General** tab in the right panel.
2. Click **Add/Remove Services**. This opens the Add/Remove Services window.
3. Make sure the role to which you wish to add services is displayed in the Role selection box.
4. In the Groups and Services panel, select the services and/or service groups you wish to add to the role, and click the **Right Arrow** button. To remove services, select them in the Selected Services panel and click the **Left Arrow** button.

NOTE: The Policy tab checks for rule conflicts when more than one service is added. See Conflict Checking for more information.

5. If you wish, you can select another role, and add or remove services from it.
6. Click **OK**.
7. Enforce to write the new information to the devices.

Removing Services from a Role

1. Select the left panel **Roles/Services > Roles** tab and expand the Roles folder.
2. Select the role from which you want to remove services, then select the **General** tab in the right panel.
3. Click **Add/Remove Services**. This opens the Add/Remove Services window.
4. Make sure the role from which you wish to remove services is displayed in the Role selection box.
5. In the Selected Services panel, select the services and/or service groups you wish to remove from the role, and click the **Left Arrow** button. To add services, select them in the Groups and Services panel and click the **Right Arrow** button.
6. If you wish, you can select another role, and remove services from or add services to it.
7. Click **OK**.
8. Enforce to write the new information to the devices.

Modifying a Role's Default Class of Service

Use the role's **General** tab to change its default class of service settings. Be sure to enforce to write the new information to the devices.

Modifying a Role's Default Access Control

Use the role's **General** tab to change its default access control. Be sure to enforce to write the new information to the devices.

Modifying a Role's Description

You can edit the description for the role on the role's **General** tab. Click **OK** to save the change to the database.

Modifying a Role's Ports

You can select a port and choose the default role on the Ports tab. You can also select **PortView** to open the PortView for the port or make changes to the port settings themselves.

1. In the **Policy** tab left panel, select a device in the **Devices** left-panel tab.
2. Select the port on which you want to set a default role.
3. Right-click the port and select **Policy > Set Default Role**.
4. Click the **Assign/Replace Default Role** checkbox. The drop-down menu is available.
5. Select the default role for the port from the drop-down menu.
6. Click **OK**.
7. Enforce to write the new information to the devices.

Mapping a Role to an HTTP Redirect Group

The HTTP Redirect action allows the role/rule to be mapped to an HTTP Redirect group index. The action widgets contain a menu to edit the group configuration.

Deleting a Role

1. In the **Policy** tab left panel, select a device in the **Devices** left-panel tab.
2. Select the port on which you want to delete the default role.
3. Right-click the port and select **Policy > Set Default Role**.
4. Click the **Clear Default Role** checkbox.
5. Select the default role for the port.
6. Click **OK**.
7. Enforce to write the new information to the devices.

Related Information

For information on related concepts:

- Traffic Classification Rules

For information on related tasks:

- Assigning Default Roles to Ports
- Clearing Default Roles from Ports
- How to Make Selections on Add/Remove Windows
- How to Assign a Default Role to a Port

For information on related windows:

- Add/Remove Services Window
- General Tab (Role)

How to Assign a Default Role to a Port

In the **Policy** tab, you can specify a default role for the port. To configure ports you use the Set Default Role window.

Assigning and Clearing a Default Role

Configuring a port allows you to set the port mode, establish login settings, set the default role, and enables you to view the current configuration on the port.

- Assigning Default Roles to Ports
- Clearing Default Roles from Ports

Assigning Default Roles to Ports

NOTE: Setting a default role on an ExtremeWireless Controller port that is not yet a VNS, creates a new VNS on the wireless controller.

1. Select a device in the left-panel **Devices** tab and expand a slot or ports grouping in the right-panel Details view.
2. Right-click the desired port and select **Policy > Set Default Role** from the menu. The Set Default Role window opens.
3. Click **Assign/Replace Default Role** and select a role in the drop-down menu.
4. Click **OK**.

Clearing Default Roles from Ports

You can clear the default role from a single port, or from multiple ports.

1. Select a device in the left-panel **Devices** tab and expand a slot or ports grouping in the right-panel Details view.
2. Right-click the desired port and select **Policy > Set Default Role** from the menu. The Set Default Role window opens.
3. Click **Clear Default Role**.
4. Click **OK**.

NOTE: If you are replacing the current default role with another one, you don't need to clear the current default role. Selecting the new default role and clicking **OK** clears the previous default role automatically.

How to Create a Quarantine Role

The Quarantine role is a highly restrictive role used to isolate users and restrict network access.

The Quarantine role is used in conjunction with the Extreme Networks Intrusion Prevention System (IPS) to create an automatic response to threats detected on the network. Once the Quarantine role has been enforced to the network and the Extreme Networks IPS is properly configured, this role can be automatically set as the default role on any port where a threat has been detected. Normally, roles are applied to ports via authentication.

You can also set the Quarantine role as a port's default role if, for example, you have modified the role to provide some limited access and you want to use it as a "guest" role.

The **Policy** tab default domain includes the Quarantine role. However, if you add a new domain, you need to create the Quarantine role. For information on how to create a role, see How to Create a Role.

After you have created the role, you can modify the role's default class of service and access control settings, and make changes to the role's services and rules using the right-panel tabs, just like any other role. If you make any changes to the Quarantine role, keep in mind that the role may be used by other applications and should remain highly restrictive in nature.

Instructions on:

- Modifying the Quarantine Role: Use the right-panel tabs to modify the Quarantine role's default values and add or remove services.
- Setting the Quarantine Role as the Default Role on a Port: Use the right-panel General tab or the Port Configuration wizard to set the Quarantine role as a default role on a port.

Modifying the Quarantine Role

Once you've created a Quarantine role, you can change its characteristics by selecting the role in the **Policy** tab's left panel and using the associated tabs in the right panel.

NOTE: You cannot rename the Quarantine role.

Modifying Default Values

Use the General tab to change the Quarantine role's default class of service and default access control settings, and to add or edit a description.

1. Select the Quarantine Role in the left-panel **Roles** tab.
2. In the right-panel **General** tab, select the desired default class of service and default access control settings.
3. If desired, add or edit the role's description.
4. Be sure to perform an Enforce to write the new Quarantine role to the devices.

Adding/Removing Services

Use the General tab to add or remove services to the Quarantine role.

1. Select the Quarantine Role in the left-panel Roles tab.
2. In the right-panel General tab, click **Add/Remove Services**. This opens the Add/Remove Services window.
3. Make sure the Quarantine role is displayed in the Role selection box.
4. Select the service or service group in the All Services & Service Groups and click the **Right Arrow** button to add them to the Selected Services & Service Groups list. To remove services, select them in the Selected Services & Service Groups list and click the **Left Arrow** button. To remove all services, click the **Double Left Arrow** button.

NOTE: The Policy tab checks for rule conflicts when more than one service is added. See Conflict Checking for more information.

5. Click OK.
6. Be sure to perform an Enforce to write the new Quarantine role to the devices.

Setting the Quarantine Role as the Default Role on a Port

There may be circumstances when you would like to use the Policy tab to assign the Quarantine role as the default role on one or more ports. For example, if you have modified the Quarantine role to provide limited access, you may want to use it as the default role for guest users on your network.

The Quarantine role is assigned as a default role just like any other role. Refer to Assigning Default Roles to Ports for instructions.

Related Information

For information on related tasks:

- Assigning Default Roles to Ports

For information on related windows:

- Add/Remove Services Window
- General Tab (Role)

How to Create a Service

Services are sets of rules that define how network traffic for a particular network service or application should be handled by a network access device. A service might consist of only one rule governing, for example, email priority, or it might consist of a complex set of rules combining class of service, filtering, rate limiting, and access control (VLAN) assignment. Extreme Management Center policy allows you to create Local Services (services unique to the current domain) and Global Services (services common to all domains). Global Services let you easily create and manage services shared between all your domains.

Services can be one of two types: Manual Service or Automated Service.

- Manual Service — This service consists of one or more traffic classification rules you create based on your requirements. Manual services are good for applying customized sets of rules to roles.
- Automated Service — This service automatically creates a rule with a specified action (class of service and/or access control), for each device in a particular network resource group or groups. You create a network resource group using a list of MAC or IP addresses, and then associate the group with the Automated service (see How to Create a Network Resource for more information). Automated rule types include Layer 2 MAC Address rules, Layer 3 IP Address and IP Socket rules, and Layer 4 IP UDP Port and IP TCP Port rules.

To create a service using the service tabs, right-click the Services tab and select **Create Service**. If you are creating a Manual service, you can then use the Create Rule menu option and the tabs for the rule to define the rules for the service. You can also use the service tabs and rule tabs to modify an existing service and its rules.

Once you've created a service, you can apply it to any number of roles in the **Policy** tab. A role may utilize both Manual and Automated services.

Instructions on:

- Using the Service Tabs
- Modifying a Service
- Deleting a Service

Using the Service Tabs

The following steps depend on whether you are creating a Manual or an Automated service. For an Automated service, you create the service, select the newly created service, and define the class of service and/or access control for the service in the right-panel. For a Manual service, you create the service and then use the Create Rule menu option and the tabs for the rule to define the rules for the service.

Creating an Automated Service

1. In the left panel, select the **Service Repository** tab.

2. Expand either the **Local Services** tab or the **Global Services** tab depending on whether you want the service to be local (unique to the current domain) or global (shared between all your domains).
3. Right-click on the **Services** tab and select **Create Automated Service**. A New Service item is created in the left panel in a highlighted box.
4. Type the service name in the Create window. The service name is case-sensitive; therefore, Extreme Management Center policy sees `Engineer` and `engineer` as two different service names. Click **OK**. If you don't do this, the name remains `New Service`. The right-panel displays the service you created.
5. Define the rule's traffic description and actions, and enter a description of the service, if desired. For information on configuring the fields on this tab, see the Automated Service window Help topic.
6. Enforce to write the new information to your devices.

Creating a Manual Service

1. In the left panel, select the **Service Repository** tab.
2. Expand either the **Local Services** tab or the **Global Services** tab depending on whether you want the service to be local (unique to the current domain) or global (shared between all your domains).
3. Right-click on the **Services** tab and select **Create Service**. A New Service item is created in the left panel in a highlighted box.
4. Type the service name in the Create window. The service name is case-sensitive; therefore, the Policy view sees `Engineer` and `engineer` as two different service names. Click **OK**. If you don't do this, the name remains `New Service`. The service is created.
5. Define rules for the service. For more information, see Using the Rule General Tab.

   NOTE: When you add more than one rule to a service, Extreme Management Center checks for conflicts with other rules in the service. See Conflict Checking for more information.

6. Enforce to write the new information to your devices.

Modifying a Service

Once you've created a service, you can change its characteristics by selecting the service or its rules in the left-panel **Services** tab and using the menu options or associated right-panel tabs.

Modifying a Service Description

You can edit the description for the service by selecting it and clicking the **Edit** button beside the **Description** field in the right-panel. Enter a description in the Edit Description window and click **Save** to save the change to the database.

Modifying a Service Name

1. In the left panel, select the **Service Repository** tab.
2. Expand the **Local** or **Global Services** tab and then the **Services** tab, and select the service you want to modify.

   NOTE: If the service is a member of a service group and it's more convenient, you can find the service under the service group in the Service Groups folder. Any change you make to the name there are also reflected in the **Services** tab.

3. Right-click the service whose name you want to change, and select **Rename**.
4. Type the new name in the Rename window.
5. Click **OK** to save the change to the database.

Modifying the Roles for a Service

You can see all the roles associated with a particular service in the Role/Service Usage window.

1. In the left-panel **Roles** tab, select the Role to which you are adding or removing a service.
2. Click the Add/Remove button in the Services section of the window to open the Add/Remove Services window.
   - Add a service by selecting it from the All Services & Service Groups column and moving it to the Selected Services & Service Groups column by clicking the right arrow.

- Remove a service by selecting it from the Selected Services & Service Groups column and moving it to the All Services & Service Groups column by clicking the left arrow.

3. Click **OK** to save the changes.
4. Enforce to write the new information to your devices.

Adding a Service to Roles

A newly created service can be added to multiple roles at once using the Add to Role(s) menu.

1. In the left panel, select the **Roles/Services** drop-down menu.
2. Right-click the service or service group(s) and select **Add to Role(s)**.
3. Select one of more Roles to add to the selected Service/Service Group(s) to.
4. Click **OK** to save the changes.

Modifying the Rules for a Manual Service

1. Select the left-panel **Services** tab and locate the service you want to modify.

NOTE: If the service is a member of a service group and it's more convenient, you can find the service under the service group in the **Service Groups** tab. Any change you make to the rule there will also be reflected in the **Services** tab.

---

2. Select the service to display its rules.
3. Select the rule you want to change, then use the right-panel tabs to make your changes.
4. Enforce to write the new information to your devices.

Modifying an Automated Service

1. Open the left-panel **Services** tab.

NOTE: If the service is a member of a service group and it's more convenient, you can find the service under the service group in the **Service Groups** tab. Any change you make to the service there are also reflected in the **Services** tab.

---

2. Select the service you want to modify. The Automated Service window opens in the right panel.

3. Modify the characteristics of the Automated service as required.
4. Enforce to write the new information to your devices.

Deleting a Service

Deleting a service removes the service and its rules. If copies of the rules exist for other services, those copies are not affected by the deletion. However, deleting the service removes it from any service groups and roles with which it was associated, so be sure the service is not needed before you delete it. Deleting a Global service deletes the service from all your domains.

1. Select the left-panel **Roles/Services > Service Repository** tab.
2. Expand the **Services** tab in either the **Local Services** or **Global Services** tab, depending on the type of service you are deleting.

   NOTE: If the service is a member of a service group and it's more convenient, you can find the service under the service group in the **Service Groups** tab. Any change you make to the service there are also reflected in the **Services** tab.

3. Right-click the service you want to delete, and select **Delete**.
4. Click **Yes** to confirm, then **OK** to clear the confirmation message.
5. Enforce to write the change to your devices.

Related Information

For information on related concepts:

- Traffic Classification Rules

For information on related tasks:

- Adding Services to Roles
- Adding Services to Service Groups
- Creating Service Groups
- How to Create a Class of Service
- How to Create a Network Resource Group
- How to Create or Modify a Rule
- How to Define a Rate Limit

For information on related windows:

- Details View Tabs
- Automated Service Tab

How to Create a Service Group

Extreme Management Center Policy lets you create service groups into which you can group Local and Global services. A service group can contain any number of services, as well as other service groups. A service can be a part of more than one group.

Instructions on:

- Creating a Service Group
- Adding Services to a Service Group
- Removing Services from a Service Group

Creating a Service Group

1. In Extreme Management Center, select the **Control** tab.
2. Open the **Policy** tab and select **Roles/Services** > **Service Repository** left-panel tab. Expand the **Local Services** or **Global Services** tab.
3. Right-click on the Service Groups folder and select **Create Service Group**. This opens the Create window where you can enter a name for the new service group.
4. Type the service group name in the highlighted box and click **OK**. You can now add services to the service group. Once a service group has been created at the top level under the Service Groups folder, it can be added to another service group.

Adding Services to a Service Group

A service group can contain any number of services, as well as other service groups. You can add services to a service group by

1. Right-click the service group from which you wish to remove services, and select **Add/Remove Services**.
2. In the Add/Remove Services window, select the services or service groups you want to add to the service group, and click the **Right Arrow** button.
3. Click **OK**.

Removing Services from a Service Group

Use the following steps to remove a service or service group from a service group. Removing a service from a service group does not delete the service itself. If you want to delete the service itself, see Deleting a Service. Keep in mind that if you change the contents of a service group, Extreme Management Center automatically updates the services list for any role that the service group is associated with, affecting the rules in the role.

1. Right-click the service group from which you wish to remove services, and select **Add/Remove Services**.
2. In the Add/Remove Services window, select the services or service groups you want to remove from the service group, and click the **Left Arrow** button.
3. Click **OK**.

Related Information

For information on related tasks:

- How to Create a Service
- Deleting a Service

For information on related windows:

- Add/Remove Services (Roles) Window

How to Create or Modify a Rule

Traffic Classification rules allow you to assign a class of service and/or access control (VLAN membership) to network traffic, depending on the traffic's classification type. Classification types are based on layers 2, 3, and 4 of the OSI model, and traffic is classified according to specific layer 2/3/4 information contained in each frame. For more information, see Traffic Classification Rules.

A rule has two main parts: Traffic Description and Actions. The Traffic Description identifies the type of traffic to which the rule pertains. Actions specify whether that traffic is assigned class of service, access control, or both.

In order to create a rule, you must first create a service with which to associate it.

Instructions on:

Creating a Rule

When you create a rule using the Rule tab, you first create and name the rule using the **Create Rule** menu option, then define its characteristics in the right panel. You can also use the right panel to modify an exiting rule's characteristics.

1. In the **Policy** tab left panel, select the **Roles/Services > Service Repository** tab.
2. Expand either the **Local** or **Global Services** folder, depending on whether the rule is going to be used locally or by all users.
3. Expand either the **Service Groups** or **Services** folder and click on the service for which you want to create a rule.
4. Right-click on the service and select **Create Rule**.
5. In the Create Rule window, enter a name for the rule and select the rule type. Click **OK**. The rule is created in the left-panel tree.
6. Select the rule to and use the associated right-panel **Rule** tab to define the rule. Refer to the Rule tab Help topic for information on configuring the rule.
7. Enforce to write the new information to the devices.

Disabling/Enabling a Rule

In the **Policy** tab, you can disable and enable individual or multiple rules. You can also disable and enable all the rules associated with a service, or all the rules for all the services in a service group. The rule icon in the left panel displays a red X if the rule is disabled.

Disabling a rule is an alternative to deleting and recreating it. If you disable a rule, it is temporarily unavailable for use by the service with which it is associated. However, the rule can be copied to another service and enabled for that service.

Disabling/Enabling an Individual Rule

You can enable or disable a rule on the Rule tab or by right-clicking on the rule in the **Service Repository** tab and selecting **Disable Rule(s)** or **Enable Rule(s)**.

1. In the **Policy** tab left panel, select the **Roles/Services > Service Repository** tab.
2. Expand either the **Local** or **Global Services** folder, depending on whether the rule is going to be used locally or by all users.
3. Expand either the **Service Groups** or **Services** folder and click on the service for which you want to create a rule.
4. Select the rule you want to disable or enable.
   The Rule tab opens in the right panel.
5. Select **Enable** or **Disable** in the **Rule Status** field. Disabling the rule turns on the red X on the rule icon in the left panel, and re-enabling it turns it off.
6. Enforce to write the new information to the devices.

Disabling/Enabling the Rules for a Service or Service Group

If a service is associated with more than one service group, disabling or enabling the rules for the service in one service group will disable/enable the rules for the service in the other service groups of which the service is a part.

1. In the **Policy** tab left panel, select the **Roles/Services > Service Repository** tab.
2. Expand either the **Local** or **Global Services** folder, depending on whether the rule is used locally or by all users.
3. Right-click the service or service group containing the rules you want to disable or enable and select **Disable Rule(s)** or **Enable Rule(s)**.
4. Click **Yes** to confirm the change.
5. Enforce to write the new information to the devices.

Deleting a Rule

Deleting a rule removes the rule from a service. If the service is also part of a service group, the rule is deleted there as well, so be sure the rule is not needed before you delete it.

1. In the **Policy** tab left panel, select the **Roles/Services > Service Repository** tab.
2. Expand either the **Local** or **Global Services** folder, depending on whether you are deleting a rule used locally or by all users.
3. Right-click the rule you want to delete, and select **Delete**.
4. Click **Yes** to confirm, then **OK** to clear the confirmation message. The rule is deleted wherever it exists.
5. Enforce to write the new information to the devices.

Related Information

For information on related concepts:

- Traffic Classification Rules

For information on related windows:

- Edit Rule Window
- Rule Tab

How to Define Rate Limits

The **Policy** tab allows you to create and define rate limits as components of a class of service. Rate limits are used to control the transmit rate at which traffic enters and exits ports in your network.

The **Policy** tab uses role-based rate limits that are tied directly to roles and rules, and are written to a device when the role/rule is enforced.

Instructions on:

- Defining Rate Limits
- Removing a Rate Limit

Defining Rate Limits

Rate limits are defined within a class of service and associated with a specific role via a rule action or as a role default. When role-based rate limits are implemented, all traffic on the port that matches the rule with the associated rate limit cannot exceed the configured limit. If the rate exceeds the configured limit, frames are dropped until the rate falls below the limit.

The rate limit remains on the port only as long as the role using the rate limit is active on the port either as the authenticated role or as the port's default role.

1. Open the **Class of Service > CoS Components** left-panel tab on the **Policy** tab.
2. Right-click the **Rate Limits** left-panel tab and select **Create Rate Limit**.
3. Create a new rate limit using the **Rate Limit** tab.

4. Select the desired CoS and in the **Class of Service** left-panel tab. Select the **View/Edit** button for the appropriate rate limit to open the Create Rate Limit/Shaper window.
5. Fill out the Create Rate Limit/Shaper window:
    a. Specify the desired rate limit.
    b. Select the action you would like performed if the rate limit is exceeded:
        - Generate System Log on Rate Violation — a syslog message is generated when the rate limit is first exceeded.
        - Generate Audit Trap on Rate Violation — an audit trap is generated when the rate limit is first exceeded.
        - Disable Port on Rate Violation — the port is disabled when the rate limit is first exceeded.

        NOTE: N-Series Gold devices do not support rate limit notification.

    c. Click **OK**.

The rate limit appears in the CoS Configuration table mapped to the CoS.

Role-based rate limits are written to your devices when you enforce the role that includes them.

Removing a Rate Limit

Rate limits remain on a port only as long as the role using the rate limit is active on the port either as the authenticated role or as the port's default role. To remove a rate limit, you must delete it from the **Policy** tab and then enforce. This removes the rate limit from any roles with it is associated.

1. Select the **Class of Service > CoS Components > Rate Limits** left-panel tab on the **Policy** tab.
2. In the right-panel table, right-click on the rate you want to remove.
3. Select **Delete**.
4. Enforce.

NOTE: If you simply select **None** from the drop-down menu, it un-maps the rate from the class of service but it does not remove the rate limit.

Related Information

For information on related concepts:

- Rate Limits

For information on related tasks:

- How to Create a Class of Service

For information on related windows:

- Create Rate Limit Window
- General Tab (Rate Limit)

How to Create a Class of Service

The **Policy** tab lets you define classes of service (CoS) that can include one or more of the following components: an 802.1p priority, an IP type of service (ToS) value, drop precedence, rate limits, and transmit queue configuration.

Initially, the Class of Service Configuration window (available from the **Policy** tab **Class of Service** left-menu tab) is pre-populated with eight static classes of service, each associated with one of the 802.1p priorities (0-7). You can use these classes of service as is, or configure them to include ToS, rate limit, and/or transmit queue values. In addition, you can also create your own classes of service.

After you have created and defined your classes of service, they are then available when you make a class of service selection for a rule action (**Rule** tab), a role default (**General** tab), or an automated service (**Automated Service** window).

It is recommended that you read Getting Started with Class of Service before creating your classes of service.

Instructions on:

- Creating a Class of Service
- Creating Class of Service Port Groups
- Deleting a Class of Service

Creating a Class of Service

The basic components for a class of service include an 802.1p priority, an IP type of service (ToS) value, drop precedence, rate limits, and transmit queue configuration.

Use the following instructions to create a new class of service using the Class of Service Configuration window.

1. Open Extreme Management Center and select **Control** tab > **Policy** tab > **Class of Service** left-menu tab.
2. Right-click the **Class of Service** tab tree and select **Create COS** from the menu. The Create window opens.
3. Enter the name for the CoS in the **Name** field and click **OK**. The new class of service opens in the right panel.
4. Click the **Edit** button to enter a description for the CoS.
5. Click the **Edit** button next to the **Transmit Queue** field to open the Edit Transmit Queue window, from which you can select a transmit queue for the class of service. If you would like to select a different transmit queue for each port type, select the **Select Q/Port Type** option. Then, when you click **OK**, a window opens where you can specify a different transmit queue for each port type.
6. Select an 802.1p priority from the drop-down menu to choose the priority (0-7 with 7 being the highest priority).
7. Click the **Edit** button to select the ToS option to associate an IP ToS (Type of Service) value with the class of service, if desired (see IP Type of Service for more information). Enter a value in the **Type of Service (ToS)** field.
8. Specify a Drop Precedence, if necessary. The Drop Precedence is used in conjunction with the Flex-Edge feature available on K-Series and S-Series (Release 7.11 or higher) devices. Flex-Edge provides the unique capability to prioritize traffic in the MAC chip as it enters the switch. When the Class of Service is assigned to a policy role, and that role is applied to a port via a MAC source address mapping or the port default role, the drop precedence dictates the internal priority (within the MAC chip) that will be used for packets received on the port. If congestion occurs, packets with a high drop precedence are discarded first. Therefore, if a packet is important, it should have a low drop precedence. Refer to the K-Series or S-Series Configuration Guide for more information on the Flex-Edge feature and drop precedence.

9. If desired, use the Rate Limiting/Rate Shaping section to select a port inbound, outbound, and transmit queue rate limit to associate with the class of service. Click **View/Edit** next to the **IRL Port Group Mappings** or **ORL Port Group Mappings** to open the **CoS - Rate Limit Mappings** tab of the Rate Limit Port Groups window where you can add, edit, or delete a rate limit. The rate limit you select here applies to all IRL/ORL port groups. Click the **View/Edit** button next to **TXQ Port Group Shapers** field to open the **CoS - Transmit Queue Mappings** tab to configure transmit queue mappings.
10. If you have ExtremeWireless Controllers on your network, you see an option to select inbound and outbound user rate limits to associate with the class of service. User rate limits specify the bandwidth given to each individual user on a port. Currently, user rate limits are only available for wireless controllers.
11. Click **Open/Manage Domain > Save Domain**. The class of service is created and is listed in the **Class of Service** tab.

After a class of service has been created, you can double-click in the Class of Service Configuration table to modify its characteristics, if necessary.

Creating Class of Service Port Groups

The **Policy** tab provides the ability to create rate limit port groups that let you group together ports with similar rate limiting requirements. For example, you might want to create a class of service where your edge ports would receive one rate limit while your core ports would receive a different rate limit. With port groups, you can create a single class of service that assigns a different rate limit to each group.

It also provides the ability to create transmit queue shaper port groups that allow you to isolate certain kinds of sensitive network traffic so that you can give it a high transmit queue priority. For example, ports on a router might be grouped together and configured with a specific rate shaping parameter. A transmit queue port group may contain multiple port queue types (for example, 4-queue ports and 16-queue ports) depending on the type of devices on your network.

Initially, all ports are grouped into a Default port group. When you create new port groups, you add ports from the Default group into your newly defined port groups.

The following instructions are for creating new port groups for an existing class of service.

1. Open the **Class of Service** left-panel tab and select the **Inbound Rate Limit Port Groups**, **Outbound Limit Port Groups**, or **Transmit Queue Port Groups** tab, depending on the type of port group you want to create.
2. Right-click the tab and select **Create Port Group** to create the desired group type: rate limit (RL) port group or transmit queue (TxQ) shaper port group.
   The Create window opens.
3. Enter a name for the port group and click **OK**.
4. The new port group appears in the **Class of Service** left-panel tab under the appropriate port group type.
5. Right-click on the new port group in the left-panel tab and select **Add/Remove Ports**.
6. The Add/Remove Ports window opens with the ports in the Default port group displayed in the left panel. Add ports to the new port group by selecting the ports in the left-panel, then selecting the port group in the right panel, and clicking **Add/Move To**. Click **OK** to save the changes and close the window.
7. Click **Save Domain** in the **Open/Manage Domain** drop-down menu.

Deleting a Class of Service

1. Open the **Class of Service** tab.
2. Right-click the class of service you want to remove, and select **Delete**.
3. Click **OK** to confirm that you want the class of service removed.
4. Click **Save Domain** in the **Open/Manage Domain** drop-down menu.

Related Information

For information on related tasks:

- Getting Started with Class of Service
- How to Define Rate Limits
- How to Configure Transmit Queues

For information on related windows:

- Class of Service Tab

How to Configure Transmit Queues

The **Policy** tab allows you to configure transmit queues as a component of a class of service (CoS).

There are two transmit queue configuration capabilities:

- Transmit Queue Configuration — Allows you to set the transmit queue associated with the class of service.
- TxQ Shaper — Transmit Queue Rate Shapers let you pace the rate at which traffic is transmitted out of a transmit queue.

These two capabilities are configured in the **Class of Service** tab available from the **Policy** tab.

For more information, see the section on transmit queues in Getting Started with Class of Service.

Instructions on:

- Transmit Queue Configuration
- Transmit Queue Rate Shapers

Transmit Queue Configuration

Transmit queues represent the hardware resources for each port used in scheduling packets for egressing the device. By default, the static classes of service 0-7 map to transmit queues 0-7. The actual transmit queue number may vary depending on the number of queues supported by the port.

The Priority column in the Class of Service Configuration window displays the actual transmit queues associated with the class of service for each port type. Double-click in the column to see a drop-down menu where you can select a new transmit queue for all port types, or select a different transmit queue for each individual port type.

TIP: For more detailed information, refer to the tooltip that appears when you hover the cursor over the Queue column.

Transmit Queue Rate Shapers

Rate shapers let you pace the rate at which traffic is transmitted out of a transmit queue. Packets received above the configured rate are buffered rather than dropped. Only when the buffer fills are packets dropped.

The following steps describe how to configure rate shapers in the **Policy** tab:

1. In the **Class of Service** left-panel tab, select the class of service where you want to configure the transmit queue.
2. Click the **Edit** button beside the **Transmit Queue** field and select the desired Transmit Queue from the drop-down menu.
3. Click **Open/Manage Domain > Save Domain** to save the configuration change to the database.

For more information, see the section on transmit queues in Getting Started with Class of Service.

NOTE: A rate shaper is associated to a specific transmit queue, not a CoS. This means that the 1) you should select the queue you want to use for a CoS first, then set the shaper and 2) all CoS using that queue uses the same rate shaper. Associating a rate shaper to a transmit queue is accomplished via the **CoS - Transmit Queue Mappings** tab. For additional information, see the CoS - Transmit Queue Mappings Tab (Transmit Queue Port Group) Help topic.

Related Information

For information on related concepts:

- Getting Started with Class of Service

For information on related tasks:

- How to Create a Class of Service

How to Define Traffic Descriptions

Traffic Classification rules allow you to assign VLAN membership and/or class of service to network traffic based on the traffic's classification type. Traffic descriptions are the part of a rule that defines this classification type. For more information, see Traffic Classification Rules.

The Edit Rule window accessed via the Traffic Description section of the Rule window is used to define traffic descriptions for new rules.

Use the following steps to create a new rule:

1. Open the **Control** tab.
2. Select the **Policy** tab.
3. In the Policy tab left panel, select the **Roles/Services** tab.
4. Open the Service Repository tab and open either the **Local** or **Global Services** tab, depending on the location of the rule being edited.
5. Open either the **Service Groups** or **Services** tab and click on the service for which you want to create a rule.
6. From the menu bar, select **Tools > Create Classification Rule**. You can also right-click on the service and select the option from the menu.
   The Rule opens in the right panel.
7. Click the **Edit** button in the Traffic Description area.
   The Edit Rule window opens.
8. Enter the information for the Traffic Description rule. For additional information, see Edit Rule window.
9. Enforce to write the new information to the devices.

Related Information

For information on related concepts:

- Traffic Classification Rules

For information on related tasks:

- How to Create or Modify a Rule

For information on related windows:

- **General** Tab (Rule)

How to Configure Flood Control

Flood Control provides rate limiting capabilities to CoS to allow certain types of flooded traffic to be dropped. The flood control traffic types are:

- unknown - unicast
- multicast
- broadcast

When Flood Control is enabled, incoming traffic is monitored over one second intervals. A traffic control rate sets the acceptable flow for each type, specified in packets per second. If, during a one second interval, the incoming traffic of a configured type reaches the traffic control rate on the port, the traffic is dropped until the interval ends. Packets are then allowed to flow again until the limit is reached.

By default, Flood Control is disabled for each CoS. Similarly to CoS Port Groups, a different configuration can be assigned for each group. Since Flood Control is shared across all CoS, once Flood Control is enabled on at least one CoS, those rates apply to all ports that have Flood Control enabled.

How to Display Flood Control Port Groups on the CoS Components Tab

1. Select the **CoS Components** left-panel tab on the **Class of Service** left-panel tab. The CoS Configuration tab opens.
2. Verify that the **Flood Control** checkbox is selected.

How to Create a Flood Control Port Group

1. From the left-panel menu, open the **CoS Components** tab and select the **Flood Control Port Groups** tab.
2. Right-click the **Flood Control Port Groups** tab and select **Create Port Groups**.
3. In the Create window, enter a name for the Flood Control Port Group and click **OK**. A New Flood Control item is added to the CoS Configuration Window.

How to Enable/Disable Flood Control for a CoS

Flood Control Rate Limits are shared across all CoS. Once a Flood Control rate has been enabled on at least one CoS, that is the rate specified for all Flood Control enabled CoS.

1. Open the **Flood Control Port Groups** tab (**Class of Service > CoS Components** tab) and select a Port Group.
2. Select a rate from the drop-down menu for the desired Flood Control broadcast traffic type Unicast, Multicast, or Broadcast.
3. Select an existing rate or create a new one.

4. Open a CoS in the **Class of Service** left-panel tab, and enable Flood Control for the CoS by selecting the **Enable** in the **Flood Ctrl Status** drop-down menu.

How to Add/Remove Ports to Flood Control Port Groups

1. From the **Class of Service** left-panel tab, select the **CoS Components > Flood Control Port Groups** tab.
2. Right-click a Flood Control Port Group, and select **Add/Remove Ports**.
3. Add or remove the ports in the Add/Remove Ports window.

Related Information

For information on related concepts:

- Getting Started with Class of Service
- Class of Service Configuration Tab

For information on related tasks:

- How to Create a Class of Service
- How to Define Rate Limits
- How to Configure Transmit Queues

For information on related windows:

- General Tab (Rate Limit)
- General Tab (Class of Service)

h gwHow to Create a VLAN

The **Policy** tab **VLANs** left-panel tab used for access control are displayed in the Access Control Configuration window. If you have enabled the Policy VLAN Islands feature, there are two tabs in the VLANs tab: Global VLANs and Policy VLAN Islands . Otherwise, only the Global VLANs folder is displayed. For more information on Policy VLAN Islands, see How to Create a Policy VLAN Island.

The **Policy** tab provides you with one Global Default VLAN, available when you first access the **Policy** tab. You can create additional VLANs by selecting the **Create VLAN** option available when you right-click on the **Global VLANs** tab.

Once a VLAN is created, you can use it as follows:

- as the default access control for a role, using the role General tab.
- as an access control action for a rule using the Rule tab.
- as an access control action for an automated service, using the Automated Service tab.
- in a Policy VLAN Island, if that feature is enabled.

See Create VLAN Window and Roles for additional information.

Instructions on:

- Creating a VLAN
- Editing an Island VLAN ID
- Deleting a VLAN

Creating a VLAN

1. Open the **Policy** tab.
2. Select the left-panel **VLANs > Global VLANs** tab.
3. Right click the **Global VLANs** tab and select **Create VLAN** from the menu.
4. Fill out the Create VLAN Window to your specifications.
5. Click **OK** to create the VLAN and close the Create VLAN window.
6. Enforce to write the new information to the devices.

Editing an Island VLAN ID

1. Open the **Policy** tab.
2. Expand the **VLANs > Policy VLAN Islands** left-panel tab.
3. Select the **VLANs** tab in the right panel.
4. Select the VLAN with which the policy VLAN island is associated in the VLANs section of the window.
5. Select the Island VLAN in the VLAN Settings section of the window and click **Edit Island VID**.
6. Enter the new VLAN ID and click **OK**.
7. Enforce to write the new information to the devices.

Deleting a VLAN

Deleting a VLAN removes it and its associations with any roles and services from the NetSight database and from the devices.

WARNING: The delete operation immediately removes the VLAN(s) from the devices in the **Devices** tab and could result in serious consequences if the VLANs are used outside the scope of the **Policy** tab.

1. Open the **Policy** tab and select the **VLANs** left-panel tab.
2. Expand the **Global VLANs** left-panel tab.
3. Right-click on the VLAN you wish to delete and select **Delete** from the menu. A confirmation window opens.
4. Click **Yes** to delete the VLAN.
5. Enforce to write the new information to the devices.

Related Information

For information on related concepts:

- Dynamic Egress
- Policy VLAN Islands

For information on related windows:

- Create VLAN Window
- General Tab (Role)

How to Create a Policy VLAN Island

VLAN islands enable you to set up, for example, a guest VLAN that restricts the guests in one facility from communicating with guests in another facility. See Policy VLAN Islands for more information.

Instructions on:

- Creating a VLAN Island
- Modifying a VLAN Island

- Deleting a VLAN Island

Creating a VLAN Island

You can create a Policy VLAN Island as follows:

Note: VLANs used in VLAN islands must be Island VLANs.

1. Open the **Policy** tab and select the **VLANs** left-panel tab.
2. In the left-panel **VLANs** tab, click the **Policy VLAN Islands** tab.
3. In the right-panel, click the VLANs Tab and click **Create** in the VLANs section.
4. In the **Create VLAN** window, enter a name for the VLAN. Click **OK**.
5. Click **Open/Manage Domains > Save Domain**.

Modifying a VLAN Island

Once you've created a VLAN island, you can change its characteristics using the right-panel tabs as follows:

- *To change a VLAN island name*: Right-click the island in the VLANs section of the **VLANs > Policy VLAN Islands** and select **Rename**.
- *To change a VLAN island description*: Use the island's Island Topology tab.
- *To edit an Island VLAN ID*: Use the **Edit Island VLAN ID** button on the island's VLANs tab.
- *To change a VLAN Island Configuration (Base ID, Offset, Naming Convention)*: Use the **Policy VLAN Islands** tab Island Topology tab .
- *To add or remove devices from a VLAN island*: Use the VLAN Islands Add/Remove Devices window.

Deleting a VLAN Island

You cannot delete the Default Island.

1. Open the **Policy** tab and select the **VLANs > Policy VLAN Islands** left-panel tab.
2. Select the VLAN island you want to delete in the VLANs section of the right panel.
3. Right-click the island you want to delete and select **Delete**.
4. Click **Yes** to confirm the deletion.

Related Information

For information on related concepts:

- Policy VLAN Islands

For information on related windows:

- Add/Remove Devices window
- VLANs Tab (Policy VLAN Islands)
- Island Topology Tab (Policy VLAN Islands)

How to Create a Network Resource

Network Resource groups provide a quick and easy way to define traffic classification rules for groups of network resources such as routers, VoIP (Voice over IP) gateways, and servers. You create a network resource group by defining a list of MAC or IP addresses for the resources you want included in the group.

In addition, you can use Network Resource Topologies to define a different resource list for different groups of devices in your domain. This enables you to set up network resource access based on the location where end users authenticate.

Once a network resource group has been defined, you can associate it with an Automated service (see How to Create a Service for more information). The Automated service automatically creates a rule with a specified action (class of service and/or access control), for each resource address in the network resource group. Automated rule types include Layer 2 MAC Address rules, Layer 3 IP Address and IP Socket rules, and Layer 4 IP UDP Port and IP TCP Port rules.

You can also create Global Network Resources shared between all your domains and can be used by global automated services. Network Resource Topologies are not available for Global Network Resources.

TIP: The Policy tab Demo.pmd file contains examples of network resource groups that you might want to create, such as Internet Proxy Servers and SAP Servers.

How to Create a Network Resource

1. From the **Policy** tab, select the **Network Resources** left-panel tab.
2. Right-click the Network Resources folder and select **Create Network Resource**. A New Network Resource item is created in the left panel in a highlighted box. (If you want to create a Global Network Resource, click on the Global Network Resources folder.)
3. Type the resource name in the Create window and click **OK**.
4. In the right-panel General tab, use the **Edit** button to add a description of the network resource, if desired.
5. Select the network resource Type:
   - Layer 2 MAC - Define a group of network resources using MAC addresses.
   - Layer 3 IP - Define a group of network resources using IP addresses.
6. Select the appropriate network resource topology. Network Resource Topologies are used to divide the devices in a domain into groups called islands. You can then define a unique resource list for each island within that topology, allowing user access to resources on the network based on the physical location at which they authenticate. If you are not using topologies to group your devices, select the Domain Wide topology, which contains just one island for all your domain devices.
7. For each topology island included in the selected topology, a tab is available where you can list the resources for that specific island. Use the address field (MAC or IP, depending on the selected type) and click the **Add** button to add a new resource to the list.

Once a network resources group has been created and defined, it can be associated with an Automated service (see How to Create a Service for more information).

How to Create a Network Resource Topology

1. From the **Policy** tab, select the **Network Resources** left-panel tab.
2. Right-click the **Network Resource Topologies** left-panel tab and select **Create Network Resource Topology**. A New Network Resource Topology item is created in the left panel in a highlighted box.
3. Type the topology name in the highlighted box.
4. Expand the topology to see the Default Island, which contains all the devices in the domain.

5. Right-click on the topology and select **Create Network Resource Island**. Type in the island name in the highlighted box and click **OK**. Use this step to create all the islands for this topology.
6. Select an island and click the **Add Devices** button to open the Add Devices to Resource Island window, where you can move devices from the Default Island to the islands you just created. Click **Add**.
7. Set any island as the [Default] island for new devices that are added to the domain by right-clicking the island and selecting **Set Default**.

The Network Resource Topology is available for selection when you create your network resources.

Related Information

For information on related tasks:

- How to Create a Service

For information on related windows:

- **General** Tab (Network Resource Group)

How to Add and Delete Devices

The Extreme Management Center database contains all the devices in your network and displays them in the left-panel device tree. The **Network** tab and the **Policy** tab share a common view of the device tree, except that only devices that support policy are displayed in the **Policy** tab tree. Any changes you make to the devices are reflected in both trees.

Initially, perform a device Discover to populate the database. Once devices have been added to the Extreme Management Center database, you must assign the devices to a Policy Domain using the **Policy** tab. As soon as the devices are assigned to a domain, they are automatically displayed in the **Policy** tab device tree. Only devices assigned to the domain you are currently viewing are displayed. For more information, see How to Create and Use Domains.

After you have initially added your devices, you can use the **Policy** tab's Add Device window to add a single device to the database and the current domain.

Instructions on:

Using Console to Discover Devices

Console Discover lets you to discover your network devices and add them to the Extreme Management Center database. You can perform a discover on a specified range of IP addresses, or perform a CDP (Cabletron Discovery Protocol) discover for CDP-compliant devices. Discover automatically explores a specific network segment and creates a list of discovered devices. You can then save all or a subset of the discovered devices to the Extreme Management Center database.

For step-by-step instructions, see the **How to Discover Devices** help topic in your Console online help system.

After devices are added to the database via Console Discover, they must be assigned to a Policy Domain (using the **Policy** tab) before they display in the **Policy** tab tree. Once they have been assigned to a domain, the devices are automatically displayed in the appropriate groups in the **Policy** tab Network Elements device tree.

Using Console to Import Devices

The Console Import Devices feature imports device information and profiles for unique devices (ones that do not exist locally) from a .ngf file, and adds them to the Extreme Management Center database. For step-by-step instructions, see the **Importing a Device List from a File** section of the **How to Export and Import a Device List** help topic in your Console online help system.

After the devices are imported to the database, they must be assigned to a Policy Domain (using the **Policy** tab) before they display in the Policy tab tree. Once they have been assigned to a domain, the devices are automatically displayed in the appropriate groups in the Policy tab Network Elements device tree.

Deleting Devices from the Database

When a device is deleted from the Extreme Management Center database, it is removed from all groups where it is a member in both the **Policy** tab and Console device tree (and any other Extreme Management Center plugin applications).

NOTE: If you want to remove a device from a domain without deleting it from the database, you must use the Assign Devices to Domain window. For more information, see Removing Devices from a Domain.

To delete devices from the Extreme Management Center database:

1. Open the **Network** tab, select the device being deleted from the Devices table.
2. Right-click the device and select **Device > Delete Device** from the menu. A confirmation message advises that you are deleting the device from the Extreme Management Center database.
3. Click **Yes** to delete the device.

Related Information

For information on related tasks:

- How to Create and Use Domains

How to Create a Port Group

The **Policy** tab allows you to group ports into user-defined port groups, similar to the way you can group services into service groups. Port groups enable you to configure multiple ports on the same device or on different devices, simultaneously. A port can be a member of more than one group.

When you create a user-defined port group, you select individual ports to add to the group.

The **Policy** tab also provides you with Pre-Defined Port Groups which are automatically populated according to port characteristics. See Pre-Defined Port Groups for more information.

Instructions on:

Creating a Port Group

1. In the left panel, click the **Devices > Port Groups** tab.
2. Right-click on the Port Groups folder and select **Create Port Group**. This opens the Create window.
3. Enter a **Name** and click **OK**.

Adding Ports to a Port Group

You can add ports directly from the port group:

1. Select the left-panel **Devices > Port Groups** tab. Expand the User-Defined Port Groups folder and select a port group.
2. Right-click the port group and select **Add/Remove Ports** from the menu.
3. In the Add/Remove Ports window, select the ports you want to add to the port group in the Devices list and click **Add to Group** to move the port to the Group Port Membership list.
4. Click **OK**.

Removing Ports from a Port Group

This procedure applies to user-defined port groups.

1. In the left-panel **Devices > Port Groups** tab, right-click the port group from which you wish to remove a port, and select **Add/Remove Ports**.
2. In the Add/Remove Ports window, select the ports you want to remove from the port group, and click **Remove**.
3. Click **OK**.

Alternatively, you can right-click a single port under the port group in the left panel or multiple ports in the right-panel Ports tab, and select **Remove Port(s) from Group**.

Related Information

For information on related windows:

- Add/Remove Ports Window

Extreme Access Control

The Access Control tab provides secure, policy-based management for the Extreme Access Control solution. It configures and manages Extreme Access Control gateways, provides user to device location mapping services, generates network endpoint audit reports and interfaces with other security management applications.

Contact your sales representative for information on obtaining an Extreme Management Center software license.

The Access Control tab contains three main navigation trees in the left-panel:

- Extreme Access Control Engine Groups
- All Extreme Access Control Engines
- Extreme Access Control Configurations

Extreme Access Control Engine Groups

The Extreme Access Control Engine Groups tree presents groups of Extreme Access Control engines you configure into engine groups. Information for engine groups is organized into four tabs in the right-panel, each showing different information relating to the engine group selected:

- Details — Displays basic information about the engine group as well as information about how the engines in the group are configured.
- Switches — Shows the switches monitored by the gateway engines in the group and allows you to add, delete, and edit the switch configuration.
- End-Systems — Displays end-systems monitored by the Extreme Access Control engines in the selected engine group.
- Extreme Access Control Engines — Displays the Extreme Access Control engines added to the engine group. Right-clicking an engine in the table displays a menu from which you can configure the engine.

All Extreme Access Control Engines

The All Extreme Access Control Engines tree displays all of your Extreme Access Control engines. Selecting an engine displays information in three tabs:

- Details — Displays basic information about the engine, provides a summary of the interface, and allows you to disable Extreme Access Control authentication and assessment.
- End-Systems — Displays end-systems monitored by the Extreme Access Control engine.
- Switches — Shows the switches monitored by the gateway engine and allows you to add, delete, and edit the switch configuration.

Extreme Access Control Configurations

The Extreme Access Control Configurations tree lets you manage the end-user connection experience and control network access based on a variety of criteria including authentication, user name, MAC address, time of day, and location. Extreme Management Center comes with a default Extreme Access Control Configuration which is automatically assigned to your Extreme Access Control engines. You can use this default configuration as is, or make changes to the default configuration, if desired.

Configure a registration that forces any new end-system connected on the network to provide the user's identity in a web page form before being allowed access to the network. End users are automatically provisioned network access on demand without time-consuming and costly network infrastructure reconfigurations. In addition, IT operations gains visibility into the end-systems and their associated users (e.g. guests, students, contractors, and employees) on the network.

Via the Extreme Access Control Configurations tree, you can also configure agent-less or agent-based security posture assessment of endpoints. The Access Control tab uses assessment servers to assess and audit connecting end-systems and provide details about an end-system's patch levels, running processes, anti-virus definitions, device type, operating system, and other information critical in determining an end-system's security compliance. End-systems that fail assessment can be dynamically quarantined with restrictive

network access to prevent security threats from entering the network.

Assisted remediation is a process that informs end users when their end-systems have been quarantined due to network security policy non-compliance, and allows end users to safely remediate their non-compliant end-systems without assistance from IT operations. Once the remediation steps have been successfully performed and the end-system is compliant with network security policy, the appropriate network resources are allocated to the end-system, again without the intervention of IT operations.

Extreme Access Control Configuration Considerations

Review the following configuration considerations when installing and configuring Extreme Management Center Extreme Access Control.

Extreme Access Control Configuration Tables

The following tables provide valuable information to help guide you through the deployment of Extreme Networks Extreme Access Control for your network. The first table displays suggested Extreme Access Control configurations to use for different network deployment circumstances (e.g. type of end-systems on the network, network topology, authentication method deployed, etc.). The second table displays details and information for each of the different suggested Extreme Access Control configurations. The information in the tables assumes that DHCP is deployed on the network.

Suggested Extreme Access Control Configuration for Different Deployments

Policy/VLAN Switch Configuration	Number of Devices Allowed to Connect to Authentication-enabled Edge Port	Type of End-Systems	Authentication Method Deployed	Switch Support IEEE 802.1X MIB	Switch Support, Session Timeout and Termination Action RADIUS Attributes	Suggested Configuration
- Policy Only (*without* changing of VLANs)	*	*	*	*	*	A
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs)	Multiple	Microsoft XP SP1 with KB822596 installed[1]	802.1X[2]	Yes	*	A
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs)	Multiple	*	802.1X[2]	Yes	*	B
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs)	Multiple	*	802.1X[2]	No	Yes	C
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs)	Multiple	*	802.1X[2]	No	No	D
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs) *[for Enterasys switch]*	Multiple	*	MAC Authentication	*	*	B
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs) *[for non-Enterasys switch]*	Multiple	*	MAC Authentication	*	Yes	C
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs) *[for non-Enterasys switch]*	Multiple	*	MAC Authentication	*	No	D
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs)	Single	Microsoft or MAC OS	*	*	*	E
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs)	Single	Linux	*	*	*	F
Wireless Device	Multiple	*	*	*	*	G

* = Any value.
N/A = Not applicable.
[1]For more information on this patch, see the following link: http://support.microsoft.com/default.aspx?scid=kb;en-

us;KB822596
[2]When 802.1X is implemented to authenticate multiple users on a single switch port, the downstream device providing connectivity to the users must support the forwarding of EAP frames. Unintelligent devices such as repeaters and switches with newer firmware releases should forward EAP frames. However, some switches do not forward EAP frames therefore preventing the 802.1X authentication of multiple users on a single port.

Extreme Access Control Configuration Details

Configuration	Port Link Control	Assessing Session Timeout	Assessing Policy Configuration	DHCP Server Configuration Considerations	Other Considerations
A	Disabled	Disabled	*	No	N/A
	NOTE: This is the simplest of configurations.				
B	Disabled	Disabled	Initial Scan Only	- Set short lease times (e.g. 1 min) for the unauthenticated, Assessing, and Quarantine VLANs - Normal lease times can be configured for the Accept (Production) VLANs	N/A
	NOTES: When an end-system transitions from the unauthenticated, Assessing, or Quarantine VLAN to another VLAN, the end-system will soon renew its IP address via DHCP to automatically re-establish connectivity to the network. When a compliant end-system on the Production VLAN is subsequently quarantined after failing a re-assessment, the end-system's connectivity to the network will be lost until expiration of the DHCP lease for the Accept (Production) VLANs.				
C	Disabled	Enabled	Initial Scan Only	- Set short lease times (e.g. 1 min) for the unauthenticated, Assessing, and Quarantine VLANs - Normal lease times can be configured for the Accept (Production) VLANs	N/A
	NOTES: When an end-system transitions from the unauthenticated, Assessing, or Quarantine VLAN to another VLAN, the end-system will soon renew its IP address via DHCP to automatically re-establish connectivity to the network. Furthermore, the end-system will continually reauthenticate to the network while it is being scanned. When a compliant end-system on the Production VLAN is subsequently quarantined after failing a re-assessment, the end-system's connectivity to the network will be lost until expiration of the DHCP lease for the Accept (Production) VLANs.				

Configuration	Port Link Control	Assessing Session Timeout	Assessing Policy Configuration	DHCP Server Configuration Considerations	Other Considerations
D	Disabled	Disabled	Initial Scan Only	- Set short lease times (e.g. 1 min) for the unauthenticated, Assessing, and Quarantine VLANs - Normal lease times can be configured for the Accept (Production) VLANs	Set short reauthentication interval manually on edge switches (e.g. 2 min)
	NOTE: This is not a very scalable configuration model, and therefore should not be implemented for a network with a large number of end-systems.				
E	Enabled	Disabled	*	No	N/A
	NOTE: End-system will be reauthenticated and will renew its IP address via DHCP with link down/up execution.				
F	Enabled	Disabled	Initial Scan Only	- Set short lease times (e.g. 1 min) for the unauthenticated, Assessing, and Quarantine VLANs - Normal lease times can be configured for the Accept (Production) VLANs	N/A
	NOTES: End-system will be reauthenticated with link down/up execution and will automatically re-establish network connectivity via DHCP upon lease expiration of the IP address in the unauthenticated, Assessing, and Quarantine VLANs. When a compliant end-system on the Production VLAN is subsequently quarantined after failing a re-assessment, the end-system will be reauthenticated and will renew its IP address via DHCP with link down/up execution.				
G	Disabled	*	*	*	RFC 3576 Reauthentication Enabled
	NOTES: Extreme Management Center supports RFC 3576 which provides for forced reauthentication (Force Reauth) of end-systems connected to an RFC 3576-capable switch. RFC 3576 defines new RADIUS messaging that allows the Extreme Access Control Gateway to send Disconnect or Change of Authorization (CoA) RADIUS messages to the authenticating switch or AP to force reauthentication on a currently authenticated end-system.				

* = Any value.
N/A = Not applicable.

General Considerations

- **Gateway RADIUS Attributes to Send - Send RFC 3580 Only Feature.** This feature (configured in the Add/Edit Switches to Identity and Access Appliance Group panel) lets you specify that an Extreme Access Control Gateway sends a VLAN (instead of a policy) via RFC 3580-defined RADIUS Tunnel attributes to the RFC 3580-enabled switches in your network. Keep in mind the following considerations when configuring this feature:

- **Send RFC 3580 Only is not supported on Matrix E7 Devices.** Matrix E7 devices should not be configured with the "Gateway RADIUS Attributes to Send" parameter set to RFC 3580 Only.
- **Send RFC 3580 Only does not support end-systems with static IP addresses.** The Send RFC 3580 Only feature is not-supported for end-systems with static IP addresses. This is because end-systems transitioned between VLANs must be assigned an IP address on the appropriate subnet to maintain IP connectivity to the network, which is facilitated dynamically through DHCP.
- **Send RFC 3580 Only requires a particular DHCP configuration for Active/Default Role port mode.** When the Send RFC 3580 Only feature is configured, the Active/ Default Role port mode on network devices requires a particular DHCP configuration. The DHCP lease time for the pool of IP addresses that corresponds to the default role's VLAN must be short (e.g. less than 1 minute) because the Active/Default Role port mode allows end-systems to obtain IP addresses via the DHCP protocol before they are authenticated to a VLAN.
- **Switch management fails with Send RFC 3580 Only and certain Auth Access Types.** Switch management via TELNET/WebView fails with the following configuration in the Add/Edit Switches to Identity and Access Appliance Group window:

  Auth Access Type = "Management Access" or "Any Access"
  Gateway RADIUS Attributes to Send = "RFC 3580 Only"

  This is because switches check the "mgmt" attribute in the Filter-ID for Telnet management. To avoid this problem, set the Auth Access Type to "Network Access."

- **Enable Port Link Control Option.** Port link control is required if you are using VLAN only (RFC 3580) switches or if you are using policy with VLANs on policy-enabled switches. When an end-system is transitioned between VLANs with a new VLAN being assigned to a switch port, the end-system is required to obtain a new IP address for the assigned VLAN. To do this, the Extreme Access Control Gateway links down the port (using the ifAdmin MIB), waits the configured amount of time, and then links up the port, causing the end-system to make a new DHCP request and get a new IP address.
  - **Port Link Control is not supported on authentication-enabled switch ports providing connectivity to multiple end-systems.** Do not enable port link control for switches authenticating multiple users per port. When an Extreme

Access Control Gateway is configured to return only the VLAN RADIUS attribute, the gateway links down the authenticated port to force the end-system to release and then renew the DHCP IP address when port link control is enabled. This action interrupts IP connectivity of other authenticated end-systems on the port. If the switch is an Enterasys switch, protection is automatically provided by reading the number of users currently on the port prior to linking down an port.

- Port Link Control is only supported on Windows XP or later. Port link control is only supported for end-users that are authenticating from end-systems running Windows XP or later. When an Extreme Access Control Gateway is configured to return only the VLAN RADIUS attribute, the gateway links down the authenticated port to force the end-system to release and then renew the DHCP IP address when port link control is enabled. However, other systems such as NT workstations, do not release their DHCP IP address when the port is linked down. To account for this scenario, disable port link control, set the Extreme Access Control Profile to "Use Assessment Policy During Initial Assessment Only," and set the DHCP lease time for the IP address pools that correspond to the VLAN(s) associated to the Quarantine and Assessing access policies, as well as the default VLAN associated to the unauthenticated state of the port, to a low value (e.g. 1 minute). This forces an end-system to send DHCP Request messages every 30 seconds while it is unauthenticated, being assessed, and quarantined. Upon passing assessment, the end-system is dynamically assigned an IP address on the production VLAN shortly after assessment is complete, establishing connectivity to the network on the production VLAN.

- Extreme Access Control Gateway DHCP Snooping:
  - Option 1: Locate the Extreme Access Control Gateway on the same subnet as the DHCP server. If the Extreme Access Control engine is in the same subnet (relay router interface) as the end-system, it is able to hear ACK responses from the DHCP server, allowing it to have more accurate DHCP entries unless the relay router (or DHCP server) sends unicast ACK responses directly to the end-system.
    Note: Whether the ACK response is sent using unicast or broadcast is normally determined by how the end-system requests the packet. If the end-system sends out a DHCP discover/request with a unicast bootp flag, then the DHCP server (or relay router) sends the ACK response using unicast. This is typically what happens. Sometimes, the end-system can request the DHCP

discover/request with a broadcast bootp flag set. In this case, the end-system gets the ACK response with broadcast, and the Extreme Access Control engine hears the ACK response if it is in the same broadcast domain.
The benefit of using option 1 over the helper-address implementation described in option 2, is that the helper-address implementation only gets the requests from the end-systems which may or may not have the correct IP address. When an Extreme Access Control Gateway learns a MAC/IP address pair, it sends a message to all other Extreme Access Control Gateways, so only one Extreme Access Control Gateway needs to live on each subnet with a DHCP server on it, to leverage this technique.

- Option 2: Add the Extreme Access Control Gateway IP address as a helper address on default gateway routers. To increase the accuracy of the MAP-to-IP resolution, the Extreme Access Control Gateway listens for DHCP traffic on port 67 and saves the MAC/IP address pairs it learns. In order to receive DHCP traffic, the IP address of any Extreme Access Control Gateway must be added as a helper address on default gateway routers on the network. Routers allow multiple IP helper address entries, so the Extreme Access Control Gateway's IP address can be added along with the actual DHCP server IP addresses. When an Extreme Access Control Gateway learns a MAC/IP address pair, it sends a message to all other Extreme Access Control Gateways, so only one Extreme Access Control Gateway IP address needs to be added.

- Configure RADIUS settings on 3rd-party switches. You must manually configure the RADIUS settings on your third-party switches communicating to the Extreme Access Control Gateway. In addition, make sure that the shared secret on the switches matches the shared secret you entered in the Advanced Switch Settings window. This is the shared secret the switches uses to communicate with Extreme Access Control Gateways.

- Configuring Agent-based Assessment Test Sets with Hotfix Checks. When configuring an Agent-based test set to perform multiple hotfix checks, make sure that the Monitoring Interval is set to at least 5 minutes, so that the assessment agent does not take a lot of CPU cycles trying to monitor these settings.

- Supported desktop browsers for end-systems connecting through Extreme Access Control. The following browsers are supported for desktop end-systems connecting to the network through Extreme Networks Extreme Access Control:

  - Microsoft Edge and Internet Explorer version 11
  - Mozilla Firefox 34 and later
  - Google Chrome 33.0 and later
- Supported mobile browsers for end-systems connecting through Extreme Access Control. The following browsers are supported for mobile end-systems connecting to the network through the Mobile Captive Portal of Extreme Networks Extreme Access Control:
  - IE11+ (Windows Phone)
  - Microsoft Edge
  - Microsoft Windows 10 Touch Screen Native (Surface Tablet)
  - iOS 9+ Native
  - Android 4.0+ Chrome
  - Android 4.4+ Native
  - Dolphin
  - Opera

    NOTES: A native browser indicates the default, system-installed browser. Although this may be Chrome (Android), this also includes the default, system-controlled browser used for a device's Captive Network Detection. Typically, this is a non-configurable option for Wi-Fi Captive Network Detection, but default Android, Microsoft of iOS devices are tested for compatibility with the Mobile Captive Portal.

    A mobile device can access the standard (non-mobile) version of the Captive Portal using any desktop-supported browsers available on a mobile device.
  - For other browsers, the Mobile Captive Portal requires the browser on the mobile device be compatible with Webkit or Sencha Touch. To confirm compatibility with Webkit or Sencha Touch, open http://<*ip_of_engine*>/mobile_screen_preview using your mobile web browser. If the browser is compatible, the page displays properly.
- RADIUS Configuration on E1 Devices. The Extreme Access Control engine opens an SSH/Telnet session on the E1 device and enable RADIUS by running a script of CLI commands. CLI credentials for the device are obtained from the device profile and must be configured in the Authorization/Device Access tool.

- RADIUS Authentication and Accounting Configuration on ExtremeXOS Devices. Extreme Management Center uses CLI access to perform RADIUS configuration operations on ExtremeXOS devices. CLI credentials for the device are obtained from the device profile and must be configured in the Authorization/Device Access tool.
- RADIUS Accounting Configuration on Fixed Switching Devices. Extreme Access Control uses CLI to configure RADIUS accounting on Enterasys fixed switching devices (A-Series, B-Series, C-Series, D-Series, G-Series, and I-Series). CLI credentials for the device are obtained from the device profile and must be configured in the Authorization/Device Access tool. This does not apply to A4, B5, and C5 devices running firmware version 6.81 and higher. Those devices support RADIUS accounting configuration using SNMP. For more information, see How to Enable RADIUS Accounting.

Considerations When Implementing Policy Roles

This section describes the communication that takes place between Extreme Access Control engines and end-systems connecting to the network. This communication should be taken into account when defining and deploying policy roles and rules on your network. It is particularly critical because certain policy roles and rules may discard traffic that is necessary for communication between the end-system and the engine. For example, in a Guest policy role, NetBIOS traffic is probably discarded, but doing so could impact the MAC to IP resolution process.

Review the following information and verify that the policy roles and rules deployed on your network will allow the required communication between end-systems and your Extreme Access Control engines.

IP resolution via NetBIOS
MAC Resolution via NetBIOS
 Extreme Access Control engine UDP Port 137 <==> End-System Port 137

Remediation and Registration
 Extreme Access Control engine (TCP or UDP) Port 80 <==> End-System Port (determined on the client) - HTTP
 Extreme Access Control engine (TCP or UDP) Port 443 <==> End-System Port (determined on the client) - HTTPS

Extreme Access Control Agent Discovery via HTTP
 Extreme Access Control engine Port TCP 8080 <==> End-System Port (determined on the client)
Extreme Access Control Agent Heartbeat via HTTPS

Extreme Access Control engine Port TCP 8443 <==> End-System Port (determined on the client)

Extreme Access Control Agent-less Assessment
All ports determined by the selected test set.

The following software is optional and may be installed with agent-less Assessment:
SAMBA add-on enabled
TCP Ports 149 and 195, and UDP Ports 137 and 138.

End-System Reachability Test (Assessment Configurations - does not apply to agent-based assessment)
ICMP Ping Test => ICMP Protocol (1), ICMP Type (8)
TCP Ping Test => Default TCP Ports: 21, 22, 23, 25, 79, 80, 111, 135, 139, 445, 497, 515, 548, 1025, 1028, 1029, 1917, 5000, 6000, 9100

ExtremeWireless Controller Configuration

- The NAS IP address used for the wireless controller should be either the management IP address or an IP address of one of its physical data ports, or all zeros to force Extreme Access Control (Extreme Access Control) to use the source IP. If a logical IP address is used, then Extreme Access Control is unable to reauthenticate end-systems.
- If you have configured Assisted Remediation, you must perform the following steps if your network includes wireless controllers:
    - Enable the "ToS override for Extreme Access Control" option configured through Wireless Manager in the Edit WLAN Service > Authentication Mode Configuration > Settings window.
    - If Policy Manager is not being used to configure policy on the wireless controller, use Wireless Manager to manually add the following rule to the VNS Quarantine, Assessing, and Unregistered filters to allow HTTP traffic to pass through (IN/OUT) the controller when end-systems are proxied to the Internet during remediation.
      `0.0.0.0/0 tcp port 80 (Allow traffic In/Out)`
    - If Policy Manager is being used to configure policy for the wireless controller, use the Classification Rule Wizard to add an "Allow HTTP" rule to a service currently included in your Quarantine, Assessing, and Unregistered policy roles. The rule would be a traffic classification type "IP TCP Port Destination"

with the TCP type set to HTTP (80) and the Access Control set to "Permit Traffic."

DNS Proxy Functionality for Registration and Remediation

Extreme Access Control (Extreme Access Control) Gateway engines provide DNS proxy functionality for use in networks that are deploying registration and/or remediation, but cannot configure the policy-based routing that is required to redirect network traffic to the web portal. Using DNS proxy, any end-system that needs to be redirected to the remediation and registration web portal has its DNS packets spoofed to direct all web page requests to the Extreme Access Control Gateway engine. This allows networks that do not have a router to deploy registration and remediation.

Basic Operation

To set up DNS proxy, the Extreme Access Control engine is configured as a secondary DNS server in the DHCP scope, in addition to the primary DNS server on the network. When an end-system is required to register or undergo remediation, access to the primary DNS server is blocked and the end-system sends its DNS requests to the DNS proxy on the Extreme Access Control Gateway engine.

The DNS proxy must determine whether to spoof the packet or forward the request to the primary DNS server. If the end-system is unregistered or quarantined, the DNS proxy spoofs the DNS packet and send back a DNS response to the end-system with the Extreme Access Control engine IP address. This redirects the end-system traffic to the web portal where the end user can register or remediate. Once the end user has registered or remediated their end-system, their DNS requests are forwarded to the primary DNS server.

For third-party devices, a dynamic ACL is configured to block access to the primary DNS server for end-systems undergoing registration or remediation. This causes the DNS requests to be sent to the DNS proxy. The DNS proxy determines whether spoofing is necessary or not by checking the state of the end-system in the database. If the end-system is unregistered or quarantined, the DNS proxy spoofs the DNS packet.

To allow access to hosts or domains for any protocol other than http, you must add the host or domain to the list of allowed web sites configured in the Network Settings view of the Extreme Access Control Edit Portal Configuration window. The DNS proxy uses this list of allowed domains to determine if the

end-system is allowed access to the requested domain. This can be useful if you want to allow end-systems to perform specific functions such as anti-virus updates or software updates that run over TCP/UDP ports.

You can also define post authorization assessment behavior using DNS proxy. End-systems in the scan state are granted access according to the assessment settings in your Extreme Access Control profile.

- If an assessment policy is not defined, the user is allowed access while being scanned.
- If an assessment policy is defined for initial assessment only, the user is allowed access if they passed the last scan. If the first or last scan resulted in quarantine, the user is redirected to the Extreme Access Control Gateway.
- If an assessment policy is defined for all assessments, the user is redirected to the Extreme Access Control Gateway.

Backup DNS Server

Because the DNS proxy forwards DNS requests to the primary DNS server, it is important to configure a backup DNS server on your network, in case the primary server is down. The DNS proxy polls the primary DNS server every minute. If the primary server is down, a backup DNS server is used. If both servers are down, all DNS requests forwarded by the DNS proxy are dropped.

Troubleshooting

DNS proxy error messages are logged in the /var/log/dnsProxy.log file on the Extreme Access Control engine. You can enable diagnostics for DNS proxy by going to the Extreme Access Control engine administration web page and enabling the DNS Proxy diagnostic group to provide troubleshooting information. Launch the Extreme Access Control engine administration web page by using the following URL: https://<Extreme Access ControlengineIP>:8443/Admin. The default user name and password for access to this web page is "admin/Extreme@pp." Click on the Diagnostics page and then the Server Diagnostics page. View the output in the /var/log/dnsProxy.log file or on the Log Files > Server Log web page.

How to Update an Extreme Access Control License

This Help topic provides instructions for saving an Extreme Access Control license and applying the license after upgrading to a new Extreme Access Control engine.

the password on the assessment agent adapter on your network assessment servers, including agent-less, Nessus, or a third-party assessment agent (an assessment agent not supplied or supported by Extreme Management Center). The assessment agent adapter enables communication between the Extreme Access Control engine and the assessment servers, and the password is used by the assessment agent adapter to authenticate Extreme Access Control engine assessment requests.

This password must match the password specified in the Extreme Access Control Options as the Assessment Agent Adapter Credentials (Administration > Options > Identity and Access > Assessment Server). If you change the password on the assessment agent adapter, change assessment agent adapter credentials in the Extreme Access Control options as well, or connection between the engine and assessment servers is lost and assessments is not performed.

To change the assessment agent adapter password:

1. Go to the install directory for the assessment agent adapter on the assessment server. This can be a Nessus server or the Extreme Access Control engine if you are using on-board agent-less assessment. On an Extreme Access Control engine, the install directory is **/opt/nac/saint**.
2. Run the **sha1.sh** script (on an Extreme Access Control engine, the script is located in located in **/opt/nac/saint/util**) using the new password as the argument. The script produces a hash string that looks something like:
   9ba2db465ff11b0bdfd188f7ee87b10fc3a145dc
3. Open the **users.properties** file (on an Extreme Access Control engine, the file is located in **/opt/nac/saint/users.properties**) and replace the existing hash string with the new one:
   `admin=<new string>`

4. Restart the assessment agent adapter. On an Extreme Access Control engine, the command is `aglsctl restart`.

Related Information

For information on related tasks:

- How to Install the Assessment Agent Adapter on a Nessus Server
- How to Set Extreme Access Control Options - Assessment Server

For information on related windows:

- Manage Assessment Settings Window
- Extreme Access Control Options - Assessment Server

How to Install the Assessment Agent Adapter on a Nessus Server

This document provides instructions to install the Extreme Networks Assessment Agent Adapter software on a Nessus Server. The Assessment Agent Adapter is required for communication between the Extreme Access Control engine and the Nessus server.

NOTE: As of Extreme Management Center version 8.1, only Nessus Version 6 is officially supported.

1. Go to the Network Management Suite (NMS) Download web page to download the Assessment Agent Adapter: https://extranet.extremenetworks.com/downloads/Pages/NMS.aspx. Select the version of Extreme Management Center you are using.
2. Scroll down to find the Identity and Access Tools section of the web page. The install file is named "Assessment Adapter (for 3rd party assessment integration)". Download the file and copy it to the Nessus server.
3. Open a shell and "cd" to the directory where you downloaded the install file.
4. Change the permissions on the install file by entering the following command at the shell prompt:
   ```
   chmod 755 EXTRAssessmentServerAgentAdapter_x.x.x.x.bin
   ```
5. Run the install program by entering the following command at the shell prompt:
   ```
   ./EXTRAssessmentServerAgentAdapter_x.x.x.x.bin
   ```
6. The Introduction screen appears. Press **Enter**.
7. Enter Nessus as the agent type to install. Press **Enter**.
8. The Choose Install Folder screen appears where you can choose the installation folder or directory. Enter an absolute path or press **Enter** to accept the default installation folder /root/AssessmentAgent. The installer requires 100 MB of memory. If the installation folder does not have enough memory, an error displays.
9. The Pre-Installation Summary screen appears. This screen shows you the locations you have chosen for the installation process and disk space requirements. Review this information to ensure its accuracy. Press **Enter**.

10. The Nessus Server Information screen appears. You must enter information in several fields in this screen.
11. Enter the port on which the Nessus daemon is running. The default value is 1241. Press **Enter**.
12. Enter the username you created when you installed the Nessus server. Press **Enter**. If you did not create a user when you installed the Nessus server, from a shell prompt, type:
    `cd /nessus installation directory/sbin`
    followed by
    `nessuscli adduser username`
    and follow the prompts to add a user to the application. Press **Enter**.
13. Enter the password for the Nessus user. Press **Enter**.
14. The SSL Server Information screen appears. Enter the port on which the HTTPS daemon is running. The default port number is 8445. Press **Enter**. The Assessment Agent Adapter begins installing.
15. If you are upgrading to a newer version of the Assessment Agent Adapter, you are asked if you want to overwrite several files: launchAS.sh, bin/nessus_cmd, and version.txt. Enter the letter "y" to answer yes and press **Enter**.
16. The Installation Complete screen appears. The installation is complete and the Assessment Agent Adapter has been installed on the server.
17. Start the Assessment Agent Adapter as a background process by entering the following command at the shell prompt:
    `/assessment agent adapter installation directory/launchAS.sh &`
18. Make sure that the Nessus daemon and the Assessment Agent Adapter are started each time the system is started, by adding this command into your rc.local script:
    `/assessment agent adapter installation directory/launchAS.sh &`
19. To verify the Assessment Agent Adapter is running on the system, from the shell prompt enter:
    `netstat –an | grep port number`
    where port number is the port you entered that has the HTTPS daemon running on it. The default value for this is 8445. Returned entries containing ESTABLISHED or LISTEN is displayed.
20. To verify the Nessus application is running on the system, from the shell prompt enter:
    `ps –eaf | grep nessusd`

A return entry similar to: "nessusd: waiting for incoming connections" is displayed. This is an indication that the Nessus process is running correctly on the system.

Related Information

For information on related tasks:

- How to Change the Assessment Agent Adapter Password
- How to Set Extreme Access Control Options - Assessment Server

For information on related windows:

- Manage Assessment Settings Window
- Edit Assessment Configuration Window

How to Configure Communication Channels

Communication channels allow you to create logical groupings of your Extreme Access Control engine groups in order to segment data and limit network traffic between geographical or customer sensitive locations.

This is an advanced feature and is only appropriate in certain network scenarios. Here are two scenarios where using communication channels could be beneficial.

- A large enterprise with remote offices.
  Sending unnecessary traffic over WAN resources can cause strain on the Extreme Management Center server and possibly increase data transmission costs. Communication channels allow you to limit network communications to each geographic location reducing the amount of data that is broadcast over the slower and more expensive WAN lines.
- A Service Provider with multiple customers, clients, or organizations that do not share Extreme Access Control engines.
  In this scenario, each service provider customer has their own Extreme Access Control engine groups, and the data from one customer's engine groups must not cross to another customer's engine groups. The engines may be located on the customer site or in the service provider's cloud. Communication channels can be created for each customer, to restrict data shared between customers and protect sensitive information.

Communication channels are not appropriate in scenarios where a service provider has multiple customer data located on the same engine. In this type of scenario the Extreme Access Control engine needs to be hosted in the cloud and physical access to the engine is never be granted to the customer.

Communication channels are also not appropriate for large university networks where students and faculty move between different portions of the network, and thus move between Extreme Access Control engines in different engine groups. Because mobility is a requirement in this scenario, communication channels should not be implemented.

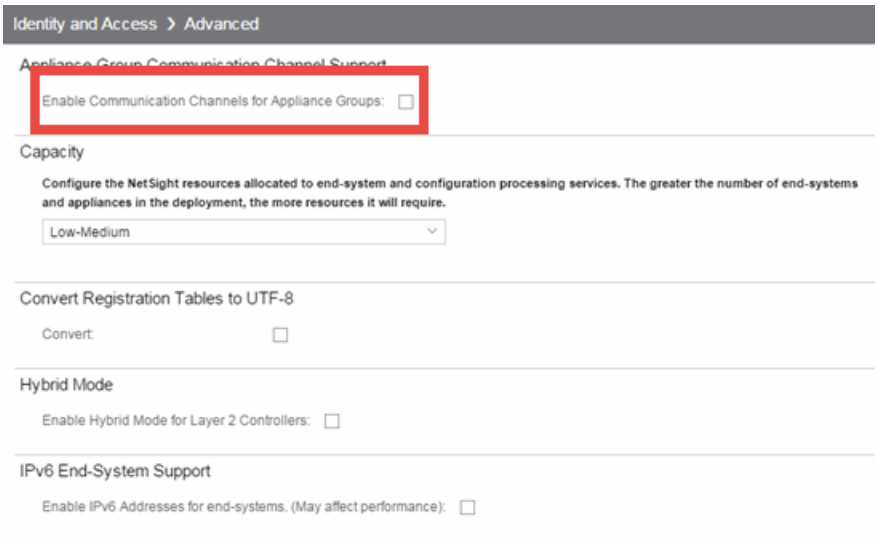
NOTES: In order to enable this feature, both the Extreme Management Center server and all the Extreme Access Control engines must be running Extreme Management Center version 4.4 or higher. This feature is not supported if there are any engines on the network running older versions.

When enabling communication channels on a network that also uses Application Analytics, the communication channels must also be configured in Application Analytics. For more information, please see the Enabling Extreme Access Control integration section of the Application Analytics Application Data Collection help topic.

Configuring Communication Channels

Use the following steps in Extreme Management Center to configure communication channels for the engine groups in your network. An engine group can only have one communication channel, but multiple engine groups can use the same communication channel.

1. Open the Extreme Access Control Options window (**Administration > Options**).
2. In the Extreme Access Control Advanced options panel, select the **Enable Communication Channels for Appliance Groups** option.



3. Open the **Control > Access Control** tab.
4. Select an engine group you want to configure as a communication channel in the Extreme Access Control Appliance Groups left-panel tree.

5. Open the **Details** tab in the right-panel. A communication channel configuration setting is displayed on the engine group's right-panel **Configuration** tab. You can add new channels using the configuration menu button to the right of the field. Any channels you create are available for all engine groups.
6. After you have created your communication channels, use the drop-down menu to select the appropriate communication channel for the engine group. When you first enable communication channels, engine groups are members of the Default channel until you change the selection.
7. Repeat steps 3 and 4 to configure communication channels for all your engine groups.
8. Click the **Enforce** button at the bottom of the left-panel to enforce the new settings to your engine groups. The communication channels are not active until you perform the enforce.

The traffic for each engine group is now restricted to its assigned communication channel. Disabling the Communication Channel option in the Extreme Access Control Options resets all channels for each engine group back to Default.

Related Information

For information on related windows:

- Advanced Settings Options

How to Deploy Extreme Access Control in an MSP or MSSP Environment

This Help topic presents instructions for deploying Extreme Access Control within an MSP (Managed Service Provider) or MSSP (Managed Security Service Provider) environment. It includes the following information:

Configuring Extreme Management Center Behind a NAT Router

If the Extreme Management Center server is located behind a NAT (Network Address Translation) router, use the following steps to add an entry to the nat_config.text file that defines the real IP address for the Extreme Management Center server. This allows the Extreme Management Center server to convert the NAT IP address received in the Extreme Access Control engine response to the real IP address used by the Extreme Management Center server.

NOTE: The text in the nat_config.text file refers to a remote IP address and a local IP address. For this configuration, the NAT IP address is the remote IP address and the real IP address is the local IP address.

1. On the Extreme Management Center server, add the following entry to the <install directory>/appdata/nat_config.text file.
   `<NAT IP address>=<real IP address>`
2. Save the file.
3. Configure your Extreme Access Control engines to use the NAT IP address for the IP address of the Extreme Management Center server. For information on how to configure or change your engine settings, refer to your Extreme Access Control engine Installation Guide.

If you have remote Extreme Management Center clients connecting to the NAT IP address, perform the following additional steps.

1. On the Extreme Management Center server, add the following text to the <install directory>/appdata/NSJBoss.properties file. In the second to last line, specify the hostname of the Extreme Management Center server.

```
# In order to connect to a NetSight server behind a NAT fi
rewall or a
# NetSight server with multiple interfaces you must define
 these two
# variables on the NetSight server. The java.rmi.server.ho
stname
# should be the hostname
(not the IP) if multiple IPs are being used
# so that each client can resolve the hostname to the corr
ect IP that
# they want to use as the IP to connect to.
java.rmi.server.hostname=<hostname of Extreme Management
Center server>
java.rmi.server.useLocalHostname=true
```

2. Save the file.
3. Add the Extreme Management Center server hostname to your DNS server.

Defining Interface Services

The advanced interface configuration mode available in Extreme Management Center allows you to define which services are provided by each of the Extreme Access Control engine's interfaces. This provides the very granular out-of-band management that is often required in MSP or MSSP environments.

For instructions, see the Interface Configuration Window Help topic.

Related Information

For information on related windows:

- Interface Configuration Window

Access Control Concepts

This Help topic explains some of the concepts you'll need to understand in order to make the most effective use of **Access Control** tab.

Information on:

Overview of the Access Control Tab

Extreme Networks Extreme Access Control is a centralized network access control solution located in the **Access Control** tab that combines authentication, vulnerability assessment, and location services to authorize network access and determine the appropriate level of service for an end-system. The Extreme Access Control solution ensures that only valid users and devices with

appropriate security postures at the proper location are granted access to your network. For end-systems which are not compliant with defined security guidelines, the Extreme Access Control solution provides assisted remediation, allowing end users to perform self-service repair steps specific to the detected compliance violation.

The Access Control tab is the management component in the Extreme Networks Extreme Access Control solution. The Access Control tab and Extreme Access Control engines work in conjunction to implement network access control. The Access Control tab provides one centralized interface for configuring the authentication, authorization, assessment, and remediation parameters for your Extreme Access Control engines. After these configurations are enforced, the Extreme Access Control engines can detect, authenticate, assess, authorize, and remediate end-systems connecting to the network according to those configuration specifications.

Extreme Access Control Engines

The Extreme Access Control engine is required for all Extreme Networks Extreme Access Control deployments. It provides the ability to detect, authenticate, and effect the authorization of end devices attempting to connect to the network. It also integrates with, or connects to, vulnerability assessment services to determine the security posture of end-systems connecting to the network. Once authentication and assessment are complete, the Extreme Access Control engine effects the authorization of devices on the network by allocating the appropriate network resources to the end-system based on authentication and/or assessment results.

If authentication fails and/or the assessment results indicate a non-compliant end-system, the Extreme Access Control engine can either totally deny the end-system access to the network or quarantine the end-system with a highly restrictive set of network resources, depending on its configuration. The Extreme Access Control engine also provides the remediation functionality of the Extreme Access Control solution by means of the remediation web server that runs on the engine. Remediation informs end users when their end-systems have been quarantined due to network security policy non-compliance, and allows end users to safely remediate their non-compliant end-systems without assistance from IT operations.

Use Scenario

The Extreme Access Control Gateway engine provides out-of-band network access control for networks where intelligent wired or wireless edge infrastructure devices are deployed as the authorization point for connecting end-systems. End-systems are detected on the network through their RADIUS authentication interchange. Based on the assessment and authentication results for a connecting device, RADIUS attributes are added/modified during the authentication process to authorize the end-system on the authenticating edge switch. Therefore, the Extreme Access Control Gateway may be positioned anywhere in the network topology with the only requirement being that IP connectivity between the authenticating edge switches and the Extreme Access Control Gateways is operational.

It is important to note that if the wired edge of the network is non-intelligent (unmanaged switches and hubs) and is not capable of authenticating and authorizing locally connected end-systems, it is possible to augment the network topology to allow implementation of inline Extreme Access Control with the Extreme Access Control Gateway. This can be accomplished by adding an intelligent edge switch that possesses specialized authentication and authorization features. The Extreme Networks K-, S-, or N-Series switch is capable of authenticating and authorizing numerous end-systems connected on a single port through its Multi-User Authentication (MUA) functionality, and may be positioned upstream from non-intelligent edge devices to act as the intelligent edge on the network. In this configuration, the K-, S-, or N-Series switch acts as the intelligent edge switch on the network, although not physically located at the access edge.

For end-systems connected to EOS policy-enabled switches, a *policy role* is specified in the Access Control tab (policy roles are defined and distributed to those switches by the Policy tab) to authorize connecting end-systems with a particular level of network access. For end-systems connected to RFC 3580-compliant switches (Enterasys and third-party), a VLAN is specified in the Access Control tab to authorize connecting end-systems with a particular level of network access, facilitated using dynamic VLAN assignment via Tunnel RADIUS attributes.

When a user or device attempts to connect to the network, the end-system is authenticated and assessed according to configurations defined in the Access Control tab. The Access Control tab uses the results of the authentication and

assessment to determine if that device meets the requirements for a compliant end-system. If the results of the authentication and security assessment are positive, Extreme Management Center authorizes the end-system with network access by assigning a designated policy role or VLAN on the switch port to which the end-system is connected. If the result of the security assessment is negative, Extreme Management Center restricts network access by assigning the user or device to a Quarantine policy role or VLAN on the switch port until the end-system is remediated and brought into a compliant state. If the result of the authentication is negative, Extreme Management Center can deny all network access for the endpoint as an invalid device or user on the network, setting the switch port to the unauthenticated state.

Depending on the engine model, the Extreme Access Control Gateway provides either on-board (integrated) vulnerability assessment server functionality and/or the ability to connect to external assessment services, to determine the security posture of end-systems connecting to the network. (On-board assessment requires a separate license.)

The number of Extreme Access Control Gateways you deploy on the network depends on the number of end-systems on the network. The following table displays the number of end-systems supported per Extreme Access Control Gateway model. Use this table to help determine the number of gateways to deploy.

Model	Number of End-Systems Supported	Notes
IA-A-20	6000	Configured Extreme Access Control Features: Authentication and OS/Device Fingerprinting, but no Registration or Assessment.
	4500	Configured Extreme Access Control Features: All features excluding Assessment.
	3000	Configured Extreme Access Control Features: All features including Assessment.

Model	Number of End-Systems Supported	Notes
IA-A-300	12000	Configured Extreme Access Control Features: Authentication and OS/Device Fingerprinting, but no Registration or Assessment.
	9000	Configured Extreme Access Control Features: All features excluding Assessment.
	6000	Configured Extreme Access Control Features: All features including Assessment.
IA-V	See Notes	The IA-V is included with the Extreme Management Center Advanced (NMS-ADV) license and is Extreme Access Controlused in conjunction with an Extreme Access Control Enterprise license (IA-ES-12K).
NAC-V-20	3000	The NAC-V-20 is a virtual engine and requires an Extreme Access Control VM license in the Extreme Management Center Server.
NAC-A-20	3000	
SNS-TAG-ITA	3000	
SNS-TAG-HPA	3000	
SNS-TAG-LPA	2000	

It is important to configure Extreme Access Control Gateway redundancy for each switch. This is achieved by configuring two different Extreme Access Control Gateway engines as a primary and secondary gateway for each switch. When connection to the primary gateway engine is lost, the secondary gateway is used. Note that this configuration supports redundancy but not load-sharing, as the secondary gateway engine is only used in the event that the primary gateway becomes unreachable. To achieve redundancy with load-sharing for two Extreme Access Control Gateways, it is suggested that one half of the switches connecting to the gateways are configured with "Extreme Access Control Gateway A" as the primary and "Extreme Access Control Gateway B" as the secondary, and the second half are configured with "Extreme Access Control Gateway B" as the primary and "Extreme Access Control Gateway A" as the secondary. In this way, Extreme Access Control Gateways are configured in redundant active-active operation on the network.

Extreme Access Control VPN Deployment

Extreme Networks Extreme Access Control provides out-of-band support for VPN remote access with specific VPN concentrators (see the Release Notes for a list of supported VPN concentrators). Out-of-band VPN support provides visibility into who and what is accessing the network over VPN. If RADIUS accounting is used, you also have the ability to determine who was on the network at any given time. In the VPN remote access use scenario, the VPN concentrator acts as a termination point for remote access VPN tunnels into the enterprise network. In addition, the Extreme Networks Extreme Access Control Gateway engine is deployed to authenticate and authorize connecting end-systems on the network and implement network access control.

The process begins when the user's end-system successfully establishes a VPN tunnel with the VPN concentrator, and the VPN concentrator sends a RADIUS authentication request with the associated credentials to the Extreme Access Control Gateway. The Extreme Access Control Gateway proxies the authentication request to a backend authentication server (RADIUS or LDAP) to validate the identity of the end user/device or can authenticate with a local password repository within Extreme Management Center. If authentication fails, the Extreme Access Control Gateway can deny the end-system access to the network by sending a RADIUS access reject message to the VPN concentrator.

After the end-system is authenticated, the Extreme Access Control Gateway requests an assessment of the end-system, if assessment is configured. Once authentication and assessment are complete, the Extreme Access Control Gateway allocates the appropriate access control to the end-system based on authentication and/or assessment results. Access control can be implemented using one of two methods. With the first method, access control is applied directly at the VPN concentrator via RADIUS response attributes, if the VPN concentrator supports this. For example, with a Cisco ASA security engine, this can be accomplished by using the filter-ID response attribute to specify the name of a valid ACL.

With the second method, an Extreme Networks K-Series, S-Series, or N-Series device is added between the VPN's internal port and the internal network as a Policy Enforcement Point (PEP). This allows the Extreme Access Control Gateway to provide a more granular access control mechanism using IP to Policy Mappings. This method must be used if you are implementing remediation on your network. If the end-system fails assessment, the Extreme Access Control

Gateway can apply a Quarantine policy on the PEP to quarantine the end-system. When the quarantined end user opens a web browser to any web site, its traffic is dynamically redirected to a Remediation web page that provides steps for the user to execute in order to achieve compliance. After executing the steps, the end user can reattempt network access and start the process again.

Access Control Tab Structure

The Access Control tab components are contained in three major navigation trees.

At the top are the following navigation trees:

- Engine Groups — Lists the Extreme Access Control engines added to the selected engine group, the end-systems connected to those engines, the switches added to the Gateway engines in the engine group, and general information about the engine group.
- All Extreme Access Control Engines — Lists all Extreme Access Control engines added to Extreme Management Center, the end-systems connected to those engines, the switches added to the Gateway engines, and general information about the engine.
- Extreme Access Control Configurations — Provides options to configure the end-user connection experience and control network access based on a variety of criteria including authentication.

Extreme Access Control Configuration

The Extreme Access Control Configuration lets you manage the end user connection experience and control network access based on a variety of criteria. The Access Control tab comes with a default Extreme Access Control Configuration which is automatically assigned to your Extreme Access Control engines. You can use this default configuration as is, or make changes to the default configuration, if desired.

The Extreme Access Control Configuration determines what Extreme Access Control Profile will be assigned to an end-system connecting to the network. It contains an ordered list of rules that are used by the configuration to assign an Extreme Access Control Profile to a connecting end-system based on rule criteria. It also specifies the Default Profile which serves as a "catch-all" profile

for any end-system that doesn't match one of the rules. By default, all end-systems match the Default Profile.

When an end-system connects to the network, the rules are evaluated in a top-down fashion, similar to the way an ACL would be evaluated. End-systems that do not match any of the rules are assigned the Default Profile.

Rule Components

The rules defined in an Extreme Access Control Configuration provide very granular control over how end-systems are treated as they come onto the network. The following criteria can be used to define the rules used in your Extreme Access Control Configuration:

- Authentication Type - for example, 802.1X or MAC authentication.
- End-System Groups - allow you to group together devices that have similar network access requirements or restrictions. For example, a list of MAC addresses, IP addresses, or hostnames.
- Device Type - allow you to group together end-systems based on their device type. The device type can be an operating system family, an operating system, or a hardware type, such as Windows, Windows 7, Debian 3.0, and HP Printers.
- Locations - allow you to specify network access requirements or restrictions based on the network location where the end user is connecting. For example, a list of switches, wireless devices, switch ports, or SSIDs.
- Time of Day - allow you to specify network access requirements or restrictions based on the day and time when the end user is accessing the network. For example, traditional work hours or weekend work hours.
- User Groups - allow you to group together end users having similar network access requirements or restrictions. For example, a list of usernames, an LDAP users group, or a RADIUS user group.

For more information, see the Manage Rule Groups window.

Extreme Access Control Profiles

Extreme Access Control Profiles specify the authorization and assessment requirements for the end-systems connecting to the network. Profiles also specify the security policies applied to end-systems for network authorization, depending on authentication and assessment results.

The **Access Control** tab comes with ten system-defined Extreme Access Control Profiles:

- Administrator
- Allow
- Default
- Guest Access
- Notification
- Pass Through
- Quarantine
- Registration Denied Access
- Secure Guest Access
- Unregistered

If desired, you can edit these profiles or you can define your own profiles to use for your Extreme Access Control Configurations. For more information, see the Manage Extreme Access Control Profiles window.

AAA Configurations

The AAA Configuration defines the RADIUS servers, LDAP configurations, and Local Password Repository that provide the authentication and authorization services for all end-systems connecting to your Extreme Access Control engines. The **Access Control** tab comes with a default Basic AAA Configuration that ships with each Extreme Access Control engine. You can use this default configuration as is, or make changes to the default configuration, if desired. For more information, see the Edit Basic AAA Configurations window.

Portal Configurations

If your network is implementing Registration or Assisted Remediation, the Portal Configuration defines the branding and behavior of the website used by the end user during the registration or remediation process. Extreme Access Control engines are shipped with a default Portal Configuration. You can use this default configuration as is, or make changes to the default configuration, if desired. For more information, see the Portal Configuration Help topic.

Access Policies

Access policies define the authorization level that the Extreme Access Control assigns to a connecting end-system based on the end-system's authentication and/or assessment results. There are four access policies used in the Access Control tab: Accept policy, Quarantine policy, Failsafe policy, and Assessment policy. In your Extreme Access Control Profiles, these access policies define a set of network access services that determine exactly how an end-system's traffic is authorized on the network. How access policies are implemented depends on whether your network utilizes Extreme Access Control Controller engines and/or Extreme Access Control Gateway engines.

For end-systems connected to EOS policy-enabled switches, Extreme Access Control Gateway engines inform the switch to assign a policy role to a connecting end-system, as specified by the access policy. These policy roles must be defined in Policy tab and enforced to the EOS policy-enabled switches in your network.

For end-systems connected to RFC 3580-enabled switches, policy roles are associated to a VLAN ID. This allows your Extreme Access Control Gateways to send a VLAN ID instead of a policy role to those switches using Tunnel RADIUS attributes.

For Extreme Access Control Controller engines, authorization of the end-system is implemented locally on the Extreme Access Control Controller engine by assigning a policy role to the end-system, as specified by the access policy. In this scenario, all policy roles must be defined in the Extreme Access Control Controller policy configuration.

Here is a description of each the Access Control tab access policy, and some guidelines for creating corresponding policy roles in the Policy tab.

Accept Policy: The Accept access policy is applied to an end-system when it has been authorized locally by the Extreme Access Control Gateway and when an end-system has passed an assessment (if an assessment was required), or if the Accept policy has been configured to replace the Filter-ID information returned in the RADIUS authentication messages. For EOS policy-enabled switches, a corresponding policy role (created in the Policy tab) would allocate the appropriate set of network resources for the end-system depending on their role in the enterprise. For example, you might associate the Accept policy in the

Access Control tab to the "Enterprise User" role that is defined in the Policy tab demo.pmd file. For RFC 3580-compliant switches, the Accept access policy may be mapped to the Production VLAN. Extreme Access Control Controllers are shipped with a default policy configuration that includes an Enterprise User policy role.

Quarantine Policy: The Quarantine access policy is used to restrict network access to end-systems that have failed assessment. For EOS policy-enabled switches, a corresponding Quarantine policy role (created in the Policy tab) should deny all traffic by default while permitting access to only required network resources such as basic network services (e.g. ARP, DHCP, and DNS) and HTTP to redirect web traffic for Assisted Remediation. For RFC 3580-compliant switches, the Quarantine access policy may be mapped to the Quarantine VLAN. Extreme Access Control Controllers are shipped with a default policy configuration that includes a Quarantine policy role.

Failsafe Policy: The Failsafe access policy is applied to an end-system when it is in an Error connection state. An Error state results if the end-system's IP address could not be determined from its MAC address, or if there was an assessment error and an assessment of the end-system could not take place. For EOS policy-enabled switches, a corresponding policy role (created in the Policy tab) allocates a nonrestrictive set of network resources to the connecting end-system so it can continue its connectivity on the network, even though an error occurred in the Extreme Access Control Solution operation. For RFC 3580-compliant switches, the Failsafe access policy may be mapped to the Production VLAN. Extreme Access Control Controllers are shipped with a default policy configuration that includes a Failsafe policy role.

Assessment Policy: The Assessment access policy may be used to temporarily allocate a set of network resources to end-systems while they are being assessed. For EOS policy-enabled switches, a corresponding policy role (created in the Policy tab) should allocate the appropriate set of network resources needed by the Assessment server to successfully complete its end-system assessment, while restricting the end-system's access to the network.

Typically, the Assessment access policy allows access to basic network services (e.g. ARP, DHCP, and DNS), permits all IP communication to the Assessment servers so the assessment can be successfully completed (using destination IP address "Permit" classification rule), and HTTP to redirect web traffic for Assisted Remediation. For RFC 3580-compliant switches, the Assessment access policy may be mapped to the Quarantine VLAN. Extreme Access Control

Controllers are shipped with a default policy configuration that includes an Assessing policy role.

It is not mandatory to assign the Assessment policy to a connecting end-system while it is being assessed. The policy role received from the RADIUS server or the Accept policy can be applied to the end-system, allowing the end-system immediate network access while the end-system assessment is occurring in the background. In this case, the policy role or Accept policy (or the associated VLAN for RFC 3580-compliant switches) must be configured to allow access to the appropriate network resources for communication with the Assessment servers.

NOTE: The Assessment server sends an ICMP Echo Request (a "ping") to the end-system before the server begins to test IP connectivity to the end-system. Therefore, the Assessment policy role, the router ACLs, and the end-system's personal firewall must allow this type of communication between end-systems and Assessment servers in order for the assessment to take place. If the Assessment server cannot verify IP connectivity, the Failsafe policy is assigned to the end-system.

For more information, refer to the How to Set Up Access Policies Help topic.

Registration

The Extreme Networks Extreme Access Control Solution provides support for Registration, a solution that forces any new end-system connected on the network to provide the user's identity in a web page form before being allowed access to the network, without requiring the intervention of network operations. This means that end users are automatically provisioned network access on demand without time-consuming and costly network infrastructure reconfigurations. In addition, IT operations has visibility into the end-systems and their associated users (e.g. guests, students, contractors, and employees) on the network without requiring the deployment of backend authentication and directory services to manage these users. This binding between user identity and machine is useful for auditing, compliance, accounting, and forensics purposes on the network.

End-system or user groups may be configured to exempt certain devices and users from having to register to the network, based on authentication type, MAC address, or user name. For example, a end-system group for the MAC OUI of the

printer vendor for the network can be configured to exempt printers from having to register for network access.

The Registration solution has minimal impact on the end user's experience by initially redirecting guests, contractors, partners, students, or other pre-defined end users to a web page for registering their end-system when it is first connected to the network. After successful registration, the end-system is permitted access, and possibly assessed for security posture compliance checking, until the registration is administratively revoked.

Registration is supported on Extreme Access Control Gateway engines and/or Layer 2 Extreme Access Control Controller engines. (Registration is not supported on the Layer 3 Identity and Access Controller engines.) Registration provides flexibility in implementation by offering the following capabilities:

- Determine "valid" end users by prompting each end user for a username with additional information such as full name and e-mail address, or a username and password (e.g. e-mail address and student ID number) which can be validated against an existing database on the network.
- Allow end users to register to the network when approved by a "sponsor" who is an internal trusted user to the organization. This is referred to as "Sponsored Registration." With sponsored registration, end users are only allowed to register to the network when approved by a sponsor. Sponsorship can provide the end user with a higher level of access than just guest or web access and allows the sponsor to fine-tune the level of access for individual end users.
- Configure the introductory message for the Registration web page (displayed to end-systems before registering to the network) to state that the end user is agreeing to the Acceptable Use Policy for the network upon registering their device.
- Specify the maximum number of registered MAC addresses per user.
- Control areas on the network where Registration is enabled.
- Provide a web-based administrative interface served over HTTPS where registrations may be viewed, manually added, deleted, and modified by administrators and sponsors without requiring access to the Access Control tab.

The Extreme Networks Extreme Access Control Solution utilizes a Registration Web Server installed on the Extreme Access Control engine to provide this registration functionality to end-systems. Note that an Extreme Access Control engine may implement both assisted remediation and registration concurrently.

There are specific network configuration steps that must be performed when using Registration in your Extreme Access Control Solution. In addition, you must configure Registration in the Access Control tab.

How Registration Works

Here is a description of how Registration works in the Extreme Networks Extreme Access Control (Extreme Access Control) Solution:

- An unregistered end-system attempts to connect to the network and is assigned the unregistered access profile without being assessed by the Extreme Access Control engine. For example, if connected to a Layer 2 Extreme Access Control Controller, the end-system may be assigned to the "Unregistered" policy as defined in the Extreme Access Control Controller's default policy configuration. If connected to an EOS policy-enabled switch, the end-system may be assigned to the "Unregistered" policy as defined in the Extreme Management Center Policy tab and enforced to the policy-enabled switches. Or, if connected to an RFC 3580-compliant switch, the end-system may be assigned to the "Unregistered" VLAN.
- The user on the unregistered end-system opens up a web browser to any URL and is redirected to the Registration Web Page served by the Extreme Access Control engine.
- The end user registers its end-system on the network by entering information such as username, full name, e-mail, and possibly a password or sponsor's email address into the Registration Web Page, and clicking the "Complete Registration" button.
- The Registration Web Server assigns the end user to an end-system group based on the Registration Behavior configured in the Extreme Access Control Configuration.
- The end-system is then automatically re-authenticated to the network by the Extreme Access Control engine. Upon re-authentication, the end-system is authenticated, assessed, and authorized as defined by the profile specified in the Extreme Access Control Configuration for the newly registered system. If the profile specifies to assess the end-system, an assessment of the end-system takes place at this time.

Assessment

The Extreme Networks Extreme Access Control Solution integrates with assessment services to determine the security posture of end-systems connecting to the network. It uses assessment servers to assess and audit

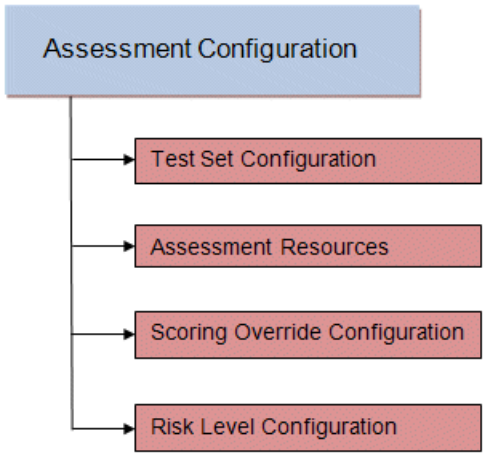
connecting end-systems and provide details about an end-system's patch levels, running processes, anti-virus definitions, device type, operating system, and other information critical in determining an end-system's security compliance. End-systems that fail assessment can be dynamically quarantined with restrictive network access to prevent security threats from entering the network.

When an assessment is performed on an end-system, a *Health Result* is generated. For each health result, there may be several *Health Result Details*. A health result detail is a result for an individual test performed during the assessment. Each health result detail is given a score ranging from 1 to 10, and based on this score, the health result is assigned a risk level. The Access Control tab uses this risk level to determine whether or not the end-system will be quarantined.

In addition, assessment tests are assigned a *scoring mode* which determines whether the resulting health result detail is applied towards the quarantine decision, or is used only for informational or warning purposes. Informational health result details can be used to gather information about the security risks on your network, while warning health result details allow you to notify end users when they have security risks that should be remediated. Informational or warning health result details have scores, however these health result details do not impact the end-system's overall risk level.

The Access Control tab lets you create multiple *assessment configurations* that can define different assessment requirements for end-systems. Assessment configurations define the following information:

- What assessment tests to run (determined by the selected test sets).
- What resources to use to run the tests (determined by the selected Assessment Resources).
- How to score assessment results (determined by the selected Risk Level and Scoring Override configurations).



Test sets let you define what type of assessment to execute, what parameters to pass to the assessment server, and which assessment server resources to use. The Access Control tab provides three default test sets; one for each type of assessment agent that is either supplied or supported by the Access Control tab. You can use these default test sets "as is" or edit them, if desired.

When you define your assessment server resources for a test set, you can specify to balance the assessment load between your all your assessment servers, or, you can specify an assessment server pool. For example, if you have four Nessus assessment servers, you can put server A and server B in server pool 1, and server C and server D in server pool 2. Then, in your test set configuration you can specify which server pool that test set should use.

You can use risk level and scoring override configurations to define how each assessment configuration will interpret an end-system's health results. The risk level configuration determines what risk level is assigned to an end-system (high, medium, or low) based on the end-system's health result details score. The scoring override configuration lets you override the default score and scoring mode assigned to a particular assessment test ID.

Once you have defined your assessment configurations, they are available for selection when creating your Extreme Access Control Profiles. In addition, the Access Control tab provides a default assessment configuration that is already set up with default assessment parameters and is ready to use in your Extreme Access Control Profiles.

Before beginning to configure assessment on your network, you should read through the following information presented in the Access Control tab online Help.

- How to Set up Assessment - Provides information on the steps that must be performed in the Access Control tab prior to deploying assessment on your network, including managing your assessment servers and adding external assessment servers. It also includes basic information on how to use the default assessment configurations provided by the Access Control tab, and enable assessment for your Extreme Access Control Configuration.
- Extreme Access Control Assessment Phased Deployment Guide - This guide describes the phased approach to introducing assessment into your Extreme Access Control deployment using Informational, Warning, and Quarantine assessment. The guide also provides information on the Access Control tab tools that can be used to monitor and evaluate assessment results, and diagnose and troubleshoot problems.
- How to Configure Assessment - Provides step-by-step instructions for configuring assessment using the phased approach described in the Extreme Access Control Assessment Phased Deployment Guide. Instructions are provided for configuring phased assessment using agent-less or agent-based assessment, or a combination of both.
- How to Deploy Agent-Based Assessment - If you are deploying agent-based assessment, this Help topic provides the configuration steps specific to deploying agent-based assessment in a Windows and Mac network environment. It includes instructions for configuring agent deployment and provides information about the agent icon and notification messages that appear on the end-user's system. It also includes instructions on performing a managed deployment or installation of the agent.
- How to Set Up Assessment Remediation - Because Warning and Quarantine assessment provides end-system remediation, you must enable remediation for your Extreme Access Control Configuration. This Help topic provides the specific steps that must be performed when setting up assisted remediation in your network.

Assessment Remediation

Remediation is a process that informs end users when their end-systems have been quarantined due to network security policy non-compliance, and allows end users to safely remediate their non-compliant end-systems without assistance from IT operations. The process takes place when an end-system

connects to the network and assessment is performed. End users whose systems fail assessment are notified that their systems have been quarantined, and are instructed in how to perform self-service remediation specific to the detected compliance violation. Once the remediation steps have been successfully performed and the end-system is compliant with network security policy, the appropriate network resources are allocated to the end-system, again without the intervention of IT operations.

The Extreme Networks Extreme Access Control Solution implements local Remediation Web Server functionality to provide web notification to end users indicating when their end-systems are quarantined and what remediation steps the end user must take. The Remediation Web Server is installed on the Extreme Access Control engine.

There are specific network configuration steps that must be performed when using assisted remediation in your Extreme Access Control Solution. In addition, you must configure assisted remediation in the **Access Control** tab. For more information, see How to Set up Assessment Remediation and Portal Configuration Help topics.

How Remediation Works

Here is a description of how assisted remediation works in the Extreme Networks Extreme Access Control Solution:

- An end-system connects to the network (where assessment has been configured) and is authorized with the level of network access defined by the Assessment access policy configuration.
- The end-system is assessed by the assessment server for security threats and vulnerabilities.
- When the end-system opens a web browser to any web site, the HTTP traffic is redirected to the Extreme Access Control engine and a web page indicating that the end-system is currently being assessed is displayed.
- When the assessment is complete, the assessment server sends the results to the Extreme Access Control engine. If the end-system failed assessment, the end-system is authorized with the level of network access defined by the Quarantine access policy configuration.
- When the quarantined end user opens a web browser to any web site, its traffic is dynamically redirected to the Extreme Access Control engine.

- The Extreme Access Control engine returns a web page formatted with self-service remediation information for the quarantined end-system. This web page indicates the reasons the end-system was quarantined and the remediation steps the end user must take.
- After taking the appropriate remediation steps, the end-user clicks a button on the web page and attempts to reconnect to the network. A re-assessment of the end-system is initiated. If the end-system is now compliant with network security policy, the Extreme Access Control engine authorizes the end-system with the appropriate access policy. If the end-system is not compliant, the Quarantine access policy is again utilized to restrict the authorization level of the end-system and the process starts again.
- After a specified number of attempts and/or maximum time to remediate have expired, the end user may be redirected to a web page requiring them to contact the helpdesk for further assistance, and a notification is sent to the helpdesk system with information regarding the non-compliant end-system.

End-System Zones

The Access Control tab end-system zones allow you to group end-systems into zones, and then limit an Extreme Management Center user's access to Extreme Management Center end-system information and configuration based on those zones.

End-system zones are configured and managed in the Access Control tab, and are enforced for Extreme Management Center end-system information and configuration.

When an end-system authenticates to the network, Extreme Access Control rules are used to assign an Extreme Access Control profile and an end-system zone to the end-system. This allows you to use a variety of rule components (such as End-System Groups, Location Groups, and User Groups) to determine which zone an end-system should be assigned to.

You can create any number of end-system zones in your network. An end-system can only be assigned to one zone (but does not have to be assigned to a zone). You can view which zone an end-system is currently assigned to in the end-systems table in the Access Control tab in Extreme Management Center.

A user's authorized zones are determined by their Extreme Management Center user group membership. User groups are created and configured in the Extreme

Management Center Authorization/Device Access Tool (accessed from the Tool menu), and authorized zones are assigned to each user group in the **Access Control** tab. For instructions, see How to Configure End-System Zones.

In addition to using end-system zones, you can also limit a user's access to Extreme Management Center operations by assigning authorized rule groups. Whenever a user initiates a change to a rule group, such as adding or removing an end-system to or from a group, a check is performed to verify that the user is authorized to change that rule group. Similar to end-system zones, a user's authorized rule groups are determined by their Extreme Management Center user group membership.

A third component that should be taken into consideration is the ability to limit user access to Extreme Management Center using authorization group capabilities. For example, you can assign a user group the Extreme Management Center End-Systems Read Access capability to allow read-only access to Extreme Management Center end-system information, and use end-system zones to limit which end-systems can be viewed. You can assign a user group the Extreme Management Center End-Systems Read/Write Access capability to allow the ability to modify rule groups, and use rule group authorization to limit which rule groups the user can perform these operations on.

Capabilities are assigned to user groups using the Authorization/Device Access Tool. The Extreme Management Center Administrator group is always assigned all capabilities.

For more information, see How to Configure User Access to Extreme Management Center Applications and Authorization Group Capabilities in the Suite-Wide Tools Help.

End-System Zone Use Cases

Here are several network scenarios where using end-system zones could be beneficial.

- **A Service Provider with multiple tenants.** If a service provider serves multiple tenants and each tenant has a clearly delineated set of switches, user access can be configured to allow each tenant's IT staff to only view the end-systems connecting to their own switches.
- **A large enterprise with network administrator groups.** In a large enterprise where specific groups of network administrators are responsible for specific groups of

switches on shared engines, user access can be configured so that each administrator can view reports and other information only for their switches and end-systems.

- A large business segmented by business function. In a large enterprise where division of control is not closely tied to switches or engines, user access can be configured so that administrators only have the ability to view and manage the appropriate end user groups.

In each of these scenarios, a restricted set of authorization group capabilities must be used to prevent users from viewing and accessing information that may not pertain to their area.

Enforcing

In the Access Control tab, enforcing means writing Extreme Access Control configuration information to one or more Extreme Access Control engines. Any time you add or make a change to the Extreme Access Control Configuration, the engines need to be informed of the change through an enforce, otherwise the changes do not take effect. When an engine needs to be enforced, the Enforce icon appears on that engine in the left-panel tree.

To enforce, use the Enforce All button in the Enforce menu at the bottom of the left-hand panel which writes the information to all the Extreme Access Control engines. You can enforce to an individual engine or engine group by clicking the Enforce menu and selecting Selection.

TIP: For a preview of what will be enforced/updated on an individual engine, right-click the engine and choose Enforce Preview from the menu.

The enforce operation is performed in two stages: first an engine configuration audit is performed and then the actual enforce to engines is performed.

The configuration audit takes place automatically after you start the enforce operation. It looks for a wide-range of engine configuration problems including a review of the Extreme Access Control Configuration, Extreme Access Control Profile, rule configuration, AAA configuration, and portal configuration. The audit results are displayed in the Enforce window, allowing you to view any warning and error information. To see warning or error details, use the + icon in the left column to expand the Details information (as shown below) or click Show Details to open the information in a new window.

If you choose to correct any problems at this point, you must close the Audit Results window. When you have made your changes, click the Enforce All button to start the enforce operation and perform a new audit.

From the Enforce window, you can click the Enforce All button to enforce all engines, or use the checkboxes in the Select column to select some of the engines to enforce and click the Enforce button. In order for the enforce operation to be carried out, none of the selected engines can have an error associated with it. Even if one of the selected engine has passed the audit, it will not be enforced if other selected engines have errors.

If none of the selected engines have errors, but a selected engine has a warning associated with it, you are given the option to acknowledge the warning and proceed with the enforce anyway. Once you acknowledge the warning and click OK, the enforce is performed.

TIP: If there are warning messages that are regularly displayed during Enforce engine audits, you can use the Enforce Warning Settings to specify that these messages should be ignored and not be displayed.

The Enforce window displays the enforce operation status, as shown below.

Advanced Enforce Options

In the Enforce window, there are two Advanced enforce options available. The two options can be used for the following situations:

- Force Reconfiguration for All Switches - This option can be used if the switch RADIUS settings were manually changed via CLI or the Policy tab. Since Identity and Access does not reconfigure the switches every time there is an enforce, selecting this option forces reconfiguration of RADIUS settings on all switches to ensure they are configured correctly.
- Force Reconfiguration for Captive Portal - During an enforce, captive portal settings are not enforced unless they have changed. You can use this option to force reconfiguration of the portal to ensure the state of the captive portal processes.

NOTE: MAC Locking to a specific port on a switch is based on the port interface name (e.g. fe.5.1). If a switch board is moved to a different slot in a chassis, or if a stack reorders itself, this name will change and break the MAC Locking settings.

NOTE: For Extreme Access Control Controller Engines.

-- On Layer 3 Extreme Access Control Controllers, do not use MAC Locking to lock a MAC address to the Controller PEP IP address **and** a port on the PEP. You can however, lock a MAC address to the PEP IP and **not** the port, which would restrict movement of the MAC address away from the Layer 3 Controller.

-- On Layer 2 Extreme Access Control Controllers, a MAC address can be locked to the Controller PEP IP address and port, or just the PEP IP address, but this only controls the movement of the end-system between the downstream ports on the PEP (IP address and port) and not the actual edge of the network.

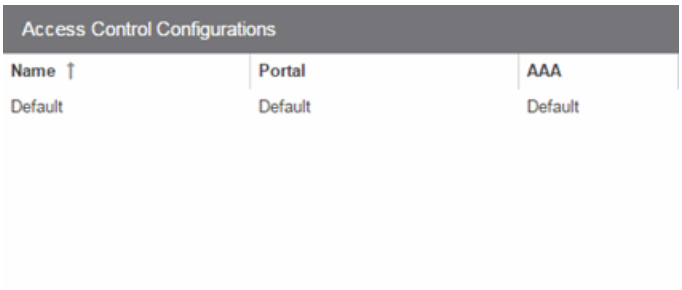
-- On Layer 3 Extreme Access Control Controllers, there may be cases where the **Access Control** tab cannot determine the MAC address of the connecting end-system (for example, DHCP is disabled and a firewall is enabled on the end-system, or the end-system is connecting through a VPN), and the MAC address for the end-system is displayed as "Unknown." In these cases, the MAC Locking feature is not supported.

Notifications

Notifications provide the ability for the **Identity and Access** tab to notify administrators or helpdesk personnel of important information through email, Trap, or Syslog messages. These notifications help administrators understand what is going on in their system on a real-time basis. For example, the **Access Control** tab could be configured to send a notification when a new end-system is learned on the network, when a MAC lock is violated, or when a new MAC address is registered on the network.

Access Control Configuration

The Access Control Configuration panel provides a central location to view the configuration parameters for all aspects of your Extreme Access Control system. Access this window by selecting Access Control Configurations from the Control > Access Control tab.



Expand the Access Control Configurations left-panel tree to access to the following Access Control system components.

Access Control Configurations

Each engine group uses one Access Control configuration that contains an ordered list of rules used to determine which Access Control profile is assigned to the end-systems connecting to the engines in that group. Access Control configurations include the following components:

Name

The Name by which the Access Control Configuration is known.

Portal Configurations

If your network is implementing Registration or Assisted Remediation, use the Portal Configuration to define the branding and behavior of the website used by the end user during the registration or remediation process.

AAA Configurations

AAA configurations define the RADIUS and LDAP configurations, and Local Password Repository that provide the authentication and authorization services to your Extreme Access Control engines.

Extreme Access Control Configuration Rules

The Rules panel in the Access Control tab displays a list of rules used by the Extreme Access Control Configuration to assign an Extreme Access Control Profile to a connecting end-system based on rule criteria.

This Help topic provides information for accessing and configuring Extreme Access Control Configuration Rules:

Accessing Extreme Access Control Configuration Rules

Use the following steps to view and edit your Extreme Access Control Configuration rules.

1. Open the Control tab in Extreme Management Center.
2. Click the Access Control tab.
3. In the left-panel tree, expand the Access Control Configurations tree.
4. Expand an Extreme Access Control Configuration and select Rules. The table of your Extreme Access Control rules is displayed in the right panel. See below for an explanation of the table columns.
5. Use the toolbar buttons at the top of the right-panel to create a new rule or edit existing rules. See below for a description of each button.

Viewing Rules in the Table

The Rules table displays the rule name, whether the rule is enabled, and summary information about the rule. It also shows the Extreme Access Control Profile assigned to any end-system that matches the rule and the portal

redirection action, if applicable. Rules are listed in order of precedence. End-systems that do not match any of the listed rules are assigned the Default Catchall rule.

TIP: Right click on a rule in the table to access a menu of options including the ability to edit the Extreme Access Control profile and any user groups included in the rule.

Enabled

This column displays whether the rule is enabled by displaying a checkmark icon ✓ or disabled, with no checkmark. Click the **Edit** button to enable or disable the rule. You cannot disable any of the system rules provided by Extreme Management Center.

Rule Name

This column displays the rule name. Double-click on the rule to open the Edit Rule window where you can edit the rule name, if desired. You cannot change the name of the system rules provided by Extreme Management Center.

Conditions

This column displays the criteria an end-system must meet in order to be assigned the rule, including the authentication method and rule groups that the end-system or user must match. Double-click on the rule to open the Edit Rule window where you can edit the rule criteria, if desired. You cannot change the criteria for the system rules provided by Extreme Management Center. Click on a rule group name to open a window where you can edit the group's parameters.

User Group

This column, hidden by default, displays the user group you configured. User groups limit an Extreme Management Center user's access based on the LDAP, RADIUS, or Username group to which they are assigned. To edit the **User Group**, click the user group in the **Conditions** column, which opens the Add/Edit User Group window.

Zone

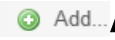
This column displays the end-system zone you configured. End-system zones allow you to group end-systems into zones, and then limit an Extreme Management Center user's access to end-system information and configuration based on those zones.

Actions
: This column displays the actions the rule takes when an end-system matches the rule's criteria. This includes the profile assigned to the end-system and the portal configuration the end user sees. Click on the profile or portal name to open a window where you can make changes, if desired.

Add or remove a column by clicking the down arrow at the right of a column header and selecting a checkbox associated with a column from the Columns menu.

Creating and Editing Rules

Use the Rules toolbar buttons to create, edit, and modify the rules in the table. Any changes made in this table are written immediately to the Extreme Management Center database.



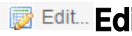
Add New Rule

Opens the Create Rule window where you can define a new rule to use in the Extreme Access Control configuration.

TIP: To add a new rule at a specific location in the table, select the rule that you want the new rule to follow, right-click and select **Add Rule** after Selection. When you create the new rule and click **OK**, it is added after the selected rule. The selected rule must be a custom (user-defined) rule, or it can be the Blacklist or Assessment Warning rule.

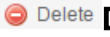
Copy Rule

Opens the Copy Rule window where you can copy the rule criteria of an existing rule for a new rule.



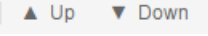
Edit Rule

Opens the Edit Rule window where you can edit the rule criteria for a selected rule.



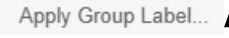
Delete Selected Rules

Deletes any rules selected in the table.



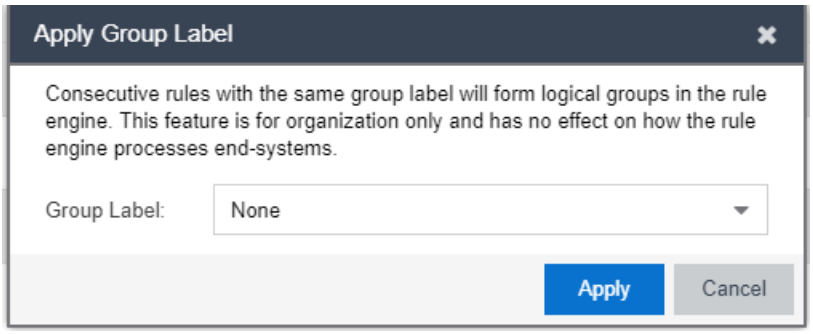
Move Rule Up/Down

Move rules up and down in the list to determine rule precedence.



Apply Group Label

Opens the Apply Group Label window where you can add a group label to selected rules to create a new group. Once the group label is applied, the new group appears in the Rules window and is collapsible.



Related Information

For information on related windows:

- AAA Configuration
- Portal Configuration

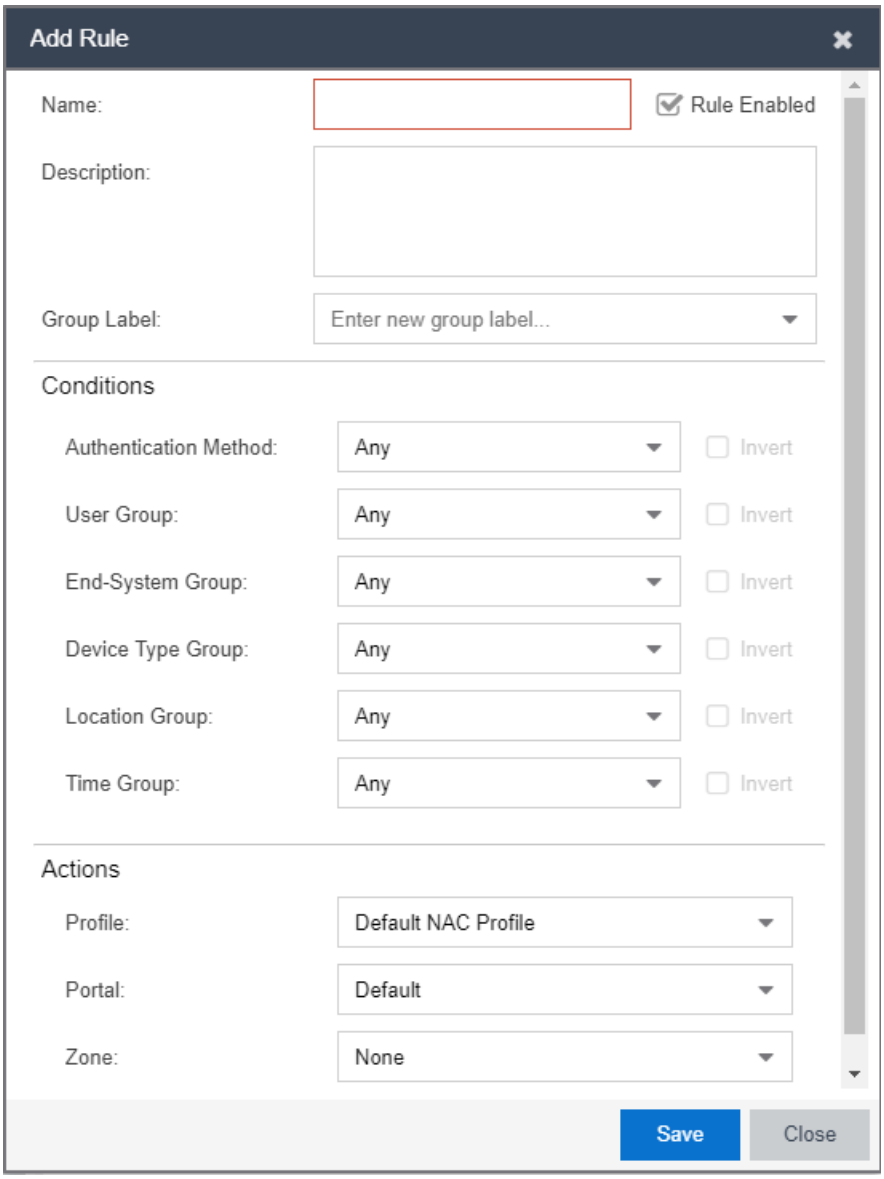
Add/Edit Rule

Use this window to add a new rule or edit an existing rule in an Extreme Access Control configuration. End-systems that match the criteria selected for the rule are assigned the Extreme Access Control profile that is specified.

To access this window:

1. Open the Control tab in Extreme Management Center.
2. Click the Extreme Access Control tab.
3. In the left-panel tree, select Extreme Access Control Configurations > Default > Rules. A table of rules for the Extreme Access Control configuration is displayed in the right panel.
4. Click the Add button in the table toolbar to open the Create Rule window.
   or
   Select a rule in the table and click the Edit button in the toolbar to open the Edit Rule window.

The image below shows a rule created to provide a different Extreme Access Control profile for authenticated registered users on mobile devices. Descriptions of the different fields and options in the window are provided below.



NOTES: For the following rule criteria:
-- If you select Any then the criteria is ignored during the rule match process.
-- If you select the Invert checkbox, it is considered a rule match if the end-system does not match the selected value.

Name

Enter a name for a new rule or change the name of an existing rule, if desired.

Rule Enabled

Select this checkbox to enable this rule in the Extreme Access Control configuration.

Description
Enter a description of the rule.

Group Label
If this rule is part of a group, select the group name from the drop-down menu or enter a new group label here.

Authentication Method
Select the authentication method that end-systems must match for this rule.

User Group
Select the user group that the end user must be a member of to match this rule. Click the Edit button

End-System Group
Select the end-system group that the end-system must be a member of to match this rule. Click the Edit button to edit the selections available in this drop-down menu.

Device Type Group
Select the device type group that the end-system must be a member of to match this rule. Click the Edit button to edit the selections available in this drop-down menu.

Location Group
Select the network location (switch and interface) that the end-system must originate from to match this rule.

Time Group
Select a time frame that the connection request must match for this rule.

Profile
Select the Extreme Access Control profile assigned to any end-system matching this rule from the drop-down menu. Select New to add a new profile in the Create New Profile window. Select Manage from the drop-down menu to be redirected to the Engine Group > Switches tab and allows you to make additions or edits to the switches in this engine group.

Click the More button to display two additional actions:

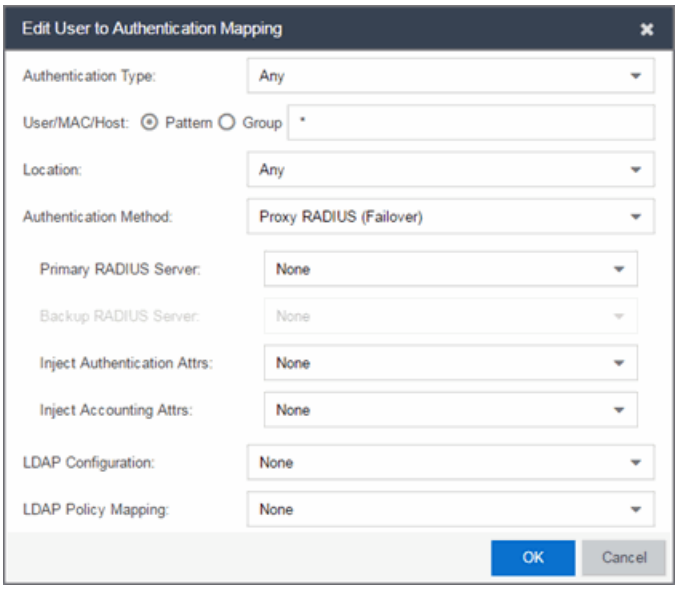
Portal
Select the portal configuration from the drop-down menu to any end-system matching this rule. Select New to add a new portal configuration in the Add New Portal Configuration window. Select Manage from the drop-down menu to be redirected to the Engine Group > Switches tab and allows you to make additions or edits to the switches in this engine group.

Zone

This field only displays if you have displayed the Zone column in the Extreme Access Control Configuration Rules table. Select the end-system zone assigned to any end-system matching this rule. Enter a new zone name if none exists. See End-System Zones for more information.

Add/Edit User to Authentication Mapping

This window lets you add or edit the user to authentication mappings that define your Advanced AAA configurations. You can access this window from the **Add** or **Edit** buttons in the AAA Configuration window.



Authentication Type

Select the authentication type that the end-system must match for this mapping. Note that individual types of 802.1X authentication are not available for selection because at this point in the authentication process, the fully qualified 802.1X authentication type cannot be determined. Select **Any** if you don't want to require an authentication match. Select **802.1X (TTLS-INNER-TUNNEL)** or **802.1X (PEAP-INNER-TUNNEL)** to authenticate via another RADIUS server using an inner tunnel to protect the authentication request.

The Management Login authentication type allows you to set up a mapping specifically for authenticating management login requests, when an administrator logs into a switch's CLI via the console connection, SSH, or Telnet. This allows you to send management requests to a different authentication server than network access requests go to. This authentication type can be used to authenticate users locally, or proxy them to specific RADIUS or LDAP servers. Make sure that the Management Login mapping is

listed above the "Any" mapping in the list of mappings in your Advanced AAA Configuration. In addition, you must set the Auth. Access Type to either "Management Access" or "Any Access" in the Add/Edit Switches window for this authentication type.

User/MAC/Host

Select the **Pattern** radio button and enter the username, MAC address, or hostname that the end-system must match for this mapping. Or, select the **Group** radio button and select a user group or end-system group from the drop-down list. If you enter a MAC address, you can use a colon (:) or a dash (-) as an address delimiter, but not a period (.).

Location

Select the location group that the end-system must match for this mapping, or select "Any" if you don't want to require a location match. You can also add a new location group or edit an existing one.

Authentication Method

Select the authentication method that the end-system must match for this mapping: Proxy RADIUS, LDAP Authentication, or Local Authentication.

Primary RADIUS Server — Use the drop-down menu to select the primary RADIUS server for this mapping to use. You can also add or edit a RADIUS server, or manage your RADIUS servers.

Backup RADIUS Server — Use the drop-down menu to select the backup RADIUS server for this mapping to use. You can also add or edit a RADIUS server, or manage your RADIUS servers.

Inject Authentication Attrs — Use the drop-down menu to select attributes to inject when proxying authentication requests to the back-end RADIUS servers. You can also add or edit a RADIUS attribute configuration, or manage your RADIUS attribute configurations.

Inject Accounting Attrs — Use the drop-down menu to select attributes to inject when proxying accounting requests to the back-end RADIUS servers. You can also add or edit a RADIUS attribute configuration, or manage your RADIUS attribute configurations.

LDAP Authentication — If you select LDAP Authentication, specify the LDAP configuration for this mapping to use.

Local Authentication — If desired, select the option to configure a password for all authentications that match the mapping. This option could be used with MAC authentication where the password is not the MAC address. For example, you may have MAC (PAP) authentication configured for all your switches, with the exception of MAC (MsCHAP) authentication configured for a wireless controller. For the wireless controller, you would add a new AAA mapping with the authentication type set to MAC (MsCHAP), the location set to the wireless controller location group, and the authentication method set to Local Authentication with the password for all authentications set to the static password configured on the wireless controller.

LDAP Configuration

Use the drop-down menu to select the LDAP configuration for the LDAP servers on your network that you want to use for this mapping. You can also add or edit an LDAP configuration, or manage your LDAP configurations. You must specify an LDAP configuration if you have selected LDAP Authentication as your authentication method. However, you might also specify an LDAP configuration if you use Proxy RADIUS to a Microsoft NPS server that is running on a domain controller. The domain controller is also an LDAP server that can do RADIUS requests and LDAP requests for users on that server.

LDAP Policy Mapping

Use the drop-down menu to select the LDAP Policy Mapping for this mapping. If you have selected an LDAP configuration, this option allows you to use a different LDAP policy mapping. This is useful if the LDAP configuration uses user attribute values that overlap with another LDAP configuration. For example, in the case of multiple companies where company A's Sales department uses one policy, but company B's Sales department uses a different policy.

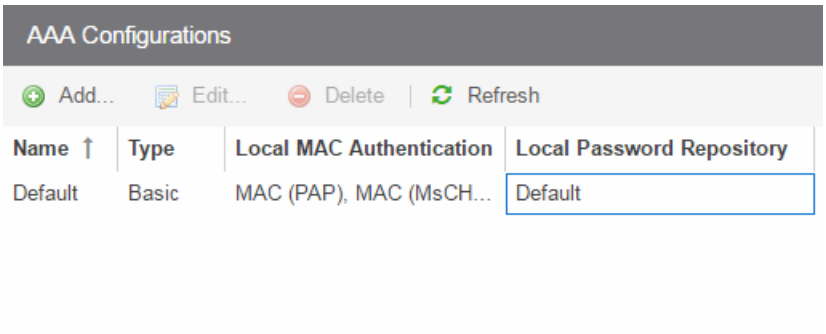
Related Information

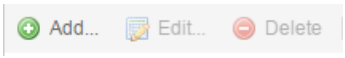
For information on related windows:

AAA Configurations

The AAA Configurations panel provides a list of your AAA configurations and buttons to add, edit, or delete configurations. AAA configurations define the RADIUS and LDAP configurations that provide the authentication and authorization services to your Extreme Access Control engines.

Access the Extreme Access Control Configurations panel in the **Control** > **Extreme Access Control** tab by expanding the **Extreme Access Control Configurations** tree in the left-panel and expanding the AAA Configurations tree. Your configurations are listed within the tree.





Use these buttons to add, edit, or delete the AAA configurations. Click **Add** to add a new configuration to the table. Then select the configuration in the table and click **Edit** to open the Edit AAA Configurations panel. Use the **Delete** button to remove any selected configuration(s).

Name

The name of the AAA Configuration.

Type

Whether the configuration is a Basic configuration or an Advanced configuration.

Local MAC Authentication

Indicates whether MAC authentication requests are handled locally by the Extreme Access Control engine and the type of MAC authentication that will be used.

Local Password Repository

The local password repository specified for this AAA configuration. Extreme Management Center supplies a default repository that can be used to define passwords for administrators and sponsors accessing the Registration administration web page and the sponsor administration web page. The default password is Extreme@pp.

Related Information

- AAA Configurations

AAA Configurations

The AAA Configuration defines the RADIUS and LDAP configurations that provide the authentication and authorization services to your Extreme Access Control engines. A AAA Configuration can be a basic or advanced configuration. Basic AAA Configurations define the authentication and authorization services for all end-systems connecting to your Extreme Access Control engines Advanced AAA configurations allow you to define different authentication and authorization services for different end users based on end-system to authentication server mappings.

This Help topic provides the following information for accessing and configuring the AAA Configuration:

NOTE: Users with a AAA configuration using NTLM authentication to a back-end active directory domain whose passwords expire are prompted via windows to change their domain password.

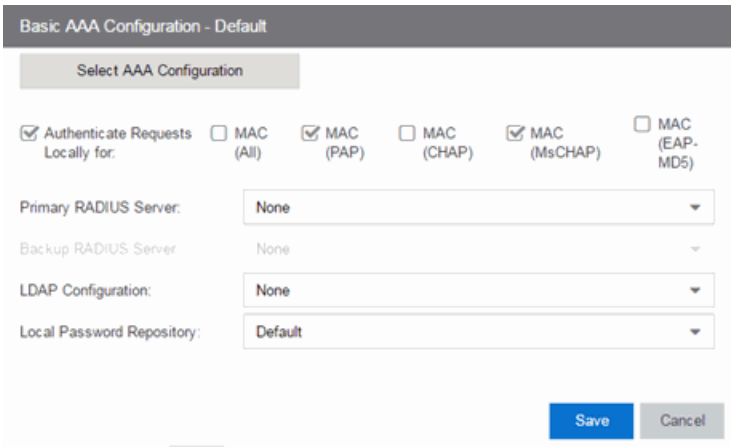
Accessing the AAA Configuration

Use the following steps to edit or change your AAA Configuration.

1. Open the Control tab in Extreme Management Center.
2. Select the Access Control tab.
3. Select AAA Configurations within the left-panel tree. The AAA Configuration is displayed in the right panel.
4. Use the fields in the right panel to edit or modify the configuration. See the sections below for a description of each field and option in the panel.
5. Click Save to save your changes.

Basic AAA Configuration

Basic AAA Configurations define the RADIUS and LDAP configurations for all end-systems connecting to your Extreme Access Control engines.



Authenticate Requests Locally

This option lets you specify that MAC authentication requests are handled locally by the Extreme Access Control engine. Select this option if all MAC authentication requests are to be authorized, regardless of the MAC authentication password (except MAC (EAP-MD5) which requires a password that is the MAC address). The Accept policy is applied to end-systems that are authorized locally.

Select one or more MAC authentication types:

- MAC (All) — includes MAC (PAP), MAC (CHAP), MAC (MsCHAP), and MAC (EAP-MD5) authentication types.
- MAC (PAP) — this is the MAC authentication type used by Extreme Networks wired and wireless devices.
- MAC (CHAP)
- MAC (MsCHAP)
- MAC (EAP-MD5) — this MAC authentication type requires a password, which must be the MAC address.

Primary/Backup RADIUS Servers

If your Extreme Access Control engines are configured to proxy RADIUS requests to a RADIUS server, use these fields to specify the primary and backup RADIUS servers

to use. Use the drop-down menu to select a RADIUS server, add or edit a RADIUS server, or manage your RADIUS servers.

LDAP Configuration

Use this field to specify the LDAP configuration for the LDAP server on your network that you want to use in this AAA configuration. Use the drop-down menu to select an LDAP configuration, add or edit an LDAP configuration, or manage your LDAP configurations.

Local Password Repository

Use this field to specify the local password repository you want for this AAA configuration. Extreme Management Center supplies a default repository to define passwords for administrators and sponsors accessing the Registration administration web page and the sponsor administration web page. The default password is Extreme@pp. Use the drop-down menu to select a repository.

Advanced AAA Configuration

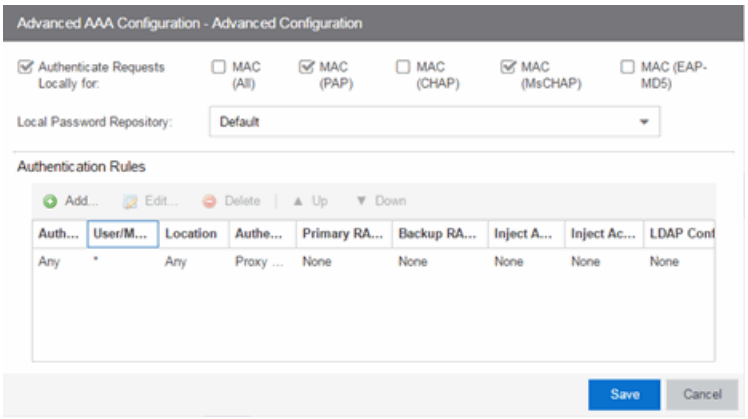
Advanced AAA configurations allow you to define different authentication and authorization services for different end users based on end-system to authentication server mappings. Mappings can be based on:

- authentication type
- username/user group
- MAC address/end-system group
- hostname/hostname group
- location group
- authentication method
- RADIUS user group
- LDAP user group

NOTE: LDAP User Group is only available with an Authentication Type of Registration.

For example, in a higher education setting, you may want faculty members authenticating to one RADIUS server and students authenticating to another. You can also create mappings specifically for authenticating management login requests, when an administrator logs into a switch's CLI via the console connection, SSH, or Telnet.

Mappings are listed in order of precedence from the top down. If an end-system does not match any of the listed mappings, the RADIUS request is dropped. Because of this, you might want to use the "Any" mapping (created automatically when you add a new advanced AAA configuration) as your last mapping in the list.



Authenticate Requests Locally for

This option lets you specify that MAC authentication requests are handled locally by the Extreme Access Control engine. Select this option if all MAC authentication requests are to be authorized, regardless of the MAC authentication password (except MAC (EAP-MD5) which requires a password that is the MAC address). The Accept policy is applied to end-systems authorized locally.

Use the drop-down menu to specify a particular type of MAC authentication:

- MAC (All) - includes MAC (PAP), MAC (CHAP), and MAC (EAP-MD5) authentication types.
- MAC (PAP) - this is the MAC authentication type used by Extreme Networks wired and wireless devices.
- MAC (CHAP)
- MAC (MsCHAP)
- MAC (EAP-MD5) - this MAC authentication type requires a password, and the password must be the MAC address.

Local Password Repository

Use this field to specify the local password repository you want for this AAA configuration. Extreme Management Center supplies a default repository that can be used to define passwords for administrators and sponsors accessing the

Registration administration web page and the sponsor administration web page. The default password is Extreme@pp. Use the drop-down menu to select a repository.

Join AD Domain

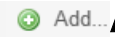
The Join AD Domain selection is only displayed if the AAA configuration has multiple mappings set to LDAP Authentication for an Active Directory domain, with different LDAP configurations specified. Specifying the domain to join is only necessary when multiple Active Directory domains are used but there is not a fully trusted relationship set up between all domains. If there is only a one-way trust set up between some domains you must choose the domain that can authenticate users from all the domains, which is determined by the configuration of a your Active Directory forest. Use the drop-down list to explicitly select which LDAP configuration of the Active Directory domain the Extreme Access Control engine joins in order to authenticate users to all Active Directory domains configured for that engine or select Auto Detect to let the Extreme Access Control engine determine the domain. Auto Detect starts at the first entry set to LDAP Authentication in the table and attempt to join that domain. If it cannot join that domain, it goes to the next entry set to LDAP Authentication and attempt to join that domain, and so on until one succeeds.

User to Authentication Mapping Table

This table lists mappings between groups of users and authentication configurations. The table displays the username to match along with the defined configuration parameters for that mapping. Mappings are listed in order of precedence from the top down. If an end-system does not match any of the listed mappings, the RADIUS request is dropped. Because of this, you might want to use an "Any" mapping as your last mapping in the list. Use the Mappings toolbar buttons to perform actions on the mappings.

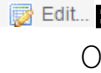
Move Mappings Up/Down

Move mappings up and down in the list to determine mapping precedence. Mappings are listed in order of precedence from the top down.



Add New Mapping

Opens the Add User to Authentication Mapping window where you can define a new mapping.



Edit Mapping

Opens the Edit User to Authentication Mapping window where you can edit the selected mapping.

Delete **Delete Selected Mappings**

Deletes any mappings selected in the table.

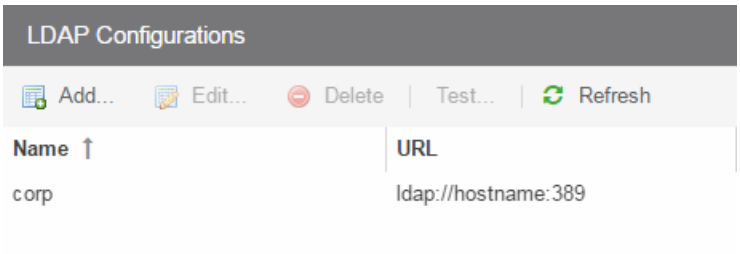
Related Information

For information on related windows:

- Add User to Authentication Mapping Window

Manage LDAP Configurations

This panel lets you view and define the LDAP configurations used in Extreme Management Center. You can access this panel by selecting LDAP Configurations from the left-panel in the Extreme Access Control Configurations > AAA Configurations tree or from AAA Configuration, by clicking the drop-down menu in the LDAP Configuration field. Any changes made are written immediately to the Extreme Management Center database.



LDAP Configurations Table

The name of the configuration and the LDAP server connection URLs specified for that configuration.

Test Configuration Button

Use this button to run a connection test for the selected configuration. The connection to the LDAP server is tested and a report on connection test results is provided. There is also a user search that lets you search on a user entry value and display the attributes associated with the user.

Add Configuration Button

Opens the Add LDAP Configuration window where you can define a new LDAP configuration.

Edit Configuration Button

Opens the Edit LDAP Configuration window where you can edit the selected LDAP configuration.

Delete Configuration Button

Deletes the selected LDAP configuration(s).

Related Information

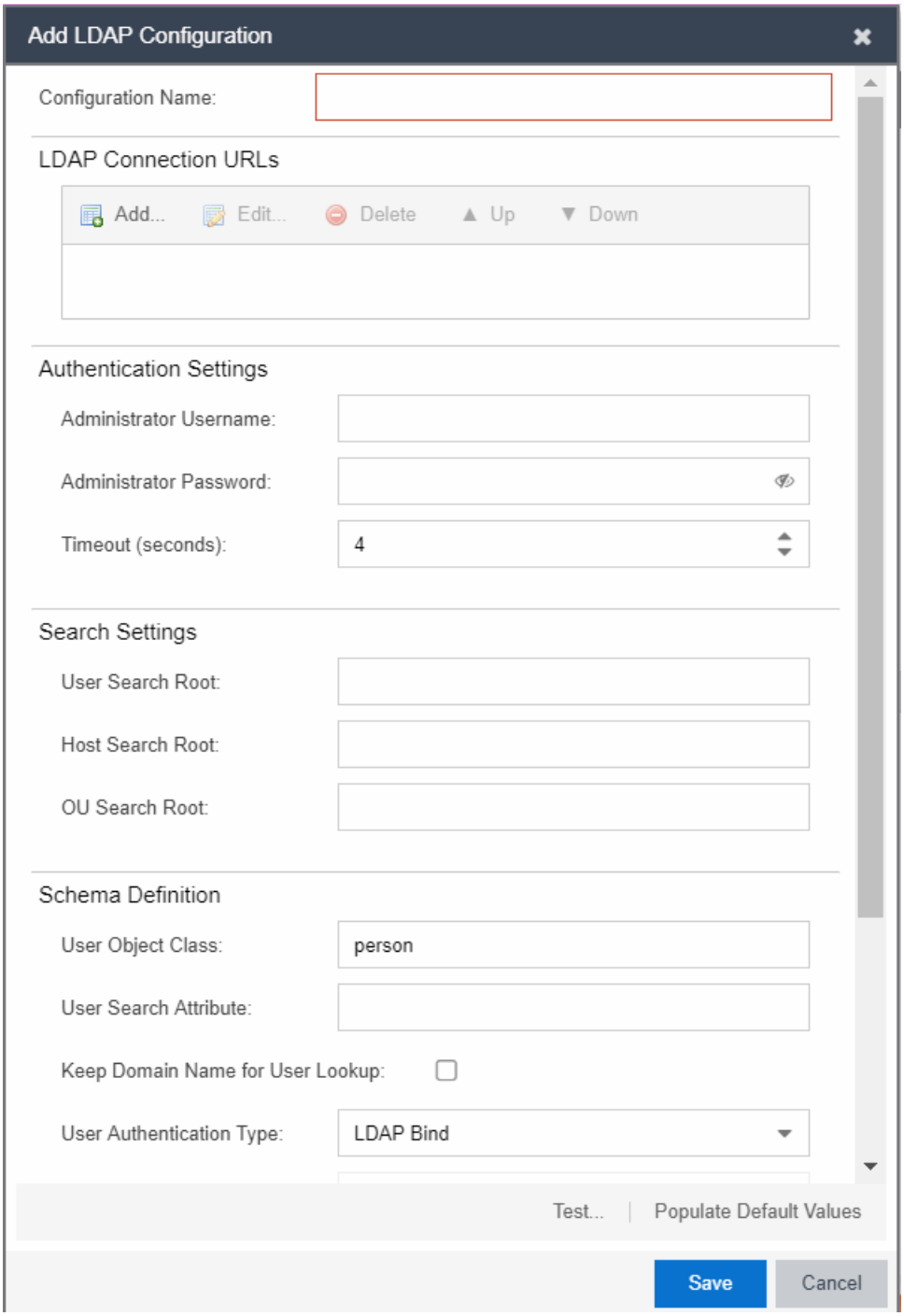
For information on related windows:

- Add/Edit LDAP Configuration window

Add LDAP Configuration Window

Use the Add LDAP Configuration window to configure the LDAP servers on your network. You can access this window from the Users/Groups tab in the Authorization/Device Access tool, or in NAC Manager from the AAA Configuration window, by selecting New from the drop-down menu in the LDAP Configuration field. You can also access this window from the Manage LDAP Configurations window. Any changes made in this window are written immediately to the Extreme Management Center database.

NOTE: If you are using LDAPS, your Extreme Management Center/Extreme Access Control environment must be configured to accept the new LDAPS server certificate. For information, see Server Certificate Trust Mode in the Secure Communications Help topic.



Configuration Name

Enter a name for the LDAP configuration.

LDAP Connection URLs

Use this table to add, edit, or delete connection URLs for the LDAP server and any backup servers you have configured. (The backup servers are redundant servers containing the same directory information.) Use the Up and Down arrows to arrange the order that the URLs are listed.

The format for the connection URL is `ldap://host:port` where host equals hostname or IP address, and the default port is 389. For example, `ldap://10.20.30.40:389`. If you are using a secure connection, the format is `ldaps://host:port` and the default port is 636. For example, `ldaps://10.20.30.40:636`. If you are using LDAPS, your Extreme Management Center/Extreme Access Control environment must be configured to accept the new LDAPS server certificate. For information, see Server Certificate Trust Mode in the Secure Communications Help topic.

If you are creating an LDAP configuration for Novell eDirectory, be aware that the eDirectory may require that the universal password lookup be done using LDAPS. If you configure the URL for LDAP only, the lookup may fail.

Authentication Settings

Enter the administrator username and password that will be used to connect to the LDAP server to make queries. The credentials only need to provide read access to the LDAP server. The timeout field lets you specify a timeout value in seconds for the LDAP server connection.

Search Settings

For the three fields, enter the root node of the LDAP server. To improve search performance, you can specify a sub tree node to confine the search to a specific section of the directory. The search root format should be a DN (Distinguished Name).

Schema Definition

Provide information that describes how entries are organized in the LDAP server.

Schema Definition fields:

- User Object Class - enter the name of the class used for users.
- User Search Attribute - enter the name of the attribute in the user object class that contains the user's login ID.
- Keep Domain Name for User Lookup - If selected, this option will allow the full username to be used when looking up the user in LDAP. For example, you

should select this option when using the User Search Attribute: userPrincipalName.

If the option is not selected, the domain name will be stripped off the username prior to performing the lookup. For example, you should deselect this option when using the User Search Attribute: sAMAccountName. Two examples of the domain name being stripped off would be:
user@domain.com -> user
DOMAIN\user -> user

- User Authentication Type - Specify how the user is authenticated. There are 4 options:
    - LDAP Bind – This is the easiest option to configure, but only works with a plain text password. It is useful for authentication from the captive portal but does not work with most 802.1x authentication types.
    - NTLM Auth – This option is only useful when the backend LDAP server is really a Microsoft Active Directory server. This is an extension to LDAP bind that uses ntlm_auth to verify the NT hash challenge responses from a client in MsCHAP, MsCHAPV2, and PEAP requests.
    - NT Hash Password Lookup – If the LDAP server has the user's password stored as an NT hash that is readable by another system, you can have Extreme Access Control read the hash from the LDAP server to verify the hashes within an MsCHAP, MsCHAPV2, and PEAP request.
    - Plain Text Password Lookup – If the LDAP server has the user's password stored unencrypted and that attribute is accessible to be read via an LDAP request, then this option reads the user's password from the server at the time of authentication. This option can be used with any authentication type that requires a password.
- User Password Attribute - This is the name of the password used with the NT Hash Password Lookup and Plain Text Password Lookup listed above.
- Host Object Class - enter the name of the class used for hostname.

- Host Search Attribute - enter the name of the attribute in the host object class that contains the hostname.
- Use Fully Qualified Domain Name checkbox - use this checkbox to specify if you want to use the Fully Qualified Domain Name (FQDN) or just hostname without domain.
- OU Object Classes - the names of the classes used for organizational units.

Test Button

The connection to the LDAP server is tested and a report on connection test results is provided. There is also a user/host search that lets you search on a user entry or host entry value and display the attributes associated with those values.

Populate Default Values Button

Select from the defaults available from the menu:

- Active Directory: User Defaults - Settings that allow user authentication when Extreme Access Control is set to proxy to LDAP and the server is an Active Directory machine.
- Active Directory: Machine Defaults - Settings that allow machine authentication when Extreme Access Control is set to proxy to LDAP and the server is an Active Directory machine.
- OpenLDAP Defaults - Settings that allow Extreme Access Control to verify the user's password via an OpenLDAP server. See the NAC Manager How to Configure PEAP Authentication via OpenLDAP Help topic for information.
- Novell eDirectory Defaults - Settings that allow Extreme Access Control to read the universal password from Novell eDirectory. You must configure eDirectory to allow that password to be read. See the NAC Manager How to Configure PEAP Authentication via eDirectory Help topic for information.

Related Information

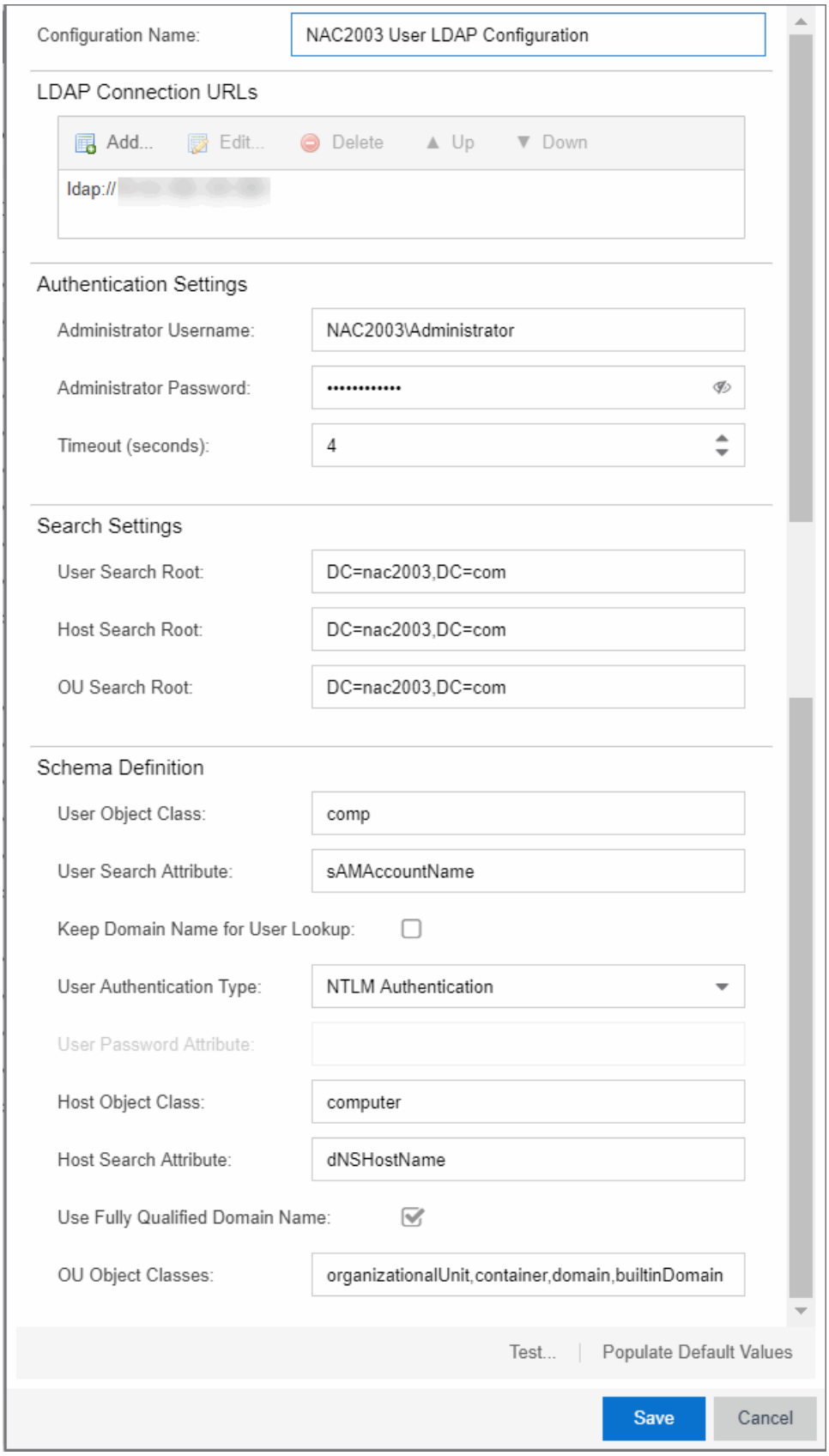
For information on related windows:

- Manage LDAP Configurations Window

Edit LDAP Configuration Window

Use the Edit LDAP Configuration window to configure the LDAP servers on your network. You can access this window from the Users tab in the Authorization/Device Access tool, or in NAC Manager from the AAA Configuration window, by selecting an LDAP configuration from the drop-down menu in the LDAP Configuration field. You can also access this window from the Manage LDAP Configurations window. Any changes made in this window are written immediately to the Extreme Management Center database.

NOTE: If you are using LDAPS, your Extreme Management Center/Extreme Access Control environment must be configured to accept the new LDAPS server certificate. For information, see Server Certificate Trust Mode in the Secure Communications Help topic.


Configuration Name:
NAC2003 User LDAP Configuration
LDAP Connection URLs
Add...
Edit...
Delete
Up
Down
ldap://
Authentication Settings
Administrator Username:
NAC2003\Administrator
Administrator Password:
Timeout (seconds):
4
Search Settings
User Search Root:
DC=nac2003,DC=com
Host Search Root:
DC=nac2003,DC=com
OU Search Root:
DC=nac2003,DC=com
Schema Definition
User Object Class:
comp
User Search Attribute:
sAMAccountName
Keep Domain Name for User Lookup:
User Authentication Type:
NTLM Authentication
User Password Attribute:
Host Object Class:
computer
Host Search Attribute:
dNSHostName
Use Fully Qualified Domain Name:
OU Object Classes:
organizationalUnit,container,domain,builtinDomain
Test...
Populate Default Values
Save
Cancel

Configuration Name

The name for the LDAP configuration you defined.

LDAP Connection URLs

Use this table to add, edit, or delete connection URLs for the LDAP server and any backup servers you have configured. (The backup servers are redundant servers containing the same directory information.) Use the Up and Down arrows to arrange the order that the URLs are listed.

The format for the connection URL is `ldap://host:port` where host equals hostname or IP address, and the default port is 389. For example, `ldap://10.20.30.40:389`. If you are using a secure connection, the format is `ldaps://host:port` and the default port is 636. For example, `ldaps://10.20.30.40:636`. If you are using LDAPS, your Extreme Management Center/Extreme Access Control environment must be configured to accept the new LDAPS server certificate. For information, see Server Certificate Trust Mode in the Secure Communications Help topic.

If you are creating an LDAP configuration for Novell eDirectory, be aware that the eDirectory may require that the universal password lookup be done using LDAPS. If you configure the URL for LDAP only, the lookup may fail.

Authentication Settings

Enter the administrator username and password that will be used to connect to the LDAP server to make queries. The credentials only need to provide read access to the LDAP server. The timeout field lets you specify a timeout value in seconds for the LDAP server connection.

Search Settings

For the three fields, enter the root node of the LDAP server. To improve search performance, you can specify a sub tree node to confine the search to a specific section of the directory. The search root format should be a DN (Distinguished Name).

Schema Definition

Provide information that describes how entries are organized in the LDAP server.

Schema Definition fields:

- User Object Class - enter the name of the class used for users.

- User Search Attribute - enter the name of the attribute in the user object class that contains the user's login ID.
- Keep Domain Name for User Lookup - If selected, this option will allow the full username to be used when looking up the user in LDAP. For example, you should select this option when using the User Search Attribute: userPrincipalName.

  If the option is not selected, the domain name will be stripped off the username prior to performing the lookup. For example, you should deselect this option when using the User Search Attribute: sAMAccountName. Two examples of the domain name being stripped off would be:
  user@domain.com -> user
  DOMAIN\user -> user
- User Authentication Type - Specify how the user is authenticated. There are 4 options:
  - LDAP Bind – This is the easiest option to configure, but only works with a plain text password. It is useful for authentication from the captive portal but does not work with most 802.1x authentication types.
  - NTLM Auth – This option is only useful when the backend LDAP server is really a Microsoft Active Directory server. This is an extension to LDAP bind that uses ntlm_auth to verify the NT hash challenge responses from a client in MsCHAP, MsCHAPV2, and PEAP requests.
  - NT Hash Password Lookup – If the LDAP server has the user's password stored as an NT hash that is readable by another system, you can have Extreme Access Control read the hash from the LDAP server to verify the hashes within an MsCHAP, MsCHAPV2, and PEAP request.
  - Plain Text Password Lookup – If the LDAP server has the user's password stored unencrypted and that attribute is accessible to be read via an LDAP request, then this option reads the user's password from the server at the time of authentication. This option can be used with any authentication type that requires a password.

- User Password Attribute - This is the name of the password used with the NT Hash Password Lookup and Plain Text Password Lookup listed above.
- Host Object Class - enter the name of the class used for hostname.
- Host Search Attribute - enter the name of the attribute in the host object class that contains the hostname.
- Use Fully Qualified Domain Name checkbox - use this checkbox to specify if you want to use the Fully Qualified Domain Name (FQDN) or just hostname without domain.
- OU Object Classes - the names of the classes used for organizational units.

Test Button

The connection to the LDAP server is tested and a report on connection test results is provided. There is also a user/host search that lets you search on a user entry or host entry value and display the attributes associated with those values.

Populate Default Values Button

Select from the defaults available from the drop-down menu:

- Active Directory: User Defaults - Settings that allow user authentication when Extreme Access Control is set to proxy to LDAP and the server is an Active Directory machine.
- Active Directory: Machine Defaults - Settings that allow machine authentication when Extreme Access Control is set to proxy to LDAP and the server is an Active Directory machine.
- OpenLDAP Defaults - Settings that allow Extreme Access Control to verify the user's password via an OpenLDAP server. See the NAC Manager How to Configure PEAP Authentication via OpenLDAP Help topic for information.
- Novell eDirectory Defaults - Settings that allow Extreme Access Control to read the universal password from Novell eDirectory. You must configure eDirectory to allow that password to be read. See the NAC Manager How to Configure PEAP Authentication via eDirectory Help topic for information.

Related Information

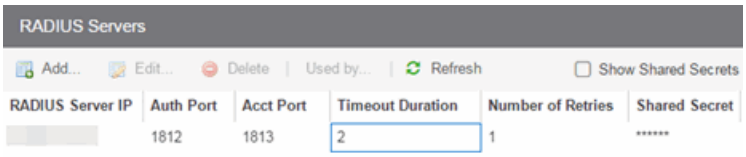
For information on related windows:

- Manage LDAP Configurations Window

Manage RADIUS Servers

This panel lets you view and define the RADIUS servers used in Extreme Management Center. RADIUS servers can be used in Extreme Management Center server authentication configurations and in Extreme Access Control AAA configurations.

You can access this panel by selecting RADIUS Servers from the Extreme Access Control Configurations > AAA Configurations > RADIUS Servers in the left-panel tree, or from the Configure Device window or AAA Configuration window. Any changes made are written immediately to the Extreme Management Center database.



RADIUS Server IP

The IP address of the RADIUS server.

Auth Port

The UDP port number (1-65535) on the RADIUS server to which the Extreme Management Center server or Extreme Access Control engine sends authentication requests; 1812 is the default port number.

Acct Port

The UDP port number (1-65535) on the RADIUS server to which the Extreme Access Control engine sends accounting requests; 1813 is the default port number.

Timeout Duration

The amount of time, in seconds, the Extreme Management Center server or Extreme Access Control engine waits for the RADIUS server to respond to an authentication or accounting request. Valid values are 2-60 seconds.

Number of Retries

The number of times the Extreme Management Center server or Extreme Access Control engine resends an authentication or accounting request if the RADIUS server does not respond. Valid values are 0-20.

Shared Secret

The shared secret used to encrypt and decrypt communication between the Extreme Management Center server or Extreme Access Control engine and the RADIUS server. In Extreme Access Control, this is also the shared secret used between the switch and the RADIUS server if the Extreme Access Control engine is bypassed or if you configured the Management RADIUS Server options when you added the switch.

Show Shared Secrets

When checked, the shared secrets are shown in text. When unchecked, the shared secrets are shown as a string of asterisks.

Used By Button

This button is only available when the panel is launched from Extreme Access Control. Opens the RADIUS Server(s) Used By window which shows where the selected servers are in use by AAA configurations.

Add Button

Opens the Add RADIUS Server window where you can define a new RADIUS server.

Edit Button

Opens the Edit RADIUS Server window where you can edit the values for the selected RADIUS server.

Delete Button

Deletes the selected RADIUS server. You cannot delete servers currently in use.

Related Information

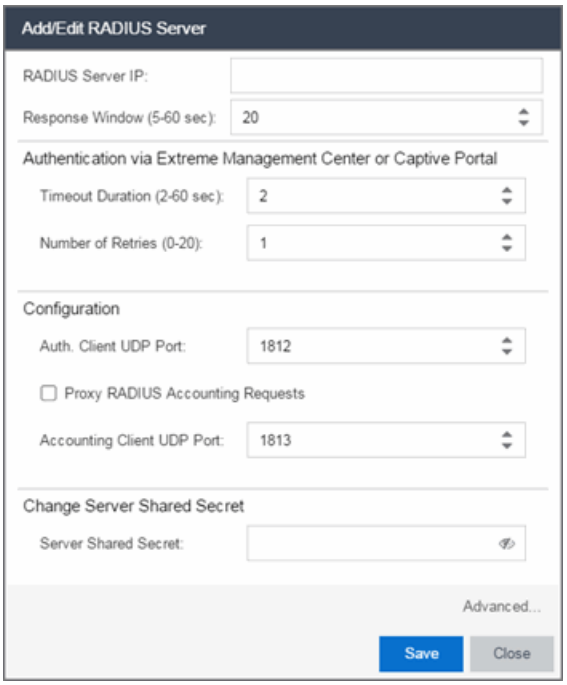
For information on related windows:

- Add/Edit RADIUS Server Window

Add/Edit RADIUS Server

Use the Add/Edit RADIUS Server window to configure the RADIUS servers used in your Extreme Management Center applications. RADIUS servers can be used in Extreme Management Center server authentication configurations and in Extreme Access Control AAA configurations.

You can access this window from the Manage RADIUS Servers window. Any changes made in this window are written immediately to the Extreme Management Center database.



RADIUS Server IP

The IP address of the RADIUS server.

Response Window

This setting is used by Extreme Access Control when proxying a RADIUS request to a backend RADIUS server. Extreme Access Control keeps a status on all backend RADIUS servers instead of going to the primary RADIUS server for every request. If a RADIUS server does not respond in the amount of time specified here, that server is marked as down until it can be verified as being up. See the Health Check section of the Advanced RADIUS Server Configuration window for information on how Extreme Access Control determines the health of a RADIUS server.

Timeout Duration

The amount of time in seconds the Extreme Management Center server or Extreme Access Control waits for the RADIUS server to respond to an authentication or accounting request. Valid values are 2-60 seconds. This setting is only used for logging into Extreme Management Center via RADIUS or logging into the Extreme Access Control Captive Portal via RADIUS.

NOTE: The Extreme Access Control engine times out a RADIUS server if it takes more than "(retries +1) * timeout" or 20 seconds, whichever is greater, for the server to respond. For example, if the number of retries is set to 1 and the timeout duration is set to 2 (the default values), then the engine times out a RADIUS server if it takes longer than 20 seconds to respond, because that is the greater value (20 to 4). If the RADIUS server times out, then Extreme Access Control fails over to the backup RADIUS server until it determines that the primary server is back up. At that point, Extreme Access Control starts proxying RADIUS requests to the primary server again.

Number of Retries

The number of times the Extreme Management Center server or Extreme Access Control engine resends an authentication or accounting request if the RADIUS server does not respond. Valid values are 0-20. This setting is only used for logging into Extreme Management Center via RADIUS or logging into the Extreme Access Control Captive Portal via RADIUS.

Auth. Client UDP Port

The UDP port number (1-65535) on the RADIUS server that the Extreme Management Center server or Extreme Access Control engine sends authentication requests to; 1812 is the default port number.

Proxy RADIUS Accounting Requests

Select this checkbox to enable the Extreme Access Control engine to proxy RADIUS accounting requests to the RADIUS server. This option must be enabled if you are doing RADIUS accounting in an Extreme Access Control environment where the primary RADIUS server is being used for redundancy in a single Extreme Access Control engine configuration (Basic AAA configuration only).

Accounting Client UDP Port

The UDP port number (1-65535) on the RADIUS server that the Extreme Access Control engine sends accounting requests to; 1813 is the default port number.

Server Shared Secret

The shared secret is a string of characters used to encrypt and decrypt communication between the Extreme Management Center server or Extreme Access

Control and the RADIUS server. In Extreme Management Center, this is also the shared secret used between the switch and the RADIUS server if the Extreme Access Control engine is bypassed or if you configured the Management RADIUS Server options when you added the switch. The shared secret must be at least 6 characters long; 16 characters is recommended. Dashes are allowed in the string, but spaces are not.

Verify Shared Secret

Re-enter the Server Shared Secret you entered above.

Show Shared Secret

Displays the secret in the Server Shared Secret and Verify Shared Secret fields.

Advanced Button

Use this button to open the Advanced RADIUS Server Configuration window, where you can configure advanced RADIUS settings used by Extreme Access Control when proxying access requests to a backend RADIUS server.

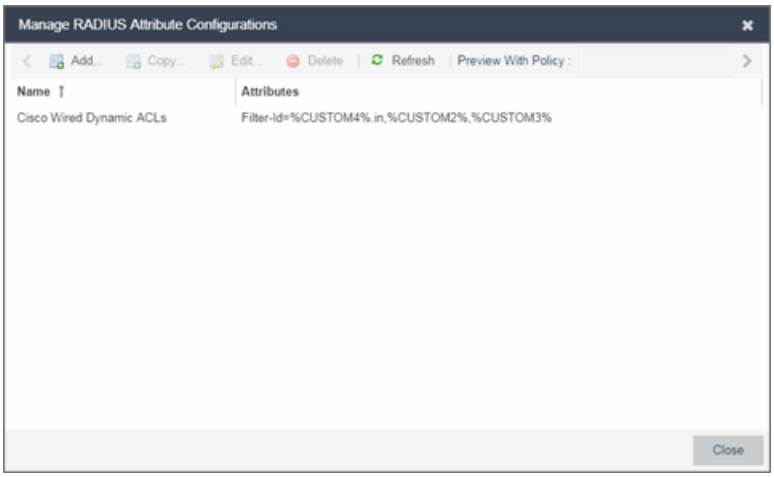
Related Information

For information on related windows:

- Manage RADIUS Servers Window
- Advanced RADIUS Server Configuration Window

Manage RADIUS Attribute Configurations Window

Use this window to view attributes injected when authentication or accounting requests are proxied to a back-end RADIUS server. Attributes you inject provide additional information about the users on your network. You can access the RADIUS Attribute Configurations window from the Add/Edit User To Authentication Mapping window.



Preview With Policy

Presents a preview of the attributes defined for selected attribute configuration.

Name

The names of the available attribute configurations. You cannot edit the name of a configuration.

Add

Select the Add button to open the Create New RADIUS Attribute Settings window, which allows you to create a new attribute configuration.

Edit

Select the Edit button to open the Edit RADIUS Attribute Settings window, which allows you to edit an existing attribute configuration.

Delete

Select an attribute and click the Delete button to remove an existing attribute configuration.

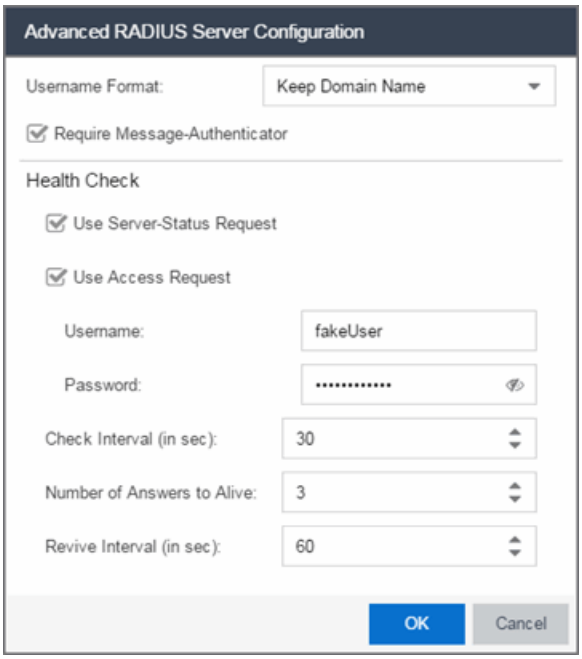
Related Information

For information on related windows:

- Add/Edit User To Authentication Mapping Window
- Create New RADIUS Attribute Settings Window

Advanced RADIUS Server Configuration

Use this window to configure advanced RADIUS settings used by Extreme Management Center when proxying authentication requests to a backend RADIUS server. You can access this window by clicking the **Advanced** button at the bottom of the Add/Edit RADIUS Server window.



Username Format

This field is used by Extreme Management Center to determine what format to use for the username when proxying a request to the backend RADIUS server. There are two options:

- Strip Domain Name *(default)* - This option removes a domain name from the username when proxying the request. Select this option unless the backend RADIUS server requires the domain name to be included.
- Keep Domain Name - This option keeps any domain names on the username when proxying the request to the backend RADIUS server. If the backend RADIUS server is a Microsoft IAS or NPS server, this option could cause the RADIUS server to time out if a guest comes onto the network with another domain. In that scenario, if the request is proxied to the backend RADIUS

server with the domain name, the server does not respond to the request because it is from an unknown domain. Therefore, if you use this option with a Microsoft IAS or NPS server, use an advanced AAA configuration so that only requests for the desired domain(s) are sent to the backend RADIUS server, and all unknown domains are processed locally so they are rejected.

Require Message-Authenticator

Enable this checkbox if the backend RADIUS server requires a message authenticator to be part of the request. If enabled, Extreme Management Center adds the message authenticator when proxying the request.

Health Check Section

Extreme Management Center uses the options in this section to determine how to check the health of a backend RADIUS server, if that server stops responding to requests.

Use Server-Status Request

When selected, Extreme Management Center attempts to use Server-Status RADIUS packets as defined by RFC 5997, to determine if the backend RADIUS server is up.

Use Access Request

When selected, Extreme Management Center attempts to use an access request message to determine if the RADIUS server is up. The request is made using the username and password specified below. The username and password do not need to be valid, as Extreme Management Center is looking for a response and a reject also works. The username/password fields are provided in case you want to prevent rejects from being logged in the backend RADIUS server.

Check Interval

The interval to wait between checks to see if the RADIUS server is up. This is only applicable if the Server-Status request or Access request methods are used.

Number of Answers to Alive

The number of times the RADIUS server must respond before it is marked as alive. This is only applicable if the Server-Status request or Access request methods are used.

Revive Interval

If Server-Status requests and Access requests are not allowed or supported by the RADIUS server, then Extreme Management Center waits the amount of time specified here before allowing requests to go to a backend RADIUS server, if it stops

responding. Only use this if there is no other way to detect the health of the backend RADIUS server.

Related Information

For information on related windows:

- Manage RADIUS Servers Window
- Add/Edit RADIUS Server Window

Policy Mapping Configuration

In your Extreme Access Control profiles, each access policy (Accept, Quarantine, Failsafe, and Assessment) is associated to a *policy mapping* that defines exactly how end-system traffic is handled on the network. Each mapping specifies a policy role (created in the **Policy** tab) and/or any additional RADIUS attributes included as part of a RADIUS response to a switch.

The RADIUS attributes required by a switch are specified in the Gateway RADIUS Attributes to Send field configured in the Edit Switch window. The actual switch RADIUS attribute values (Login-LAT-Port, Custom 1, etc.) are defined within each policy mapping configured in this window. Each policy mapping is associated with the access policy selected in your Extreme Access Control profiles.

When an end-system authenticates to the network, the Extreme Access Control profile is applied and the appropriate RADIUS response attributes are extracted from the mapping based on the switch the authentication request originated from. The attributes are returned to the switch in the RADIUS Access-Accept response.

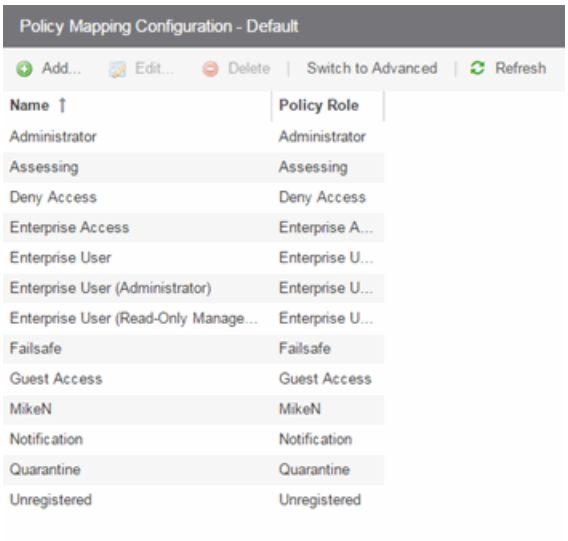
For more information on configuring policy mappings, see How to Set Up Access Policies and Policy Mappings. For a description of each Extreme Access Control access policy, and some guidelines for creating corresponding policy roles in the **Policy** tab, see the section on Access Policies in the Concepts file.

To access this window, click on the **Policy Mappings** left-panel option in the **Extreme Access Control Configurations** > **Access Control** left-panel menu.

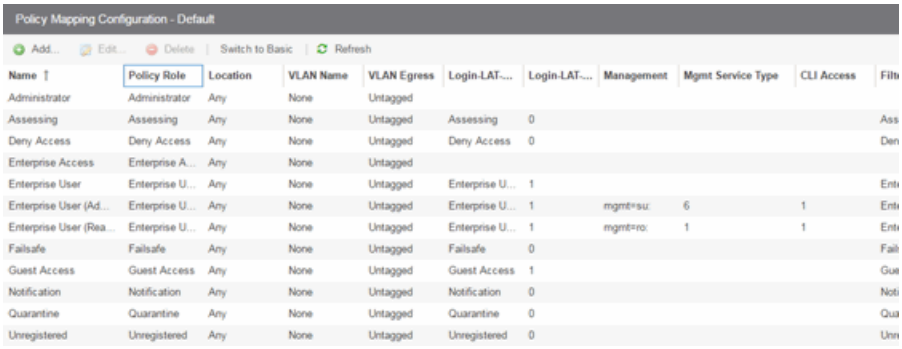
The columns displayed in this window vary depending on whether you are using a Basic or Advanced policy mapping configuration. For a definition of each column, see below.

Basic AAA Configuration

Basic AAA Configurations define the RADIUS and LDAP configurations for all end-systems connecting to your Extreme Access Control engines.



Advanced Policy Mapping Configuration



Column Definitions

Name

The policy mapping name.

Policy Role

The policy role assigned to this mapping. All policy roles used in your mappings must be part of your Extreme Access Control (Extreme Access Control) Controller policy configuration and/or defined in the **Policy** tab and enforced to the policy-enabled switches in your network.

Location

Policy mapping locations allow authentication requests that match the same Extreme Access Control rule and corresponding Extreme Access Control profile to be authorized to different accept attributes (policy/VLAN/Custom Attribute) based

on the location the request originated from. For example, in the Policy Mapping Configuration screenshot above, the Administration policy mapping has five entries, with each entry assigning a different VLAN (for RFC 3580-enabled switches) for authentication requests matching the specified location. Requests originating from the 1st floor South location will be authorized to VLAN 100, and requests originating from the 2nd floor North location (matching the same Extreme Access Control rule) is authorized to VLAN 220. Using locations in this manner lets you authorize end-systems to different access criteria using a single Extreme Access Control rule, whereas the alternative would be to create multiple location-based Extreme Access Control rules each with an Extreme Access Control Profile that corresponds with the desired access value.

When policy mapping locations are used in this manner, it is important to include a catch-all policy mapping (the fifth Administration mapping in the example above) that has a location of "any" and sets the access behavior for an authorization originating from any other location. The access behavior could be a policy/VLAN/Custom Attribute that grants some form of restricted access, or denies access altogether. If a catch-all mapping is not included, a warning message may appear on enforce indicating that there is no catch-all mapping configured, and authorizations that match the policy but do not originate from a defined location, may result in errors or unpredictable behavior.

VLAN Name

If you have RFC 3580-enabled switches in your network, this column displays the VLAN name assigned to this mapping.

VLAN Egress

If you have RFC 3580-enabled switches in your network, this column displays the VLAN ID assigned to this mapping.

Filter

This value is only displayed in Basic mode if ExtremeWireless Controllers have been added to Extreme Management Center. The Filter column typically maps to the Filter-Id RADIUS attribute. This value applies to ExtremeWireless Controllers and other switches that support the Filter-Id attribute.

Login-LAT-Group

If your network devices require a Login-LAT-Group, it displays here.

Login-LAT-Port

If you have ExtremeWireless Controllers on your network, the Login-LAT-Port is an attribute returned in the default RADIUS response. The Login-LAT-Port value is used by the controller to determine whether the authentication is fully authorized. A value of "1" indicates the authentication is authorized, where a value of "0" indicates that authorization is not complete. The value of "0" is used by the controller to determine that additional authentication is required and is a signal for the controller to engage its external captive portal and use HTTP redirection to force HTTP traffic from the end-system to the defined Extreme Access Control engine. This is used in conjunction with the Registration and Assessment features of Extreme Access Control.

Management

The authorization attribute returned for successful administrative access authentication requests that originate from network equipment configured to use RADIUS as the authentication mechanism for remote management of switches, routers, VPN concentrators, etc. Examples of management values for EOS devices are: "mgmt=su:", "mgmt=rw:", or "mgmt=ro:". The management attribute determines the level of access the administrator will have when authorized to access the device: superuser, read/write, or read-only.

Custom

Some network devices require additional RADIUS response attributes in order to provide authorization or define additional parameters for the authenticated session. These additional attributes can be defined in the five available Custom option fields.

Attribute List 1-3

The Attribute List fields display additional RADIUS response attributes in a single mapping. For example, you can use each field to provide a complete ACL for a different third-party vendor.

Related Information

For information on related windows:

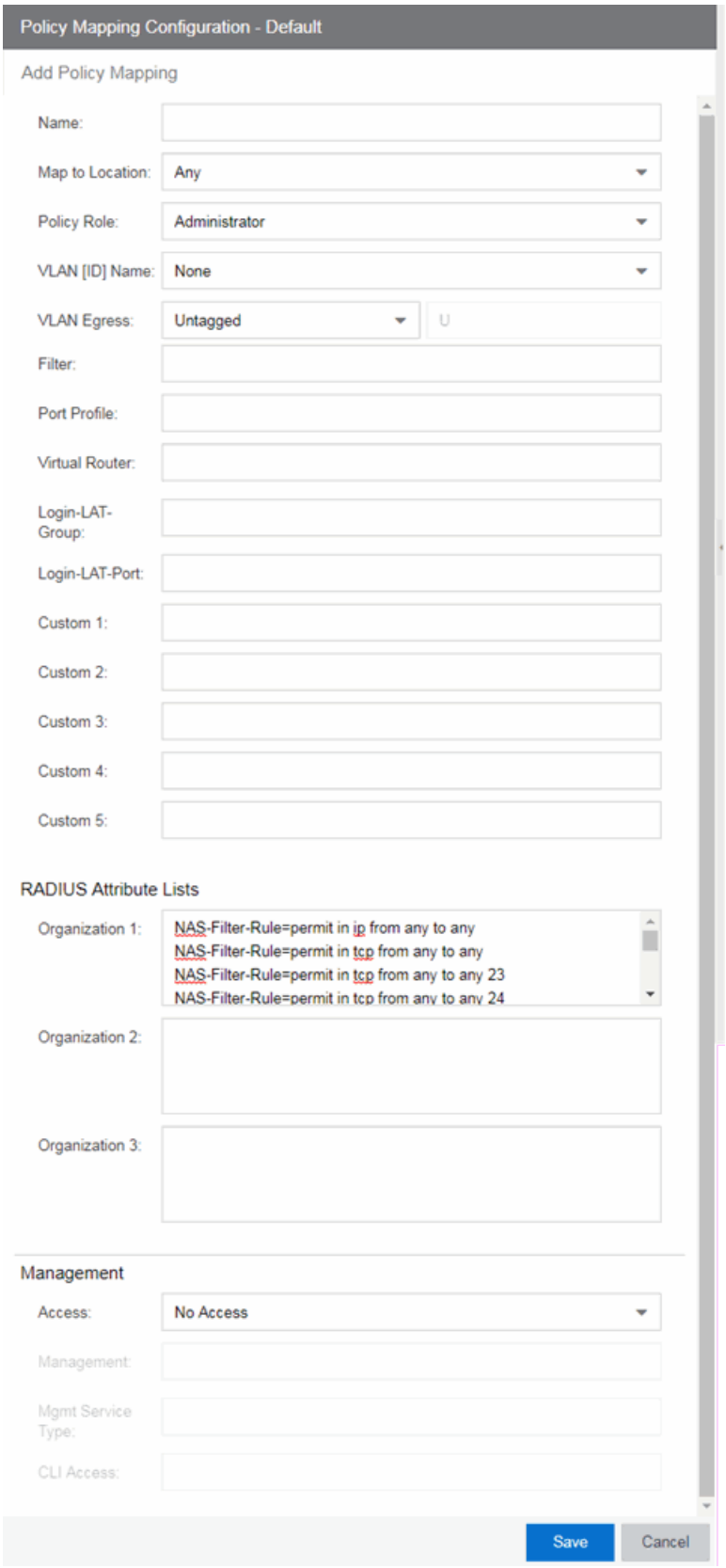
- Add/Edit Policy Mapping Window
- How to Set Up Access Policies and Policy Mappings

Add/Edit Policy Mapping

Use this window to add a new policy mapping or edit an existing policy mapping. A policy mapping specifies a policy role (created on the **Policy** tab) and/or any additional RADIUS attributes included as part of a RADIUS response to a switch (as defined in the Gateway RADIUS Attributes to Send field configured in the Edit Switch window). For additional information about configuring policy mappings, see How to Set Up Access Policies and Policy Mappings.

Access this window by clicking the **Add** or **Edit** toolbar buttons in the Edit Policy Mapping Configuration window.

The fields in this window vary depending on whether you are using a basic or advanced policy mapping configuration. For a definition of each field, see below.


Policy Mapping Configuration - Default
Add Policy Mapping
Name:
Map to Location:
Any
Policy Role:
Administrator
VLAN [ID] Name:
None
VLAN Egress:
Untagged
U
Filter:
Port Profile:
Virtual Router:
Login-LAT-Group:
Login-LAT-Port:
Custom 1:
Custom 2:
Custom 3:
Custom 4:
Custom 5:
RADIUS Attribute Lists
Organization 1:
NAS-Filter-Rule=permit in ip from any to any
NAS-Filter-Rule=permit in tcp from any to any
NAS-Filter-Rule=permit in tcp from any to any 23
NAS-Filter-Rule=permit in tcp from any to any 24
Organization 2:
Organization 3:
Management
Access:
No Access
Management:
Mgmt Service Type:
CLI Access:
Save
Cancel

Name

Enter a name for the policy mapping.

Map to Location

Allows you to specify a certain location for the mapping. You should first configure your locations using the Location Group (Control tab > Extreme Access Control > Extreme Access Control Configurations > Group Editor > Location Groups) or you can click the Edit button to the right of the field to add a location group to the list. For more information on using the Location option in Policy Mappings, see the Edit Policy Mapping Configuration Window Help topic.

Policy Role

Use the drop-down menu to select a policy role, or enter a policy role in the field. The drop-down menu displays any policy roles you have created and saved in the Policy tab and/or all the policy roles contained in the Extreme Access Control Controller policy configuration. Roles from all your policy domains are listed; if there are duplicate names, only one is listed. The list is not case sensitive, so "Enterprise User" and "enterprise user" are considered duplicate policy names. All policy roles used in your mappings must be part of your Extreme Access Control) Controller policy configuration and/or defined in Policy tab and enforced to the EOS policy-enabled switches in your network.

NOTE: Entering a new policy role does not create a new role in the Policy tab.

VLAN [ID] Name

Use the drop-down menu to select the appropriate VLAN associated with the policy. This list displays any VLANs defined in Extreme Management Center. Click the configuration menu button to the right of the field to add a VLAN to the list. VLANs you add remain in the list only as long as they are used in a mapping and they are not added to the Extreme Management Center database.

VLAN Egress

Use the drop-down menu to select the appropriate VLAN the egress forwarding state: Tagged (frames are forwarded as tagged), Untagged (frames are forwarded as untagged), Same as Ingress (frames are forwarded as specified by the VLAN Ingress), or User Defined (you define how frames are forwarded).

Filter

If your network devices require a custom Filter-Id, enter it here. The Filter column typically maps to the Filter-Id RADIUS attribute. This value applies to ExtremeWireless Controllers and other switches that support the Filter-Id attribute.

Port Profile

For ExtremeXOS devices on which legacy firmware is installed, this field indicates the profile used by Extreme Policy.

Login-LAT-Group

If your network devices require a Login-LAT-Group, enter it here.

Login-LAT-Port

If you have ExtremeWireless Controllers on your network, the Login-LAT-Port is an attribute returned in the default RADIUS response. The Login-LAT-Port value is used by the controller to determine whether the authentication is fully authorized. A value of "1" indicates the authentication is authorized, where a value of "0" indicates that authorization is not complete. The value of "0" is used by the controller to determine that additional authentication is required and is a signal for the controller to engage its external captive portal and use HTTP redirection to force HTTP traffic from the end-system to the defined Extreme Access Control engine. This is used in conjunction with the Registration and Assessment features of Extreme Access Control.

Custom

If your network devices require additional RADIUS response attributes in order to provide authorization or define additional parameters for the authenticated session, you can define them in the five available Custom option fields.

Organization 1-3

Enter additional RADIUS response attributes in a single mapping in the Organization fields. For example, you can use each field to provide a complete ACL for a different third-party vendor.

Management

Enter a management attribute used to authenticate requests for administrative access to the selected switches, for example, "mgmt=su:", "mgmt=rw:", or "mgmt=ro:". The management attribute determines the level of access the administrator will have to the switch: superuser, read/write, or read-only. Be sure to include the final colon (":") in the attribute, or the management access will not work.

Related Information

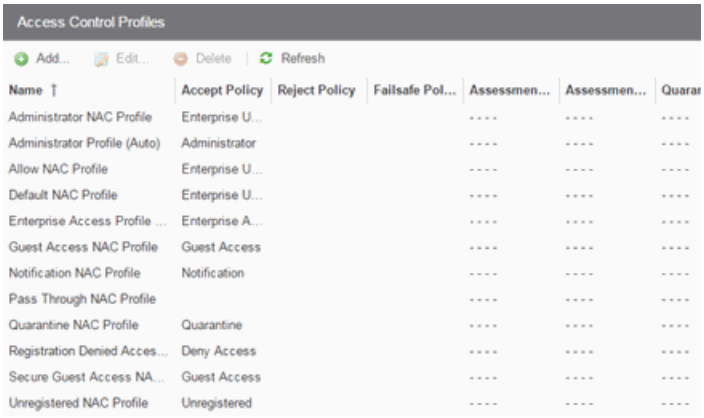
For information on related windows:

- Edit Policy Mapping Configuration Window

Access Control Profiles

Extreme Management Center comes with ten system-defined Extreme Access Control profiles that define the authorization and assessment requirements for the end-systems connecting to the network. The system-defined profiles are: Administrator, Allow, Default, Guest Access, Notification, Pass Through, Quarantine, Registration Denied Access, Secure Guest Access, and Unregistered. You can use this window to view and edit these profiles, and define new profiles if desired. Any changes made in this window are written immediately to the Extreme Management Center database.

To access this window, select the Extreme Access Control Profiles left-panel option in the **Access Control** tab.



Add Button Add...

Use this button to open the New Extreme Access Control Profile window, where you can add an Extreme Access Control profile.

Edit Button Edit...

Use this button to open the Edit Extreme Access Control Profile window, where you can edit an existing Extreme Access Control profile.

Delete Button Delete

Use this button to add an Extreme Access Control profile.

Name

The name of the Extreme Access Control profile.

Accept Policy
The Accept policy defined for this profile. An Accept policy is applied to an end-system when

- an end-system has been authorized locally by the Extreme Access Control engine and has passed an assessment (if assessment in enabled).
- authentication is configured to replace the attributes returned from the RADIUS server with the Accept policy.

Reject Policy
Indicates whether all authentication requests are rejected.

Failsafe Policy
The Failsafe policy defined for this profile. A Failsafe policy is applied to an end-system if the end-system's IP address cannot be determined from its MAC address, or if there has been a scanning error and a scan of the end-system could not take place.

Assessment Configuration
The assessment configuration defined for this profile. The configuration define the assessment requirements for end-systems

Assessment Interval
If assessment is required, this defines the interval between required assessments for an end-system.

Quarantine Policy
The Quarantine policy defined for this profile. A Quarantine policy is applied to an end-system if the end-system fails an assessment.

Assessment Policy
The Assessment policy defined for this profile. An Assessment policy is applied to an end-system while it is being assessed.

Hide Assessment/Remediation Details
Denotes whether the option to hide assessment or remediation information on the Remediation Web Page has been selected.

Related Information

For information on related windows:

- New/Edit Extreme Access Control Profile Window

New/Edit Extreme Access Control Profile

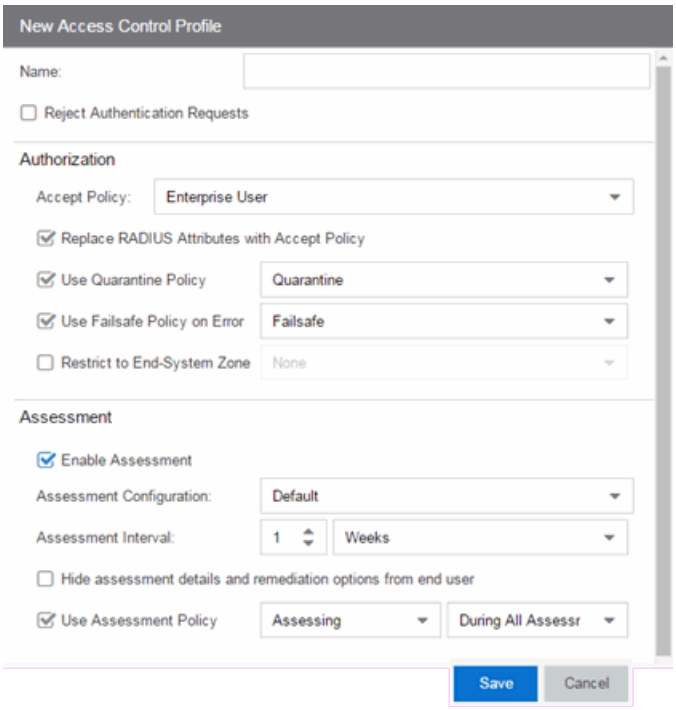
Extreme Access Control Profiles specify the authorization and assessment requirements for the end-systems connecting to the network. Profiles also specify the security policies that will be applied to end-systems for network authorization, depending on authentication and assessment results.

Extreme Management Center comes with ten system-defined Extreme Access Control profiles:

- Administrator
- Allow
- Default
- Guest Access
- Notification
- Pass Through
- Quarantine
- Registration Denied Access
- Secure Guest Access
- Unregistered

You can edit these profiles or you can define your own profiles to use for your Extreme Access Control configurations. Use this window to create a new profile, or edit an existing profile. When you create a new profile, it is added to the Manage Extreme Access Control Profiles window. When you edit a profile, it changes the profile wherever it is used, so you don't have to do individual edits for each profile.

To create a new profile, click the **Add** button in the Manage Extreme Access Control Profiles window. To edit an existing profile, select a profile in the Manage Extreme Access Control Profiles window and click the **Edit** button or select it from the left-panel.



Name

Enter a name for a new profile. If you are editing a profile, the name of the profile is displayed and cannot be edited. To change the name of a profile, right-click on the profile name in the Extreme Access Control Profiles left-hand panel navigation tree and select Rename from the menu.

Reject Authentication Requests

If you select this checkbox, all authentication requests are rejected.

Authorization

Accept Policy

Use the drop-down menu to select the Accept policy you want to use in this Extreme Access Control profile. An Accept policy is applied to an end-system when:

- an end-system has been authorized locally (MAC authentication) by the Extreme Access Control engine and has passed an assessment (if assessment in enabled).
- you have selected the Replace RADIUS Attributes with Accept Policy option.

If you select "No Policy", then the Extreme Access Control engine does not include a Filter ID or VLAN Tunnel Attribute in the RADIUS attributes returned to the switch,

and the default role configured on the port is assigned to the end-system. This option is necessary when configuring single user plus IP phone authentication supported on C2/C3 and B2/B3 devices.

Replace RADIUS Attributes with Accept Policy

When this option is checked, the attributes returned from the RADIUS server are replaced by the policy designated as the Accept policy. If the RADIUS server does not return a Filter ID or VLAN Tunnel attribute, the Accept policy is inserted. When this option is unchecked, the attributes returned from the RADIUS server are forwarded back "as is" and the Accept Policy would only be used to locally authorize MAC authentication requests. If the RADIUS server does not return a Filter ID or VLAN Tunnel attribute, no attributes are returned to the switch.

Use Quarantine Policy

Select this checkbox if you want to specify a Quarantine policy. The Quarantine policy is used to restrict network access for end-systems that have failed the assessment. You must have the Enable Assessment checkbox selected to activate this checkbox.

If a Quarantine policy is not specified and you have configured RADIUS in your AAA configuration, then the policy from the RADIUS attributes would be applied (unless Replace RADIUS Attributes with Accept Policy has been selected, in which case the Accept policy would be used.) If Authorize Authentication Requests Locally has been selected in your AAA configuration, then the Accept policy would be applied to those end-systems that are authorized locally. This allows an end-system onto the network with its usual network access even though the end-system failed the assessment.

Use Failsafe Policy on Error

Select this checkbox if you want to specify a Failsafe policy to be applied to an end-system when it is in an Error connection state. An Error state results if the end-system's IP address could not be determined from its MAC address, or if there was a scanning error and a scan of the end-system could not take place. A Failsafe policy should allocate a nonrestrictive set of network resources to the connecting end-system so it can continue its work, even though an error occurred in Extreme Access Control operation.

If a Failsafe policy is not specified and you have configured RADIUS in your AAA configuration, then the policy from the RADIUS attributes would be applied (unless Replace RADIUS Attributes with Accept Policy has been selected, in which case the Accept policy would be used.) If Authorize Authentication Requests Locally has

been selected in your AAA configuration, then the Accept policy would be applied to those end-systems that are authorized locally. This allows end-systems onto the network with their usual network access when an error occurs in Extreme Access Control operation.

Assessment

Enable Assessment

Select the Enable Assessment checkbox if you want to require that end-systems are scanned by an assessment server.

NOTE: If you require end-systems to be scanned by an assessment server, you need to configure the assessment servers performing the scans. The Manage Assessment Settings window is the main window used to manage and configure assessment servers. To access this window, select Assessment from the Extreme Access Control Configurations > Extreme Access Control Profiles left-hand panel navigation tree.

Assessment Configuration

Use the drop-down list to select the assessment configuration you would like to use in this Extreme Access Control Profile. Use the Edit button to add a new assessment configuration or edit a configuration, if needed. Once an assessment configuration has been created, it becomes available for selection in the list.

Assessment Interval

Enter an assessment interval that defines the interval between required assessments:

- Minutes - 30 to 120
- Hours - 1 to 48
- Days - 1 to 31
- Weeks - 1 to 52
- None

Hide Assessment Details and Remediation Options from User

If you select this option, the end user does not see assessment or remediation information on the Remediation Web Page. They are informed that they are quarantined, and told to contact the Help Desk for assistance.

Use Assessment Policy

Select this checkbox if you want to specify a certain policy to be applied to an end-system while it is being assessed. Use the drop-down menu to select the desired policy.

Select when to apply the policy:

- During Initial Assessment Only - Only initial assessments receive the assessment policy. If the end-system is being re-assessed, it remains in its current policy.
- During All Assessments - All end-systems being assessed receive the specified assessment policy.

If an assessment policy is not specified and you have configured RADIUS in your AAA configuration, then the policy from the RADIUS attributes are applied (unless "Replace RADIUS Attributes with Accept Policy" is selected, in which case the Accept policy is used.) If "Authorize Authentication Requests Locally" is selected in your AAA configuration, then the Accept policy is applied to those end-systems authorized locally. This allows the end-system immediate network access without having to wait for assessment to be complete.

Related Information

For information on related windows:

- Manage Identity and Access Profiles Window
- Manage Assessment Settings Window
- Edit Assessment Configuration Window

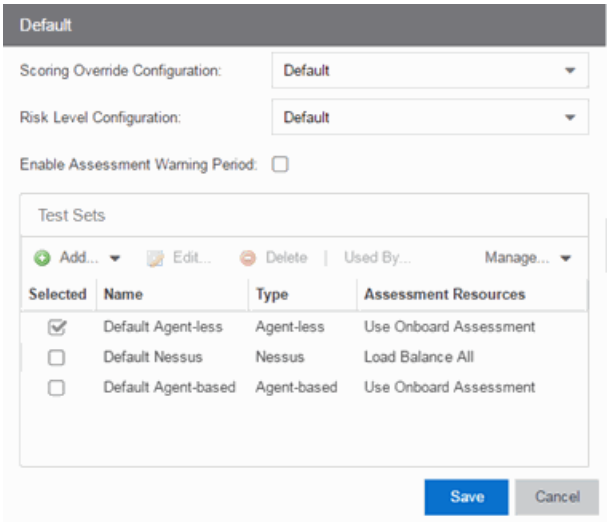
Edit Assessment Configuration

This window lets you view and configure the assessment configurations that define the assessment requirements for end-systems. Assessment configurations define the following information:

- How to score assessment results (determined by the selected Risk Level and Scoring Override configurations).
- What assessment tests to run (determined by the selected test sets).

Once you have defined your assessment configurations, they are available for selection when creating your Extreme Access Control configurations.

To access this window, select **Extreme Access Control Configurations > Extreme Access Control Profiles > Assessment** in the left-hand menu to open the Manage Assessment Settings window. Select an existing configuration and click **Edit** to open the Edit Assessment Configuration window, or you can click **Add** to add a new assessment configuration, and then open the Edit Assessment Configuration window.



Scoring Override Configuration

Use the drop-down menu to select the scoring override configuration for this assessment configuration. Scoring overrides let you override the scoring mode and test result scores for a particular assessment test. The default scoring override configuration provided by Extreme Management Center specifies no overrides, but can be edited to contain overrides, if desired.

Risk Level Configuration

Use the drop-down menu to select the risk level configuration for this assessment configuration. The risk level configuration determines what risk level is assigned to an end-system (high, medium, or low) based on the end-system's health result details score.

Advanced

The Advanced section allows you to enable assessment warning periods. Warning periods let you specify a grace period and probation period used for assessment warnings.

- Grace Period — specify the number of days the end user has to resolve the warning issues before the end-system is quarantined.
- Probation Period — The number of days after an end user is quarantined that additional warnings results in immediate quarantine. This allows administrators to block repeat offenders by limiting their access to the network. Once the probation period has passed, the end user can again receive assessment warnings. Setting the probation period to 0 is the same as having no probation period.

Test Sets

Select one or more test sets to run for this assessment configuration. Test sets define which type of assessment to launch against the end-system, what parameters to pass to the assessment server, and what assessment server resources to use.

If you select multiple agent-based test sets, the first test set you select is called the Master test set. A Master test set includes the Agent Configuration settings, the Advanced Settings, and all the specified test cases. Each subsequent agent-based test set that you select for the configuration is a "supporting" test set. For supporting test sets, only the "Application" test cases are used; all other configuration values are ignored. In the list of Test Sets, Master test sets have a "(Master)" designation after them.

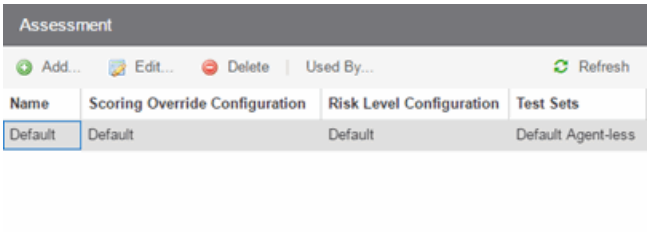
For example, you might want to use multiple agent-based test sets if you are managing multiple networks, and you have a unique agent-based test set for each network as well as secondary test sets for specific application tests that all the networks would use. In the assessment configuration for each network, select the unique test set as the Master test set and then select any number of secondary test sets to be included in the configuration as well.

If the Master test set is deselected, then a new master is automatically selected. To specify a different test set as Master, deselect all test sets, select the desired Master test set first, and select the additional supporting test sets.

Manage Assessment Settings

The Manage Assessment Settings panel is the main panel used to manage and configure the assessment servers performing the end-system assessments in your network. To access this window, select **Extreme Access Control Configurations > Extreme Access Control Profiles > Assessment** from the menu bar.

Assessment configurations define the different assessment requirements for end-systems connecting to your network. When you create an Extreme Access Control profile, you select an assessment configuration that defines the assessment requirements for the end-systems using that profile. You can also click the **Used By** button to view a list of all assessment configurations currently being used by Extreme Access Control configurations.



Name

The name of the assessment configuration. This is the name that is entered when you add an assessment configuration in the Edit Assessment Configuration window.

Scoring Override Config

The scoring override configuration for this assessment configuration. The scoring override configuration lets you override the default scoring assigned by the assessment server to a particular assessment test ID.

Risk Level Config

The risk level configuration for this assessment configuration. The risk level configuration determines what risk level is assigned to an end-system (high, medium, or low) based on the end-system's health result details score.

Test Sets

The test sets that runs for this assessment configuration. Test sets define which type of assessment to launch against the end-system, what parameters to pass to the assessment server, and what assessment server resources to use.

Related Information

For information on related windows:

- Edit Assessment Configuration

Portal Configuration Overview

If your network is implementing registration or assessment / remediation, you define the branding and behavior of the portal website used by the end user during the registration or assessment/remediation process using a Portal Configuration. Extreme Access Control engines ship with a default Portal Configuration. You can use this default configuration as is, or make changes to the default configuration using this window, if desired.

Accessing the Portal Configuration

Use the following steps to access the Portal Configuration:

1. Open the Control > Extreme Management Center tab.
2. Expand the Portal tree in the left-panel.
3. Expand a Portal Configuration.

Network Settings

Use this panel to configure common network web page settings that are shared by both the Assessment / Remediation and the Registration portal web pages.

Administration

Use this panel to configure settings for the Registration Administration web page and grant access to the page for administrators and sponsors.

The Registration Administration web page allows Helpdesk and IT administrators to track the status of registered end-systems, as well as add, modify, and delete registered end-systems on the network.

Look and Feel

Use the Look and Feel panel to configure common web page settings shared by both the Assessment / Remediation and the Registration portal web pages.

Guest Access and Registration

Guest Web Access provides a way for you to inform guests that they are connecting to your network and lets you display an Acceptable Use Policy (AUP).

Guest Registration forces any new end-system connecting on the network to provide the user's identity in the registration web page before being allowed access to the network.

Secure Guest Access provides secure network access for wireless guests via 802.1x PEAP by sending a unique username, password, and access instructions for the secure SSID to guests via an email address or mobile phone (via SMS text). Secure Guest Access supports both pre-registered guests and guests self-registering through the captive portal. No agent is required.

Authenticated Web Access

Authenticated Web Access provides a way to inform end users that they are connecting to your network and lets you display an Acceptable Use Policy. End users are required to authenticate to the network using the Authenticated Web Access login page. However, end users are only granted one-time network access for a single session, and no permanent end user registration records are stored. Authentication is required each time a user logs into the network, which can be particularly useful for shared computers located in labs and libraries.

Authenticated Registration

Authenticated Registration provides a way for existing corporate end users to access the network on end-systems that don't run 802.1X (such as Linux systems) by requiring them to authenticate to the network using the registration web page. After successful registration, the end-system is permitted access until the registration expires or is administratively revoked.

Assessment / Remediation

Use this panel to configure settings for the Assessment / Remediation portal web page.

Website Configuration

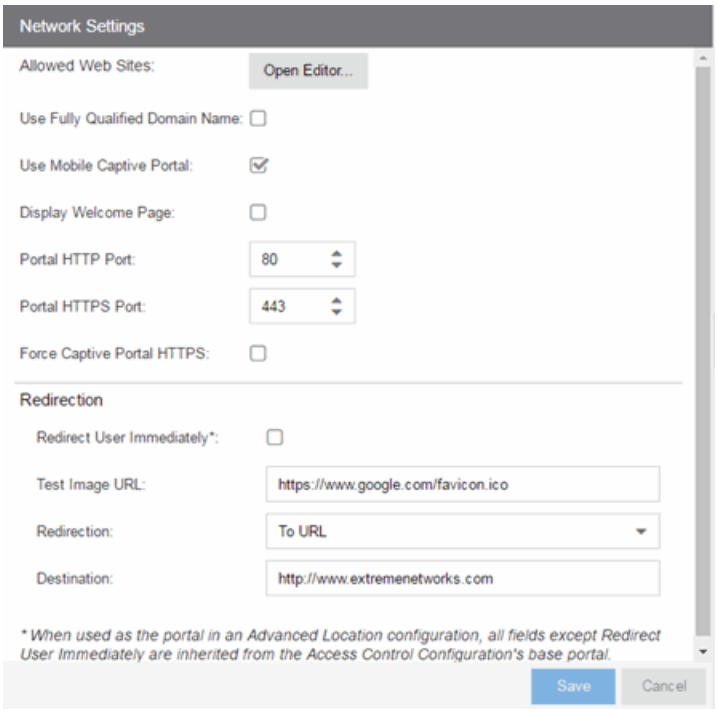
Use this tab to configure the common settings used by the different registration web pages, including selecting guest access, authentication settings, and whether assessment and remediation is supported.

Related Information

- Portal Configuration Network Settings
- Portal Configuration Administration
- Portal Configuration Look and Feel
- Portal Configuration Guest Access
- Portal Configuration Guest Registration
- Portal Configuration Authentication
- Portal Configuration Assessment / Remediation
- Portal Configuration Website Configuration

Portal Configuration Network Settings

Use this panel to configure common network web page settings that are shared by both the Assessment / Remediation and the Registration portal web pages.



Allowed Web Sites

Click on the **Open Editor** button to open the Allowed Web Sites window, where you can configure the web sites to which end users are allowed access during the assessment/remediation and registration process.

Use Fully Qualified Domain Name

Select this checkbox if you would like the URLs in the portal web pages to display the engine's hostname instead of IP address. When this is enabled, the user's browser does a DNS lookup to find the IP address for the fully qualified hostname of the Extreme Access Controlengine. Enable this option only if all Extreme Access Controlengines have their hostname defined in DNS.

Use Mobile Captive Portal

Select this checkbox to allow end users using mobile devices to access the network via captive portal registration and remediation. In addition, it allows Helpdesk and IT administrators to track the status of registered end-systems, as well as add, modify, and delete registered end-systems on the network using a mobile device. This feature is supported on the following mobile devices: IPod Touch, IPad, IPhone, Android Phone/Tablet/NetBook, and Windows phones.

Display Welcome Page

Select this checkbox to display the welcome page. If the checkbox is not selected, users bypass the welcome page and access the portal directly.

Portal HTTP Port

Specify which port the Extreme Management Center server and Extreme Access Controlengine use for HTTP web server traffic. Any change does not take effect on the Extreme Access Controlengine until an Enforce is performed.

Portal HTTPS Port

Specify which port the Extreme Management Center server and Extreme Access Controlengine use for HTTPS web server traffic. Any change does not take effect on the Extreme Access Controlengine until an Enforce is performed.

Force Captive Portal HTTPS

Select this checkbox to force captive portal web pages to be served securely over HTTPS (instead of HTTP) to end users on the network. It is recommended this checkbox is enabled if Authenticated Registration is configured for the registration process. The default setting is unchecked, specifying to serve the captive portal web pages over HTTP.

Redirect User Immediately

This option redirects end users to the specified test image URL as soon as they have network access. The redirect happens regardless of where the end user is in the connection process. If the end-system's browser can reach the test image URL, then it assumes the end user has network access and redirects the end user out of the captive portal. The test image URL should be an internal image on your own website that end users don't have access to until they're accepted. It is recommended that the test image URL is a link to an SSL site because if the Extreme Access Control captive portal is configured for Force Captive Portal HTTPS, the browser does not allow the attempt to an HTTP test image site. It is also recommended that the captive portal policies, (typically the Unregistered, Assessing, and Quarantine policies), are configured to deny HTTPS traffic. This prevents the test image connection attempt from successfully completing and moving the end-system out of the captive portal prematurely. In the event access to the test image is available, the user may experience the captive portal reverting to the "click here to access the network page", and then upon selecting the link, returning to the previous page based on their state. This behavior continues until the user is finally accepted on the network.

NOTE: If using the portal for an Extreme Access Control Advanced Location, all portal configurations are inherited from the Extreme Access Control base portal.

Redirection

There are three Redirection options that specify where the end user is redirected following successful registration or remediation, when the end user is allowed on the network:

- To URL — This option lets you specify the URL for the web page where the end user is redirected. When selected, the Destination field displays, allowing you to indicate the URL of the web page.
- Disabled — This option disables redirection. The end user stays on the same web page where they were accepted onto the network.
- To User's Requested URL — This option redirects the end user to the web page they originally requested when they connected to the network.

Related Information

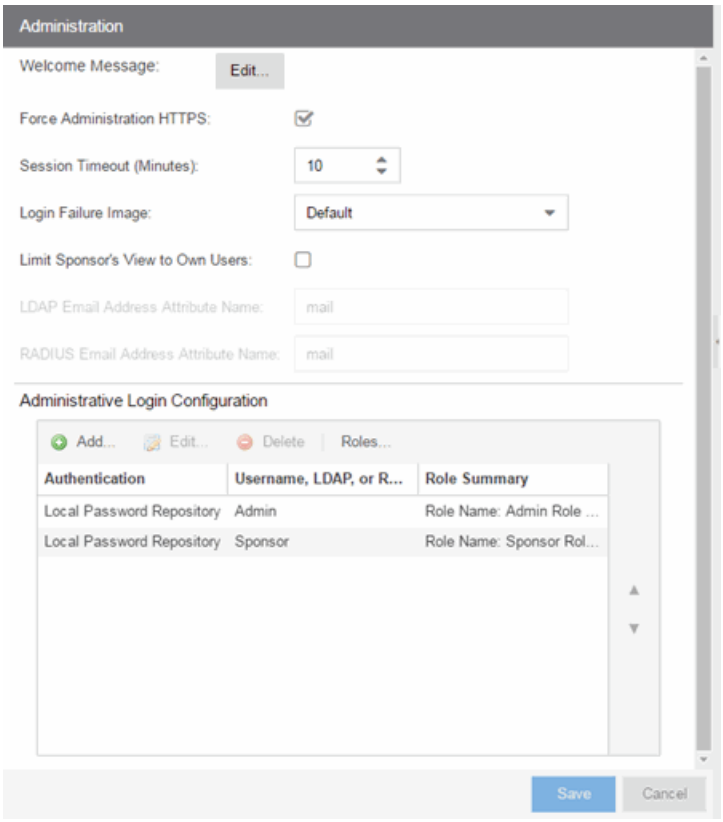
- Portal Configuration Overview

Portal Configuration Administration

The Registration Administration web page allows Helpdesk and IT administrators to track the status of registered end-systems, as well as add, modify, and delete registered end-systems on the network.

Administration

Use this panel to configure settings for the Registration Administration web page and grant access to the page for administrators and sponsors.



Administration Web Page Settings

Welcome Message

Click on the Edit button to open a window where you can modify the message displayed to users when they log into the administration or sponsor portal. The default welcome message is *Registration System Administration*.

Force Administration HTTPS

Select this checkbox to force the administration web page to be served securely over HTTPS (instead of HTTP) to administrators and sponsors on the network. It is recommended this is enabled for additional security.

Session Timeout (Minutes)

This field specifies the length of time an administrator can be inactive on the administration web page before automatically being logged out. The default value is 10 minutes.

Login Failure Image

Select an image to display when the end user fails to correctly log in to the web page. The drop-down selection menu displays all the images defined in the Images

window for your selection. To add a new image, access the Look & Feel panel.

Limit Sponsor's View to Own Users

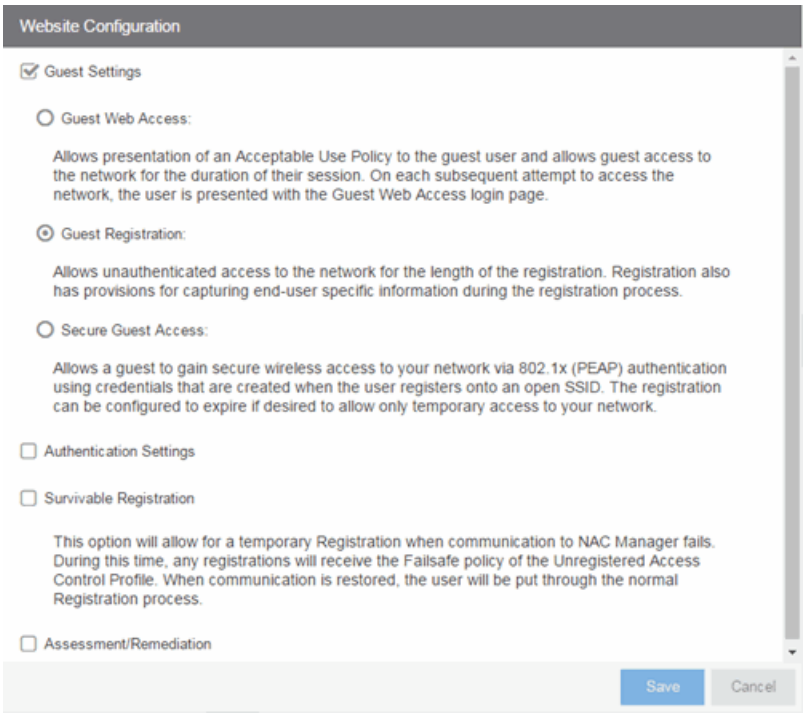
Select this checkbox if you want to limit a sponsor's view to only the users they have sponsored. This option is valid only if you configure LDAP or RADIUS authentication of your sponsors. If you select this checkbox, you must enter the LDAP Email Address Attribute Name or RADIUS Email Address Attribute Name so a sponsor's login name can be matched to their email address, and only the registered users for that sponsor are displayed.

Related Information

- Portal Configuration Overview

Portal Configuration Website Configuration

Use this tab to configure the common settings used by the different registration web pages, including selecting guest access, authentication settings, and whether assessment and remediation is supported. The options selected in this panel change the panels displayed in the left-panel Website Configuration tree.



Guest Settings

Select the behavior of the web site for users with guest access and the level of access to your network. For additional information, see the Guest Web Access, Guest Registration, and Secure Guest Access sections.

Authentication Settings

Select the behavior of the web site for users with authentication credentials and their level of access to your network. For additional information, see the Authenticated Web Access and Authenticated Registration sections.

Enable Survivable Registration

This feature provides temporary Registration for unregistered end-systems when the Extreme Management Center server is unreachable. If you select this checkbox, unregistered users that try to register while the Extreme Management Center server is unreachable are redirected to the Registration web page. After entering the required information, users are assigned the Failsafe policy and allowed on the network. Once the connection to the Extreme Management Center server is reestablished, the users are reassigned the Unregistered policy and forced to re-register. If you enable Survivable Registration, make sure that the Failsafe policy provides the appropriate network services for unregistered users.

Assessment/Remediation

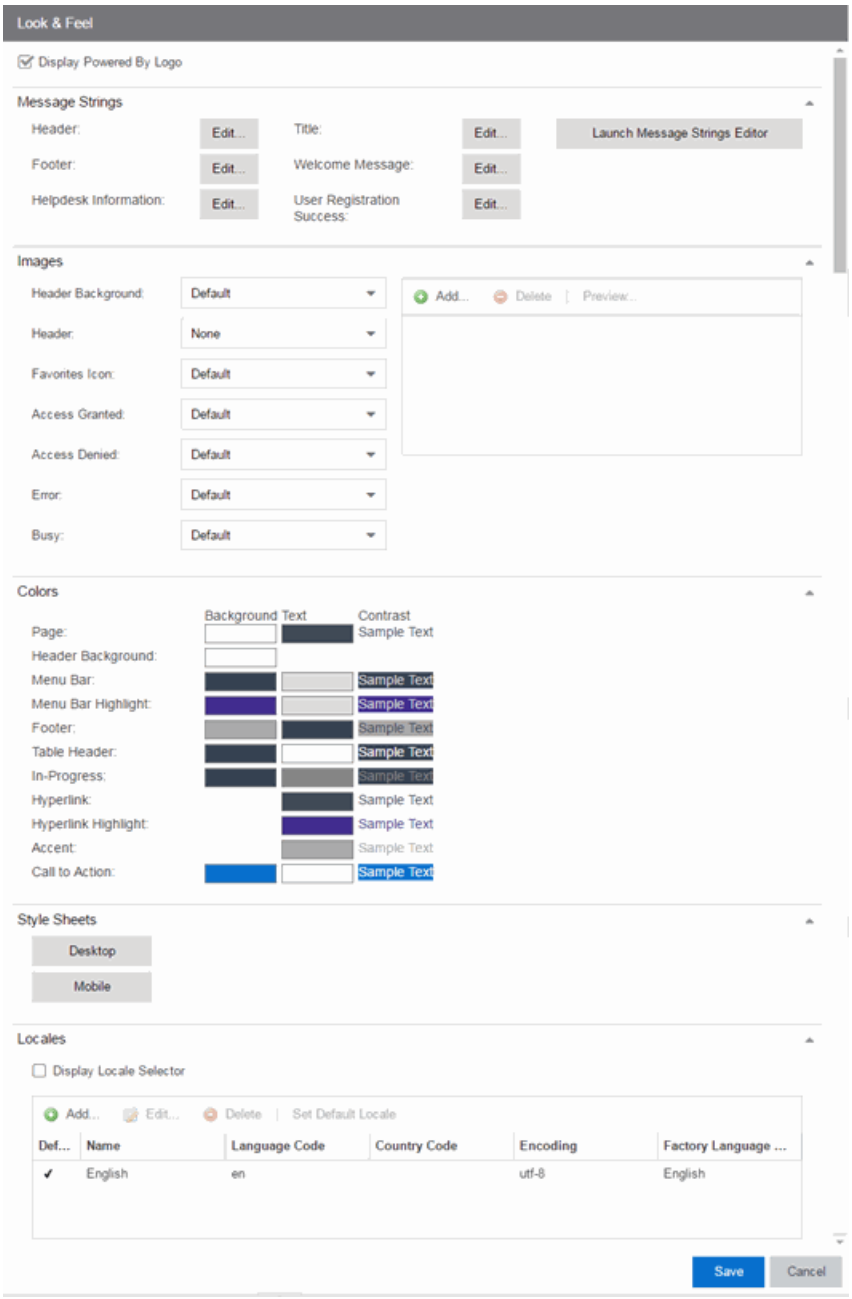
Allows you to configure the behavior of the Assessment/Remediation web portal. For additional information, see the Assessment/Remediation section.

Related Information

- Portal Configuration Overview

Portal Configuration Look and Feel

Use this panel to configure common web page settings shared by both the Assessment/Remediation and the Registration portal web pages.



Display Powered by Logo

Select this checkbox to display the Extreme Networks logo at the bottom of all of your portal web pages.

Header

Click on the Edit button to open a window where you can configure the link for the header image displayed at the top of all portal web pages. By default, the header

image is configured as the Extreme Networks logo acting as a link to the Extreme Networks website. Text entered in this window can be formatted in HTML.

Footer

Click on the Edit button to open a window where you can configure the footer displayed at the bottom of all portal web pages. By default, the footer is configured with generalized information concerning an organization. Change the *example* text in this section to customize the footer to your own organization. Text entered in this window can be formatted in HTML.

Helpdesk Information

Click on the Edit button to open a window where you can configure the Helpdesk contact information provided to end users in various scenarios during the assessment/remediation and registration process (e.g. an end-system exceeded the maximum number of remediation attempts). By default, this section is configured with generalized Helpdesk information, such as contact URL, email address, and phone number. Change the *example* text to customize the Helpdesk information for your own organization. Text entered in this window can be formatted in HTML. In addition, the entire contents of the Helpdesk Information section are stored in the variable "HELPDESK_INFO". By entering "HELPDESK_INFO" (without the quotation marks) in any section that accepts HTML in the Common Page Settings (or any other settings), all information configured in this section will be displayed in place of "HELPDESK_INFO".

Title

Click on the Edit button to open a window where you can modify the text that appears in the title bar of the registration and web access page browser tabs. The default page title is "Enterprise Registration."

Welcome Message

Click on the Edit button to open a window where you can modify the message displayed to users on the menu bar of any registration or web access page. The default welcome message is "Welcome to the Enterprise Network's Registration Center."

User Registration Success

Click the Edit button to open a window where you can edit the message displayed to the end user after successfully registering their end-system to the network.

Images

Using the dropdown menus, you can specify the image files used in the portal web pages. All image files used for Assessment/Remediation and Registration portal web

pages must be defined in this list. The image files defined here are sent to the Extreme Access Controlengine along with the web page configuration. Use the **Add** button to select an image file to add to the list. You can select an image in the list and use the **Preview** button to preview the image.

Once an image file is defined here, it is available for selection from the configuration drop-down lists (for example, when you configure the Access Granted Image), and may be referenced in the sections supporting HTML. Available drop-down lists include:

- **Header Background Image**
  Select the background image displayed behind the header image at the top of all portal web pages. The drop-down menu displays all the images defined in the Images window for your selection. To add a new image, select **Add** to open the Images window.
- **Header Image**
  Select the image displayed at the top of all portal web pages. The drop-down menu displays all the images defined in the Images window for your selection. To add a new image, select **Add** to open the Images window.
- **Favorites Icon**
  Select the image displayed as the Favorites icon in the web browser tabs. The drop-down menu displays all the images defined in the Images window for your selection. To add a new image, select **Add** to open the Images window.
- **Access Granted Image**
  Select the image displayed when the end user is granted access to the network either based on compliance with the network security policy or upon successful registration to the network. The drop-down menu displays all the images defined in the Images window for your selection. To add a new image, select **Add** to open the Images window.
- **Access Denied Image**
  Select the image you would like displayed when the end user has been denied access to the network. The drop-down selection list displays all the images defined in the Images window for your selection. To add a new image, select Manage Images to open the Images window.

- **Error Image**
  Select the image displayed when there is a communication error with the Extreme Management Center Server. The drop-down menu displays all the images defined in the Images window for your selection. To add a new image, select Add to open the Images window.

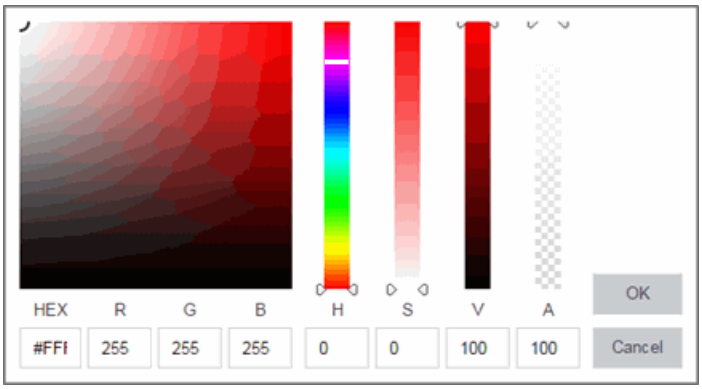
- **Busy Image**
  Select the progress bar image displayed to the end user when the web page is busy processing a request. The drop-down menu displays all the images defined in the Images window for your selection. To add a new image, select Add to open the Images window.

Colors

Click on the Background or Text color box corresponding to each item to open the Choose Color window, displayed below, where you can define the colors used in the portal web pages:

- Page — Define the background color and the color of all primary text on the web pages.
- Header Background Color — Define the background color displayed behind the header image.
- Menu Bar — Define the background color and text color for the menu bar.
- Menu Bar Highlight — Define the background color and text color used for the menu bar highlights in the Administration pages.
- Footer — Define the background color and text color for the footer.
- Table Header — Define the background color and text color for the table column headers in the Administrative web pages.
- In-Progress — Define the background color and text color for task in-progress images.
- Hyperlink — Define the color used for hyperlinks on the web pages.
- Hyperlink Highlight — Define the color of a hyperlink when it is highlighted.
- Accent — Define the color used for accents on various parts of the web pages.

Click OK to save the changes.



Style Sheets

Click on the Desktop or Mobile buttons to open the Edit Style Sheet window where you can create a style sheet that adds to or overwrites the formatting styles for the portal, or mobile version of the portal web pages, respectively.

Locales

This field lists the locales (languages) presented as options to the user in the captive portal, in addition to the default locale.

You can also define the default locale (language), displayed to any captive portal user unless the client locale detected from their browser matches one of the defined supplemental locales. The list of available locales includes the current default locale and any supplemental defined locales.

Display Locale Selector

Select this checkbox if you want a locale (language) selector to display as a drop-down menu in the menu bar on the captive portal welcome and login pages. This is useful for a shared machine where the users of the machine may speak different languages. (On the mobile captive portal, the selector is displayed as a list of links at the bottom of the welcome screen.)

Related Information

- Portal Configuration Overview

Portal Configuration Authenticated Access and Registration

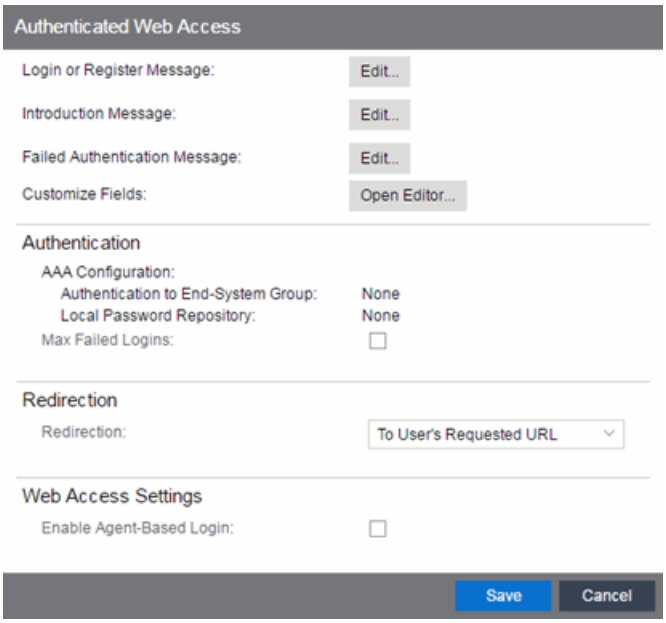
Authenticated web access provides a way to inform end users that they are connecting to your network and lets you display an Acceptable Use Policy. Authenticated registration provides a way for existing corporate end users to access the network on end-systems that don't run 802.1X (such as Linux systems) by requiring them to authenticate to the network using the registration web page.

NOTE: The Authentication and Redirection settings are shared by the Authenticated Web Access and Authenticated Registration access types. Changing them for one type also changes them for the other.

Authenticated Web Access

End users are required to authenticate to the network using the Authenticated Web Access login page. However, end users are only granted one-time network access for a single session, and no permanent end user registration records are stored. Authentication is required each time a user logs into the network, which can be particularly useful for shared computers located in labs and libraries.

Implementing authenticated web access requires web redirection or DNS proxy.



Login or Register Message

Click the Edit button to open a window where you can edit the message displayed to the end user when they are registering. By default, the message states that the end user is required to register before being allowed on the network.

Introduction Message

Click the Edit button to open a window where you can edit the introductory message displayed to the end user when they are registering. By default, the message states that the end user is agreeing to the terms and conditions in the Acceptable Use Policy.

Failed Authentication Message

Click the Edit button to open a window where you can edit the message displayed to the end user if the end user fails authentication. By default, this message advises the end user to contact their network administrator for assistance. Note that the default configuration of the message references the "HELPDESK_INFO" variable which represents the Helpdesk Information that is defined in the Look and Feel Settings.

Customize Fields (Shared)

Click the Open Editor button to open the Manage Custom Fields window where you can manage the fields displayed in the Registration web page.

Authentication

AAA Configuration

This section displays the name of the AAA configuration being used by the Access Control configuration and provides a link to open the AAA Configuration window where you can make changes to the AAA Configuration, if desired. If the portal configuration is shared between multiple Extreme Access Control Configurations using different AAA configurations, the different AAA configurations are listed here (maximum of 3), allowing you to open the appropriate AAA configuration.

The section also displays the method(s) utilized for validating the credentials entered during registration (LDAP, RADIUS, and/or a Local Password Repository) as specified in the AAA configuration(s).

- Authentication to End-System Group — Click the Change button to open the User Group to End-System Group Map window where you can map the LDAP/RADIUS/Local User Group to the appropriate end-system group to specify end user access levels. Once an end-system group has been mapped to a user group, the icon for the end-system group changes to display a key indicating that it is no longer available for general use. You can use the Move Up/Move Down arrows to set the precedence order for the mappings, allowing you to change the authentication order that takes place during the user authenticated registration.
- Local Password Repository — If you are using a local repository, authenticated end users are assigned to the Web Authenticated Users group. Click the Default button to open a window where you can edit the Local Password Repository. Multiple links may be listed if there are different repositories associated with different AAA configurations.

Max Failed Logins

Select this checkbox to specify the maximum consecutive number of times an end user can attempt to authenticate on an end-system and fail. You can specify a lockout period that must elapse before the user can attempt to log in again on that end-system.

Redirection

Redirection

There are four Redirection options that specify where the end user is redirected following successful registration, when the end user is allowed on the network. The

option selected here overrides the Redirection option specified on the Network Settings.

- Use Network Settings Redirection — Use the Redirection option specified on the Network Settings panel.
- Disabled — This option disables redirection. The end user stays on the same web page where they were accepted onto the network.
- To User's Requested URL — This option redirects the end user to the web page they originally requested when they connected to the network.
- To URL — This option lets you specify the URL of the web page to which the end user is redirected. This is typically the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Web Access Settings

Enable Agent-Based Login

If this option is enabled, when the end user connects to the network with an agent installed, the login dialog is displayed in an agent window instead forcing the user to go to the captive portal via a web browser. This allows you to provide authenticated web access without having to set up the captive portal. Agent-based login is useful for shared access end-systems running an agent because it prompts for a login dialog and also provides a logout option. Login credentials are limited to username/password and an Acceptable Use Policy is not displayed.

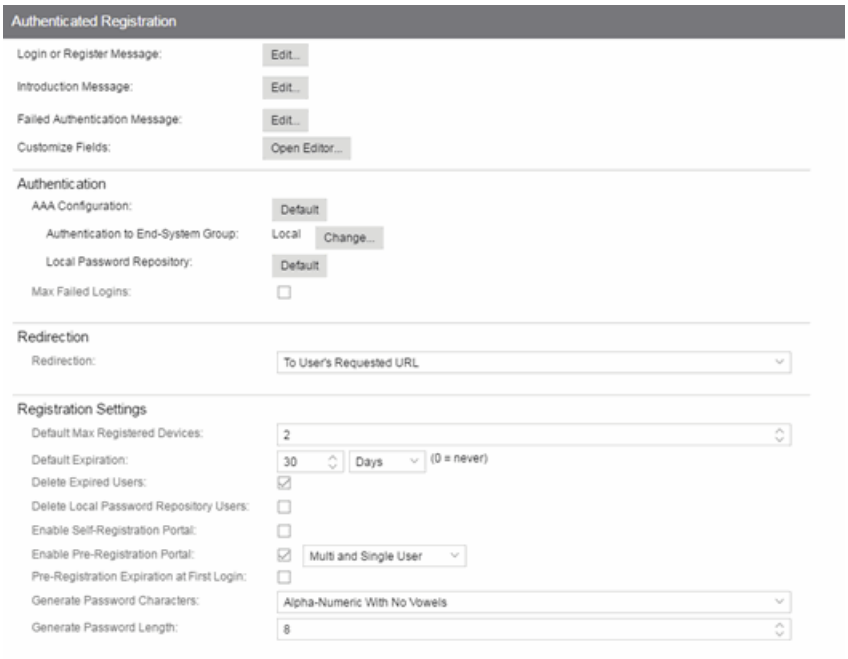
You can customize the messages in the Agent Login window using the Message Strings Editor available in the Look and Feel Settings. Use the agentLoginMessage string to change the message. Any changes you make in the Message Strings Editor override the internationalized messages used in the Agent Login window.

Authenticated Registration

Authenticated registration provides a way for existing corporate end users to access the network on end-systems that don't run 802.1X (such as Linux systems) by requiring them to authenticate to the network using the registration web page. After successful registration, the end-system is permitted access until the registration expires or is administratively revoked.

It is recommended that the Force Captive Portal HTTPS option is enabled if authenticated registration is required for security reasons.

NOTE: If you configure both guest registration and authenticated registration for an area on your network, the end user is presented with a choice on the registration web page whether or not to authenticate.



Login or Register Message

Click the **Edit** button to open a window where you can edit the message displayed to the end user when they are registering. By default, the message states that the end user is required to register before being allowed on the network.

Introduction Message

Click the **Edit** button to open a window where you can edit the introductory message displayed to the end user when they are registering. By default, the message states that the end user is agreeing to the terms and conditions in the Acceptable Use Policy.

Failed Authentication Message

Click the **Edit** button to open a window where you can edit the message displayed to the end user if the end user fails authentication. By default, this message advises the end user to contact their network administrator for assistance. Note that the default configuration of the message references the "HELPDESK_INFO" variable which represents the Helpdesk Information that is defined in the Look and Feel Settings.

Customize Fields (Shared)

Click the Open Editor button to open the Manage Custom Fields window where you can manage the fields displayed in the Registration web page.

Authentication

These settings are shared by the Authenticated Web Access and Authenticated Registration access types. Changing them for one type also changes them for the other.

AAA Configuration

This section displays the name of the AAA configuration being used by the Access Control configuration and provides a link to open the AAA Configuration window where you can make changes to the AAA Configuration, if desired. If the portal configuration is shared between multiple Extreme Access Control Configurations using different AAA configurations, the different AAA configurations are listed here (maximum of 3), allowing you to open the appropriate AAA configuration.

The section also displays the method(s) utilized for validating the credentials entered during registration (LDAP, RADIUS, and/or a Local Password Repository) as specified in the AAA configuration(s).

- Authentication to End-System Group — Click the Change button to open the User Group to End-System Group Map window where you can map the LDAP/RADIUS/Local User Group to the appropriate end-system group to specify end user access levels. Once an end-system group has been mapped to a user group, the icon for the end-system group changes to display a key indicating that it is no longer available for general use. You can use the Move Up/Move Down arrows to set the precedence order for the mappings, allowing you to change the authentication order that takes place during the user authenticated registration.
- Local Password Repository — If you are using a local repository, authenticated end users are assigned to the Web Authenticated Users group. Click the Default button to open a window where you can edit the Local Password Repository. Multiple links may be listed if there are different repositories associated with different AAA configurations.

Max Failed Logins

Select this checkbox to specify the maximum consecutive number of times an end user can attempt to authenticate on an end-system and fail. You can specify a

lockout period that must elapse before the user can attempt to log in again on that end-system.

Redirection

These settings are shared by the Authenticated Web Access and Authenticated Registration access types. Changing them for one type also changes them for the other.

Redirection

There are four Redirection options that specify where the end user is redirected following successful registration, when the end user is allowed on the network. The option selected here overrides the Redirection option specified on the Network Settings.

- Use Network Settings Redirection — Use the Redirection option specified on the Network Settings.
- Disabled — This option disables redirection. The end user stays on the same web page where they were accepted onto the network.
- To User's Requested URL — This option redirects the end user to the web page they originally requested when they connected to the network.
- To URL — This option lets you specify the URL of the web page to which the end user is redirected. This is typically the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Registration Settings

The Generate Password Character and Generate Password Length settings are shared by Authenticated Registration and Secure Guest Access.

Default Maximum Registered Devices

Specify the maximum number of MAC addresses each authenticated end user is allowed to register on the network. If a user attempts to register an additional MAC address that exceeds this count, an error message is displayed in the Registration web page stating that the maximum number of MAC addresses is registered to the network and to call the Helpdesk for further assistance. The default value for this field is 2.

Default Expiration

Enter a value and select a unit of time to configure the amount of time before an end user's registration automatically expires. When the registration expires, the end user is either suspended (registration must be manually approved by administrator/sponsor) or permanently deleted from the registration list. If a registration is deleted, the end-user must re-enter all their required personal information the next time they attempt to access the network. Individual registration expiration time can also be set by the administrator/sponsor through the Registration Administration web page.

Delete Expired Users

Select this checkbox to delete a user from the Registered users list in the Registration Administration web page when their registration expires. If a registration is deleted, the end-user must re-enter all their required personal information the next time they attempt to access the network.

Delete Local Password Repository Users

If you select Delete Expired Users, then selecting this checkbox also deletes the expired user from the local password repository.

Enable Self-Registration Portal

This checkbox allows an authenticated and registered user to be directed to a URL (provided by an administrator) to self-register additional devices that may not support authentication (such as Linux machines) or may not have a web browser (such as game systems). For example, a student may register to the network using their PC. Then, using a self-registration URL provided by the system administrator, they can register their additional devices. Once the additional devices have been registered, the student can access the network using those devices. The URL for the Self Registration web page is `https://<Extreme Access ControlEngineIP>/self_registration`. You can change the instructions displayed on this web page using the Message Strings Editor on the Look and Feel Settings; select the selfRegIntro message string.

Enable Pre-Registration Portal

Select this checkbox to enable pre-registration functionality. With pre-registration, guest users can be registered in advance, allowing for a more streamlined and simple registration process when the guest user connects to the network. This is useful in scenarios where guest users are attending a company presentation, sales seminar, or a training session. From the drop-down menu, select whether you want to pre-register a single user (when you want to pre-register one user at time) or

multiple users (when you have a larger group of users to pre-register) or both. For more information, see How to Configure Pre-Registration.

Pre-Registration Expiration at First Login

Select this checkbox to set the Default Expiration of a pre-registered user to begin when the user first registers a device, instead of setting it the moment the pre-registered user is created (added via the pre-registration administration process). Select Enable Pre-Registration Portal to enable this option. For more information, see How to Configure Pre-Registration.

NOTE: This option is only valid when importing a CSV file to pre-register multiple users in the Pre-Registration Portal and not when entering information for a single user.

Generate Password Characters

This option is available if you select Enable Pre-Registration Portal. During the pre-registration process, Extreme Management Center can automatically generate the password that the guest user uses when connecting to the network. The password is generated according to the specification selected here. This setting is shared by Authenticated Registration and Secure Guest Access. Changing it for one access type also changes it for the other.

Generate Password Length

This option is available if you select Enable Pre-Registration Portal. During the pre-registration process, Extreme Management Center can automatically generate the password that the guest user uses when connecting to the network. The password length is generated according to the number of characters specified here.

Related Information

- Portal Configuration Overview

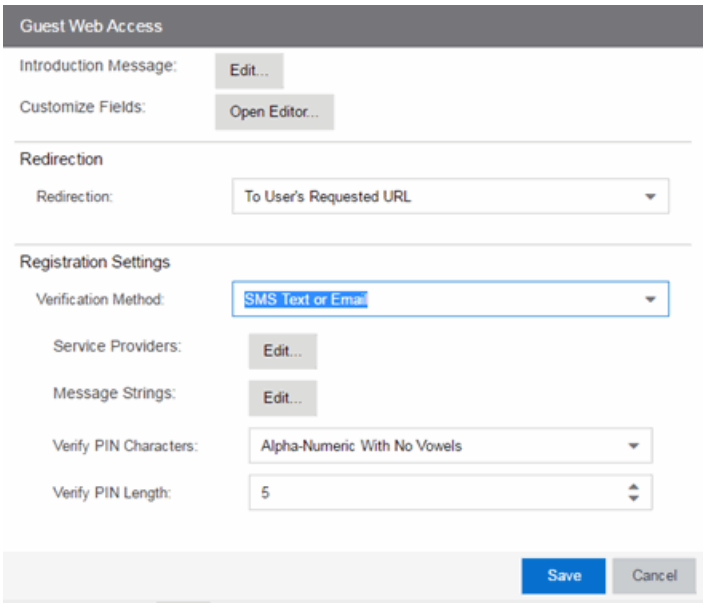
Portal Configuration Guest Access

Guest Web Access provides a way for you to inform guests that they are connecting to your network and lets you display an Acceptable Use Policy (AUP).

End users are initially redirected to the captive portal when they first connect to the network. After the user enters the required information on the Guest Web Access login page (typically, their name and email address), they are allowed access on the network according to the assessment and authorization defined in the Guest Access profile.

Guest web access provides a single session, and no permanent end user records are stored. This provides increased network security, and also allows you to minimize the number of registration records stored in the Extreme Management Center database.

Implementing guest web access requires web redirection or DNS proxy.



Introduction Message

Click the Edit button to open a window where you can edit the introductory message displayed to end users when gaining web access as guests. It may include an introduction to the network and information stating that the end user is agreeing to the Acceptable Use Policy (AUP) for the network upon registering their device. A

link to the URL that contains the full terms and conditions of the network's AUP can be provided from this introductory message. Note that the URL for this link must be added as an Allowed URL in the Allowed Web Sites window accessed from the Network Settings. By configuring the introductory message with this information, end users can be held accountable for their actions on the network in accordance with the terms and conditions set forth by the network's AUP. This message is shared by Guest Web Access and Guest Registration. Changing it for one access type also changes it for the other.

Customize Fields

Click the Open Editor button to open the Manage Custom Fields window where you can manage the fields displayed in the Guest Web Access login page. These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing them for one access type also changes them for the others.

Redirection (Shared)

There are four Redirection options that specify where the end user is redirected following successful access, when the end user is allowed on the network. The option selected here overrides the Redirection option specified on the Network Settings. This setting is shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing it for one access type also changes it for the others.

- Use Network Settings Redirection — Use the Redirection option specified on the Network Settings.
- Disabled — This option disables redirection. The end user stays on the same web page where they were accepted onto the network.
- To User's Requested URL — This option redirects the end user to the web page they originally requested when they connected to the network.
- To URL — This option lets you specify the URL for the web page where the end user will be redirected. This would most likely be the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Registration Settings

Verification Method

User verification requires that guest end users registering to the network enter a verification code that is sent to their email address or mobile phone (via SMS text) before gaining network access. This ensures that network administrators have at least one way to contact the end user. For more information and complete instructions, see How to Configure Verification for Guest Registration.

Select from the following verification methods:

- Email — The end user must enter an email address in the Guest Web Access login page. The Email Address field must be set to Required in the Manage Custom Fields window.
- SMS Gateway — The end user must enter a mobile phone number in the Guest Web Access login page. The Phone Number field must be set to Required in the Manage Custom Fields window.
- SMS Gateway or Email — The end user must enter a mobile phone number or email address in the Guest Web Access login page. The Phone Number and Email Address fields must be set to Visible in the Manage Custom Fields window.
- SMS Text Message — The end user must enter a mobile phone number in the Guest Web Access login page. The Phone Number field must be set to Required in the Manage Custom Fields window.
- SMS Text or Email — The end user must enter either a mobile phone number or email address in the Guest Web Access login page. The Phone Number and Email Address fields must be set to Visible in the Manage Custom Fields window.

If you have selected the "SMS Text Message" or the "SMS Text or Email" Verification method: click the Service Providers Edit button (below the verification method) to configure the list of mobile service providers from which end users can select on the Registration web page. This setting allows Extreme Access Control to correctly format the email address to which to send an email. This email is then received by the service provider and converted to an SMS text which is sent the user. The default configuration provides lists of the major US cellular service providers.

NOTE: Not all cellular service providers provide a way to send SMS text messages via email.

If you have selected the "SMS Gateway" or "SMS Gateway or Email" method: enter the SMS Gateway Email address provided by the SMS Gateway provider.

For all methods: use the Message Strings Edit button (below the verification method) to open the Message Strings Editor and modify the registration verification messages displayed to the user during the verification process. For example, if you have selected Email, you need to modify the

"registrationVerificationEmailSentFromAddress" message string to be the appropriate email address for your company.

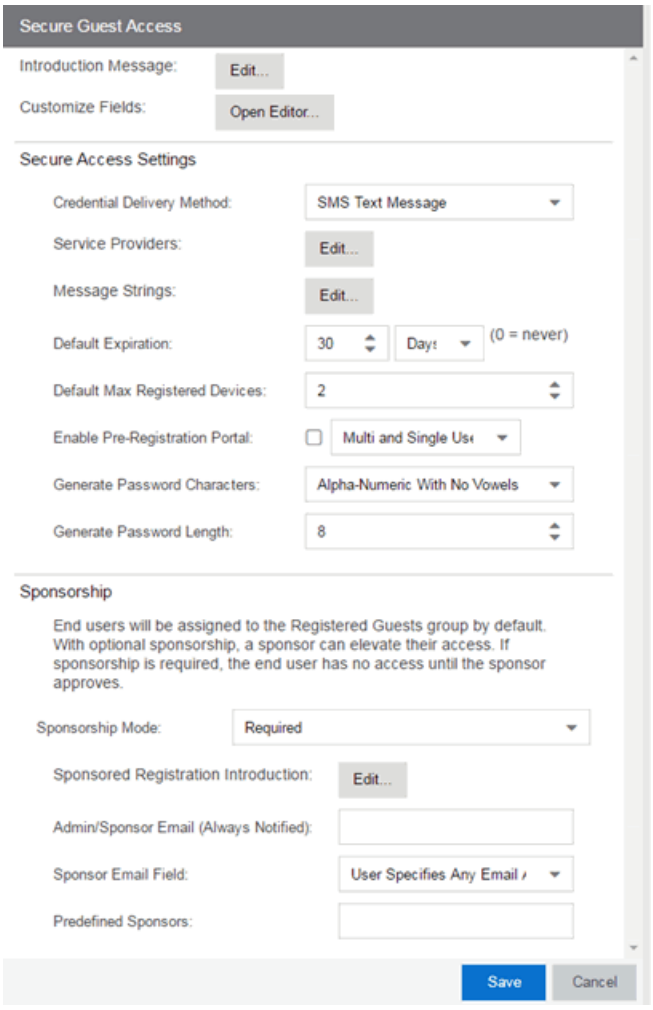
For all methods: set the Verify Pin Characters and Verify Pin Length options to define the characteristics and length of the verification code that is sent to the guest end user. This setting is shared by Guest Registration and Guest Web Access. Changing it for one access type also changes it for the other.

Secure Guest Access

Secure Guest Access provides secure network access for wireless guests via 802.1x PEAP by sending a unique username, password, and access instructions for the secure SSID to guests via an email address or mobile phone (via SMS text). Secure Guest Access supports both pre-registered guests and guests self-registering through the captive portal. No agent is required.

Here are three scenarios where Secure Guest Access provides increased network security:

- An enterprise provides secure guest access for visitors. Guests self-register through the captive portal and receive connection credentials and instructions for the secure SSID via a text message on their mobile phone.
- A hospitality company provides guests with secure Internet access using pre-registration. A receptionist generates a voucher using the Extreme Access Control pre-registration portal. The voucher is handed to the guest, providing them with instructions and credentials for connecting directly to the secure SSID.
- An enterprise provides secure guest access with the option of elevated access through employee sponsors. Guests self-register through the captive portal and receive connection credentials and instructions via a text message. Sponsors approve guests for secure guest access. Later, sponsors can elevate guest access using the sponsorship portal.



Introduction Message

Click the **Edit** button to open a window where you can edit the introductory message displayed to end users when registering as guests. It may include an introduction to the network and information stating that the end user is agreeing to the Acceptable Use Policy (AUP) for the network upon registering their device. A link to the URL that contains the full terms and conditions of the network's AUP can be provided from this introductory message. Note that the URL for this link must be added as an Allowed URL in the Allowed Web Sites window accessed from the Network Settings. By configuring the introductory message with this information, end users can be held accountable for their actions on the network in accordance with the terms and conditions set forth by the network's AUP. This message is shared by Guest Web Access and Guest Registration. Changing it for one access type also changes it for the other.

Customize Fields

Click the Open Editor button to open the Manage Custom Fields window where you can manage the fields displayed in the Registration web page. These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing them for one access type also changes them for the others.

Secure Access Settings

Credential Delivery Method

Select the method that will be used to send guests their credentials and access instructions for the secure SSID. For more information and complete instructions, see How to Configure Credential Delivery for Secure Guest Access.

- Captive Portal — The credential information displays on the Registration web page.
- Email — The end user must enter an email address in the Registration web page. The Email Address field must be set to Required in the Manage Custom Fields window.
- SMS Gateway — The end user must enter a mobile phone number in the Registration web page. The Phone Number field must be set to Required in the Manage Custom Fields window.
- SMS Gateway or Email — The end user must enter a mobile phone number or email address in the Registration web page. The Phone Number and Email Address fields must be set to Visible in the Manage Custom Fields window.
- SMS Text Message — The end user must enter a mobile phone number in the Registration web page. The Phone Number field must be set to Required in the Manage Custom Fields window.
- SMS Text or Email — The end user must enter either a mobile phone number or email address in the Registration web page. The Phone Number and Email Address fields must be set to Visible in the Manage Custom Fields window.

If you have selected the "SMS Text Message" or the "SMS Text or Email" Verification method: click the Service Providers Edit button (below the verification method) to configure the list of mobile service providers from which end users can select on the Registration web page. This setting allows Extreme Access Control to correctly format the email address to which to send an email. This email is then received by the service provider and converted to an SMS text which is sent the user. The default configuration provides lists of the major US cellular service providers.

NOTE: Not all cellular service providers provide a way to send SMS text messages via email.

If you have selected the "SMS Gateway" or "SMS Gateway or Email" method: enter the SMS Gateway Email address provided by the SMS Gateway provider.

For all methods: use the Message Strings **Edit** button (below the verification method) to open the Message Strings Editor and modify the registration verification messages displayed to the user during the verification process. For example, if you have selected "Email", you need to modify the "secureGuestAccessEmailSentFromAddress" message string to be the appropriate email address for your company.

Default Expiration

Enter a value and select a unit of time to configure the amount of time before an end user's registration automatically expires. When the registration expires, the end user is either suspended (registration must be manually approved by administrator/sponsor) or permanently deleted from the guest registration list. If a registration is deleted, the end-user must re-enter all their personal information the next time they attempt to access the network. Individual expiration time can also be set by the sponsor.

Default Max Registered Devices

Specify the maximum number of MAC addresses each authenticated end user is allowed to register on the network. If a user attempts to register an additional MAC address that exceeds this count, an error message is displayed in the Registration web page stating that the maximum number of MAC addresses has already been registered to the network and to call the Helpdesk for further assistance. The default value for this field is 2.

Enable Pre-Registration Portal

Use this checkbox to enable Pre-Registration functionality. With pre-registration, guest users can be registered in advance, allowing for a more streamlined and simple registration process when the guest user connects to the network. This can be particularly useful in scenarios where guest users will be attending a company presentation, sales seminar, or a training session. From the drop-down menu, select whether you want to pre-register a single user (when you want to pre-register one user at time) or multiple users (when you have a larger group of users to pre-register) or both. For more information, see How to Configure Pre-Registration.

Generate Password Characters (Shared)

Extreme Access Control uses this option when generating passwords for guest users who are either self-registering or are pre-registered, to use when connecting to the network. This setting is shared by Authenticated Registration and Secure Guest Access. Changing it for one access type also changes it for the other.

Generate Password Length (Shared)

NAC Manager will use this option when generating passwords for guest users who are either self-registering or are pre-registered, to use when connecting to the network. The password length is generated according to the number of characters specified here. This setting is shared by Authenticated Registration and Secure Guest Access. Changing it for one access type also changes it for the other.

Sponsorship

Use this section to configure sponsorship for Secure Guest Access registration. Select the Sponsorship Mode required. Additional settings are displayed if you select optional or required sponsorship. For information on each option, see How to Configure Sponsorship for Guest Registration.

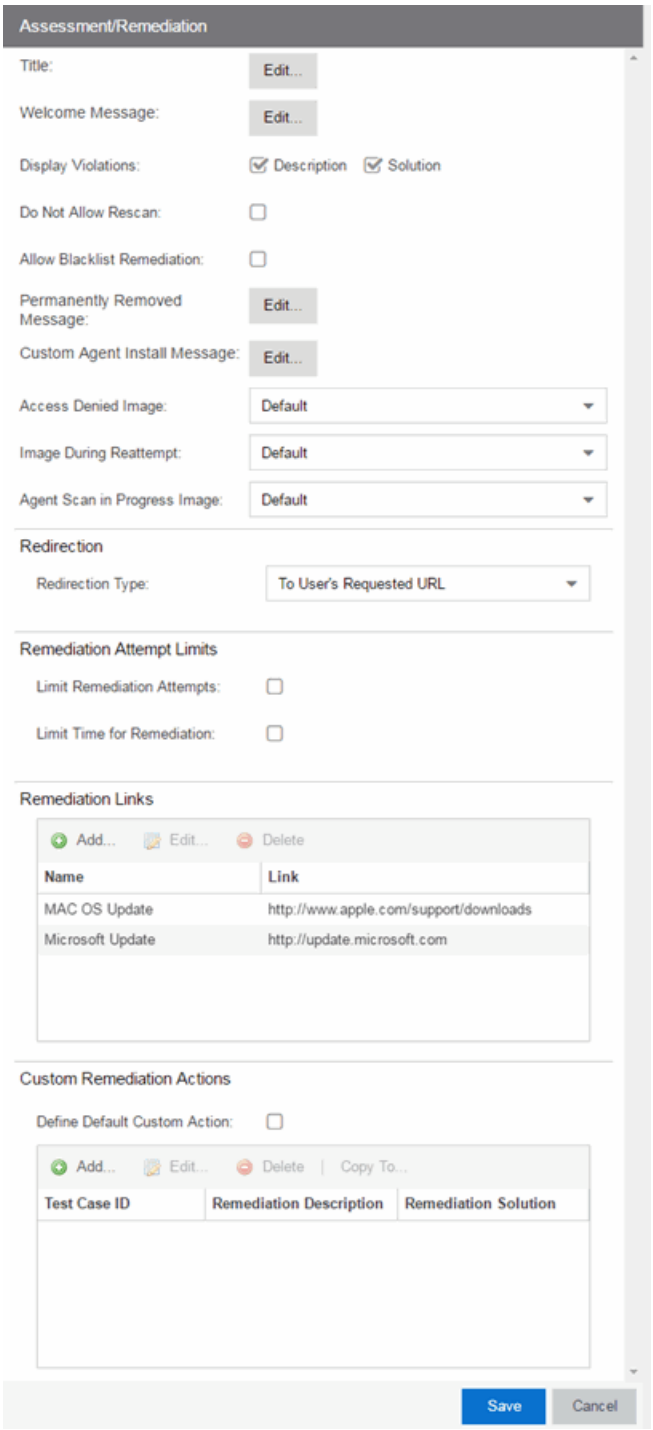
With sponsored registration, end users are only allowed to register to the network when approved by a "sponsor," an internal trusted user to the organization. Sponsorship can provide the end user with a higher level of access than just guest access and allows the sponsor to fine-tune the level of access for individual end users. The end user registers and declares a sponsor's email address. The sponsor is notified and approves the registration, and can assign an elevated level of access, if desired.

Related Information

- Portal Configuration Overview

Portal Configuration Assessment / Remediation

Use this panel to configure settings for the Assessment/Remediation portal web page. Also, the Network Settings and Look and Feel panels provide you access to common settings that are shared by the Assessment/Remediation portal web page.


Assessment/Remediation
Title:
Edit...
Welcome Message:
Edit...
Display Violations:
Description
Solution
Do Not Allow Rescan:
Allow Blacklist Remediation:
Permanently Removed Message:
Edit...
Custom Agent Install Message:
Edit...
Access Denied Image:
Default
Image During Reattempt:
Default
Agent Scan in Progress Image:
Default
Redirection
Redirection Type:
To User's Requested URL
Remediation Attempt Limits
Limit Remediation Attempts:
Limit Time for Remediation:
Remediation Links
Add...
Edit...
Delete
Name
Link
MAC OS Update
http://www.apple.com/support/downloads
Microsoft Update
http://update.microsoft.com
Custom Remediation Actions
Define Default Custom Action:
Add...
Edit...
Delete
Copy To...
Test Case ID
Remediation Description
Remediation Solution
Save
Cancel

Web Page Settings

Title

Click the Edit button to open a window where you can modify the message displayed in the title bar of the Assessment/Remediation web pages. The default page title is "Enterprise Remediation."

Welcome Message

Click the Edit button to open a window where you can modify the message displayed in the banner at the top of the Assessment/Remediation web page. The default welcome message is "Welcome to the Enterprise Remediation Center."

Display Violations

Use the checkboxes to select the assessment violation information that displays to the end user:

- None — No violations are displayed to the web page. This option might be used for an Extreme Access Controlengine that is serving web pages to guest users, when you do not want the guest users to attempt to remediate their end-system.
- Description — Only the description is displayed for violations. This provides the end user with information concerning what violation was found, but no information concerning how it can be fixed. This configuration may be appropriate for scenarios where the user population of the network does not possess technical IT knowledge and is not expected to self-remediate. It provides the Helpdesk personnel with technical information about the violation when the end user places a call to the Helpdesk.
- Solution — Only the solution is displayed for violations, allowing the end user to perform self-service remediation without knowing what the violation is. This configuration may be appropriate for scenarios where the user population on the network does not possess technical IT knowledge but is expected to self-remediate.
- Description and Solution — Both the description and solution are displayed for violations. This provides the end user with information concerning what violation was found and how to fix it. Providing complete information concerning the violation gives the end user the best chance of self-remediation, however, the technical details of the violation may result in end user confusion. Therefore, this configuration may be appropriate for scenarios

where the user population of the network possesses more technical IT knowledge.

Do Not Allow Rescan

Select this checkbox if you do not want the end-user to have the ability to initiate a rescan of their end-system when quarantined. When selected, the Reattempt Network Access button is removed from the Assessment/Remediation web page, and the user is not provided with any way to initiate a rescan on-demand for network access. The end user is forced to contact the Help Desk for assistance. You can edit the "Permanently Removed Message" which, by default, advises the end user to contact the Helpdesk to obtain access to the network. Note that the default configuration of the "Permanently Removed Message" references the "HELPDESK_INFO" variable which represents the Helpdesk Information that is defined in the Look and Feel Settings.

Allow Blacklist Remediation

Select this checkbox if you want black-listed end users to have the ability to remediate their problem and attempt to reconnect to the network. When selected, a "Reattempt Network Access" button is added to the Blacklist web page, allowing end users to remove themselves from the blacklist and reauthenticate to the network.

Permanently Removed Message

Click the Edit button to open a window where you can modify the message displayed when users can no longer self-remediate and must contact the Help Desk for assistance. Note that the default message references the "HELPDESK_INFO" variable which represents the Helpdesk Information that is defined in the Look and Feel Settings.

Custom Agent Install Message

Click the Edit button to open a window where you can create a message containing additional agent install information to add to the default text on the Install Agent portal web page.

Access Denied Image

Select the image you want displayed when the end user is quarantined and denied access to the network. The drop-down menu displays all the images defined in the Images window for your selection.

Image During Reattempt

Select the image you want displayed when the end-user is reattempting network access after they repair their system. The drop-down menu displays all the images defined in the Images window for your selection.

Agent Scan in Progress Image

Select the progress bar image you want displayed while the end-user is being scanned. The drop-down menu displays all the images defined in the Images window for your selection.

Redirection

There are four Redirection options that specify where the end-user is redirected following successful remediation, when the end-user is allowed on the network. The option selected here overrides the Redirection option specified in the Network Settings for Remediation only.

- Use Network Settings Redirection — Use the Redirection option specified in the Network Settings.
- Disabled — This option disables redirection. The end-user stays on the same web page where they were accepted onto the network.
- To User's Requested URL — This option redirects the end user to the web page they originally requested when they connected to the network.
- To URL — This option lets you specify the URL of the web page to which the end-user is redirected. This is typically the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Remediation Attempt Limits

Limit Remediation Attempts

Select this checkbox to limit the maximum number of times an end-user is allowed to initiate a rescan of their end-system after initially being quarantined, in an attempt to remediate their violations. If selected, enter the number of attempts allowed.

Limit Time for Remediation

Select this checkbox to limit the total interval of time an end user is allowed to initiate a rescan of their end-system after initially being quarantined, in an attempt to remediate their violations. If selected, enter the amount of time in minutes.

Remediation Links

This table lists the links displayed on the Assessment/Remediation web page for the end users to use to remediate their end-system violations. There are two default remediation links: Microsoft Support and MAC OS Support. Use this tab to add additional links such as an internal website for patches. Links must contain a valid protocol prefix (http://, https://, ftp://).

Click Add to open a window where you can define a new link's name and URL. Select a link and click Edit to edit the link's information. Click Delete to remove a URL from the table.

Custom Remediation Actions

Use this table to create your own custom remediation action for a particular violation to use in place of the remediation action provided by the assessment server.

Use the following steps to add a custom remediation action:

1. Click the Add button to open the Add Custom Remediation Action window.
2. Enter the Test Case ID for the particular violation being remediated by the custom action. Test Case ID is found in the Health Results Details subtab in the End-Systems tab.
3. Add a custom description of the violation (required) and an optional custom solution.
4. If you have multiple portal configurations and you want to use this custom remediation action in all of your configurations, select the Add to All Portal Configurations option. This option overwrites any existing custom actions defined for the test case ID.
5. Click OK. Whenever the test case ID is listed as a violation on the web page, the custom violation description and solution you define is displayed instead of the remediation actions provided by the assessment server.

Select the Define Default Custom Action checkbox to advise end-users to contact the Helpdesk regarding additional security violations not explicitly listed with custom remediation actions. If this checkbox is selected, only the violations and associated custom remediation actions listed in the table would be presented to the user, along with a message advising them to contact the Helpdesk for any other security violations not explicitly configured with a custom remediation action. Click the Edit button to edit this message.

To copy a custom action to another portal configuration, select the action in the table and click the Copy To button. A window opens where you can select the portal configurations where you want to copy the action, and whether you want it to overwrite any existing custom remediation actions already defined for that test case ID.

Portal Web Page URLs

The following table provides a list of URLs for accessing commonly used portal web pages. You can also access these web pages using the **Engine Portal Pages** button at the bottom of the Portal Configuration window.

Web Page	URL
Preview Web Page Allows you to preview the web pages that may be accessed by the end user during the assessment/remediation and registration process.	https://*Extreme Access ControlengineIP*/screen_preview
Registration Administration Page Lets administrators view registered devices and users, and manually add, delete, and modify users.	https://*Extreme Access ControlengineIP*/administration
Registration Sponsor Page Lets sponsors view registered devices and users, and manually add, delete, and modify users.	https://*Extreme Access ControlengineIP*/sponsor
Pre-Registration Page The pre-registration web page lets selected personnel easily register guest users in advance of an event, and print out a registration voucher that provides the guest user with their appropriate registration credentials.	https://*Extreme Access ControlengineIP*/pre_registration
Self-Registration Page Allows an authenticated and registered user to self-register additional devices that may not have a web browser (for example, game systems).	https://*Extreme Access ControlengineIP*/self_registration

Related Information

- Portal Configuration Overview

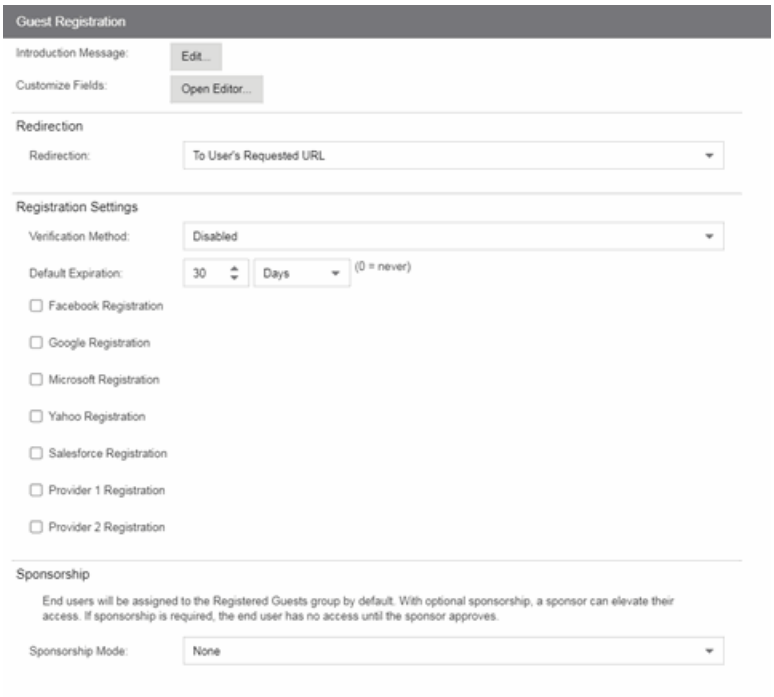
Portal Configuration Guest Registration

Guest registration forces any new end-system connecting on the network to provide the user's identity in the registration web page before being allowed access to the network. Guests are initially redirected to a web page for registering their end-system when it is first connected to the network. After successful registration, the end-system is permitted access until the registration expires or is administratively revoked.

The end user's level of network access is determined by the settings specified here, and whether they are required to have a sponsor. With sponsored registration, end users are only allowed to register to the network when approved by a "sponsor," an internal trusted user to the organization. Sponsorship can provide the end user with a higher level of access than just guest registration and allows the sponsor to fine-tune the level of access for individual end users. The end user registers and declares a sponsor's email address. The sponsor is notified and approves the registration, and can assign an elevated level of access, if desired.

NOTES: If you configure both Guest Registration and Authenticated Registration for an area on your network, the end user is presented with a choice on the registration web page whether or not to authenticate.

The Network Settings and Look and Feel panels provide you access to common settings that are shared by the Registration portal web page.



Introduction Message

Click the **Edit** button to open a window where you can edit the introductory message displayed to end users when registering as guests. It may include an introduction to the network and information stating that the end user is agreeing to the Acceptable Use Policy (AUP) for the network upon registering their device. A link to the URL that contains the full terms and conditions of the network's AUP can be provided from this introductory message. Note that the URL for this link must be added as an Allowed URL in the Allowed Web Sites window accessed from the Network Settings. By configuring the introductory message with this information, end users can be held accountable for their actions on the network in accordance with the terms and conditions set forth by the network's AUP. This message is shared by Guest Web Access and Guest Registration. Changing it for one access type also changes it for the other.

Customize Fields

Click the **Open Editor** button to open the Manage Custom Fields window where you can manage the fields displayed in the Registration web page. These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing them for one access type also changes them for the others.

Redirection

There are four Redirection options that specify where the end user is redirected following successful registration, when the end user is allowed on the network. The

option selected here overrides the Redirection option specified on the Network Settings. This setting is shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing it for one access type also changes it for the others.

- Use Network Settings Redirection — Use the Redirection option specified on the Network Settings.
- Disabled — This option disables redirection. The end user stays on the same web page where they were accepted onto the network.
- To User's Requested URL — This option redirects the end user to the web page they originally requested when they connected to the network.
- To URL — This option lets you specify the URL for the web page where the end user is redirected. This would most likely be the home page for the enterprise website, for example, "http://www.ExtremeNetworks.com."

Registration Settings

Verification Method

User Verification requires that guest end users registering to the network enter a verification code sent to their email address or mobile phone (via SMS text) before gaining network access. This ensures that network administrators have at least one way to contact the end user.

Select from the following verification methods:

- Email — The end user must enter an email address in the Registration web page. The Email Address field must be set to **Required** in the Manage Custom Fields window.
- SMS Gateway — The end user must enter a mobile phone number in the Registration web page. The Phone Number field must be set to **Required** in the Manage Custom Fields window.
- SMS Gateway or Email — The end user must enter a mobile phone number or email address in the Registration web page. The Phone Number and Email Address fields must be set to **Visible** in the Manage Custom Fields window.
- SMS Text Message — The end user must enter a mobile phone number in the Registration web page. The Phone Number field must be set to **Required** in the Manage Custom Fields window.

- SMS Text or Email — The end user must enter either a mobile phone number or email address in the Registration web page. The Phone Number and Email Address fields must be set to Visible in the Manage Custom Fields window.

If you have selected the "SMS Text Message" or the "SMS Text or Email" Verification method: click the Service Providers link (below the verification method) to configure the list of mobile service providers from which end users can select on the Registration web page. This setting allows Extreme Management Center to correctly format the email address to which to send an email. This email is then received by the service provider and converted to an SMS text which is sent the user. The default configuration provides lists of the major US cellular service providers. NOTE: Not all cellular service providers provide a way to send SMS text messages via email.

If you have selected the "SMS Gateway" or "SMS Gateway or Email" method: enter the SMS Gateway Email address provided by the SMS Gateway provider.

For all methods: use the Message Strings link (below the verification method) to open the Message Strings Editor and modify the registration verification messages displayed to the user during the verification process. For example, if you have selected Email, you need to modify the "registrationVerificationEmailSentFromAddress" message string to be the appropriate email address for your company.

For all methods: set the Verify Pin Characters and Verify Pin Length options to define the characteristics and length of the verification code sent to the guest end user. This setting is shared by Guest Registration and Guest Web Access. Changing it for one access type also changes it for the other.

Default Expiration

Enter a value and select a unit of time to configure the amount of time before an end user's registration automatically expires. When the registration expires, the end user is either suspended (registration must be manually approved by administrator/sponsor) or permanently deleted from the guest registration list. If a registration is deleted, the end-user must re-enter all their personal information the next time they attempt to access the network. Individual expiration time can also be set by a sponsor.

Registration

The Registration checkboxes indicate the providers from which ExtremeControl can gather registration information: Facebook, Google, Microsoft, Yahoo, and Salesforce.

You can configure these providers or configure additional OpenID Connect providers using the **Provider Registration** fields.

Sponsorship

Use this section to configure sponsorship for Guest Registration. Select the Sponsorship Mode required. Additional settings display if you select optional or required sponsorship.

With sponsored registration, end users are only allowed to register to the network when approved by a "sponsor," an internal trusted user to the organization. Sponsorship can provide the end user with a higher level of access than just guest registration and allows the sponsor to fine-tune the level of access for individual end users. The end user registers and declares a sponsor's email address. The sponsor is notified and approves the registration, and can assign an elevated level of access, if desired.

Portal Web Page URLs

The following table provides a list of URLs for accessing commonly used portal web pages. You can also access these web pages using the **Engine Portal Pages** button at the bottom of the Portal Configuration window.

Web Page	URL
Preview Web Page Allows you to preview the web pages that may be accessed by the end user during the assessment/remediation and registration process.	https://*Extreme Access ControlengineIP*/screen_preview
Registration Administration Page Lets administrators view registered devices and users, and manually add, delete, and modify users.	https://*Extreme Access ControlengineIP*/administration
Registration Sponsor Page Lets sponsors view registered devices and users, and manually add, delete, and modify users.	https://*Extreme Access ControlengineIP*/sponsor

Web Page	URL
Pre-Registration Page The pre-registration web page lets selected personnel easily register guest users in advance of an event, and print out a registration voucher that provides the guest user with their appropriate registration credentials.	https://*ExtremeAccessControlengineIP*/pre_registration
Self-Registration Page Allows an authenticated and registered user to self-register additional devices that may not have a web browser (for example, game systems).	https://*ExtremeAccessControlengineIP*/self_registration

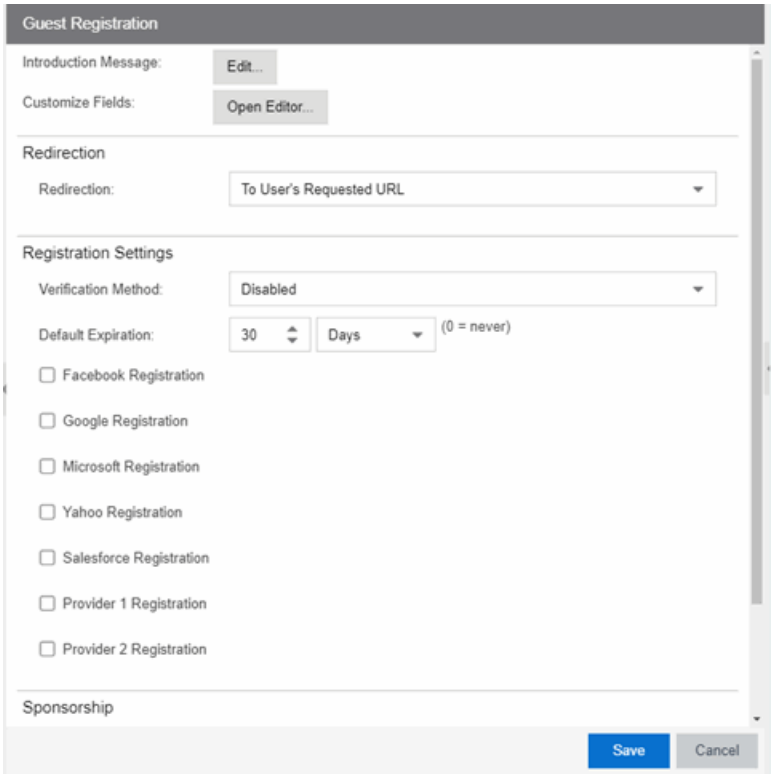
Related Information

- Portal Configuration Overview

Portal Configuration Provider Registration

The Registration Section includes a list of providers from which ExtremeControl can gather registration information. Configure registration using these providers or configure other OpenID Connect providers using the Provider 1 Registration and Provider 2 Registration options.

NOTE: Guest OAuth (e.g. Google, Yahoo) may not support native mobile browsers and display a “user agent” error. To access the network, use a standard browser application (e.g. Google Chrome).



Facebook Registration

1. Select the Facebook Registration checkbox if you are implementing guest registration using Facebook as a way to obtain end user information. In this scenario, the Guest Registration portal provides the end user with an option to log into Facebook in order to complete the registration process.
2. Enter the Facebook App ID – When you create an application you are given a Facebook App ID to enter here.
3. Enter the Facebook App Secret – When you create an application you are given a Facebook App Secret to enter here.
4. Enter the Facebook Redirect URI – This information allows you to configure the provider as `fb_oauth.`
5. Press OK to save your changes.

Google Registration

1. Select the Google Registration checkbox if you are implementing guest registration using Google as a way to obtain end user information. In this scenario, the Guest Registration portal provides the end user with an option to log into Google in order to complete the registration process.
2. Enter the Google Discovery URI – (a benefit of Open ID Connect) - This url gives you access to all the end-points you need to complete authorizations of user data.
3. Enter the Google App ID – When you create an application you are given a Google App ID to enter here.
4. Enter the Google App Secret – When you create an application you are given a Google App Secret to enter here.
5. Enter the Google Redirect URI – This information allows you to configure the provider as `google_oauth.`
6. Press OK to save your changes.

Microsoft Registration

1. Select the Microsoft Registration checkbox if you are implementing guest registration using Microsoft as a way to obtain end user information. In this scenario, the Guest Registration portal provides the end user with an option to log into Microsoft in order to complete the registration process.
2. Enter the Microsoft Discovery URI – (a benefit of Open ID Connect) - This url gives you access to all the end-points you need to complete authorizations of user data.
3. Enter the Microsoft App ID – When you create an application you are given a Microsoft App ID to enter here.
4. Enter the Microsoft App Secret – When you create an application you are given a Microsoft App Secret to enter here.
5. Enter the Microsoft Redirect URI – This information allows you to configure the provider as ms_oauth.
6. Press OK to save your changes.

Yahoo Registration

1. Select the Yahoo Registration checkbox if you are implementing guest registration using Yahoo as a way to obtain end user information. In this scenario, the Guest Registration portal provides the end user with an option to log into Yahoo in order to complete the registration process.
2. Enter the Yahoo Discovery URI – (a benefit of Open ID Connect) - This url gives you access to all the end-points you need to complete authorizations of user data.
3. Enter the Yahoo App ID – When you create an application you are given a Yahoo App ID to enter here.
4. Enter the Yahoo App Secret – When you create an application you are given a Yahoo App Secret to enter here.
5. Enter the Yahoo Redirect URI – This information allows you to configure the provider as `yahoo_oauth`.
6. Press OK to save your changes.

Salesforce Registration

1. Select the Salesforce Registration checkbox if you are implementing guest registration using Salesforce as a way to obtain end user information. In this scenario, the Guest Registration portal provides the end user with an option to log into Salesforce in order to complete the registration process.
2. Enter the Salesforce Discovery URI – (a benefit of Open ID Connect) - This url gives you access to all the end-points you need to complete authorizations of user data.
3. Enter the Salesforce App ID – When you create an application you are given a Salesforce App ID to enter here.
4. Enter the Salesforce App Secret – When you create an application you are given a Salesforce App Secret to enter here.
5. Enter the Salesforce Redirect URI – This information allows you to configure the provider as `salesforce_oauth`.
6. Press OK to save your changes.

Provider Registration (Generic)

1. To add a provider not already considered by Access Control, but uses Open ID Connect, click the box near Provider 1 (generic).
2. Provider 1 Discovery URI – (a benefit of Open ID Connect) – You can use the company's own discovery URI. This feature gives you access to all the end-points that you need to complete authorizations of user data
3. Provider 1 App ID – This information is given by the provider.
4. Provider 1 App Secret – This information is given by the provider.
5. Provider 1 Image – You can add an image or a logo by selecting New from the drop-down menu. Drag and drop a file or select a file using the browser to add an image for this provider.
6. Provider 1 Text – Press the Text button to open the Localized Message String Editor window. Use the box to add text. Press OK to save your changes.
7. Provider 1 Redirect URI - This information allows you to configure the provider as `genprovider_oauth`.

The Enterprise Registration Center will include logos buttons for providers in Register as Guest panel. Click each logo to be redirected to the provider's website for user authentication. You will then be redirected back to complete Open ID access authorization.

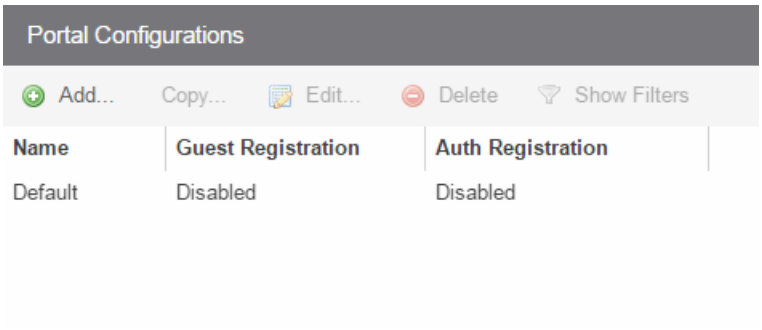
Related Information

- Portal Configuration Overview

Portal Configurations

The Portal Configurations panel in the **Control** > **Extreme Access Control** tab lets you view and edit all the portal configurations defined in Extreme Management Center.

To access the Portal Configurations panel, select **Extreme Access Control Configurations > Portal** from the left-menu tree. If you expand the Portal tree, the Default portal configuration plus any other configurations you have defined are displayed.



Related Information

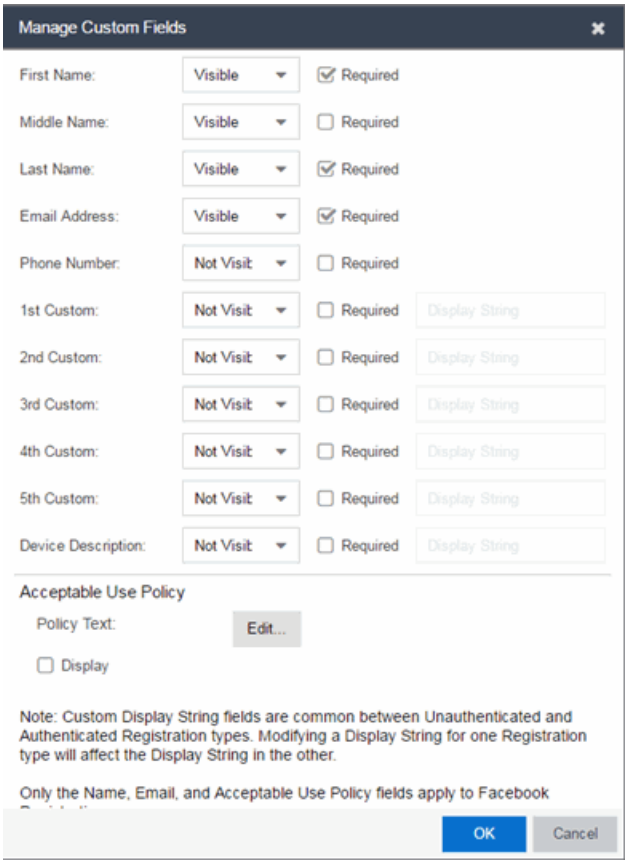
- Portal Configuration
- AAA Configuration
- Extreme Access Control Configuration Rules

Manage Custom Fields

This window lets you manage the fields displayed in the web pages presented to the end user when they access the network. It is configured as part of your portal configuration, and is accessed from the Customize Fields Open Fields button in the Edit Portal Configuration panel. You can manage custom fields for both guest and authenticated access types:

- Guest Access Types — By default, the guest login/registration web page displays the First Name, Last Name, and Email Address fields. You can use this window to specify other fields you would like to be displayed (visible) and required. These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Modifying settings for one access type also changes them for the others.
- Authenticated Access Types — By default, the authenticated login/registration web page displays only the Acceptable Use Policy. You can use this window to specify other fields you would like to be displayed (visible) and required. These settings are shared by the Authenticated Web Access and Authenticated Registration access types. Modifying settings for one access type also changes them for the other.

Sample Manage Custom Fields Window



For each field, use the drop-down menu to select whether the field is:

- Visible - the field is displayed in the login/registration web page for the end user. If you want the field information to be required (the end user must enter the information), select the "Required" checkbox.
- Not Visible - the field is not displayed in the login/registration web page for the end user.
- Admin Only - the field is visible to network administrators only, in the Add/Edit User web page accessed from the Registration System Administration web page. The end user is not able to see or edit the field.

NOTES: For Guest Registration and Guest Web Access: If you are configuring a Verification Method, the Email Address field and/or the Phone Number field are required (depending on the verification method you have selected) and must be set to **Visible/Required**. For more information, see How to Configure Verification for Guest Access Registration.

For Secure Guest Access: The Credential Delivery method requires the Email Address field and/or the Phone Number field (depending on the delivery method you have selected) to be set to **Visible/Required**. For more information, see Credential Delivery Method in the Edit Portal Configuration panel.

For Facebook Registration: Only the First Name, Last Name, and Email Address fields are filled using Facebook data. These fields and the Acceptable Use Policy (AUP) option are the only fields that apply to Facebook registration. If the display AUP option is selected, the captive portal verifies that the AUP is acknowledged before redirecting the user to Facebook.

Use the **Custom fields** to add additional fields to the login/registration web page. Set the field to **Visible**, and then add the text to display by adding a display string. Here are some examples of how to use custom fields:

- In a higher education environment a custom field display string may be set to "Student ID Number" or "Dorm Room Number" to record additional information about students registering to the network.
- In a corporate environment, a custom field display string may be set to "Company Name" to obtain information about organization to which a partner or guest belongs. Or, you might want the end user to enter a device description, such as an asset tag number.
- In a convention deployment, the field may be set to "Booth Number" to record the booth to which a registering end-system is associated.

Select the **Acceptable Use Policy** checkbox if you would like the web page to display your organization's Acceptable Use Policy (AUP) and click the **Edit** button to open a window where you can add the AUP text.

NOTE: The Pre-Registration web page always displays the First Name and Last Name fields even if they are not selected as visible/required in the Manage Custom Fields window. If they are selected as required, they are displayed as required on the Pre-Registration web page, otherwise they are displayed as optional. This is because it is important to prompt for a first and last name to be included on the pre-registration voucher printed out.

Related Information

- Edit Portal Configuration Panel

Keywords

The Custom Arguments field is used to specify the arguments passed to a program. Each argument is delimited by spaces. An argument can be a literal, passed to the program exactly as typed, or a variable, specified as $keyword. A group of literals and variables can be combined into a single argument by using double quotes. The value "all" is a special value that tells Extreme Management Center to pass all variable values to the program as individual arguments. See below for a list of available keywords, along with their definitions.

Keyword Definitions

There are certain "keywords" that you can use in your email, syslog, and trap messages to provide specific information. These $keywords are replaced with information from the notification when the notification action is executed.

Following is a list of available keywords for Extreme Access Control notifications, along with the value the keyword return. The keywords are organized according to the notification type they pertain to (End-System, Registration, Health Result, User Group, or End-System Group), and can only be used when that specific type of notification action is being edited. The Default keywords can be used with any notification type.

Keyword	Returned Value
Default Keywords	
$type	The notification type.
$trigger	The notification trigger.
$conditions	A list of the conditions specified in the notification action.
$server	The Extreme Management Center server IP address.
End-System Keywords	
$macAddress	The end-system's current MAC address.

Keyword	Returned Value
$oldmacAddress	The end-system's previous MAC address.
$ipAddress	The end-system's current IP address.
$oldipAddress	The end-system's previous IP address.
$username	The current username used to authenticate the end-system.
$oldusername	The previous username used to authenticate the end-system.
$hostname	The end-system's hostname.
$oldhostName	The end-system's previous hostname.
$operatingSystemName	The full operating system running on the end-system.
$oldoperatingSystemName	The previous full operating system the end-system was running.
$ESType	The end-system's current operating system family (for example, Windows, Mac, or Linux).
$oldESType	The end-system's previous operating system family (for example, Windows, Mac, or Linux).
$state	The end-system's current state: ACCEPT, REJECT, SCAN, QUARANTINE, DISCONNECTED, or ERROR.
$oldstate	The end-system's previous state: ACCEPT, REJECT, SCAN, QUARANTINE, DISCONNECTED, or ERROR.
$stateDescr	A description of the end-system's current state.
$oldstateDescr	A description of the end-system's previous state.
$extendedState	An extended description of the end-system's current state.
$oldextendedState	An extended description of the end-system's previous state.
$switchIP	The IP address of the switch to which the end-system is currently connected.
$oldswitchIP	The IP address of the switch to which the end-system was previously connected.

Keyword	Returned Value
$switchLocation	The physical location of the switch the end-system is currently connected to (for example, the building/floor location).
$oldswitchLocation	The physical location of the switch the end-system was previously connected to (for example, the building/floor location).
$switchPort	The ifIndex of the switch port the end-system is currently connected to.
$oldswitchPort	The ifIndex of the switch port the end-system was previously connected to.
$switchPortId	The name of the switch port the end-system is currently connected to (for example, ge.1.1).
$oldswitchPortId	The name of the switch port the end-system was previously connected (for example, ge.1.1).
$authType	The latest authentication method used by the end-system to connect to the network.
$oldauthType	The previous authentication method used by the end-system to connect to the network.
$allAuthTypes	A comma-separated list of authentication types currently used for this end-system in its current location. The list is only provided if there is more than one authentication type.
$oldallauthTypes	A comma-separated list of authentication types previously used for this end-system in its current location. The list is only provided if there is more than one authentication type.
$nacProfileName	The Extreme Access Control profile currently assigned to the end-system.
$oldnacProfileName	The Extreme Access Control profile previously assigned to the end-system.
$reason	The reasons why the end-system is assigned its current Extreme Access Control profile or is in a particular state.

Keyword	Returned Value
$oldreason	The reasons why the end-system was assigned its previous Extreme Access Control profile or is in a particular state.
$policy	The access policy currently assigned to the end-system, if on a policy-based switch.
$oldpolicy	The access policy previously assigned to the end-system, if on a policy-based switch.
$firstSeentime	The first time the end-system was seen by the Extreme Access Control engine.
$lastSeenTime	The last time the end-system was seen by the Extreme Access Control engine.
$oldlastSeenTime	The previous last time the end-system was seen by the Extreme Access Control engine.
$nacApplianceIp	The IP address of the Extreme Access Control engine on which the end-system authenticated.
$oldnacApplianceIp	The IP address of the previous Extreme Access Control engine on which the end-system authenticated.
$nacapplianceGroupName	The engine group for the Extreme Access Control engine where the end-system was last heard.
$oldnacApplianceGroupName	The previous engine group for the Extreme Access Control engine where the end-system was last heard.
$lastScanTime	The last time a scan was performed on the end-system.
$lastScanResultState	The resulting state of the last scan: ACCEPT, QUARANTINE, or empty.
$ssid	The Service Set Identifier (SSID) of the wireless network to which the end-system is connected.
$oldssid	The Service Set Identifier (SSID) of the wireless network to which the end-system was previously connected.

Keyword	Returned Value
$wirelessAp	The name of the Wireless Access Point (AP) to which the end-system is connected. If the AP's name is unavailable, then the AP's MAC address is reported. If the MAC address is unavailable, then the AP's serial number is reported.
$oldwirelessAp	The name of the Wireless Access Point (AP) to which the end-system was previously connected. If the AP's name is unavailable, then the AP's MAC address is reported. If the MAC address is unavailable, then the AP's serial number is reported.
$ifAlias	The ifAlias of the switch port to which the end-system is currently connected.
$oldifAlias	The ifAlias of the switch port to which the end-system was previously connected.
$ifDescription	The ifDescription of the switch port to which the end-system is currently connected.
$oldifDescription	The ifDescription of the switch port to which the end-system was previously connected.
$ifName	The ifName of the switch port to which the end-system is currently connected.
$oldifName	The ifName of the switch port to which the end-system was previously connected.
$custom1	The text from the Custom 1 end-system information column.
$custom2	The text from the Custom 2 end-system information column.
$custom3	The text from the Custom 3 end-system information column.
$custom4	The text from the Custom 4 end-system information column.
$regName	The registered username supplied by the end user during the registration process.

Keyword	Returned Value
$regEmail	The email address supplied by the end user during the registration process.
$regPhone	The phone number supplied by the end user during the registration process.
$regData1	The text from the Custom 1 registration field supplied by the end user during the registration process.
$regData2	The text from the Custom 2 registration field supplied by the end user during the registration process.
$regData3	The text from the Custom 3 registration field supplied by the end user during the registration process.
$regData4	The text from the Custom 4 registration field supplied by the end user during the registration process.
$regData5	The text from the Custom 5 registration field supplied by the end user during the registration process.
$regDeviceDescr	The device description supplied by the end user during the registration process.
$regSponsor	The registered device's sponsor.
$memberOfGroups	The current list of MAC end-system groups listed in the Groups end-system information column.
$oldmemberOfGroups	The previous list of MAC end-system groups listed in the Groups end-system information column.
$groupDescr1	The entry description that was entered when the end-system was added to a MAC-based end-system group.
$groupDescr2	The entry description that was entered when the end-system was added to a MAC-based end-system group.
$groupDescr3	The entry description that was entered when the end-system was added to a MAC-based end-system group.
Registration Keywords	

Keyword	Returned Value
$category	The type of action that was performed, for example: Registered Device Added, Registered Device Updated, Registered User Added; Registered Device Removed, Registered User Removed.
$time	The time the end-system registered to the network.
$source	The MAC address of the registered device or the name of the registered user.
$message	A message describing the action that was performed (for example, Added Registered Device for User: <username> - MacAddress: <MAC address>).
Health Result Keywords	
$macAddress	The end-system's MAC address.
$ipAddress	The end-system's IP address.
$startScanDate	The date and time the scan started.
$endScanDate	The date and time the scan ended.
$hostUnreachable	Whether the host was unreachable before or after the scan was run: true or false.
$testSets	A list of test sets that were run during assessment.
$totalScore	The total sum of the scores for all the health details for the health result.
$topScore	The highest score received for a health detail in the health result.
$riskLevel	The risk level assigned to the end-system based on the health result.
$riskLevelReason	The reason the health result was placed into the specified risk level.
$assessmentSummary	A list of all the test cases that were run against the device during assessment.
$statusDetail	A list of the vulnerabilities that were found during assessment.

Keyword	Returned Value
$assessmentServerIpAddress	The IP address of the assessment server that performed the scan.
$assessmentServerName	The name of the assessment server that performed the scan.
User Group Keywords	
$name	The name of the user group.
$createdBy	The name of the user that created the user group.
$creationTime	The time and date the user group was created.
$description	A description of the user group (if one was defined when the group was created).
$added	A comma-separated list of user entries that were added to the group during the change.
$removed	A comma-separated list of user entries that were removed from the group during the change.
$lastModifiedTime	The last time the user group was modified.
$oldlastModifiedTime	The previous last time the user group was modified.
$lastModifiedBy	The name of the user who most recently edited the user group.
$oldlastModifiedBy	The name of the user who had previously edited the user group.
$revisionCounter	The current revision count (the number of changes that have been made) for the user group.
$oldrevisionCounter	The previous revision count (the number of changes that have been made) for the user group.
$listtype	One of the following types: Username, LDAP User Group, RADIUS User Group.
End-System Group Keywords	
$name	The name of the end-system group.
$createdBy	The name of the user that created the end-system group.
$creationTime	The time and date the end-system group was created.

Keyword	Returned Value
$description	A description of the end-system group (if one was defined when the group was created).
$added	A comma-separated list of end-system entries that were added to the group during the change.
$removed	A comma-separated list of end-system entries that were removed from the group during the change.
$lastModifiedTime	The last time the end-system group was modified.
$oldlastModifiedTime	The previous last time the end-system group was modified.
$lastModifiedBy	The name of the user who most recently edited the end-system group.
$oldlastModifiedBy	The name of the user who had previously edited the end-system group.
$revisionCounter	The current revision count (the number of changes that have been made) for the end-system group.
$oldrevisionCounter	The previous revision count (the number of changes that have been made) for the end-system group.
$listtype	One of the following types: MAC, IP, Hostname.

Related Information

For information on related windows:

- Extreme Access Control Options Panel

Allowed Web Sites

Use this window to configure the web sites end users are allowed to access during the Extreme Access Control Assisted Remediation and Registration process. This window is configured as part of your portal configuration, and is accessed by clicking the **Open Editor** button in the Network Settings panel of the Portal Configuration tree.

There are three subtabs in the window: Allowed URLS, Allowed Domains, and Web Proxy Servers.

Allowed URLs

This tab lists the URLs that end-systems can access while the end-system is being assessed, when the end-system is quarantined, or when the end-system is not registered on the network. The Extreme Access Control engine proxies these HTTP connections to the allowed URLs as long as the engine is configured with an appropriate DNS server.

Any URLs that you may have referenced in the captive portal configuration must be entered into this tab so an end-system with restricted access to the network is permitted to communicate to the URL. For example, a URL entered in the Helpdesk Information section should be entered here so a quarantined end-system may access the Helpdesk web site while quarantined.

Enter the URL you want to add to the list and click **Add**. URLs must be entered without "http://www". For example, if "http://www.apple.com" is an allowed website, then enter "apple.com" as the allowed URL.

You can use the **Import** button to import a file of URLs to the list. Files must be formatted to contain one URL per line. Lines starting with "#" or "//" are ignored.

NOTE: It is not necessary to enter URLs that are accessed over secure HTTP (HTTPS). To restrict access to these URLs, you must configure network policy to allow or disable HTTPS traffic all together or restrict it to specific IP ranges.

When an allowed URL is added, all web pages located within the directory are also allowed. For example, if apple.com is configured as an allowed URL, then HTTP connections for the following URLs are also permitted:

```
www.apple.com/downloads
www.apple.com/downloads/macosx
```

HTTP connections to URLs located on different hosts than that of the allowed URL entry are not permitted. These HTTP connections are redirected to the Assisted Remediation or MAC Registration web page. Using the same example, if apple.com is configured as an allowed URL, HTTP connections for the following URLs are not allowed:

```
store.apple.com
store.apple.com/download
```

Images on the web page may not be displayed properly if the images are served on a separate HTTP connection at a different URL. For example, the web page `http://www.apple.com/support/downloads/` contains images downloaded from `http://images.apple.com`. Therefore, if `apple.com/support/downloads/` is configured as an allowed URL, all of the text on the web page would be displayed properly, but the images would not be displayed on the web page unless `images.apple.com` is also entered as an Allowed URL.

Allowed Domains

This tab lists the domains to which end users can browse while the end-system is being assessed, the end-system is quarantined, or when the end-system is not registered on the network. The Extreme Access Control engine proxies these HTTP connections to the allowed domains as long as the engine is configured with an appropriate DNS server.

The higher-level domain information not explicitly specified in an allowed domain entry are also permitted for an end-system as well as any web pages served from within the domain. For example, if apple.com is configured as an allowed domain, then HTTP connections for the following URLs are also permitted:

```
www.apple.com
www.info.apple.com
store.apple.com
store.apple.com/info
images.apple.com
www.apple.com/software
apple.com/software
```

HTTP connections not matching the specified domain level information in an allowed domain entry are not permitted. These HTTP connections are redirected

to the Assisted Remediation or Registration web page. Using the same example, if apple.com is configured as an allowed domain, HTTP connections for the following URLs are not allowed:

```
www.apple2.com
store.apple-chat.com
www.msn.com
```

If multiple allowed domain entries are configured with overlapping first-level and second-level domain information, then the allowed domain entry that is more specific takes precedence. For example, if `apple.com` and `store.apple.com` are configured as allowed domain entries, then the `apple.com` entry is effectively disabled. Therefore, HTTP connections for the following URLs are allowed:

```
store.apple.com
store.apple.com/info
www.store.apple.com/info
```

The following HTTP connections are not allowed:

```
www.apple.com
www.apple.com/support
images.apple.com
```

The following is a list of default allowed domains that are pre-configured for Extreme Access Control remediation. These allowed domains are provided as part of the assisted remediation assessment functionality, which allows end-users limited Internet access to update patches, antivirus definitions, and to upgrade vulnerable software in order to comply with the network security policy. The Extreme Access Control engine proxies traffic to these allowed domains when an end user clicks on a remediation link presented on the violations page.

A default allowed domain should only be deleted if it is determined that a quarantined user should not be able to access it. In some cases, you may need to add additional URLs or domains. If a quarantined user selects a remediation link to resolve an issue and is redirected back to the remediation web page, the domain or URL needs to be added to provide access to that site.

adobe.com	akadns.net	akamai.com
akamai.net	altn.com	apache.org
apple.com	archives.neohapsis.com	asp.net

aws.amazon.com	bitdefender.com	bugzilla.org
ca.com	cdnetworks.com	cert.org
cisco.com	clamav.net	cve.mitre.org
debian.org	drupal.org	eset.com
eu.ntt.com	f-secure.com	gnu.org
godaddy.com	ibm.com	ipswitch.com
isc.org	kaspersky.com	lac.co.jp
level3.com	localmirror.com	kaspersky-labs.com
macromedia.com	mandriva.com	mcafee.com
microsoft.com	mozilla.org	mysql.com
netwinsite.com	norton.com	novell.com
nsatc.net	openssl.org	oracle.com
osvdb.org	pandasecurityusa.com	php.net
phpnuke.org	redhat.com	samba.org
secunia.com	securiteam.com	securityfocus.com
securitytracker.com	sendmail.org	sophos.com
sourceforge.net	squid-cache.org	sun.com
support.citrix.com	suse.com	suse.de
symantec.com	symantecliveupdate.com	techtarget.com
trendmicro.com	ubuntu.com	us-cert.gov
verisign.com	verisigninc.com	vmware.com
vupen.com	web.mit.edu	webroot.com
windows.com	windowsupdate.com	wireshark.org
xforce.iss.net	zerodayinitiative.com	zope.org

Web Proxy Servers

This tab is used to specify the web proxy server(s) deployed on the network. The Extreme Access Control engine proxies end-system Allowed URL and Allowed Domain HTTP traffic to the defined web proxy servers if the network utilizes proxy servers to access the Internet.

If multiple web proxy servers are configured, the Extreme Access Control engine round robins HTTP connections to the configured proxy servers. If the allowed web site is located with the Extreme Access Control engine's configured domain, the Extreme Access Control engine directly contacts the web site and does not go through the configured web proxy servers.

Related Information

For information on related help topics:

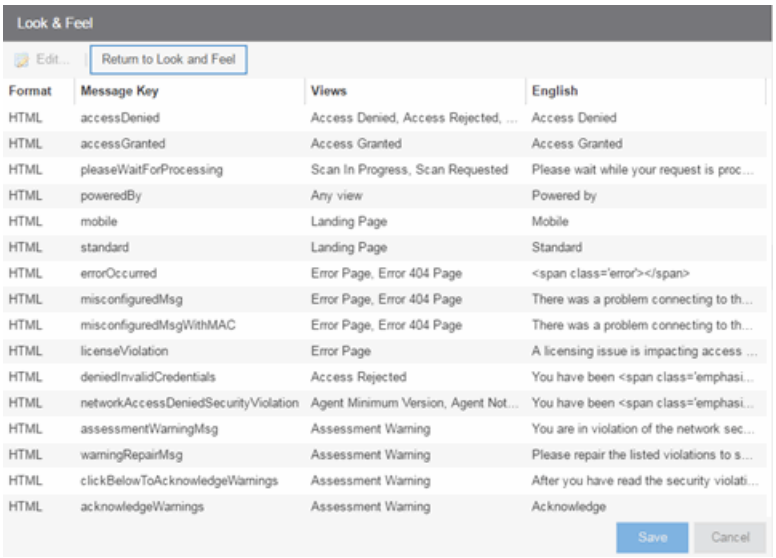
- Edit Portal Configuration Panel

Message Strings Editor

The Message Strings Editor is where you can edit the text and formatting of the various system-defined messages used on the portal web pages, or add a custom message string, if desired. You can also import a file of message strings or export message strings to a file.

To access the Editor, click the Message Strings Launch Message Strings Editor button in the Portal Look and Feel view in the Control > Access Control tab. Message strings are listed alphabetically according to the Message Key, which is the message identifier. Double-click a message string to open a window where you can edit the message.

Click the down arrow in the right corner of the column header to filter and sort information in the table, and add or remove columns from the table.



Edit... Edit Message

Select a message in the table and click this button (or double-click the message) to open the Modify Localized Entry window where you can modify the text for the message. Use the Next/Previous buttons in the window to cycle through all the message strings for easy editing.

NOTE: To change the Message Key for a user-defined message, you must delete and recreate the message using the new key.

Message Strings Table

This table displays all the message strings used in the Access Control tab. It includes the following columns:

- Format — Displays the supported format for the message text: HTML or Text.
- Message Key — The message identifier.
- Views — The portal views where this message is used.
- English — The text of the message.
- Additional columns for each supplemental locale (language) you have configured in the portal configuration.

Related Information

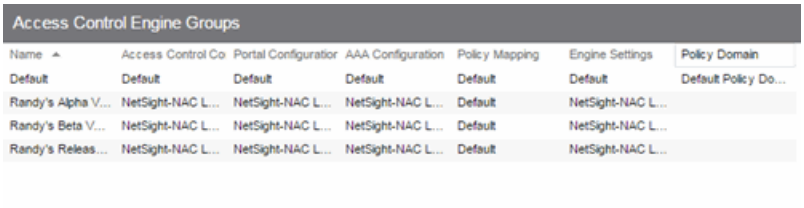
For information on related help topics:

- Portal Configuration

Extreme Access Control Engine Groups

The Extreme Access Control Engine Groups panel is displayed in the right panel when you select the Extreme Access Control Engine Groups folder in the left panel. (The Extreme Access Control Engine Groups folder is only displayed if you have created engine groups.) The tab displays a table of information about the engine groups in the folder.

Use the table options and tools to filter, sort, and customize table settings. You can access the options by clicking the down arrow in the right corner of any column header.



Name

The name of the engine group.

Extreme Access Control Configuration
The Extreme Access Control Configuration currently selected for this engine group.

Portal Configuration
If your network is implementing Registration or Assisted Remediation, the Portal Configuration that defines the branding and behavior of the website used by the end user during the registration or remediation process.

AAA Configuration
The AAA Configuration used by this engine group.

Policy Mapping
The Default policy mapping can be viewed in the Extreme Access Control Configurations tree (under Extreme Access Control Profiles) or accessed from the Edit Extreme Access Control Profile window.

Engine Settings
The Engine Settings configured for the group. Use the Edit Engine Settings window to specify and configure engine settings.

Related Information

For information on related windows:

- Edit Portal Configuration Window

Group Editor

This panel lists the various rule groups used to define the criteria for the rules used in your Extreme Access Control configuration. You can use this window to view and edit the defined rule groups and also to add new rule groups for use in your Extreme Access Control configuration. Any changes made in this window are written immediately to the Extreme Management Center database.

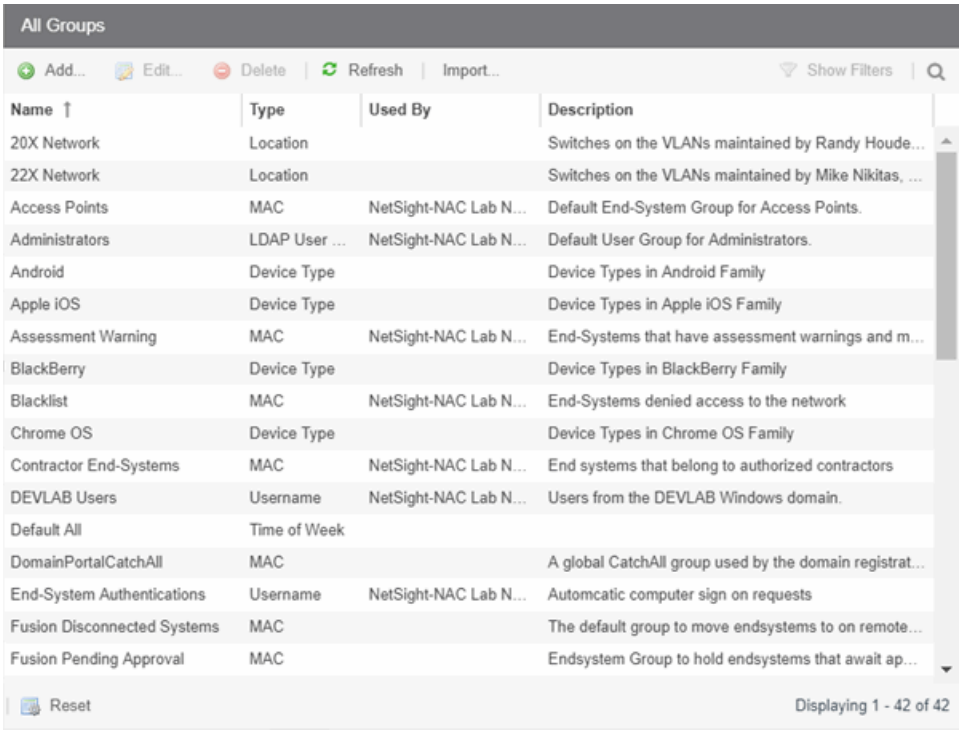
Extreme Management Center comes with system-defined rule groups. Extreme Management Center also contains system-defined end-system groups that automatically populate. The Assessment Warning end-system group includes end-systems that have assessment warnings and must acknowledge them before being granted access to the network. The Blacklist end-system group includes end-systems denied access to the network. The other system-defined groups are populated as the end-systems register through the Registration portal.

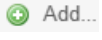
Select from the following rule group categories when you create a new rule group:

Category	Group Types	Value Types
All Groups	All Types	A list of all group types.
Device Type Groups	Device Type	A list of device types.
End-System Groups	Hostname	A list of hostnames, which can be an exact match or wild card (for example, *.extremenetworks.com).
	IP	A list of IP addresses or subnets.
	LDAP Host Group	A way to group hosts by doing an LDAP lookup on the resolved hostname of the end-system detected on the network, which can be an exact match or wild card.
	MAC	A list of MAC addresses, MAC OUI, or MAC masks.
Location Groups	Location	A list of switches, switches and ports, or switches and SSIDs.

Category	Group Types	Value Types
Time Groups	Time of Week	A list of the times of the week when the end user is accessing the network. You can only add a new Time Group via NAC Manager.
User Groups	LDAP User Group	A list imported from an LDAP Server, organized by Organization Unit (OU), which can be an exact match or wild card.
	RADIUS User Group	A list of attributes returned by the RADIUS server, which can be an exact match or wild card.
	Username	A list of usernames, which can be based on an exact match or a wild card.

To access this window, open the **Access Control** tab and select Extreme Access Control Configurations > Group Editor in the left-panel.



Add Button 

Use this button to add rule groups or to import MAC entries from a file for viewing and assigning to various end-system groups.

Edit Button 

Use this button to edit existing rule groups.

Delete Button Delete
Use this button to delete existing rule groups.

Import button
Use this button to import group entries from files.

Name
The name of the rule group.

Type
The type selected for the specific rule group; for example, an end-system group could have a type of MAC.

Used By
The name of the Identity and Access configuration using this rule group.

Description
A description of the rule group.

Related Information

For information on related windows:

- Create Rule Window

Add/Edit Device Type Group

There are nine system-defined operating system family device type groups that are automatically populated by Extreme Management Center: Android, Apple iOS, Blackberry, Chrome OS, Game Console, Linux, Mac, Windows, and Windows Mobile. You can view these system-defined groups and your other device type groups by expanding the Extreme Access Control Configurations > Group Editor > Device Type Groups left-panel tree.

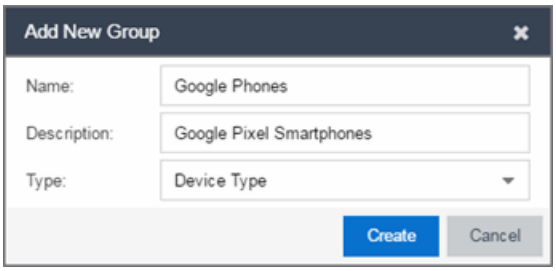
Device type groups are comprised of entries that Extreme Access Control uses to determine if an end-system's device type matches the group. Entries can be a specific device type or a wildcard, such as Windows 7 or win*. If an entry does not already contain a wildcard, Extreme Management Center creates a wildcard by adding an asterisk (*) to the beginning and end of the entry. For example, if the entry is Gentoo, the match pattern is *Gentoo* allowing a match for any end-system device type that contains Gentoo. This allows you to restrict the match to a very specific value that might include a version number or model number, or expand the match to include all versions and model numbers of a certain operating system or hardware family.

For additional information about how to use device type groups, see How to Use Device Type Profiling.

NOTE: Changes to rule groups do not require an enforce. Changes are automatically synchronized with engines on the next status update. Changes do not affect end-systems until the next authentication and/or assessment occurs.

To access the Add New Group window, click Add (Add...) in the Device Type Groups right panel.

The Add New Group window opens.



Name

Enter a new name for the device type group. Once a group is created, you cannot edit the name of the group.

Description

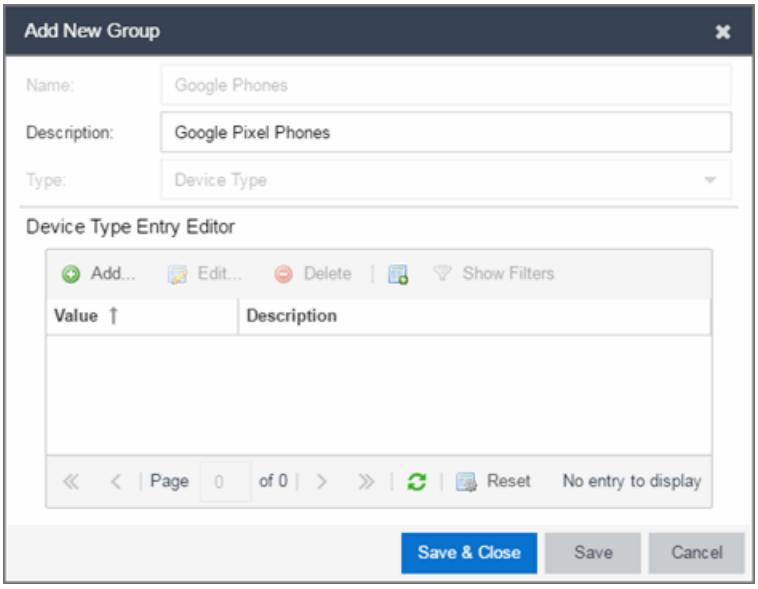
Enter a description of the device type group.

Type

To create a new device type group, select **Device Type** from the drop-down menu.

Click the **Create** button to open the Device Type Entry Editor section of the window.

Click the **Select from Existing Types** button ( ) to open the Select Device Types window from which you can choose a list of predefined entries. Click the **Add** button in the Device Type Entry Editor section of the window to open the Add Entry window.



Use this window to add a new entry by entering a device type or a wildcard, such as Google Pixel or *pixel. Alternately, you can select a type from a list of entries that already appear in existing device type groups from the Select Device Types window. This window can be accessed by clicking the **Select from Existing Types** button. This list allows you to multi-select entries, and each entry appears as a separate row in the table. The list also allows you to select **Unknown** that matches against any device that does not have an operating system name, either due to failed detection or because detection hasn't happened yet.

All entries selected from the list are assigned the same description. If you would like a separate description for each type, you need to add each entry individually.

Related Information

For information on related windows:

- Create Rule Window
- Manage Rule Groups Window

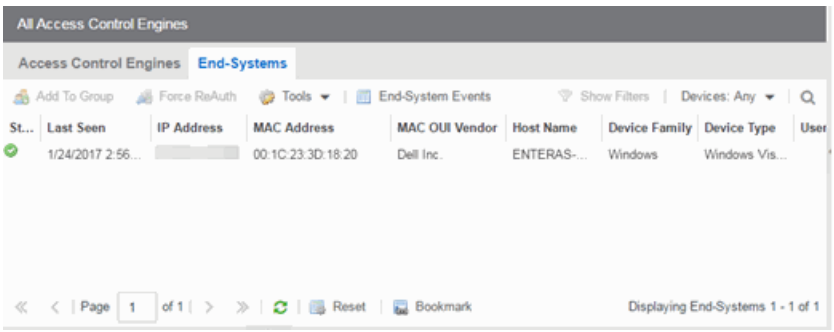
End-Systems

The End-Systems tab presents end-system connection information for a single Extreme Access Control engine, all Extreme Access Control engines, or all the engines in an engine group, depending on what you select in the left-panel tree. You can also monitor end-system events and view the health results from an end-system's assessment.

The End-Systems tab is the first tab displayed when accessing the Control > Access Control tab. A high-level overview of the functionality found in the Extreme Access Control tab is also available.

To access this tab, select a single Extreme Access Control engine, the All Extreme Access Control Engines folder, or an engine group in the left-panel tree, then click the End-Systems tab in the right panel.

Use the table options and tools to filter, sort, and customize table settings. Access the options by clicking the down arrow in the right corner of any column header.



End-Systems

This table displays the last known connection state for each end-system that has attempted connection.

State

The end-system's connection state:

- Scan — The end-system is currently being scanned.
- Accept — The end-system is granted access with either the Accept policy or the attributes returned from the RADIUS server.
- Quarantine — The end-system is quarantined because the assessment failed.
- Reject — The end-system was rejected because the assigned Extreme Access Control profile was set to Reject, the MAC Locking test failed, or the RADIUS server was reachable but rejected the authentication request.
- Disconnected — All sessions for the end-system are disconnected. This state is only applicable for end-systems connected to switches that have RADIUS accounting enabled.
- Error — Indicates one of nine problems:
  - the MAC to IP resolution failed, if assessment is enabled
  - the MAC to IP resolution timed out, if assessment is enabled
  - all RADIUS servers are unreachable
  - the RADIUS request was non-compliant
  - all assessment servers are unavailable
  - the assessment server can't reach the end-system
  - no assessment servers are configured
  - the assessment server is not compatible with the current version of Extreme Access Control
  - the username and password configured in the Assessment Server panel of the Extreme Access Control options (Administration > Options > Extreme Access Control > Assessment Server) are incorrect for the assessment server.

MAC Address

The end-system's MAC address. MAC addresses can be displayed as a full MAC address or with a MAC OUI (Organizational Unique Identifier) prefix.

MAC OUI Vendor
The vendor associated with the MAC OUI.

IP Address
The end-system's IP address.

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

Switch Port
The port alias (if defined) followed by the switch port number to which the end-system connected. If the end-system is connected to a Layer 2 Extreme Access ControlController engine, this is the Extreme Access Control Controller PEP (Policy Enforcement Point) port. However, for Layer 3 Extreme Access Control Controller engines this column is blank.

If you add or update the port alias on the switch, you must enforce the Extreme Access Control engine in order for the new information to be displayed in the End-Systems table.

If you don't want the port alias displayed, remove the PORT_DESCRIPTION_FORMAT variable from the /opt/nac/server/config/config.properties file. If this variable is removed, only the switch port number is displayed.

Username
The username used to connect.

Hostname
The end-system's hostname.

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

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

Authentication Type
Identifies the latest authentication method used by the end-system to connect to the network. (For Layer 3 Extreme Access Control Controller engines, this column displays "IP.")

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 Extreme Access Control Controller engines, this column displays the policy assigned to the end-system for its authorization.

Profile

The name of the Extreme Access Control profile that was assigned to the end-system when it connected to the network.

Risk

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

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

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.

Extended State

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

State Description

This column provides more details about the end-system state.

Last Seen

The last time the end-system was seen by the Extreme Access Control engine.

First Seen

The first time the end-system was seen by the Extreme Access Control engine.

Last Scanned

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

Last Scan Result

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

Extreme Access Control Engines/Source IP

The Extreme Access Control engine to which the end-system is connecting.

Engine Group

This column is only displayed if you have multiple engine groups. It displays what engine group the Extreme Access Control engine was in when the end-system event was generated. For example, if the engine was in Engine Group A when an end-system connected, but then later the engine was moved to Engine Group B, this column would still list Engine Group A for that end-system's entry.

Switch Location

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

All Authentication Types

This column displays all the authentication methods the end-system has used to authenticate. The authentication types are listed in order of precedence from highest to lowest: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking. View details about each authentication session (such as the Extreme Access Control profile that was assigned to the end-system for each authentication type) in the End-System Events tab.

RFC3580 VLAN

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

Score

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

Top Score

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

Actual Score

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

Custom 1

Use this column to add additional information you want to display. To add or edit custom information, right-click on the table and select Edit Custom Information. You can add information for up to four Custom columns. The columns for Custom 2, Custom 3, and Custom 4 are hidden by default. To display these columns, click the down arrow to the right of the table header and select Columns > Column 2, Column 3, or Column 4.

Groups

Displays any end-system and/or user groups to which the end-system belongs.

Zone

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

Actions

TIP: These actions are also available from the right-click menu off an end-system entry in the table.

Force Reauth

Forces the selected end-system to re-authenticate. End-systems authenticated to a VPN device are disconnected from the VPN.

Force Reauth and Scan

Forces the selected end-system to re-authenticate and undergo an assessment (scan). (End-systems authenticated to a VPN device are disconnected from the VPN.) The assessment only takes place if scanning is enabled in the Extreme Access Control profile assigned to the end-system.

Add to Group

Lets you add the selected end-system to a specific end-system or user group. If the end-system is a registered device, it can be added to a registration group. After adding an end-system to a group, any rules created that involved that group apply to the end-system as well. Changes to end-system group membership do not require an enforce and are synchronized with engines immediately. Changes do not affect the end-system until the next authentication or assessment occurs.

Lock MAC

Opens the Add MAC Lock window where you can lock the MAC address of the selected end-system to a switch or switch and port.

Show Details

Opens the End-System Details tab where you can view summary information for the end-system selected in the table.

Delete

Deletes the selected end-system entries from the table and also deletes the associated end-system events. You are given the option to delete any custom information, group assignment, MAC locks, and registration and web authentication associated with the end-systems.

The Force Delete of End-System option completely deletes the end-system from Extreme Management Center, regardless of whether the end-system reauthentication is successful when the delete is executed. The option is deselected by default. When deselected, it prevents possible synchronization conditions where the authentication session remains active on the switch even though the end-system has been deleted from Extreme Management Center. These conditions can occur when there are underlying issues that prevent the end-system reauthentication from completing properly.

NOTES: The Delete operation does not remove an end-system from the Blacklist group. Blacklist is a special group that requires end-systems to be manually removed using the Edit End-System Group window.

Deleting an end-system from the table also deletes the user's current authentication. If the user is connected to the network at the time of the delete, they are forced to re-authenticate.

Menu Buttons

The menu at the top of the window contains most of the options available via a right-click previously mentioned in the Actions section above, as well as the End-System Events button, described below.

End-System Events

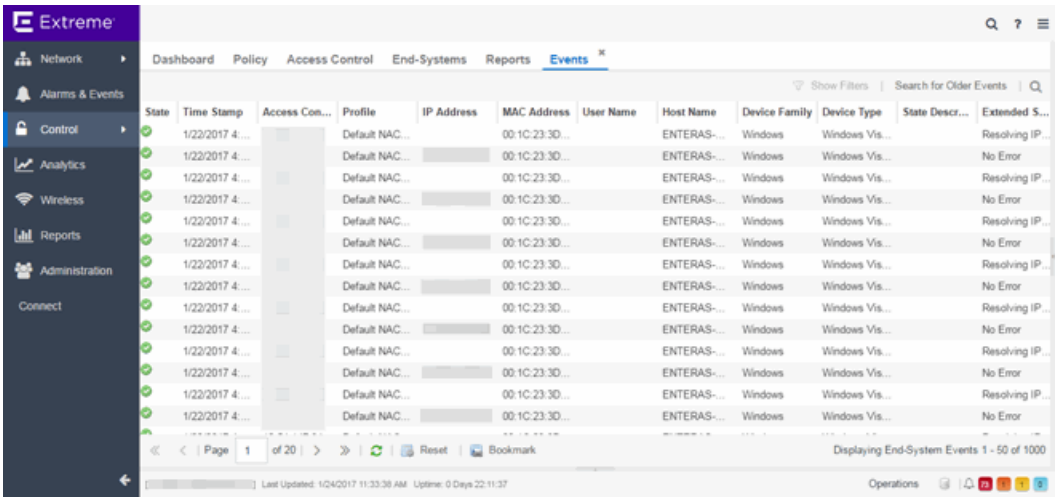
Opens the End-System Events tab where you can view information about events for the end-system selected in the table.

End-System Events Tab

This tab displays historical connection information for the end-system selected in the table above. End-system events are stored daily in the database. In addition, the end-system event cache stores in memory the most recent end-

system events and displays them here in this tab. This cache allows Extreme Management Center to quickly retrieve and display end-system events without having to search through the database. You can configure parameters for the event cache (such as the number of events to display) using the End-System Event Cache options in the Extreme Access Control Options view (Administration > Options > Extreme Access Control > End-Systems Event Cache).

NOTE: The **End-System Events** tab displays events up to the most recent delete event for the end-system, if one exists. If you want to see events that happened prior to the most recent delete event, use the **Search for Older Events** button.



State

The end-system's connection state:

- Scan — The end-system was scanned.
- Accept — The end-system was granted access with either the Accept policy or the attributes returned from the RADIUS server.
- Quarantine —The end-system was quarantined because the assessment failed.
- Reject — The end-system was rejected because the assigned Extreme Access Control profile was set to Reject, the MAC Locking test failed, or the RADIUS server was reachable but rejected the authentication request.
- Disconnected — This end-system session was disconnected, however other sessions for the end-system may still be active. For example, the end-system may have a disconnected session with an authentication type of 802.1X, but

still have an active MAC authentication session. This state is only applicable for end-systems connected to switches that have RADIUS accounting enabled.

- Error — Indicates one of nine problems:
  - the MAC to IP resolution failed
  - the MAC to IP resolution timed out
  - all RADIUS servers are unreachable
  - the RADIUS request was non-compliant
  - all assessment servers are unavailable
  - the assessment server can't reach the end-system
  - no assessment servers are configured
  - the assessment server is not compatible with the current version of Extreme Management Center
  - the username and password configured in the Assessment Server panel of the Extreme Access Control options (Administration > Options > Extreme Access Control > Assessment Server) are incorrect for the assessment server

Time Stamp
The date and time the end-system connected.

IP Address
The end-system's IP address.

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

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

Switch Port
The switch port number to which the end-system is connected. If the end-system is connected to a Layer 2 Extreme Access Control Controller engine, this is the Extreme Access Control Controller PEP (Policy Enforcement Point) port. However, for Layer 3 Extreme Access Control Controller engines this column is blank.

Username
The username used to connect.

Hostname
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.

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

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

Profile
The name of the Extreme Access Control 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 provides information as to the reason a policy is applied to the end-system or the reason the end-system is rejected.

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

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.

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

Engine Group

This column is only displayed if you have multiple engine groups. It displays what engine group the Extreme Access Control engine is in when the end-system event was generated. For example, if the engine began in Engine Group A when an end-system connected, then the engine is moved to Engine Group B, this column still lists Engine Group A for that end-system's entry.

Zone

Displays the end-system zone to which the end-system is assigned. For additional information, see End-System Zones.

Search for Older Events

This button lets you search for older events stored in the database outside of the end-system events cache. The maximum search parameters for this extended search are configured in the End-System Event Cache options in the Extreme Access Control Options view (Administration > Options > Extreme Access Control > End-System Event Cache). The search is ended when any one of the parameters is reached.

- Maximum number of results to return from search
- Maximum time to spend searching for events (in seconds)
- Maximum number of days to go back when searching

Related Information

For information on related topics:

- Add MAC Lock Window
- End-System Details Tab

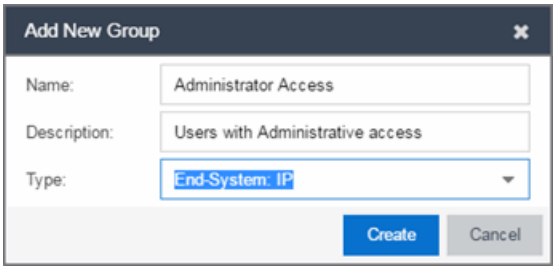
Add/Edit End-System Group

Use this window to add a new end-system group or edit an existing end-system group. End-system groups are rule components that allow you to group together devices having similar network access requirements or restrictions. You can access the Add/Edit End-System Group window from the Manage Rule Groups window or from the end-system group field in the Create Rule window.

There are six system-defined end-system groups automatically populated by Extreme Management Center. The first is the Assessment Warning end-system group that includes end-systems that have assessment warnings and must acknowledge them before being granted access to the network. The second is the Blacklist end-system group that includes end-systems denied access to the network. The other four system-defined groups are populated as end-systems register through the Registration portal.

You can access the Add/Edit Location Group window by accessing the **Access Control** tab and selecting Extreme Access Control Configurations > Group Editor > End-System Groups in the left-panel menu and clicking the **Add** button in the right panel.

NOTE: Changes to rule components do not require an enforce. Changes are automatically synchronized with engines on the next status update. Changes do not affect end-systems until the next authentication and/or assessment occurs.



Name

Enter a new name for the end-system group. You cannot edit the name of a group.

Description

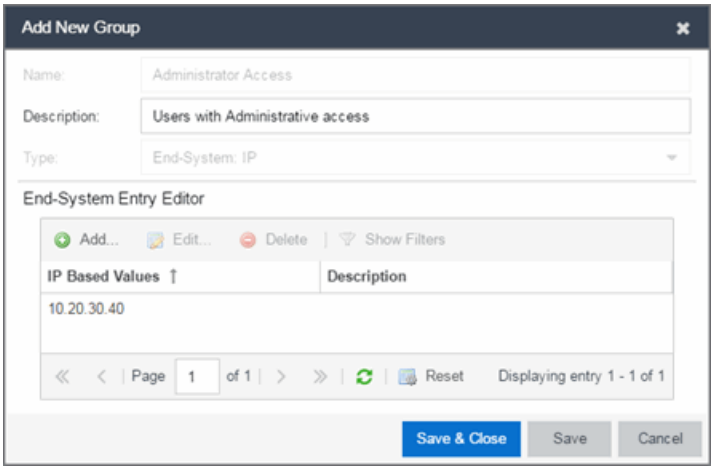
Enter a description of the end-system group. If you are using Data Center Manager (DCM), the end-system group description contains the DCM specific settings as key/value pairs.

Type

Specify whether the end-system group be based on:

- MAC - a list of MAC addresses, MAC OUI, or MAC Masks.
- IP - a list of IP addresses or subnets.
- Hostname - a list of hostnames: exact match or wild card (for example, *.extremenetworks.com).
- LDAP Host Group - a way to group hosts by doing an LDAP lookup on the resolved hostname of the end-system detected on the network. Note for the standard use with Active Directory, the Engine Settings > Hostname Resolution must be configured to use DNS Hostname Resolution so Extreme Management Center can resolve the Fully Qualified Domain Name. In the LDAP configuration, you must also have the "Use Fully Qualified Domain Name" checkbox selected.

Click **Create** to display the End-System Entry Editor section of the window. This section varies depending on the **Type** selected.



Value

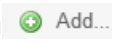
The MAC address, IP address, Hostname, or Attribute value of the end-system.

Description

The description of the end-system group.

Mode

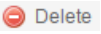
For LDAP Host Groups, the mode option lets you specify whether to match any or match all of the LDAP attributes listed below. You can also use "Exists" to just check to see if a host is present in LDAP.

Add Button 

Click the Add button to open the Add Entry window, from which you can add an entry to the Entry Editor section.

Edit Button 

Select an entry in the Entry Editor section of the window and click the Edit button to open the Edit Entry window, from which you can edit an existing entry.

Delete Button 

Select an entry in the Entry Editor section of the window and click the Delete button to delete an existing entry.

Save Button

Click the Save button to save the location group.

Use the Multiple MAC OUI Entries button to open a window where you can select MAC OUI vendors.

Filter

Use the Filter field to filter for a specific entry based on a numeric value or text.

Custom 1

This column allows you to add additional information. To add or edit custom information, right-click on the table entry and select Edit Custom Information. You can add information for up to four Custom columns. The columns for Custom 2, Custom 3, and Custom 4 are hidden by default. To display these columns, click the down arrow next to the Custom 1 column header and select Columns > Custom 2, Custom 3, or Custom 4.

Related Information

For information on related windows:

- Create Rule Window
- Manage Rule Groups Window

End-System Details

The End-System Details window provides connection state and assessment information for a single end-system. It is launched from the End-Systems View in the Control tab, by double-clicking any end-system in the table or selecting an end-system and then selecting Show Details from the Tools menu.

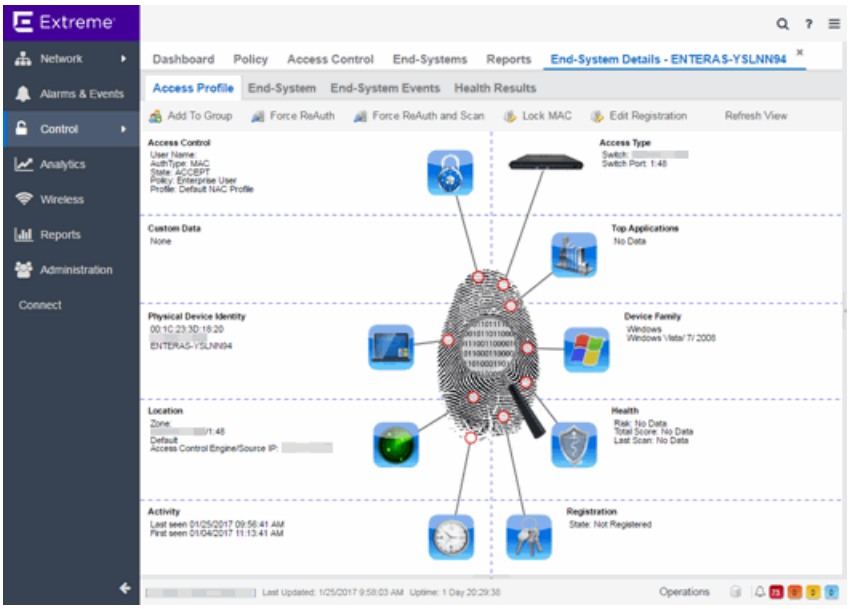
The End-System Details window has four tabs. The Access Profile tab provides end-system summary information. The End-System tab provides end-system connection state information. The End-System Event tab displays end-system event information. The Health Results tab displays end-system assessment result information.

This Help topic provides information on the four tabs:

- Access Profile Tab
- End-System Tab
- End-System Events Tab
- Health Results Tab

Access Profile Tab

The Access Profile tab presents a graphical view of end-system and health result information, providing an at-a-glance end-system summary. Click on the information in each section to link to more detailed information.



Access Type

Displays the switch IP address, port index, and port that the end-system is connected to. Click to open a PortView for the switch in a new tab.

Top Application Flows

Lists the top five applications and flow counts for the end-system, listed in descending order by flow count. Click to open the Applications Dashboard in a new tab.

Device Family

Displays the end-system's operating system (OS) family (for example: Windows, Linux, Android) and OS name. Use the device family icon to quickly determine the end-system type. Click to open the **End-System** tab where you can view additional end-system details.

Health

Displays health data from the latest scan, including risk level, total score, and last scan time. Use the health icon to quickly determine risk level by color. Click to open the **Health Results** tab where you can view additional health result information and details.

Registration

Displays the end-system's registration state, user name, and sponsor. Click to open the **End-System** tab where you can view additional registration information.

Activity
: Displays the last seen and first seen times for the end-system. Click to open the **End-System** tab where you can view additional end-system details.

Location
: Displays location summary information, including end-system zone membership, access point information, engine group, and engine IP address. Click to open the **End-System** tab where you can view additional location information.

Physical Device Identity
: Displays the end-system's MAC address, IP address, and host name. The device icon displays the end-system's physical device type with a small OS-based icon in the corner. Click to open the **End-System** tab where you can view additional end-system details.

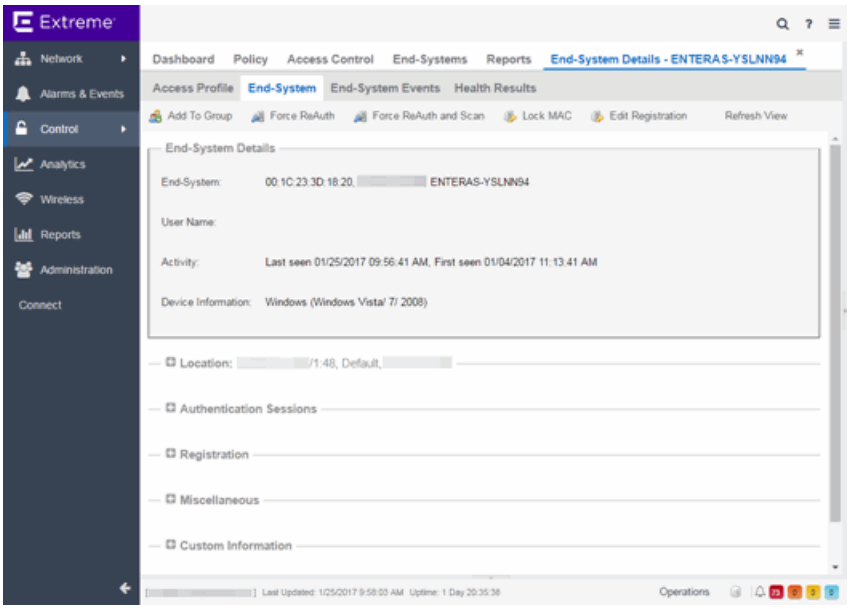
Virtual Device Identity
: If the end-system is a virtual machine, this section displays virtual device information, including VM name, ID, Guest Name, and manufacturer. Use the icon to quickly determine the virtual machine's operating system. If the end-system is not a virtual machine, this section is replaced by Custom Data.

Custom Data
: Displays any custom information associated with the end-system. Custom information for an end-system is added in the End-Systems tab or End-Systems View. If the end-system is a virtual machine, this section is replaced by Virtual Device Identity.

Identity and Access
: Displays the end-system's user name, authentication type, connection state, policy, and profile. Click to open the **End-System** tab where you can view additional end-system authentication session details.

End-System Tab

This tab presents detailed information on the selected end-system's connection, authentication, and registration. Expand the sections using the arrow buttons to see additional information.

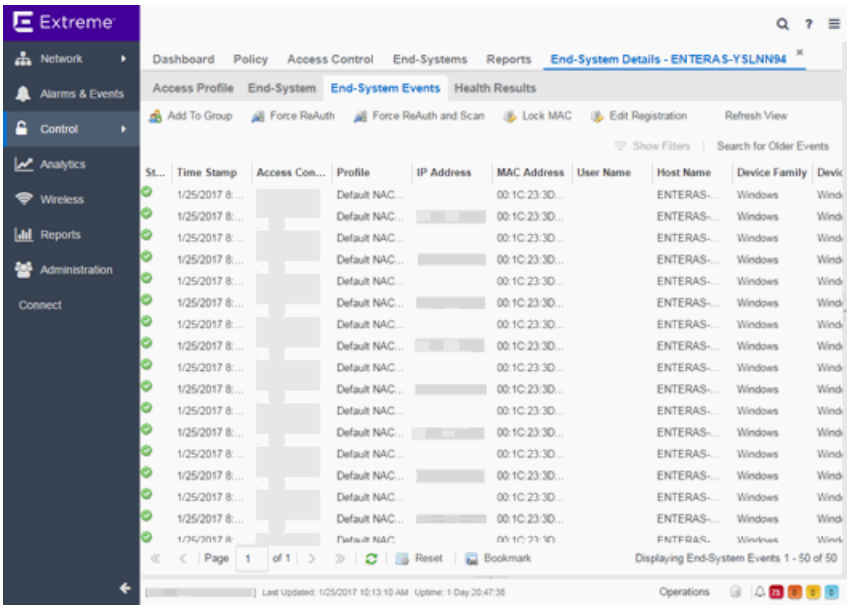


For a definition of various fields, see the End-Systems View Column Definitions section.

Changes to group membership do not require an enforce and will be synchronized with engines immediately. Changes will not affect the end-system until the next authentication or assessment occurs.

End-System Events Tab

The End-System Events tab shows all the events for the selected end-system.



You can manipulate the table data in this window in several ways to customize the view for your own needs:

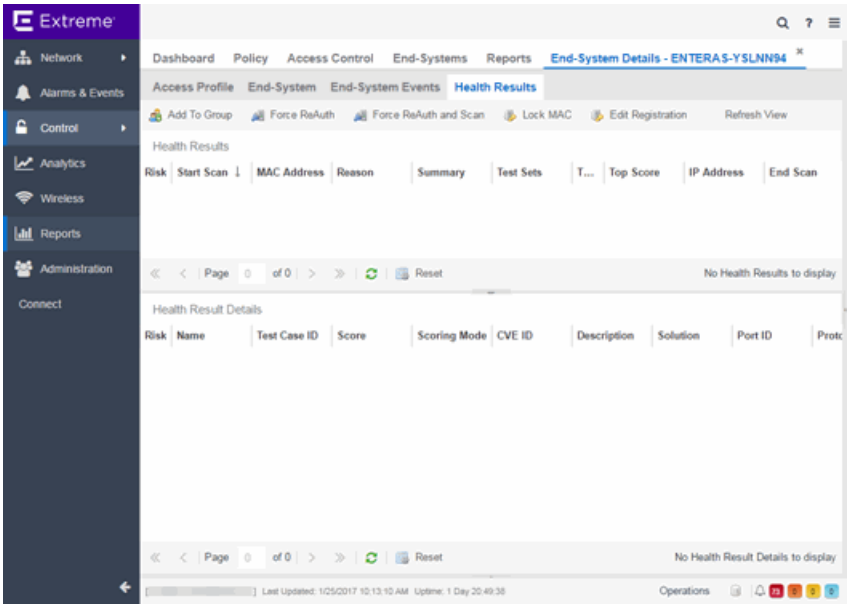
- Click on the column headings to perform an ascending or descending sort on the column data.
- Hide or display different columns by clicking on a column heading and selecting the column options from the menu.
- Rearrange columns by dragging a column heading to the desired position.
- Filter the data in each column in the table.

You can use the Search for Older Events to search for older events stored in the database outside of the end-system events cache. The maximum search parameters for this extended search are configured in the End-System Event Cache options in the Identity and Access Options view (Tools > Options). The search is ended when any one of the parameters is reached:

- Maximum number of results to return from search
- Maximum time to spend searching for events (in seconds)
- Maximum number of days to go back when searching

Health Results Tab

The top table in the Health Results tab provides summary information on scan results obtained for the selected end-system. The bottom table presents the individual health result details for the scan selected in the top table. Double-click any row in the bottom table to open the Health Result Details window and view a description, solution, and result for the health result. Information is displayed in this tab only if assessment is enabled on the network and there are health results in the database.



Health Results

This table presents health results for all the scans performed on the end-system.

Risk

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

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

Start Scan
The date and time the scan started.

MAC Address
The end-system's MAC address.

Reason
The reason the health result was placed into the specified risk level. This is based on the risk level configuration that was used for the assessment, for example, if there was one or more health result detail with a score greater than 7. If the end-system is NAP capable, then this is based on the values returned from NAP.

Summary
A list of all the test cases that were run against the device during assessment. The test case name will be listed, or if that is not available, the test case ID will be listed.

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

Total Score
The total sum of the scores for all the health details that were included as part of the quarantine decision, followed by the actual score in parenthesis. The actual score is what the total score would be if all the health details were included as part of the quarantine decision. It includes all scores, including those marked Informational and Warning. If the total score and the actual score are the same, only one score is shown.

Top Score
The highest score received for a health detail that was included as part of the quarantine decision. Scores that are marked as Informational or Warning are not considered.

IP Address
The end-system's IP address.

End Scan
The date and time the scan ended.

Server Name

The name of the assessment server. For on-board assessment servers, the name is determined by the name of the Extreme Access Control engine. For example, if you create an Extreme Access Control engine and name it MyAccessControlengine, then the on-board assessment server name will be listed as MyAccessControlengine as well.

Server IP

The IP address of the assessment server. For on-board assessment servers, the IP address is determined by the address of the Extreme Access Control engine. For example, if you create an Extreme Access Control engine with an IP address of 10.20.80.8, then the on-board assessment server IP address is listed as 10.20.80.8 as well.

Server Port

The port number on the assessment server to which the Extreme Access Control engine sends assessment requests.

Host Unreachable

Displays whether the end-system was unreachable and could not be scanned: Yes or No.

Warning Count

The total number of health result details that are marked as Warnings.

Health Result Details

This table displays the individual health result details for the scan selected in the top table. Double-click any health result detail to open the Health Result Details window that displays a description, solution, and result for the health result.

Risk

The risk level assigned to the problem found on the port:

- Red - High (corresponds to a Hole)
- Orange - Medium (corresponds to a Warning)
- Yellow - Low (corresponds to a Note)
- Black - No Result Available

Name

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

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

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

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

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

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

Description
This column lists information about the health result detail.

Solution
A solution for the problem found in the health result detail.

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

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

Value
What this specific test case is testing or checking for on the end-system.

Assessment Type
The type of assessment server used in the test set.

Remediation Success

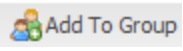
For agent-based assessment, this column lists the results of remediation attempts: Remediation Successful, Remediation Failed, or Not Applicable.

Type

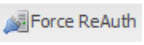
A "type" is assigned to each security risk found on a port during an assessment, and is used to determine whether to Quarantine an end-system. Types are configurable on the assessment agent. There are three types:

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

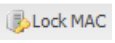
Buttons and Paging Toolbar



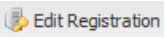
Lets you add the selected end-system to a specific end-system or user group. After adding an end-system to a group, any rules that have been created that involved that group will now apply to the end-system as well. Changes to end-system group membership do not require an enforce and will be synchronized with engines immediately. Changes will not affect the end-system until the next authentication or assessment occurs.



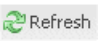
Forces the selected end-system to re-authenticate.



Opens the Add MAC Lock window where you can lock the MAC address of the selected end-system to a switch or switch and port.



Opens a window where you can edit the expiration time and maximum registered device count for the end user.

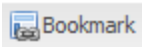


Refreshes the page.

The Health Result tables are presented in pages. The paging toolbar provides four buttons that let you easily page through the table: first, previous, next, and last page.

It also displays an indicator of the current and total number of pages. Enter a page number in the Page field and press Enter to quickly move to that page.

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. It opens a new window for the current report with a link that can be bookmarked in your browser. You can then use the bookmark whenever you want the same search, sort, and filtering options.

Related Information

For information on related tabs:

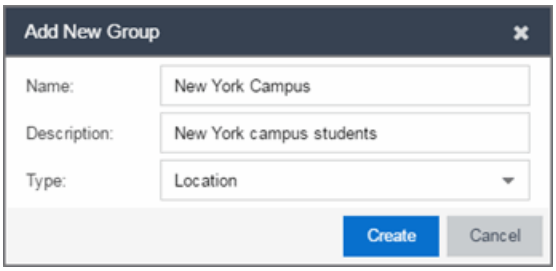
- End-Systems Tab

Add/Edit Location Group

Use this window to add a new location group or edit an existing location group. Location Groups are rule components that allow you to specify network access requirements or restrictions based on the network location where the end-user is connecting. For example, in an enterprise environment, an engineer logging on to the network from the corporate cafeteria could receive different network access than an engineer logging on from the engineering development area.

You can access the Add/Edit Location Group window by accessing the Extreme Access Control tab and selecting Extreme Access Control Configurations > Group Editor > Location Groups in the left-panel menu and clicking the Add button in the right panel.

NOTE: Changes to rule components do not require an enforce. Changes are automatically synchronized with engines on the next status update. Changes do not affect end-systems until the next authentication and/or assessment occurs.

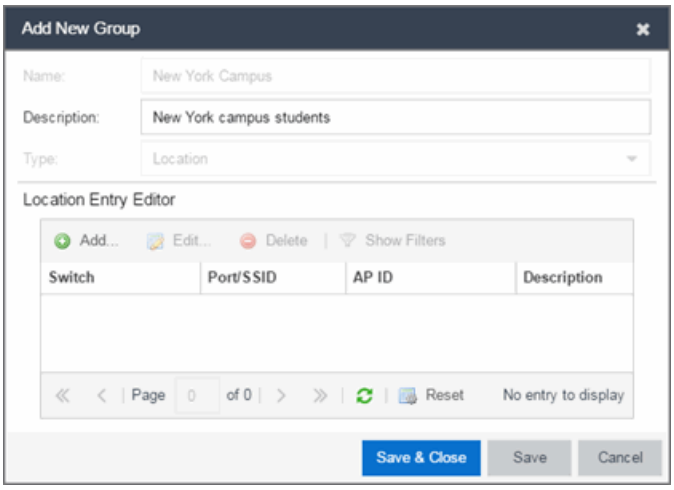


Name
Enter a name for a new location group. You cannot edit the name of a group.

Description
Enter a description of the location group.

Type
Select Location to create a Location group.

Click Create to display the Entry Editor section of the window. This section varies depending on the Type selected.



Switch

The IP address of the switches added to the location.

Port/SSID

The port or port range for a wired switch or the SSIDs for a wireless switch.

AP ID

The access point identifiers for a wireless switch.

Description

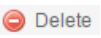
The description of the location group.

Add Button 

Click the Add button to open the Add Entry window, from which you can add an entry to the Entry Editor section.

Edit Button 

Select an entry in the Entry Editor section of the window and click the Edit button to open the Edit Entry window, from which you can edit an existing entry.

Delete Button 

Select an entry in the Entry Editor section of the window and click the Delete button to delete an existing entry.

Save Button

Click the Save button to save the location group.

Related Information

For information on related windows:

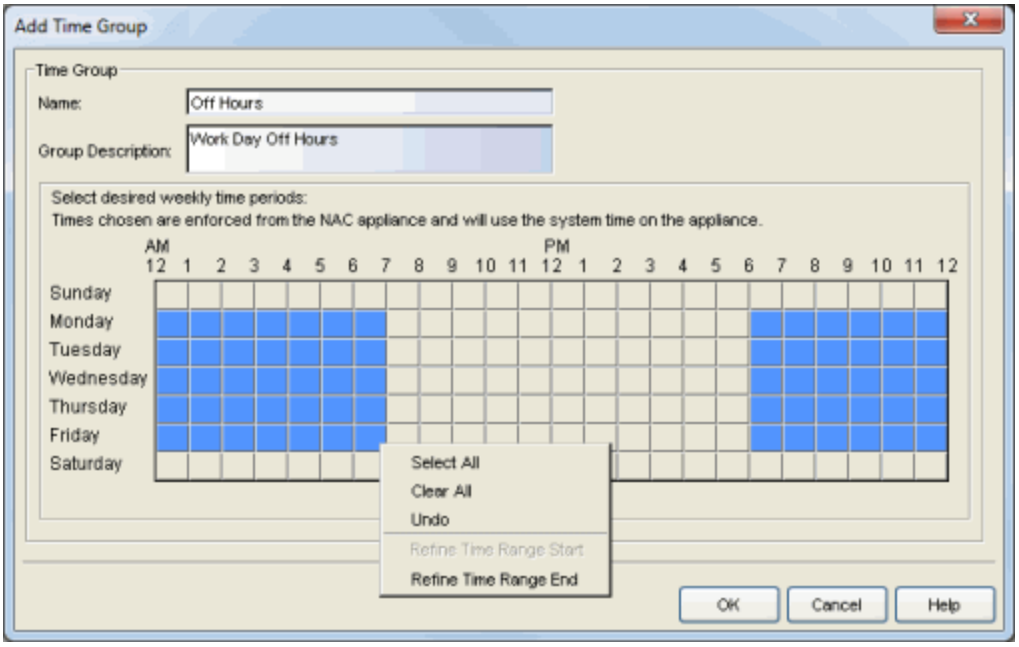
- Create Rule Window
- Manage Rule Groups Window

Add/Edit Time Group Window

Use this window to add a new time group or edit an existing time group. Time groups are rule components that allow you to specify network access requirements or restrictions based on the day and time when the end user is accessing the network. For example, in an enterprise environment, an employee could be assigned different access privileges based on whether they log in during traditional work hours or after hours.

You can access the Add/Edit Time Group window from the Manage Rule Groups window or from the time group field in the Create Rule window.

NOTE: Changes to rule components do not require an enforce. Changes will be automatically synchronized with engines on the next status update. Changes will not affect end-systems until the next authentication and/or assessment occurs.



Name

Enter a name for a new time group. You cannot edit the name of an existing group. If you want to change the name, you must create a new time group with a new name and then delete the old time group.

Group Description

Enter a description of the time group. This description will be displayed in the Manage Rule Groups window.

Calendar

Use the calendar to select the desired weekly time periods. Click to select a specific day and time, or click and drag to quickly select a time sequence or series of days. For example, you can click on Monday at 8 AM and drag down to select that hour for Monday through Friday. The click and drag feature makes it easy to select an entire week or chunk of time with just one action. Right click on a selected square to access menu options that let you select all or clear all squares, and undo the last action. If a square is the first or last in a series, right click to access the Refine Time Range Start/End options that let you specify hourly increments for the start and end times.

Related Information

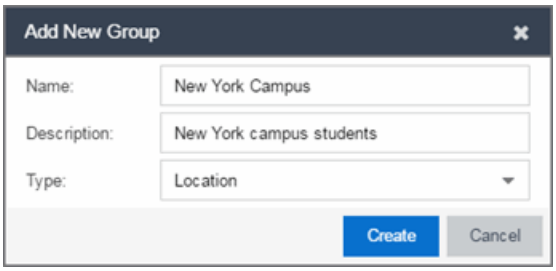
For information on related windows:

- Create Rule Window
- Manage Rule Groups Window

Add/Edit User Group

Use this window to add a new user group or edit an existing user group. User groups are rule components that allow you to group together end users having similar network access requirements or restrictions. You can access the Add/Edit User Group window from the Manage Rule Groups window or from the user group field in the Create Rule window.

NOTE: Changes to rule components do not require an enforce. Changes are automatically synchronized with engines on the next status update. Changes do not affect end-systems until the next authentication and/or assessment occurs.



Name

Enter a name for a new user group. You cannot edit the name of a group.

Description

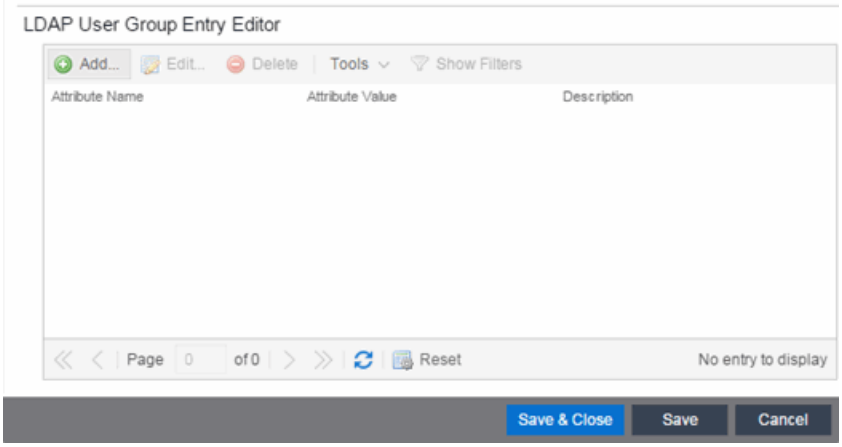
Enter a description of the user group.

Type

Select User to create an end-system group. Specify whether the user group is based on:

- Username — a list of usernames which can be based on an exact match or a wild card.
- LDAP User Group — a list imported from an LDAP Server, organized by Organization Unit (OU), or a custom attribute lookup for any user or MAC address if they match a AAA configuration entry that assigns the request a valid LDAP Configuration.
- RADIUS User Group — a list of attributes returned by the RADIUS server.

Click Create to display the Entry Editor section of the window. This section varies depending on the Type selected.



Match Mode

For LDAP and RADIUS user groups, the **Match Mode** option lets you select whether to match any or match all of the LDAP or RADIUS User Group entries (attribute names) listed below.

For LDAP User Groups, you can also select **Exists**, as the username can be used to verify this criteria after the initial authentication (i.e., using Registration). The **Exists** mode is not available for RADIUS User Groups because they cannot be verified after an initial registration as the user credentials are not stored on the Extreme Access Control engine for re-verification.

Attribute Name

The name of the LDAP or RADIUS Attribute.

Value

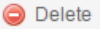
The Attribute value of the user group or username.

Add Button 

Click the **Add** button to open the Add Entry window, from which you can add an entry to the Entry Editor section.

Edit Button 

Select an entry in the Entry Editor section of the window and click the **Edit** button to open the Edit Entry window, from which you can edit an existing entry.

Delete Button 

Select an entry in the Entry Editor section of the window and click the **Delete** button to delete an existing entry.

Tools

Use the Tools menu button to either open a window where you can select a file for importing usernames (if you are creating username entries) or open a window where you can configure an LDAP OU import (if you are creating an LDAP user group).

Filter

Use the Filter field to filter for a specific entry based on a numeric value or text.

Related Information

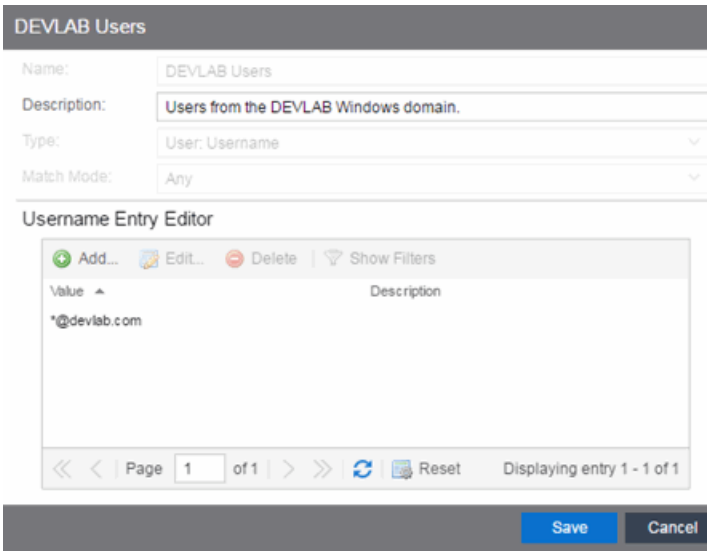
For information on related windows:

- Create Rule Window
- Manage Rule Groups Window

Add/Edit User Group Window

Use this Extreme Access Control window to add a new user group or edit an existing user group. User groups are rule components that allow you to group together end-users having similar network access requirements or restrictions. You can access the Add/Edit User Group window from the Group Editor or from the user group field in the Add Rule window.

NOTE: Changes to rule components do not require an enforce. Changes automatically synchronize with the engines on the next status update. Changes do not affect end-systems until the next authentication and/or assessment occurs.



Name

Enter a name for a new user group. You cannot edit the name of a group.

Description

Enter a description of the user group.

Type

Specify the criteria on which the user group is based:

- Username - a list of usernames which can be based on an exact match or a wild card.
- LDAP User Group - a list imported from an LDAP Server, organized by Organization Unit (OU), or a custom attribute lookup for any user or MAC

address if they match a AAA configuration entry that assigns the request a valid LDAP Configuration.

- RADIUS User Group - a list of attributes returned by the RADIUS server.

Match Mode

For LDAP and RADIUS user groups, the Match Mode option lets you select whether to match any or match all of the LDAP or RADIUS User Group entries (attribute names) listed below.

For LDAP User Groups, you can also select "Exists", since the username can be used to verify this criteria after the initial authentication (i.e., using Registration). The "Exists" mode is not available for RADIUS User Groups because they cannot be verified after an initial registration as the user credentials are not stored on the Extreme Access Control engine for re-verification.

Username Entry Editor

Use the buttons to add, edit, or delete entries in the group. Usernames can be an exact match or use wildcards.

Filter

Use the Filter field to filter for a specific entry based on a numeric value or text.

Related Information

For information on related windows:

- Add/Edit Rule Window
- Group Editor

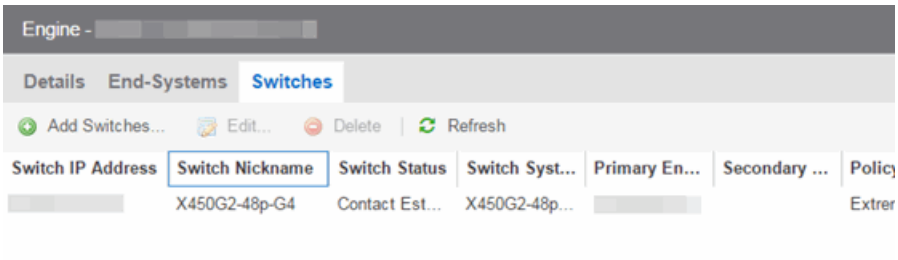
Switches

This tab provides information about the switches assigned to an Extreme Access Control Gateway engine or Extreme Access Control Engine Group. To access this tab, select a gateway or engine group in the left-panel tree, then click the Switches tab in the right panel.

You can right-click on one or more switch for a menu of options.

If you are using the Policy tab, you can also right-click on one or more switch and select from the options in the Policy menu.

Use the table options and tools to filter, sort, and customize table settings. You can access the options by clicking the down arrow in the right corner of any column header.



Switch IP Address

The switch's IP address.

Switch Nickname

The nickname assigned to the switch when it is added to the Extreme Management Center database.

Switch Status

The current operational status of the switch, based on the Extreme Management Center device poll. If the device poll did not update the status of a switch, and a Verify RADIUS Configuration operation is performed on that switch, the switch status in the Switches tab may differ from the switch status in the Verify RADIUS Configuration window.

Switch System Name

The assigned name of the device as stored in the device's sysName MIB object.

Primary Gateway

The name and IP address of the switch's primary Extreme Access Control Gateway. If load balancing has been configured for the engine group, the Extreme Management Center server determines the primary and secondary gateways at Enforce, and this field displays "Determined by Load Balancer."

Secondary Gateway

The name and IP address of the switch's secondary Extreme Access Control Gateway. If load balancing has been configured for the engine group, the Extreme Management Center server determines the primary and secondary gateways at Enforce, and this field displays "Determined by Load Balancer."

Policy/VLAN

The RADIUS attributes included as part of the RADIUS response.

Policy Domain

The Policy Manager domain the switch is assigned to (if any). You can populate this field by right-clicking on a switch and selecting Policy > Verify Domain. This information does not automatically update if there are domain assignment changes. You need to re-select the menu option to update the domain information.

Auth Access Type

The type of authentication access allowed for this switch:

- Any access — the switch can authenticate users originating from any access type.
- Management access — the switch can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- Network access — the switch can only authenticate users accessing the network via the following authentication types: MAC, PAP, CHAP, and 802.1X. If RADIUS accounting is enabled, then the switch also monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions.
- Monitoring - RADIUS Accounting — the switch monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. Extreme Access Control learns about these session via RADIUS accounting. This allows Extreme Access Control to be in a listen mode, and to display access control, location information, and identity information for end-systems without enabling authentication on the switch.
- Manual RADIUS Configuration — RADIUS configuration was performed manually on the switch using Policy Manager or CLI.

Switch Type

Specifies the switch type: a switch that authenticates layer 2 traffic via RADIUS to an out-of-band Extreme Access Control gateway, or a VPN concentrator being used in an Extreme Access Control VPN deployment.

Switch Location

The physical location of the switch.

Switch Contact

The person responsible for the switch.

Switch Description

A description of the switch, which may include its manufacturer, model number, and firmware revision number.

Management RADIUS Servers

RADIUS servers used to authenticate requests for administrative access to the switch.

RADIUS Accounting

Displays whether RADIUS accounting is enabled or disabled on the switch. RADIUS accounting can be used to determine the connection state of the end-system sessions on the Extreme Access Control engine, providing real-time connection status in Extreme Management Center. RADIUS accounting is also used to monitor switches for Auto Tracking, CEP (Convergence End Point), and Switch Quarantine authentication sessions, when used in conjunction with the Monitoring or Network Access switch authentication access types. For more information, see the Auth. Access Type section of the Add/Edit Switch Window Help topics.

IP Subnet for IP Resolution

Displays the IP subnet that the switch is using as an inclusive list for MAC to IP resolution. Specifying an IP subnet in a static IP network allows for a router to be used for IP resolution in cases where it would not be discovered via DHCP. IP Subnets also contain an IP range which can be used to filter out secondary IP addresses that are not valid for the network.

Policy Enforcement Points

If the switch is a VPN device (see Switch Type column), this column displays the Policy Enforcement Points that are being used to provide authorization for the connecting end-systems.

Add Switch

Opens the Add Switches to Extreme Access Control Engine Group window where you can select switches to add to the engine or engine group.

Edit

Select a switch and click this button to open the Edit Switches in Extreme Access Control Engine Group window where you can change the switch's primary and secondary Extreme Access Control Gateway (Gateway), and also edit other switch attributes, if desired.

Delete

Select a switch and click this button to delete the switch from Extreme Management Center's device database. The switch's primary gateway enforces its own primary RADIUS server as both the primary and secondary RADIUS servers on the switch.

Related Information

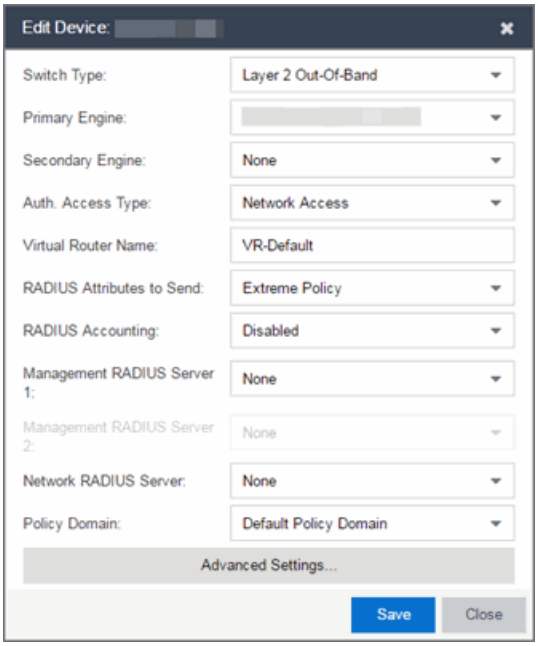
For information on related windows:

- Add Switches to an Extreme Access Control Engine Group Window
- Edit Switches in Extreme Access Control Engine Group Window

Edit Switches in Extreme Access Control Engine Group

Use this window to change a switch's primary and secondary Extreme Access Control Gateway, and also edit other switch parameters including the switch's authentication access type and the RADIUS attributes to send, if desired.

You can access this window by selecting an engine or engine group in the left-panel tree. Then, in the right-panel Switches tab, select the switches you wish to edit and click the **Edit** button.



Switch Type

Use the drop-down list to change the type of switch:

- Layer 2 Out-Of-Band — A switch that will do authentication on layer 2 traffic via RADIUS to an out-of-band Extreme Access Control 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 Extreme Access Control engine, Extreme Management Center 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 Extreme Management Center, because only one authenticated session is allowed per end-system within Extreme Management Center.
- Layer 2 RADIUS Only — In this mode, Extreme Access Control 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 Extreme Access Control 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 Extreme Access Control is unable to apply policies to restrict access after the user is granted access.

Primary Gateway

Use the drop-down menu to select the primary Extreme Access Control Gateway for the selected switches. If load balancing has been configured for the switch, this field is not displayed.

Secondary Gateway

Use the drop-down menu to select the secondary Extreme Access Control Gateway for the selected switches. If load balancing has been configured for the switch, this field is not displayed.

Auth Access Type

Use the drop-down menu 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. Extreme Access Control 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. For management requests handled through Extreme Access Control, make sure that an appropriate administrative access configuration is in place by assigning a profile such as "Administrator Extreme Access Control Profile" to grant proper access to users. Also, verify that the current switch CLI credentials for the admin user are defined in the database against which Extreme Access Control authenticates management login attempts.
- Switching from an Auth type of "Any Access" or "Management Access" back to "Network Access" can restrict access to the switch after an enforce is performed. Verify that the current switch CLI credentials for the admin user are defined locally on the switch.

- Any Access — the switch can authenticate users originating from any access type.
- Management Access — the switch can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- Network Access - the switch can only authenticate users accessing the network via the following authentication types: MAC, PAP, CHAP, and 802.1X. If RADIUS accounting is enabled, then the switch also monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. If there are multiple sessions for a single end-system, the session with the highest precedence will be displayed to provide the most accurate access control information for the user. The Extreme Access Control authentication type precedence from highest to lowest is: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.
- Monitoring - RADIUS Accounting — the switch will monitor Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. Extreme Management Center learns about these session via RADIUS accounting. This allows Extreme Management Center 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

Extreme Access Control authentication type precedence from highest to lowest is: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.

- Manual RADIUS Configuration — Extreme Management Center 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

Select the checkbox to enter the name of the Virtual Router. The default value for this field is VR-Default.

WARNING: For ExtremeXOS devices only. If Extreme Management Center 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 menu to select the RADIUS attributes settings included as part of the RADIUS response from the Extreme Access Control engine to the switch.

RADIUS Accounting

Use the drop-down menu to enable RADIUS accounting on the switch. RADIUS accounting can be used to determine the connection state of the end-system sessions on the Extreme Access Control engine, providing real-time connection status in Extreme Management Center. It also allows Extreme Access Control to monitor Auto Tracking, CEP (Convergence End Point), and Quarantine (anti-spoofing) sessions.

Management RADIUS Server

Use the drop-down menu to specify RADIUS servers used to authenticate requests for administrative access to the selected switches. Select from the RADIUS servers you have configured in Extreme Management Center, or select New or Manage to open the Add/Edit RADIUS Server or Manage RADIUS Servers windows.

Network RADIUS Server

This option lets you specify a backup RADIUS server to use for network authentication requests for the selected switches. This allows you to explicitly configure a network RADIUS server to use if there is only one Extreme Access Control engine. (This option is only available if a Secondary Gateway is not specified.) Select from the RADIUS servers you have configured in Extreme Control,

or select **New** or **Manage** to open the Add/Edit RADIUS Server or Manage RADIUS Servers windows.

Policy Domain

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

NOTE: Selecting **-- Do Not Set --** for an Extreme Access Control engine on which a Policy Domain is configured does not unassign the Policy Domain. To unassign a Policy Domain, use the **Policy** tab.

Advanced Settings

Select this button to open the Advanced Switch Settings window.

Related Information

For information on related windows:

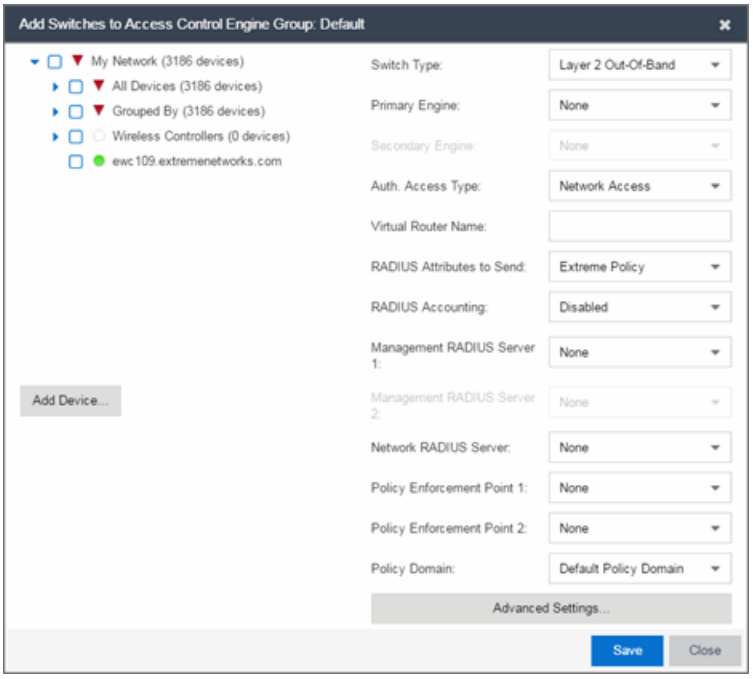
- Switches Tab
- Add Switches to an Engine Group Window
- Advanced Switch Settings Window

Add Switches to Extreme Access Control Engine Group

Use this window to select switches to add to a gateway engine or engine group. The window allows you to select one or more switches from the device tree, and set the primary and secondary Extreme Access Control Gateways for the switches. It also lets you set other parameters including the authentication access type for the switches and the RADIUS attributes to send.

NOTE: If desired, you can set only the primary Extreme Access Control Gateway for the switches; Extreme Management Center does not require the secondary Extreme Access Control Gateway to be set. If only the primary Extreme Access Control Gateway is set, then by default that gateway uses its primary proxy RADIUS server as a secondary direct RADIUS server to the switch. This allows for redundancy without the requirement for a secondary Extreme Access Control Gateway. In this scenario, if contact with the Extreme Access Control Gateway fails, authentication traffic would bypass the Extreme Access Control gateway, but normal authentication would continue in the network, and still provide some security.

1. Access the **Control > Access Control** tab.
2. Select an engine or engine group from the left-panel
3. Click the **Add Switch** button in the right-panel Switches tab.



Device Tree

This area displays the device tree. Expand the tree and select the switches you want to add to the engine or engine group.

Add Device

Opens the Add Device window where you can add a device to the Extreme Management Center database. The device is displayed in the My Network folder in the device tree.

Switch Type

Use the drop-down menu 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 Extreme Access Control 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 Extreme Access Control engine, Extreme Access Control removes the end-system authentication from their prior port/switch. This allows VMs that quickly move from one server to another and then back

again to still have their location updated in Extreme Management Center, because only one authenticated session is allowed per end-system in Extreme Management Center.

- Layer 2 RADIUS Only — In this mode, Extreme Management Center 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 Extreme Access Control 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 Extreme Management Center is unable to apply policies to restrict access after the user is granted access.

Primary Gateway

Use the drop-down menu to select the primary Extreme Access Control Gateway for the selected switches. If load balancing has been configured for the engine group, the Extreme Management Center server determines the primary and secondary gateways at Enforce, and this field displays Determined by Load Balancer.

Secondary Gateway

Use the drop-down menu to select the secondary Extreme Access Control Gateway for the selected switches. If load balancing has been configured for the engine group, the Extreme Management Center server determines the primary and secondary gateways at Enforce, and this field displays Determined by Load Balancer.

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

Auth. Access Type

Use the drop-down menu 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. Extreme Access Control 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 Extreme Access Control Profile" to grant proper access to users. Also, verify that the current switch CLI credentials for the admin user are defined in the database that Extreme Management Center 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 Extreme Access Control authentication type precedence from highest to lowest is: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.
- Monitoring - RADIUS Accounting - the switch monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. Extreme Management Center learns about these session via RADIUS accounting. This allows Extreme Management Center 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 Extreme Access Control authentication type precedence from highest to

lowest is: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.

- Manual RADIUS Configuration - Extreme Management Center 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 Extreme Management Center 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 menu to select the RADIUS attributes included as part of the RADIUS response from the Extreme Access Control engine to the switch. You can also select New or Manage from the menu to open the RADIUS Attribute Settings window where you can define, edit, or delete the available attributes.

RADIUS Accounting

Use the drop-down menu to enable RADIUS accounting on the switch. RADIUS accounting can be used to determine the connection state of the end-system sessions on the Extreme Access Control engine, providing real-time connection status in Extreme Management Center.

Management RADIUS Server 1 and 2

Use the drop-down menu to specify RADIUS servers used to authenticate requests for administrative access to the selected switches. Select from the RADIUS servers you have configured in Extreme Management Center, 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 Extreme Access Control engine. (This option is only available if a Secondary Gateway is not specified.) Select from the RADIUS servers you have configured in Extreme

Management Center, or select New or Manage RADIUS Servers to open the Add/Edit RADIUS Server or Manage RADIUS Servers windows.

Policy Enforcement Point 1 and 2

Select the Policy Enforcement Points used to provide authorization for the end-systems connecting to the VPN device you are adding. The list is populated from the N-Series, S-Series, and K-Series devices in your Console device tree. If you do not specify a Policy Enforcement Point, then Extreme Access Control is unable to apply policies to restrict end user access after the user is granted access.

Policy Domain

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

Advanced Settings

Click the Advanced Settings button to open the Advanced Switch Settings window.

Related Information

For information on related windows:

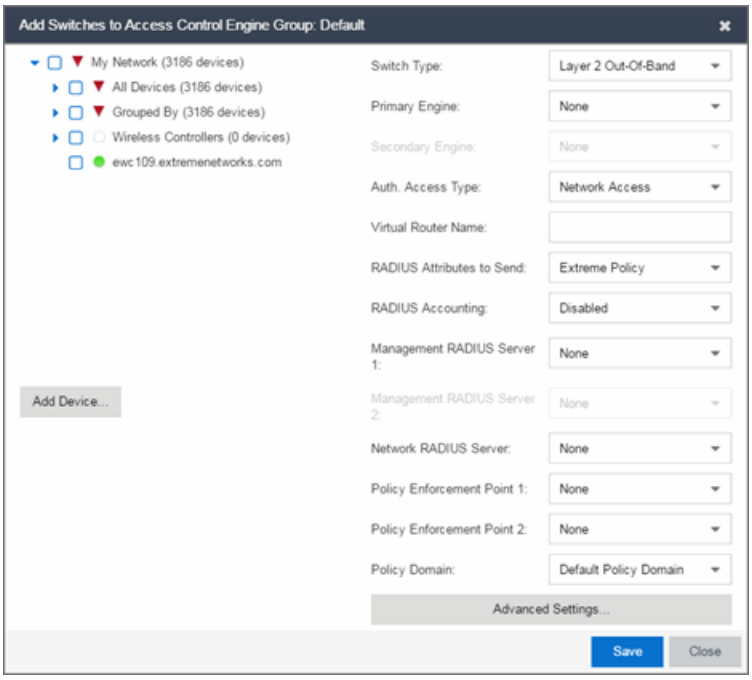
- Switches Tab
- Edit Switches in Engine Group Window

Add Switches to Extreme Access Control Engine Group

Use this window to add switches to a gateway engine or engine group. The window allows you to select one or more switches from the device tree, and set the primary and secondary Extreme Access Control Gateways for the switches. It also lets you set other parameters including the authentication access type for the switches and the RADIUS attributes to send.

NOTE: If desired, you can set only the primary Extreme Access Control Gateway for the switches; Extreme Management Center does not require the secondary Extreme Access Control Gateway to be set. If only the primary Extreme Access Control Gateway is set, then by default that gateway uses its primary proxy RADIUS server as a secondary direct RADIUS server to the switch. This allows for redundancy without the requirement for a secondary Extreme Access Control Gateway. In this scenario, if contact with the Extreme Access Control Gateway fails, authentication traffic would bypass the Extreme Access Control gateway, but normal authentication would continue in the network, and still provide some security.

You can access this window by selecting an engine or engine group and clicking the **Add Switch** button in the right-panel Switches tab.



Device Tree

This area displays the device tree. Expand the tree and select the switches you want to add to the engine or engine group.

Add Device

Opens the Add Device window where you can add a device to the Extreme Management Center database. The device is displayed in the My Network folder in the device tree.

Switch Type

Use the drop-down menu 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 Extreme Access Control 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 Extreme Access Control engine, Extreme Access Control removes the end-system authentication from their prior port/switch. This allows VMs that quickly move from one server to another and then back again to still have their location updated in Extreme Management Center,

because only one authenticated session is allowed per end-system in Extreme Management Center.

- Layer 2 RADIUS Only — In this mode, Extreme Management Center 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 Extreme Access Control 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 Extreme Management Center is unable to apply policies to restrict access after the user is granted access.

Primary Gateway

Use the drop-down menu to select the primary Extreme Access Control Gateway for the selected switches. If load balancing has been configured for the engine group, the Extreme Management Center server determines the primary and secondary gateways at Enforce, and this field displays Determined by Load Balancer.

Secondary Gateway

Use the drop-down menu to select the secondary Extreme Access Control Gateway for the selected switches. If load balancing has been configured for the engine group, the Extreme Management Center server determines the primary and secondary gateways at Enforce, and this field displays Determined by Load Balancer.

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

Auth. Access Type

Use the drop-down menu 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. Extreme Access Control 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 Extreme Access Control Profile" to grant proper access to users. Also, verify that the current switch CLI credentials for the admin user are defined in the database that Extreme Management Center 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 Extreme Access Control authentication type precedence from highest to lowest is: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.
- Monitoring - RADIUS Accounting - the switch monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. Extreme Management Center learns about these session via RADIUS accounting. This allows Extreme Management Center 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 Extreme Access Control authentication type precedence from highest to

lowest is: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.

- Manual RADIUS Configuration - Extreme Management Center 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 Extreme Management Center 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 menu to select the RADIUS attributes included as part of the RADIUS response from the Extreme Access Control engine to the switch. You can also select New or Manage from the menu to open the RADIUS Attribute Settings window where you can define, edit, or delete the available attributes.

RADIUS Accounting

Use the drop-down menu to enable RADIUS accounting on the switch. RADIUS accounting can be used to determine the connection state of the end-system sessions on the Extreme Access Control engine, providing real-time connection status in Extreme Management Center.

Management RADIUS Server 1 and 2

Use the drop-down menu to specify RADIUS servers used to authenticate requests for administrative access to the selected switches. Select from the RADIUS servers you have configured in Extreme Management Center, 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 Extreme Access Control engine. (This option is only available if a Secondary Gateway is not specified.) Select from the RADIUS servers you have configured in Extreme

Management Center, or select New or Manage RADIUS Servers to open the Add/Edit RADIUS Server or Manage RADIUS Servers windows.

Policy Enforcement Point 1 and 2

Select the Policy Enforcement Points used to provide authorization for the end-systems connecting to the VPN device you are adding. The list is populated from the N-Series, S-Series, and K-Series devices in your Console device tree. If you do not specify a Policy Enforcement Point, then Extreme Access Control is unable to apply policies to restrict end user access after the user is granted access.

Policy Domain

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

Advanced Settings

Click the Advanced Settings button to open the Advanced Switch Settings window.

Related Information

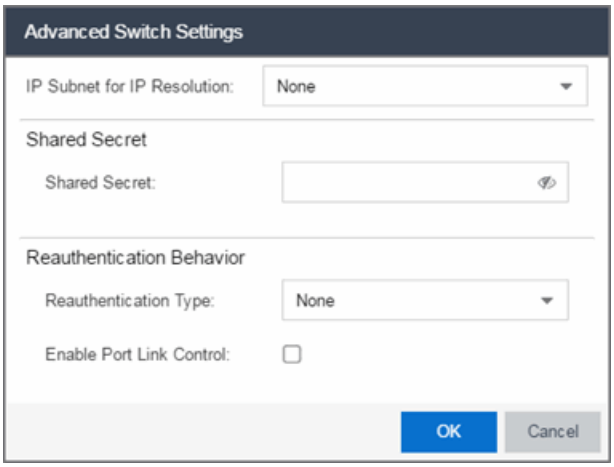
For information on related windows:

- Switches Tab
- Edit Switches in Engine Group Window

Advanced Switch Settings

This window allows you to configure settings for switches that require a different configuration than your standard switch settings set in the Engine Settings window.

You can access the window from the Add Switch to Extreme Access Control Engine Group window or from the Edit Switches in Extreme Access Control Engine Group window.



IP Subnet for IP Resolution

Click the drop-down menu to display a list of the IP subnets configured in the Engine Settings window. If you select a subnet, the switch uses it as an inclusive list for MAC to IP resolution. Specifying an IP subnet in a static IP network allows for a router to be used for IP resolution in cases where it would not be discovered via DHCP. IP subnets also contain an IP range which can be used to filter out secondary IP addresses that are not valid for the network.

Shared Secret

A string of alpha-numeric characters used to encrypt and decrypt communications between the switch and the Extreme Access Control engine. The shared secret is shown as a string of asterisks. When the Show Password option is selected, the shared secret is shown in text.

Reauthentication Type

Select the reauthentication type for the switch:

- SNMP - uses SNMP to trigger reauthentication using various OIDs in different MIBs. The Extreme Access Control engine checks a series of proprietary Enterasys MIBs, standardized MIBs, and proprietary third-party MIBs to determine availability, and forces reauthentication using any available SNMP method.
- Session Timeout - causes Extreme Access Control to return a session timeout and terminate action to the end-system via RADIUS response attributes. The use of this mechanism causes the user to be automatically reauthenticated at a specified interval by the switch to which they are connected. Only use this option for wireless switches that do not have RFC 3576 support or wired switches that do not have SNMP support.

- RFC 3576 - a method of reauthenticating RADIUS sessions through the use of Disconnect-Request messages as defined by RFC 3576. (For more information, see http://www.ietf.org/rfc/rfc3576.txt). RFC 3576 configurations must be customized to work with the specific vendor implementation for each device type. To add, edit, or delete an RFC 3576 configuration, click the Manage RFC 3576 Configurations button.

Enable Port Link Control

Port link control allows the toggle of the operational mode of a port. Select this option to enable port link control for specific switches.

Related Information

For information on related windows:

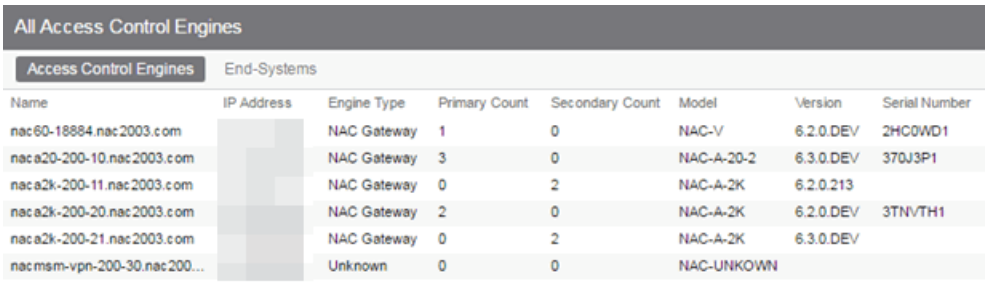
- Edit Switches in Extreme Access Control Engine Group Window
- Add Switches to Extreme Access Control Engine Group Window

All Access Control Engines

The All Extreme Access Control Engines tab is displayed in the right panel when you select the All Extreme Access Control Engine tree in the left panel or when you select the Extreme Access Control Engines tab when an Extreme Access Control Engine Group is selected. The panel displays a table of information about the engines in the folder or group. Right-click an engine for a menu of options.

Use the table options and tools to filter, sort, and customize table settings. You can access the options by clicking the down arrow in the right corner of any column header.

NOTE: The Extreme Access Control Engine administration web page allows you to access status and diagnostic information for an Extreme Access Control engine. Access the administration web page using the following URL: https://*Extreme Access ControlEngineIP*:8444/Admin. The default user name and password for access to this web page is "admin/Extreme@pp."



Name

The name of the Extreme Access Control engine (assigned when the engine is created).

IP Address

The Extreme Access Control engine's IP address.

Engine Type

The Extreme Access Control engine type: Extreme Access Control Gateway, Extreme Access Control Layer 2 (L2) Controller, or Extreme Access Control Layer 3 (L3) Controller.

Primary Count

The number of switches for which the Extreme Access Control engine is the primary engine.

Secondary Count

The number of switches for which the Extreme Access Control engine is the secondary engine.

Model

The Extreme Access Control engine's model number.

Version

The Extreme Access Control engine's version number.

CPU Load (0-100%)

The percentage of the engine's CPU currently being used. This value gives you an indication of how busy the engine is and helps you determine if your network needs additional engines, or if you need to change your network configuration so that the load is more evenly distributed among your existing engines.

Memory Used

The amount of memory used by the engine.

Memory Available
The amount of memory available on the engine.

Connected Agents
The number of assessment agents connected to the engine.

Capacity
The engine's current capacity, which is the number of end-systems that have authenticated within the last 24 hours out of the maximum number of authenticating end-systems supported for the engine.

Related Information

For information on related windows:

- End-Systems Tab

Engine Settings Window

Engine settings provide advanced configuration options for Extreme Access Control engines. Extreme Management Center comes with a default engine settings configuration. If desired, you can edit these default settings or you can define your own settings to use for your Extreme Access Control engines.

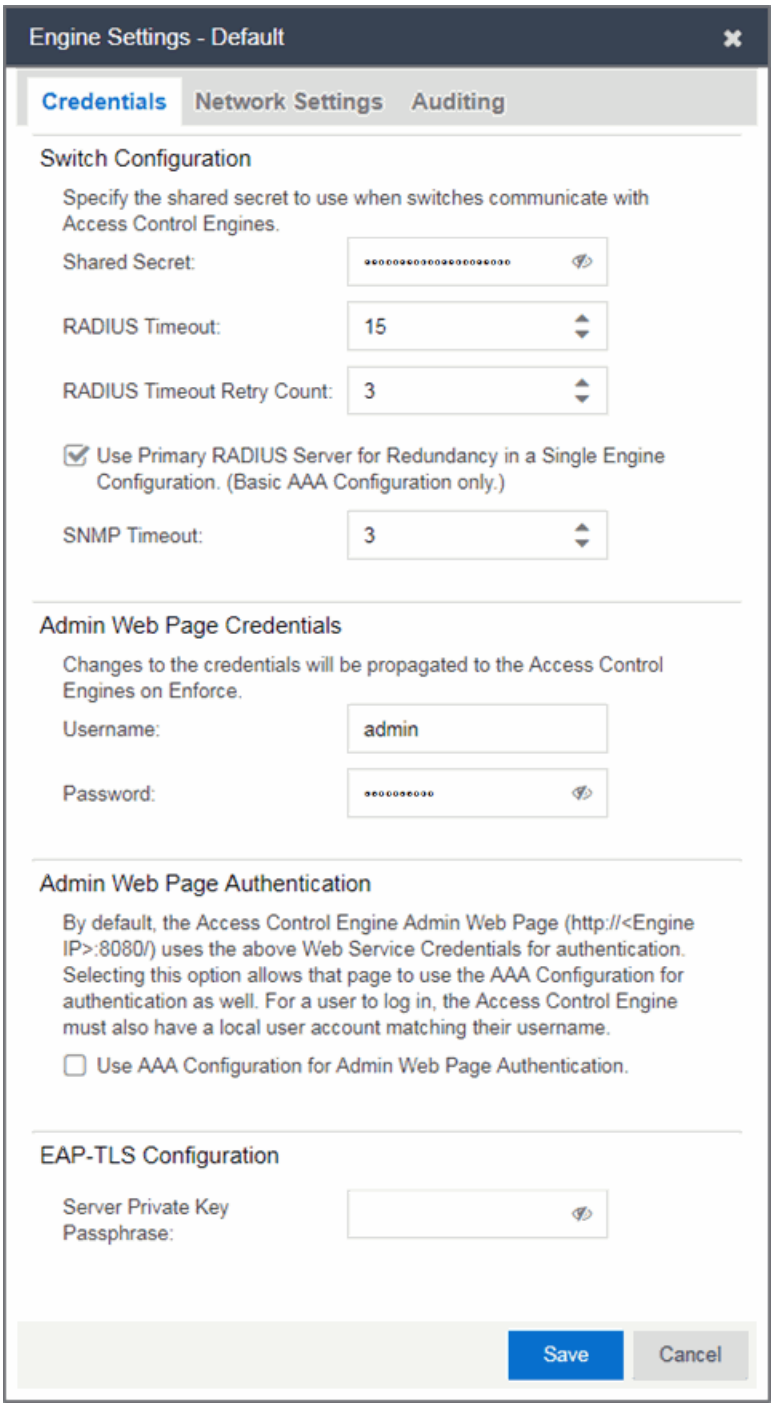
You can launch the Engine Settings window by right-clicking an engine or engine group in the Extreme Access Control Engine Groups left-panel tree or by right-clicking an Extreme Access Control engine in the All Extreme Access Control Engines. The Engine Settings window opens with the following tabs available for configuration:

- Credentials Tab
- Network Tab
- Auditing Tab

NOTE: To access status and diagnostic information for an Extreme Access Control engine, launch the Extreme Access Control Engine administration web page by using the following URL: https://<Extreme Access ControlEngineIP>:8444/Admin. The default user name and password for access to this web page is "admin/Extreme@pp." The username and password can be changed in the Web Service Credentials field on the Credentials Tab in the Engine Settings window.

Credentials

Use this tab to configure various parameters for your network engines including switch configuration, web service credentials, and EAP-TLS configuration.



Switch Configuration

Enter the shared secret that switches uses when communicating with Extreme Access Control engines.

Shared Secret

A string of alpha-numeric characters used to encrypt and decrypt communications between the switch and the Extreme Access Control engine. The shared secret is shown as a string of asterisks. Click the Eye icon to view the shared secret.

RADIUS Timeout

The amount of time (in seconds) that a switch waits before re-sending a RADIUS request to the Extreme Access Control engine. The default is 15 seconds and the maximum is 60 seconds.

NOTES: The time specified should be long enough to allow the Extreme Access Control engine to receive a response from the RADIUS server.

Although this option allows a maximum of 60 seconds, the actual maximum time allowed varies depending on the switch model. If a switch does not support the timeout value specified here, then the value is not set on the switch and an error message displays in the Extreme Access Control engine log. Check your switch documentation to verify supported values.

RADIUS Timeout Retry Count

The number of times the switch attempts to contact an Extreme Access Control engine with a RADIUS request, when an attempted contact fails. The default setting is 3 retries, which means that the switch retries a timed-out request three times, making a total of four attempts to contact the engine.

Use Primary RADIUS Server for Redundancy in Single Extreme Access Control Engine Configuration

If your Extreme Access Control deployment has only one Extreme Access Control engine, this option allows you to configure redundancy by using the primary RADIUS server as a backup when configuring the switches. This option would not apply to Extreme Access Control deployments using advanced AAA configurations with more than one set of RADIUS servers, or if you have configured primary and secondary Extreme Access Control engines.

Web Service Credentials

Extreme Access Control Engine Web Service Credentials

The credentials specified here provide access to the Extreme Access Control engine administration web page and the web services interface between the Extreme Management Center server and the Extreme Access Control engine. NAC Manager

provides default credentials that can be changed, if desired. Changes to the credentials are propagated to the Extreme Access Control engines on Enforce.

Extreme Access Control Admin Web Page

By default, the Extreme Access Control engine administration web page (https://<Extreme Access ControlEngineIP>:8444/Admin/) uses the above Web Service Credentials for authentication. However, you can configure the web page to use the AAA Configuration assigned to that engine for authentication as well. This allows you to use LDAP or RADIUS authentication for the web page.

There are three steps for setting up the web page to use LDAP or RADIUS authentication:

1. Verify that the Extreme Access Control Configuration assigned to the engine has LDAP or RADIUS authentication configured in its AAA Configuration.
2. Create a local user account on the Extreme Access Control engine that matches the user name of the user logging in. Use the `useradd` command on the Extreme Access Control engine CLI to create the local user account.
3. Select the Use Extreme Access Control AAA Configuration for Admin Web Page authentication option here on the Credentials tab. Click OK. Enforce the change to the engine.

The Extreme Access Control engine begins using the AAA configuration for the administration web page authentication. Note that it may take the Linux operating system on the Extreme Access Control engine up to two minutes to recognize that the new user is valid.

EAP-TLS Configuration

Server Private Key Passphrase

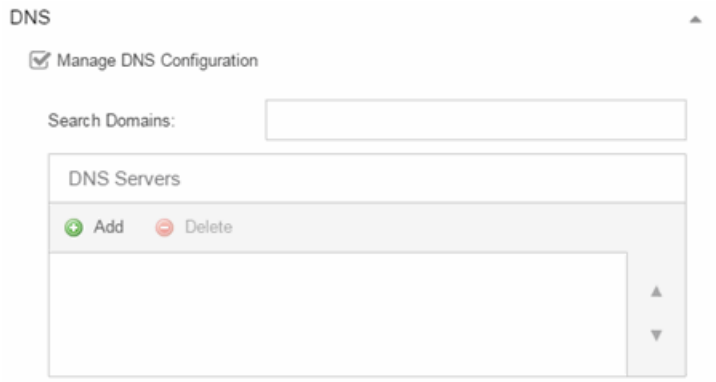
The Server Private Key Passphrase is used to encrypt the private key created during certificate request generation of server certificates for use by Extreme Access Control engines during Local EAP-TLS Authentication. The passphrase must be identical for all Extreme Access Control engines, and must be configured properly, or Local EAP-TLS Authentication does not operate successfully.

Network Settings

Use this tab to configure the following network services for the Extreme Access Control engine: DNS, NTP, SSH, and SNMP.

Manage DNS Configuration

Select the Manage DNS Configuration checkbox and enter a list of search domains and DNS servers.



Search Domains
: A list of search domains used by the Extreme Access Control engine when doing lookups by hostname. When an attempt to resolve a hostname is made, these domain suffixes are appended to the hostname of the device. For example, if someone does a ping to server1, NAC Manager appends the search domains in an attempt to resolve the name: server1.domain1 server1.domain2, and so on.

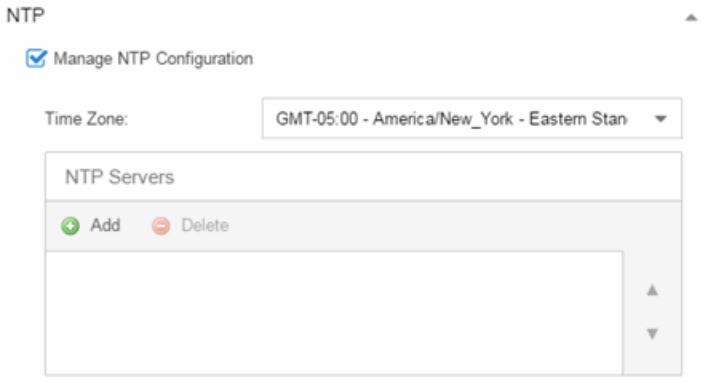
DNS Servers
: A list of DNS servers the Extreme Access Control engine sends DNS lookups to for name resolution. The list is used by both hostname resolution and by the DNS proxy. You can enter multiple servers for redundancy. Use the Up and Down arrows to list the servers in the order they should be used.

Manage NTP Configuration

NTP (Network Time Protocol) configuration is important for protocols such as SNMPv3 and RFC3576 which incorporate playback protection. In addition,

having accurate time configured on the Extreme Access Control engine is essential for event logging and troubleshooting.

Select the Manage NTP Configuration checkbox, specify the appropriate time zone, and create a list of NTP servers.



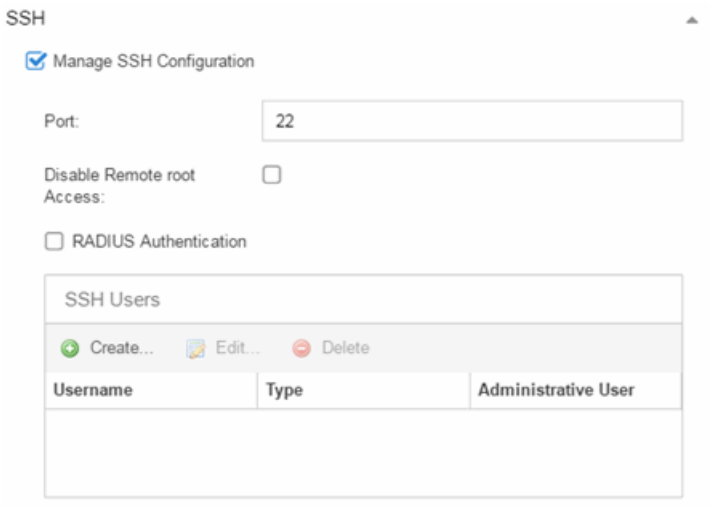
Time Zone
: Select the appropriate time zone. This allows NAC Manager to manage all date/time settings.

NTP Servers
: A list of NTP servers. You can enter multiple servers for redundancy. Use the Up and Down arrows to list the servers in the order they should be used.

Manage SSH Configuration

SSH configuration provides additional security features for the Extreme Access Control engine.

Select the Manage SSH Configuration checkbox and provide the following SSH information.



Port

The port field allows you to configure a custom port to be used when launching SSH to the engine. The standard default port number is 22.

Disable Remote root Access

Select this option to disable remote root access via SSH to the engine and force a user to first log in with a real user account and then su to root (or use sudo) to perform an action. When remote root access is allowed, there is no way to determine who is accessing the engine. With remote root access disabled, the /var/log/message file displays users who log in and su to root. The log messages looks like these two examples:

```
sshd[19735]: Accepted password for <username> from
10.20.30.40 port 36777 ssh2
su[19762]: + pts/2 <username>-root
```

Enabling this option does not disable root access via the console. Do not disable root access unless you have configured RADIUS authentication or this disables remote access to the Extreme Access Control engine.

RADIUS Authentication

This option lets you specify a centralized RADIUS server to manage user login credentials for users that are authorized to log into the engine using SSH. Select a primary and backup RADIUS server to use, and use the table below to create a list of authorized RADIUS users.

SSH Users Table

Use the toolbar buttons to create a list of users allowed to log in to the Extreme Access Control engine using SSH. You can add Local and RADIUS

users and grant the user Administrative privileges, if appropriate. A user that is granted administrative rights can run sudo commands and commands that only a root user would be able to run. For example, some commands that require administrative rights to run would be:

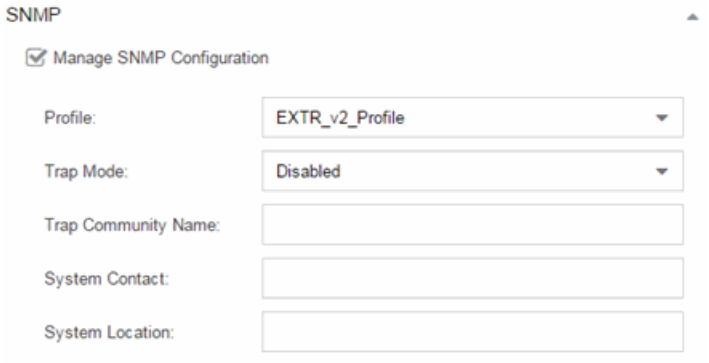
sudo nacctl restart
sudo reboot
sudo nacdb

If a user is not granted administrative rights, they can log in, view files, and run some commands such a ping and ls.

SNMP Configuration

The SNMP configuration section allows you to deploy SNMP credentials for the Extreme Access Control engine. The credentials can include different read/write credentials, for example, the read credential can be "public" and the write credential can be "private". In addition, basic host traps can be enabled from the Extreme Access Control engine.

Select the Manage SNMP Configuration checkbox and provide the following SSH information.



Profile

Use the drop-down menu to select a device access profile to use for the Extreme Access Control engine.

Trap Mode

Set the trap mode.

Trap Community Name

Supply the trap community name.

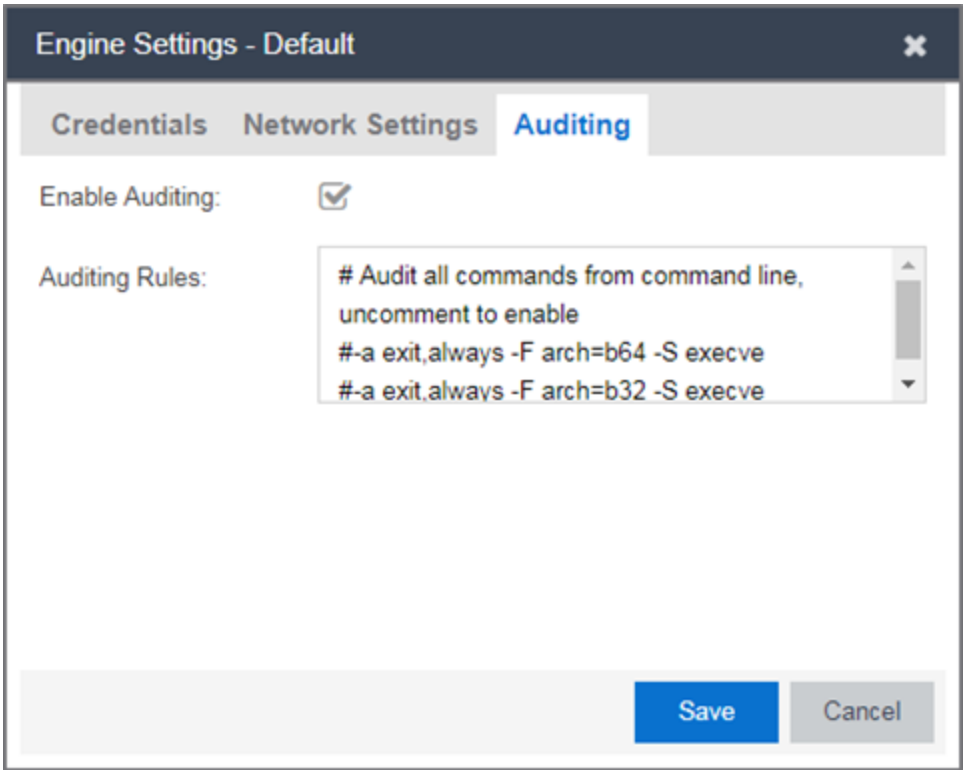
System Contact

Enter the name of the system contact.

System Location
Enter the location of the system.

Auditing

Use this tab to enable auditing of users connected to the Extreme Access Control engine CLI via SSH.



Enable Auditing
Selecting the Enable Auditing option enables the Auditing Rules field, where you can configure Extreme Management Center to store all commands entered by a user connected to the Extreme Access Control engine CLI via SSH in the engine's local syslog file.

Auditing Rules
Remove the # symbol from the beginning of a command line to enable the command and store user commands entered using the Extreme Access Control engine CLI.

Related Information

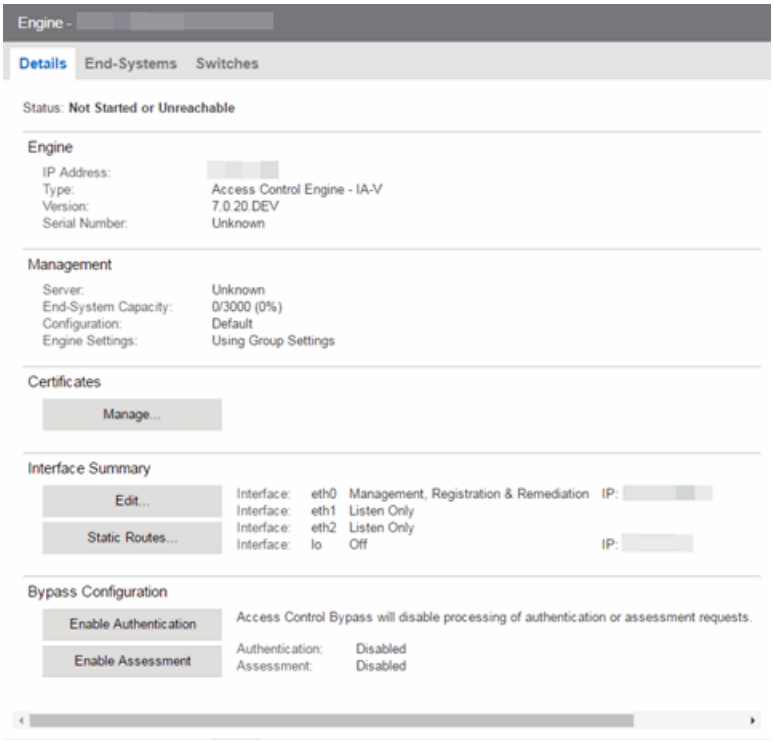
For information on related windows:

- All Extreme Access Control Engines

Details (Extreme Access Control Engine)

This tab provides information about an Extreme Access Control engine's configuration. The information changes depending on the type of engine selected in the left-panel tree.

To access this tab, select an Extreme Access Control engine in the left-panel tree, then click the **Details** tab in the right panel.



General Information

This section displays general information about the Extreme Access Control engine, including its name, IP address, type (Extreme Access Control Gateway or Layer 2/Layer 3 Extreme Access Control Controller), the engine version, the IP address of

the Extreme Management Center Management server, and the Extreme Access Control engine status.

End-System Capacity

This field lists the engine's current capacity, which is the number of end-systems that authenticated within the last 24 hours out of the maximum number of authenticating end-systems supported for the engine.

Extreme Access Control Configuration

Displays the Extreme Access Control Configuration assigned to the engine. The Extreme Access Control Configuration determines the Extreme Access Control Profile assigned to an end-system connecting to the network.

Engine Settings

Indicates whether the engine is using Group Settings or has an engine settings override configured.

Interface Summary

Displays a summary of the current engine interface configuration.
Click Edit to open the Interfaces window, where you can change the engine Host Name and Gateway..
Click Static Routes to open the Static Routes window, where you can add or edit the static routes used for advanced routing configuration..

Extreme Access Control Bypass Configuration

The Extreme Access Control Bypass Configuration feature allows you to bypass Extreme Access Control processing of authentication requests from end-systems connecting to the network and also disable the Extreme Access Control assessment process. For Extreme Access Controlauthentication bypass, Extreme Access Control either configures the switch to authenticate directly to a RADIUS server to which Extreme Access Control is configured to proxy authentication requests, or it disables RADIUS authentication on the switch. This capability is useful for troubleshooting purposes. For example, if there is a problem with an Extreme Access Control Configuration, the Disable button lets you remotely disable Extreme Access Control functionality until the problem is resolved. You can then use the Enable button to re-enable Extreme Access Control functionality on the engines. When Extreme Access Control authentication or assessment is disabled, the Extreme Access Control engine name and IP address display in red text in the left-panel tree indicating the engine is in Bypass mode.

For Extreme Access Control Gateway engines, when you select the option to disable Extreme Access Control authentication processing, if proxy

RADIUS servers are configured for authentication in a Basic AAA Configuration, the Extreme Access Control Engine configures the switches to send RADIUS packets directly to the primary and secondary RADIUS servers (from the Basic AAA Configuration), instead of talking to the RADIUS proxy through the Extreme Access Control gateway. RADIUS authentication is not disabled on the switch, and end users still need to authenticate in order to connect to the network. The switches must be defined in the back-end proxy RADIUS server as RADIUS clients with the same shared secret used by the Extreme Access Control Gateway engines. If there are no proxy RADIUS servers configured in a Basic AAA Configuration, or if an Advanced AAA Configuration is used, RADIUS authentication on the switch is disabled when Extreme Access Control authentication processing is disabled.

NOTES: If you have disabled Extreme Access Control authentication processing and then enforce with new switches, the new switches are configured to send RADIUS packets directly to the primary and secondary RADIUS servers. These switches are reconfigured to talk to the RADIUS proxy when you enable Extreme Access Control; a second enforce is not necessary.

Bypass is not an option for switches set to Manual RADIUS Configuration or ExtremeWireless controllers not configured for RADIUS strict mode.

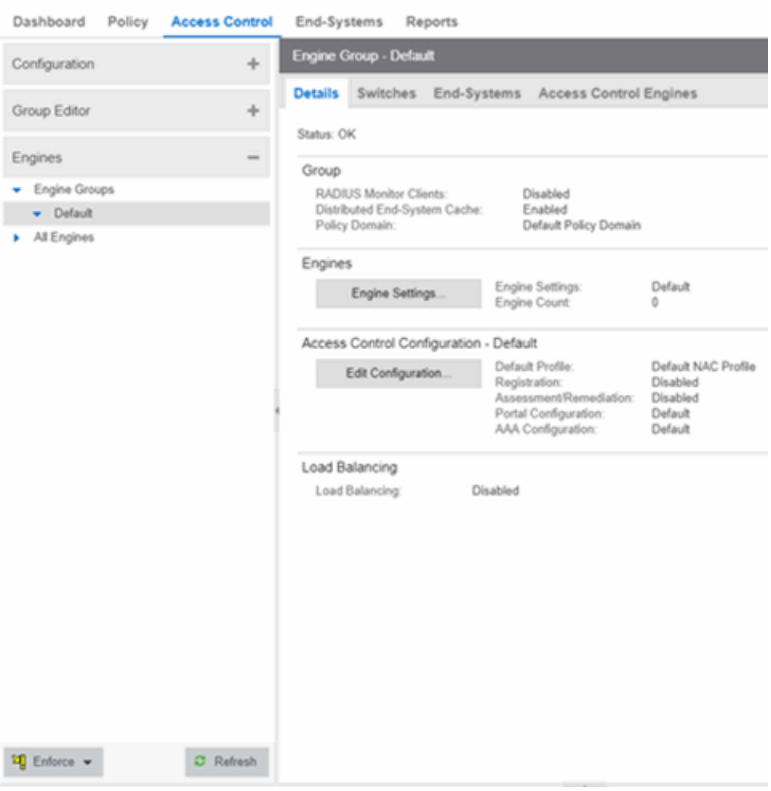
For Extreme Access Control Controller engines, when you disable Extreme Access Control authentication, then the Extreme Access Control Controller does not send RADIUS packets directly to the RADIUS servers. Authentication is disabled on the Extreme Access Control Controller and end-systems do not need to authenticate to the network. Traffic from the end-systems bypass the Extreme Access Control Controller and go directly onto the network.

The Status fields provide the current status of the Extreme Access Control authentication or assessment process. The authentication status field also includes a link to the Verify RADIUS Configuration on Switches feature. This feature is available for Extreme Access Control Gateway engines and Layer 2 Extreme Access Control Controllers, and can be used to alert you to any RADIUS configurations that are out of sync and could cause RADIUS authentication problems on the network.

Details (Extreme Access Control Engine Groups)

This tab provides information about the Extreme Access Control Details being used by your Extreme Access Control engines.

To access this tab, select an engine group from within the Engine Group tree in the left-panel tree, then click the **Details** tab in the right panel.



RADIUS Monitor Clients

Displays whether RADIUS Monitor Clients are enabled for the Extreme Access Control engines in the folder.

Distributed End-System Cache

Displays whether the Distributed End-System Cache option is enabled for the Extreme Access Control engines in the folder.

Policy Domain

Displays the policy domainfor the Extreme Access Control engines in the folder.

Engine Settings

The engine settings configuration being used by your Extreme Access Control engines. Engine settings are configurable through the Extreme Access Control Configurations view, by expanding the Extreme Access Control Configurations tree from the left panel.

Engine Count

The number of engines in the engine group.

Configuration

The name of the Extreme Access Control Configuration being used by your Extreme Access Control engines. The Extreme Access Control Configuration determines the Extreme Access Control Profile assigned to an end-system connecting to the network.

Default Profile

The name of the Default Profile specified in the Extreme Access Control Configuration. The Default Profile serves as a "catch-all" profile for any end-system that doesn't match one of the rules listed in the Extreme Access Control Configuration.

Registration

Whether a registration/web access feature is enabled or disabled for the Extreme Access Control Configuration.

Assessment/Remediation

Whether the assessment/remediation feature is enabled or disabled for the Extreme Access Control Configuration.

Portal Configuration

The name of the Portal Configuration specified in the Extreme Access Control Configuration. If your network is implementing Registration or Assisted Remediation, the Portal Configuration defines the branding and behavior of the website used by the end user during the registration or remediation process.

AAA Configuration

The name of the AAA Configuration specified in the Extreme Access Control Configuration.

Load Balancing

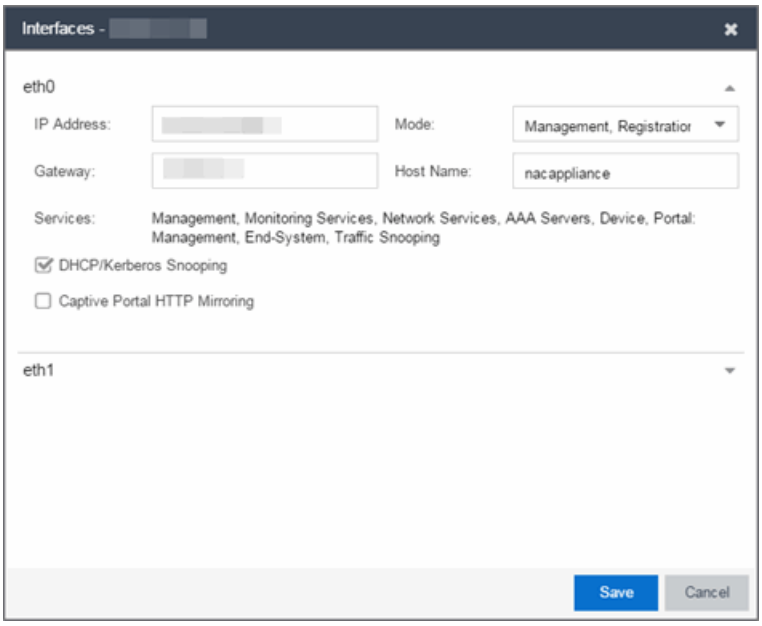
This section allows you to configure load balancing for the engine group. Extreme Management Center provides two different load balancing configuration options: either ExtremeXOS/EOS firmware on S-Series and K-Series devices, or utilizing

external load balancers. Load balancing allows you to evenly distribute authentication requests and switch configuration ownership among your Extreme Access Control gateway engines. This can be useful in Extreme Access Control deployments with a large number of switches, where manual delegation of switch resources would be cumbersome.

Interface Configuration Window

Use this Extreme Management Center window to configure the interfaces on an Extreme Access Control engine. Interface configuration allows you to separate management traffic from end-system traffic, providing another layer of protection for sensitive data. It also provides the ability to snoop mirrored traffic on other ports.

This window is accessed from the **Control** > **Extreme Access Control** tab by selecting an Extreme Access Control engine, opening the **Details** tab, and clicking the **Edit** button in the Interface Summary section.



Interface Modes

There are five different modes that can be configured for an interface: Management, Registration & Remediation, Management Only, Registration & Remediation Only, Listening Only, Advanced Configuration, and Off. The mode determines the type of traffic allowed on the interface and the services provided by the interface.

You can configure all the interfaces on an engine; however, you cannot change the management interface and you are only allowed to configure one interface to allow management traffic.

Management, Registration & Remediation – This mode is the in-band management mode where both management traffic and registration, assessment, and remediation traffic use the same interface. In this mode, the engine does not limit traffic to each of the services.

Management Only – In this mode, the engine binds all management services to this interface. This includes:

- traffic to Extreme Management Center and other engines (JMS and HTTP)
- all traffic to switches
- all LDAP and RADIUS traffic
- traffic for the following services: SSH daemon, SNMP daemon, and RADIUS server
- traffic for captive portal administration, sponsorship, pre-registration, and screen preview (on ports 80 and 443)
- traffic for WebView pages and Extreme Management Center web services (on ports 8080 and 8443)

Registration & Remediation Only – In this mode, the engine binds all registration and remediation services to this interface. All traffic to end-systems is initiated through this interface, including:

- assessment traffic
- NetBIOS for IP and hostname resolution
- traffic for registration pages, remediation pages, and self-registration (on ports 80 and 443)
- all agent communication traffic (on ports 8080 and 8443)

Listen Only – In this mode, the engine allows DHCP and Kerberos snooping to be performed on the interface. No IP address or hostname can be assigned to the interface.

Advanced Configuration - This mode allows you to configure the services that are provided by the selected interface, using the link in the Services field. This is useful for Extreme Access Control deployments in MSP or MSSP environments.

Off – The interface is disabled and not used in any way.

Services

The Services field displays the services that are provided by the Extreme Access Control engine interface, as determined by the selected interface mode. Each mode provides a different set of services on the interface.

If the mode is set to Advanced Configuration, the services list becomes a link that launches an Edit window where you can select or deselect the services provided by the interface. This granularity is useful for Extreme Access Control deployments in MSP or MSSP environments.

The following list describes the various services that are provided by the different modes:

- Management - The communication to and from the Extreme Management Center server. Sub-services include JMS, Web Services, and Syslog.
  NOTE: The Management service cannot be moved from eth0.
- Monitoring Services - The services used to monitor or contact an engine. Sub-services include the SSH daemon and SNMP agent.
- Network Services - The communication to external servers that provide networking services. Sub-services include DNS servers and NTP servers.
  NOTE: The Network Services service can only be applied to one interface.
- AAA Servers - The communication used by external servers for authentication and authorization. Sub-services include RADIUS servers and LDAP servers.
  NOTE: The AAA Servers service can only be applied to one interface.
- Device - The communication to and from a NAS (switch, router, VPN, or wireless controller). Sub-services include SNMP, RADIUS, RFC3576, SSH/Telnet, and TFTP.
- Portal: Management - the captive portal registration management services for an engine.
- End-System - The communication to and from end-systems. Sub-services include portal registration and remediation, assessment, NetBIOS, and DNS proxy.
- Traffic Snooping - DHCP and Kerberos snooping on the interface. This service is listed if the DHCP/Kerberos Snooping option is set to Enabled.

DHCP/Kerberos Snooping

Use the DHCP/Kerberos Snooping option to enable or disable DHCP and Kerberos snooping on the interface. DHCP snooping is used for IP resolution and OS detection. Kerberos snooping is used for user name detection and elevated access.

Captive Portal HTTP Mirroring

This is an advanced option that allows the interface to accept mirrored HTTP traffic which is used to display the captive portal to end users. This option is an alternative to using Policy-Based Routing and DNS Proxy.

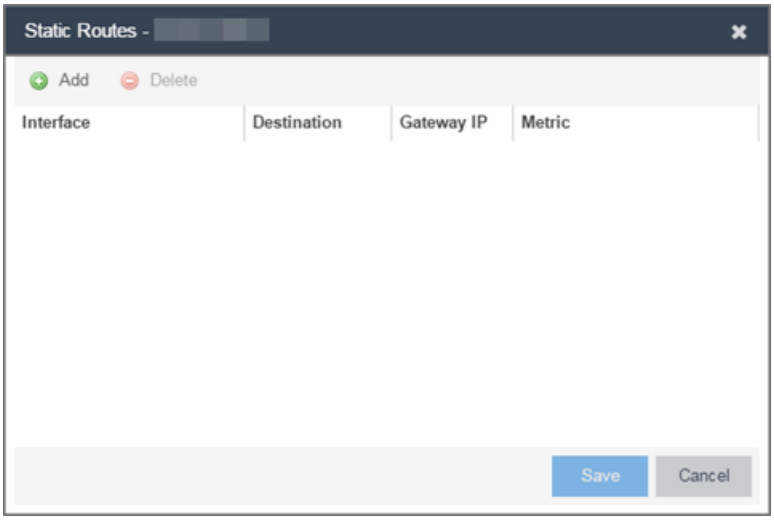
Tagged VLANs

If the mirrored traffic includes an 802.1Q VLAN tag, then the list of VLANs to capture must be explicitly stated in this field by entering a comma-separated list of VLAN IDs from 1 to 4094. If the mirrored traffic is not tagged then this field can be left blank.

Static Route Configuration Window

This window displays the static routes used for advanced routing configuration. Use the toolbar buttons to add, edit, or delete a route.

This window is accessed from the Control > Extreme Access Control tab by selecting an Extreme Access Control engine, opening the Details tab, and clicking the Static Routes button in the Interface Summary section.



Interface
: The Extreme Access Control engine interface used for the static route.

Destination
: The IP address used to define the subnet or individual device whose traffic is assigned to the route.

Gateway IP
: The IP address of the device where traffic matching the Network value is sent.

Metric
: A number used to configure route precedence. The lower the number, the higher the precedence.

How To Use Access Control

The How To section contains Help topics that give you instructions for performing tasks in the Access Control tab.

How to Use Device Type Profiling

This Help topic describes how to set up device type profiling in your Extreme Access Control Configuration using device type rule groups. Device type profiling lets you assign Extreme Access Control profiles to end-systems based on operating system family, operating system, or hardware type. This allows you to use the end-system's device type to determine the end user's level of network access control and whether the end-system is scanned. For more information on device type groups, see the Add/Edit Device Type Group Window Help topic.

NOTE: Assessment provides the most accurate determination of device type. If the initial device type determination is not based on assessment results, it may be less reliable. For that reason, device type rule groups should be based on broad families of device types.

Here are some examples of how device type profiling can be used to determine network access:

- When an end user with valid credentials logs in to the network on a registered iPad versus a registered Windows 10 machine, they receive a lower level of network access.
- When an end user registers a Windows machine using its MAC address, another user cannot spoof that MAC address using a Linux system. (Device profiling does not resolve this issue in environments with dual boot machines.)
- If an end user exports a certificate from a corporate PC to an iPad and successfully authenticates with 802.1x, the iPad is not allowed full network access.

Device Profiling Use Case

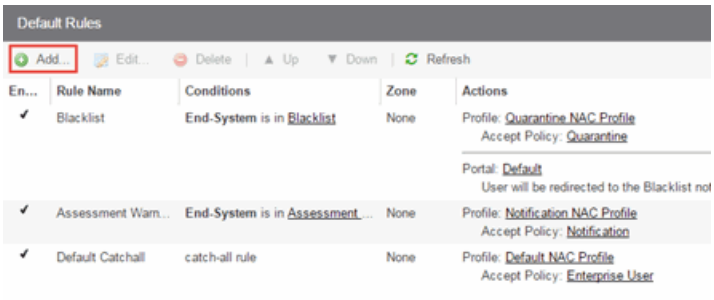
This section provides high-level instructions for configuring device type profiling for a sample use case. In this scenario, the network administrator has the following network access requirements:

- All Windows registered devices should be assigned the "Default Extreme Access Control Profile."
- All Windows 10 registered devices should be assigned the "Windows10 Profile."

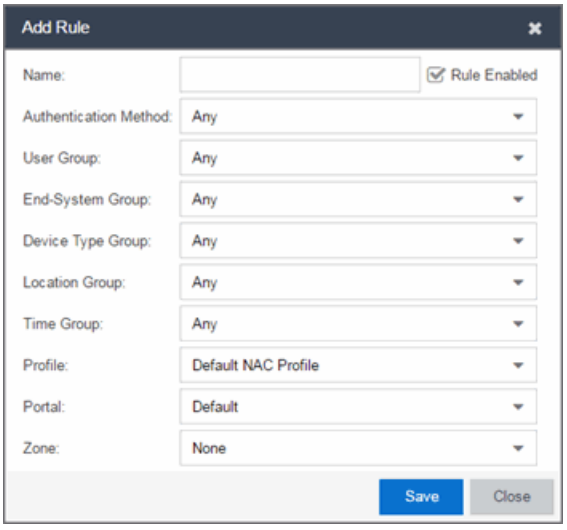
- All Linux registered devices should be assigned the "Default Extreme Access Control Profile." In addition, a new Linux version called SuperLinux needs to be added to the Linux family device type.
- All HP Printers should be assigned the "HP Printer Profile."

To do this, create four rules in your Extreme Access Control configuration that use device type as criteria for matching rules to end-systems authenticating to the network. The following instructions assume that you already created your profiles: Basic Profile, Windows10 Profile, and HP Printer Profile.

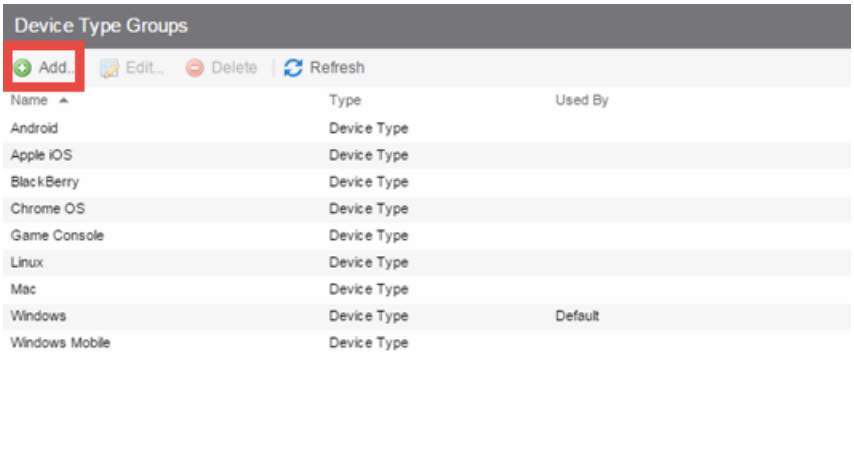
1. Expand the Default left-panel tree (Control > Extreme Access Control> Extreme Access Control Configurations > Default).
2. Select the Rules left-panel option and click the **Add** button in the right panel.



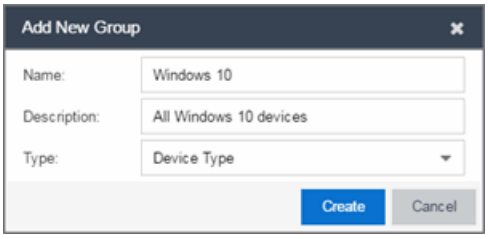
3. Create a rule that assigns the Default Extreme Access Control Profile to all Registered Guests using Windows devices as shown below.



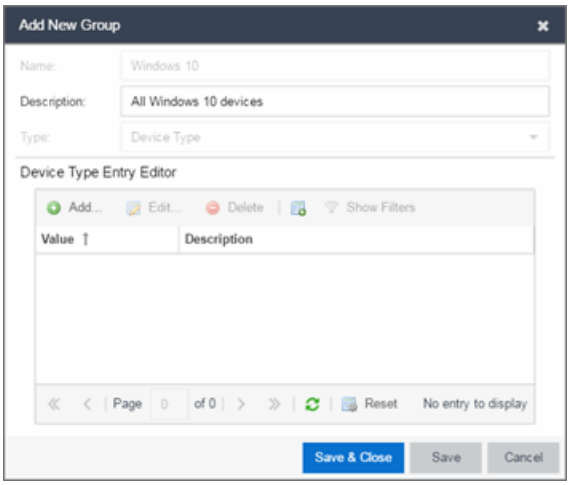
4. Create a rule that assigns the Windows10 Profile to all Windows 10 registered devices. To do this, you need to create a new Windows 10 device type group.
    a. From the Extreme Access Control Configurations left-panel tree, expand the Group Editor tree.
    b. Select Device Type Groups and click the **Add** button in the right panel.



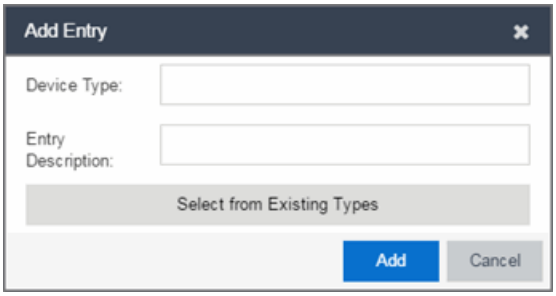
    c. Create a new device type group with the name Windows 10.



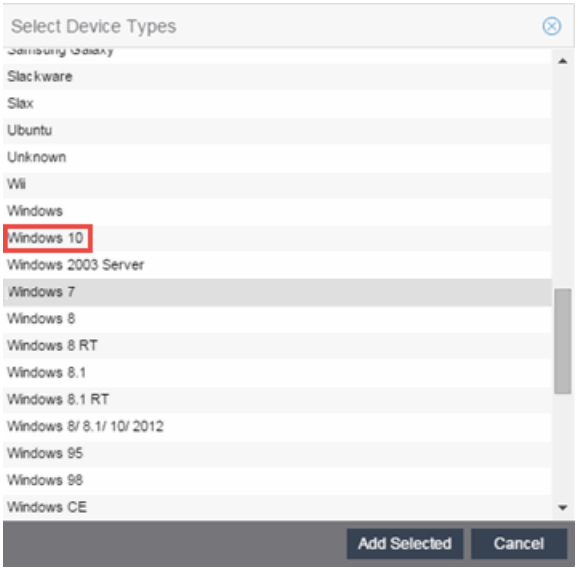
d. Click **Create**. The Device Type Entry Editor appears.



e. Click the **Add** button. The Add Entry window appears.



f. Click the **Select from Existing Types** button and in the Select Device Types window, select Windows 10.



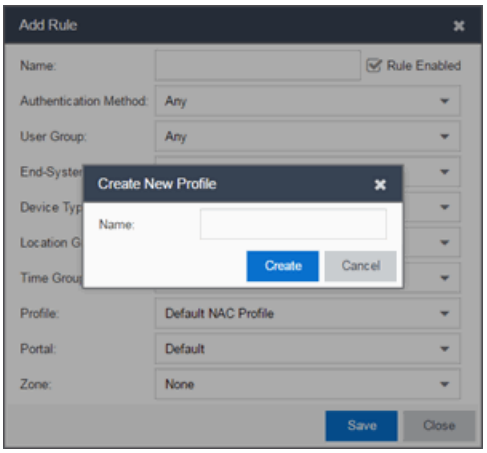
g. Click the **Add Selected** button.

h. Click the **Save & Close** button on the Add New Group window.

i. You can then create the rule.

j. Select the Extreme Access Control Configurations > Default > Rules left-panel option and click the **Add** button in the right panel.

k. In the Profile drop-down menu, select **New**. The Create New Profile window appears.

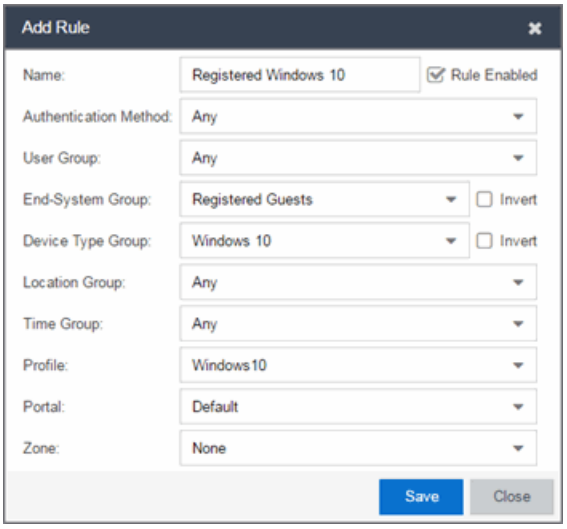


l. Enter the name **Windows10** in the **Name** field and click the **Create** button.

The Extreme Access Control Profile window opens.

m. Click **Save**.

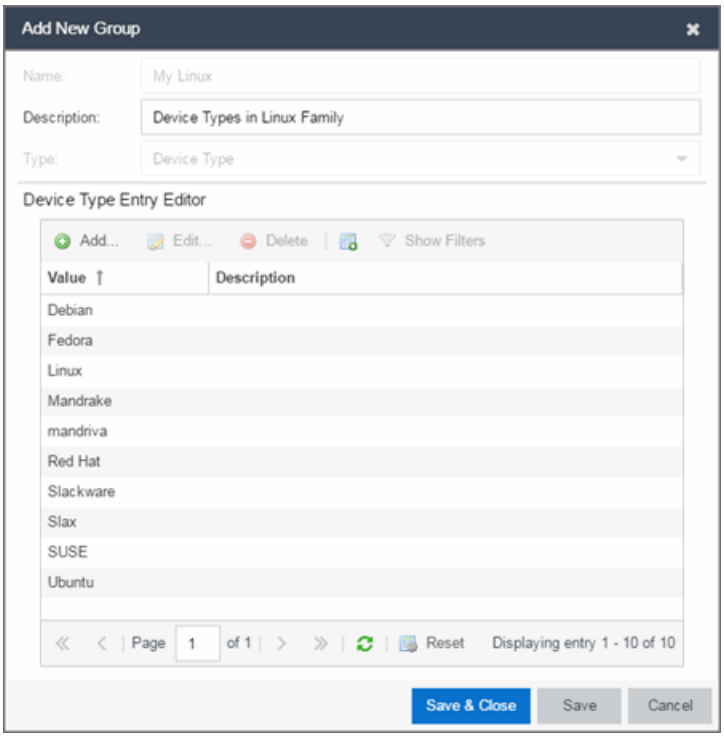
n. Configure the rule as shown in the screenshot below.



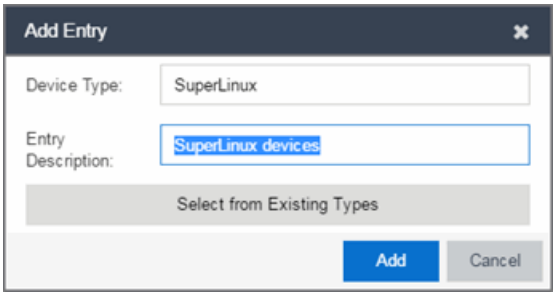
o. Click **Save**.

5. Create a rule that assigns the Default Extreme Access Control Profile to all Linux registered devices and add the SuperLinux version to the Linux family device type. To do this, you need to create a new Linux device type group that includes SuperLinux.

   a. Create the My Linux device type group to include the devices in the Linux device type group using the **Select from Existing Types** button in the Add Entry window as discussed in step 4f above.



b. Click the **Add** button and in the Add Entry window, create the **SuperLinux** Device Type as shown below.

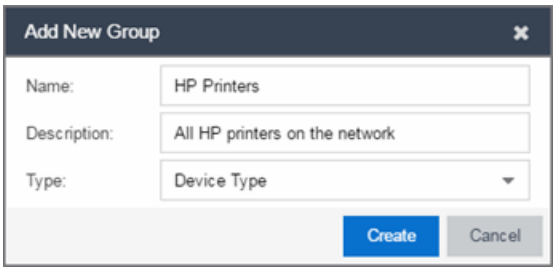


c. Click **Add** to save the SuperLinux device type to the My Linux device type group.

d. Click the **Save & Close** button on the Add New Group window.

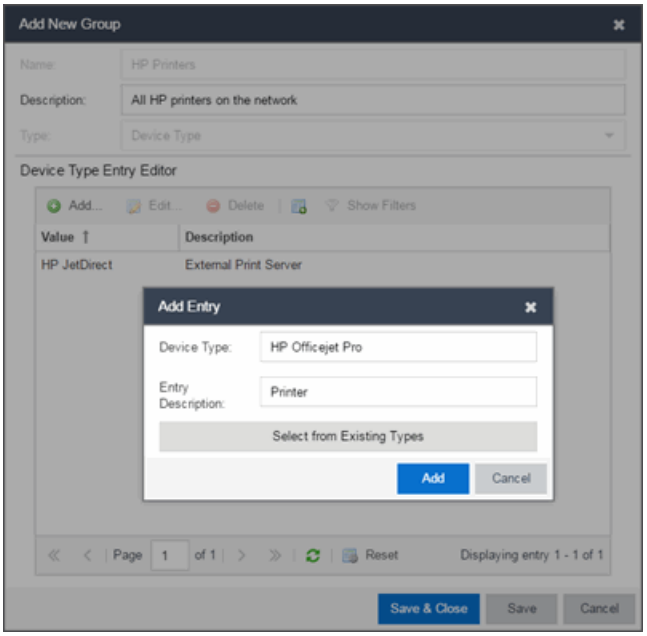
6. Create a rule that assigns the HP Printer Profile to all HP printers on the network. To do this, create a new HP Printers device type group.

   a. Open the Add New Group window by clicking the **Add** button on the Extreme Access Control Configurations > Group Editor > Device Type Groups panel.



b. Click **Create**. The Device Type Entry Editor section appears.

c. Add the HP Printers via the Add Entry window by clicking the **Add** button as shown below.



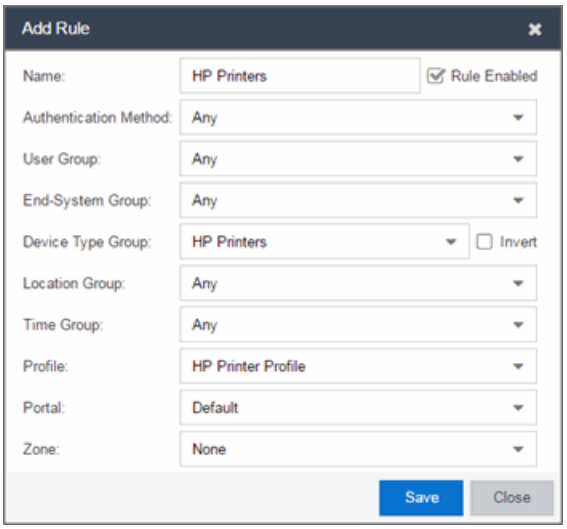
d. Click **Save & Close** to save the HP Printers group.

e. Select Rules in the left-panel tree (Extreme Access Control Configurations > Default > Rules).

f. Click **Add** in the right-panel to open the Add Rule window.

g. Click the New option in the Profile drop-down menu and create the **HP Printer Profile**.

h. Create the HP Printers rule using the following criteria.



i. Click **Save**.

7. Your Extreme Access Control Configuration now contains the following rules used to determine network access and assessment requirements based on device type.

Related Information

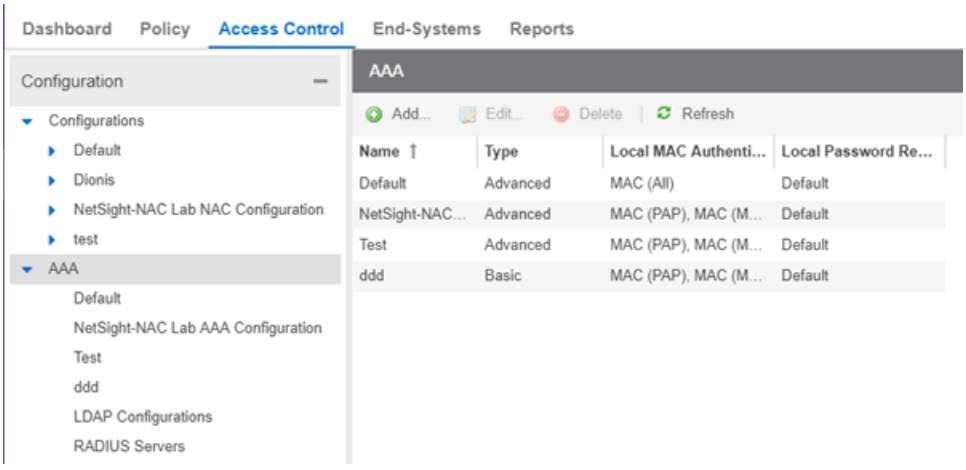
- Add/Edit Device Type Group Window
- Create Rule Window
- Manage Rule Groups Window

How to Configure LDAP for End Users and Hosts via Active Directory in Extreme Management Center

This Help topic provides instructions for creating LDAP configurations in Access Control that provide authentication and authorization for network end users and host machines via Active Directory.

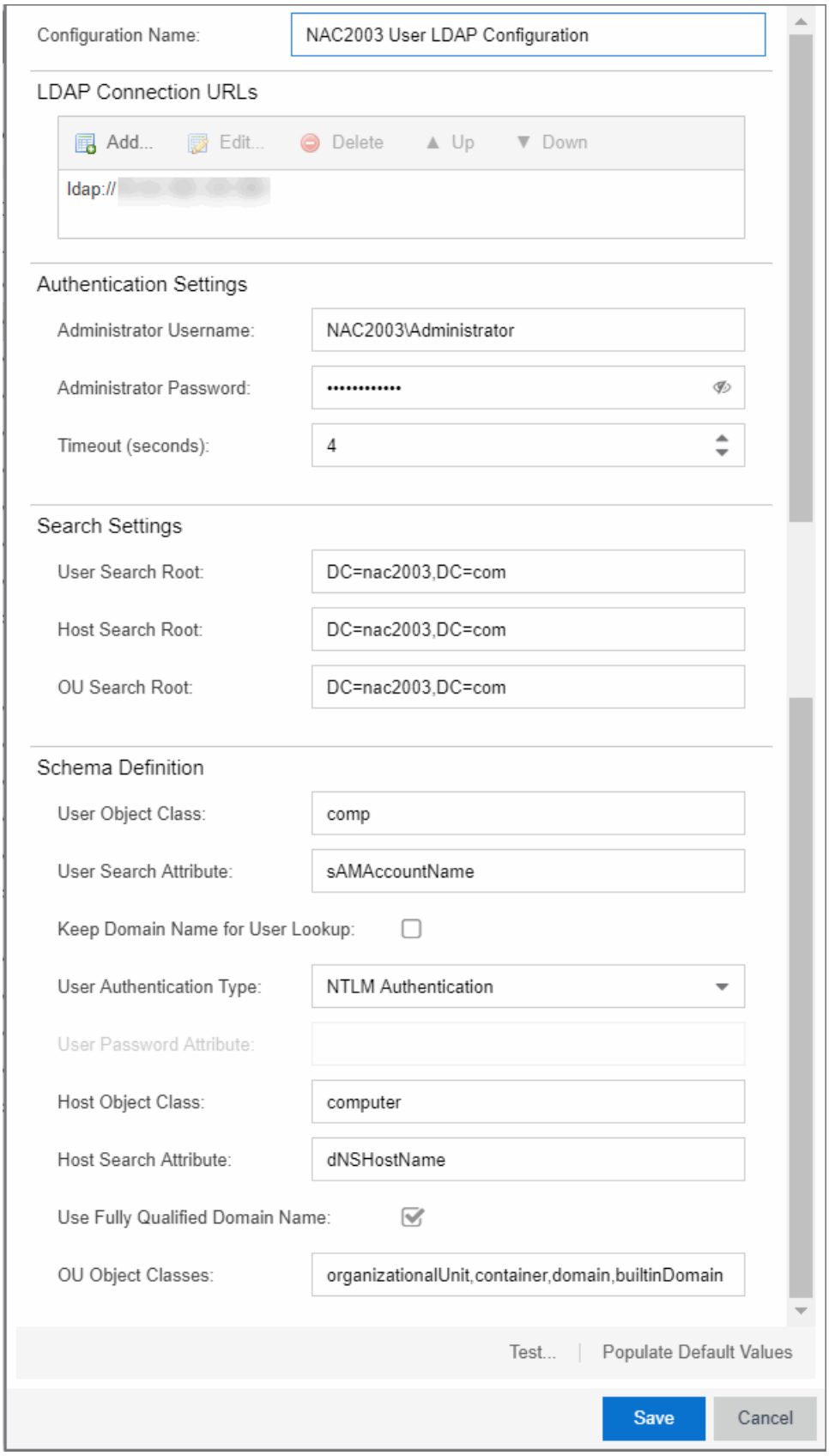
In Access Control, you can create an Advanced AAA configuration that contains one mapping rule for your host machines and two mapping rules for your users. These mappings are the same except for their LDAP configuration. You need to create two LDAP configurations: one for the hosts mapping and one for the users mapping. The LDAP configurations are identical except for the User Search Attribute. When you have completed these instructions, Access Control uses the new AAA onfiguration to authenticate both end users and host machines via your Active Directory server.

1. Click Control > Access Control > Configuration tab.
2. In the left-panel tree, select the AAA tab to open the AAA Configuration window to the right.

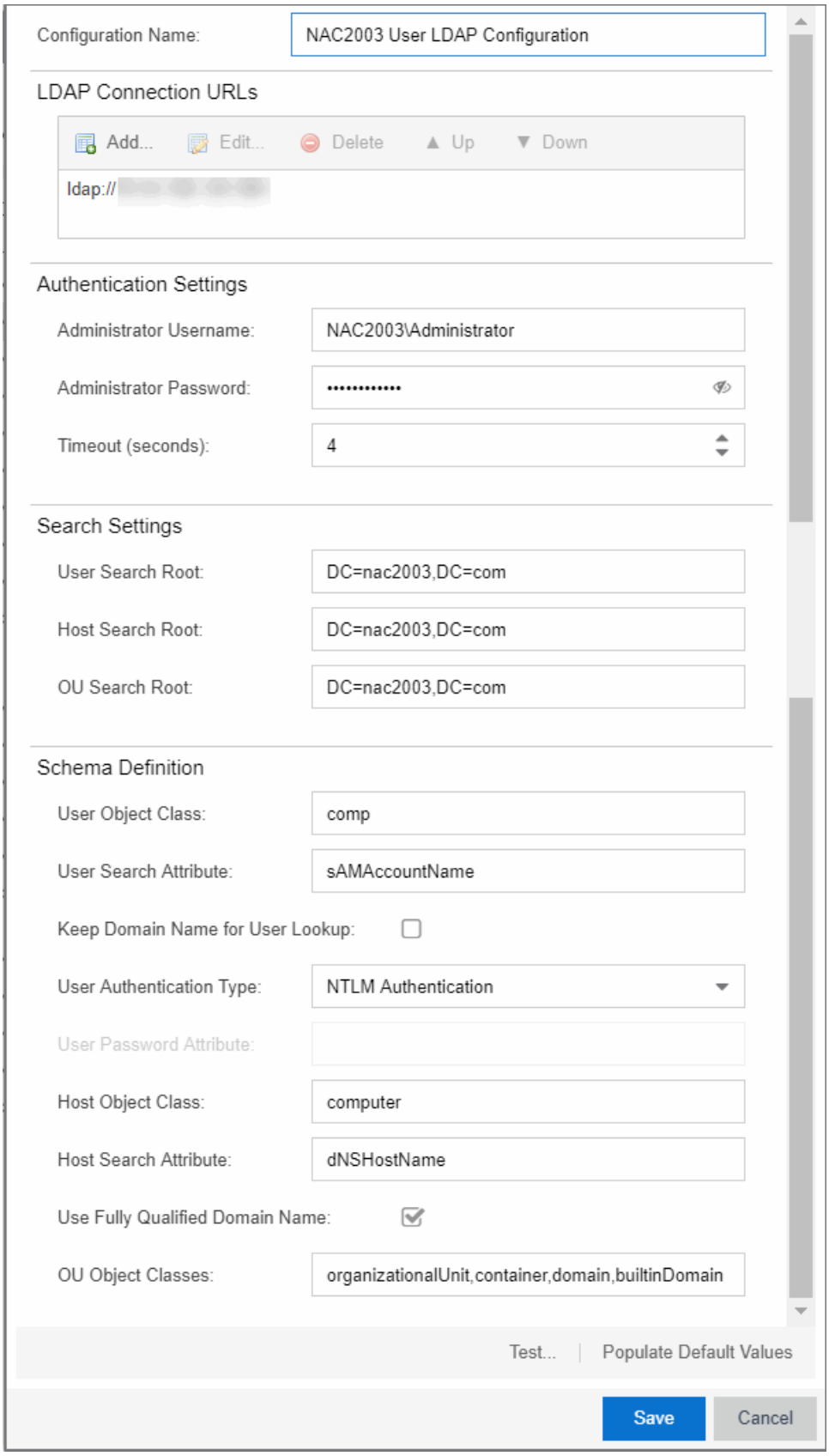


3. Click the Add button in the AAA Configuration panel create a new AAA Configuration.

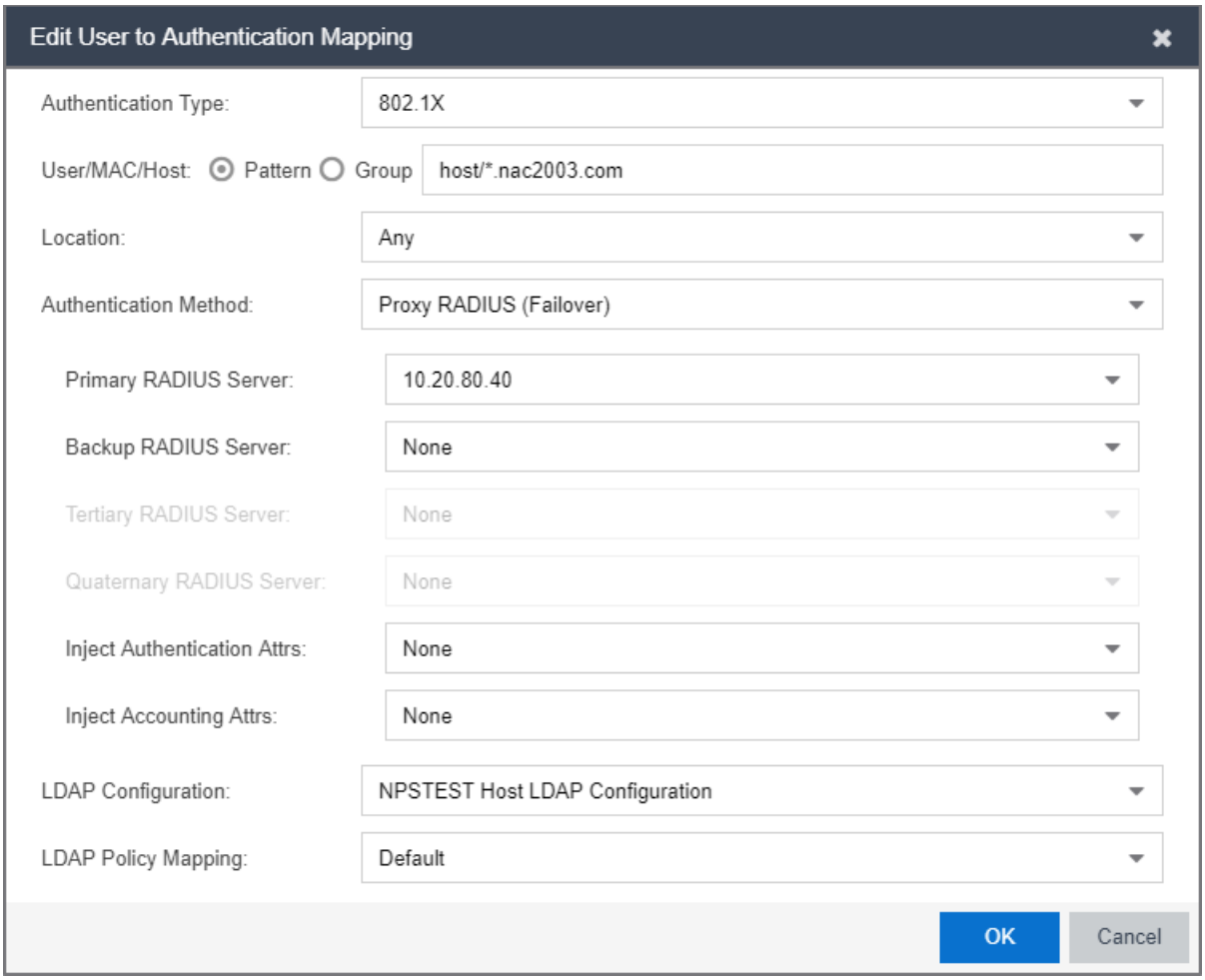
4. Click LDAP Configuration in the left-panel tree to open the LDAP Configuration window.
5. Create an LDAP configuration for use with end users that authenticate to the network using the sample below as a guide. Click Save.


Configuration Name:
NAC2003 User LDAP Configuration
LDAP Connection URLs
Add...
Edit...
Delete
Up
Down
ldap://
Authentication Settings
Administrator Username:
NAC2003\Administrator
Administrator Password:
Timeout (seconds):
4
Search Settings
User Search Root:
DC=nac2003,DC=com
Host Search Root:
DC=nac2003,DC=com
OU Search Root:
DC=nac2003,DC=com
Schema Definition
User Object Class:
comp
User Search Attribute:
sAMAccountName
Keep Domain Name for User Lookup:
User Authentication Type:
NTLM Authentication
User Password Attribute:
Host Object Class:
computer
Host Search Attribute:
dNSHostName
Use Fully Qualified Domain Name:
OU Object Classes:
organizationalUnit,container,domain,builtinDomain
Test...
Populate Default Values
Save
Cancel

6. Open the Add LDAP Configuration window to add another LDAP configuration that will be used for host machines that authenticate to the network using the sample below as a guide. Note that the only difference between the two LDAP configurations is the User Search Attribute. Click Save.

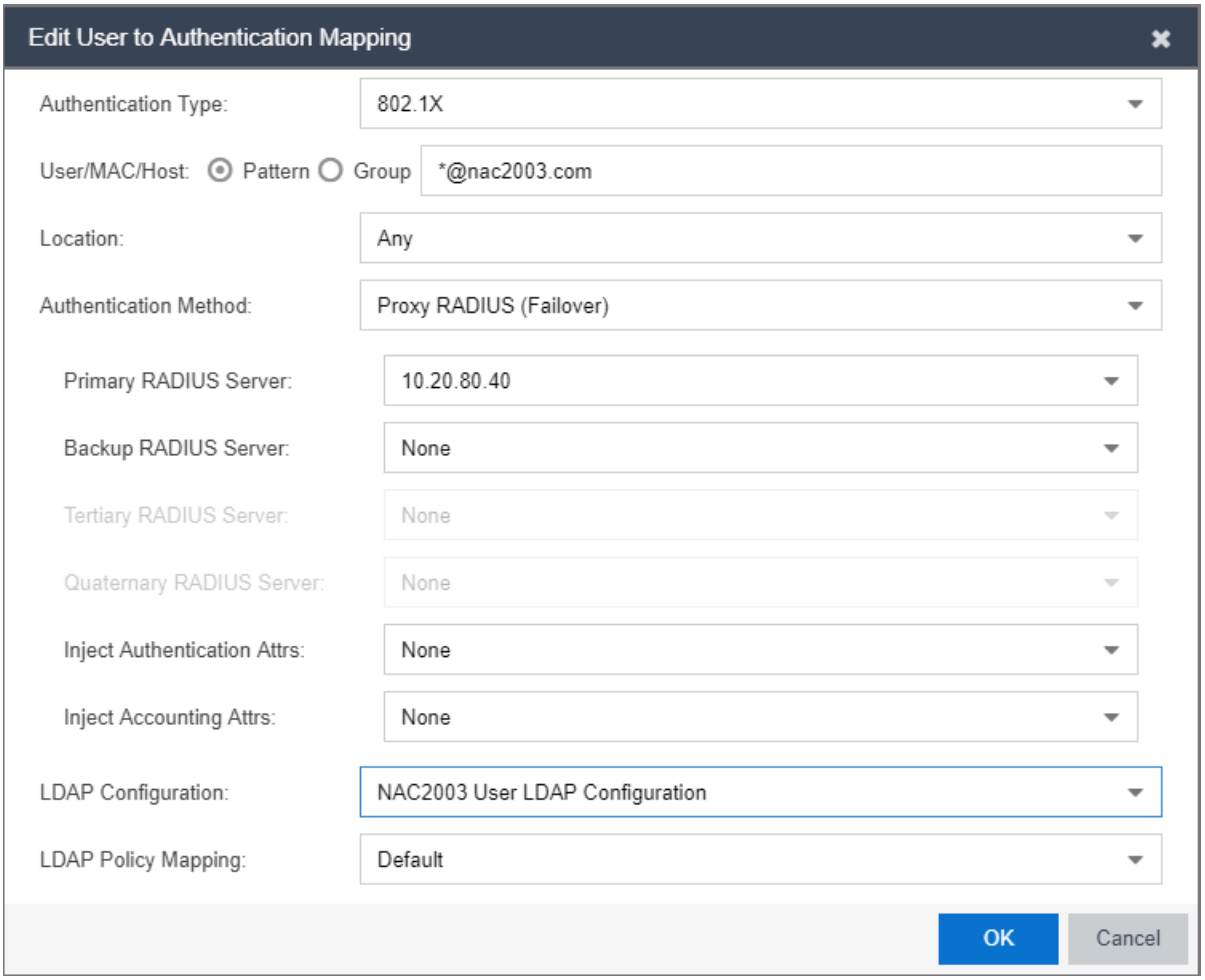

Configuration Name:
NAC2003 User LDAP Configuration
LDAP Connection URLs
Add...
Edit...
Delete
Up
Down
ldap://
Authentication Settings
Administrator Username:
NAC2003\Administrator
Administrator Password:
Timeout (seconds):
4
Search Settings
User Search Root:
DC=nac2003,DC=com
Host Search Root:
DC=nac2003,DC=com
OU Search Root:
DC=nac2003,DC=com
Schema Definition
User Object Class:
comp
User Search Attribute:
sAMAccountName
Keep Domain Name for User Lookup:
User Authentication Type:
NTLM Authentication
User Password Attribute:
Host Object Class:
computer
Host Search Attribute:
dNSHostName
Use Fully Qualified Domain Name:
OU Object Classes:
organizationalUnit,container,domain,builtinDomain
Test...
Populate Default Values
Save
Cancel

7. In the left-panel tree, click an AAA Configuration to open the Advanced AAA Configuration window.
8. In the Authentication Rules panel of the Advanced AAA Configuration window, click the **Add** button to open the Add User to Authentication Mapping window.
9. Create your first mapping rule to capture machine authentications using the sample below as a guide. In the example below, **host/*.nac2003.com** will capture the machine authentications for the NAC2003 active directory domain. Be sure to select the host LDAP Configuration that you created. Click OK.

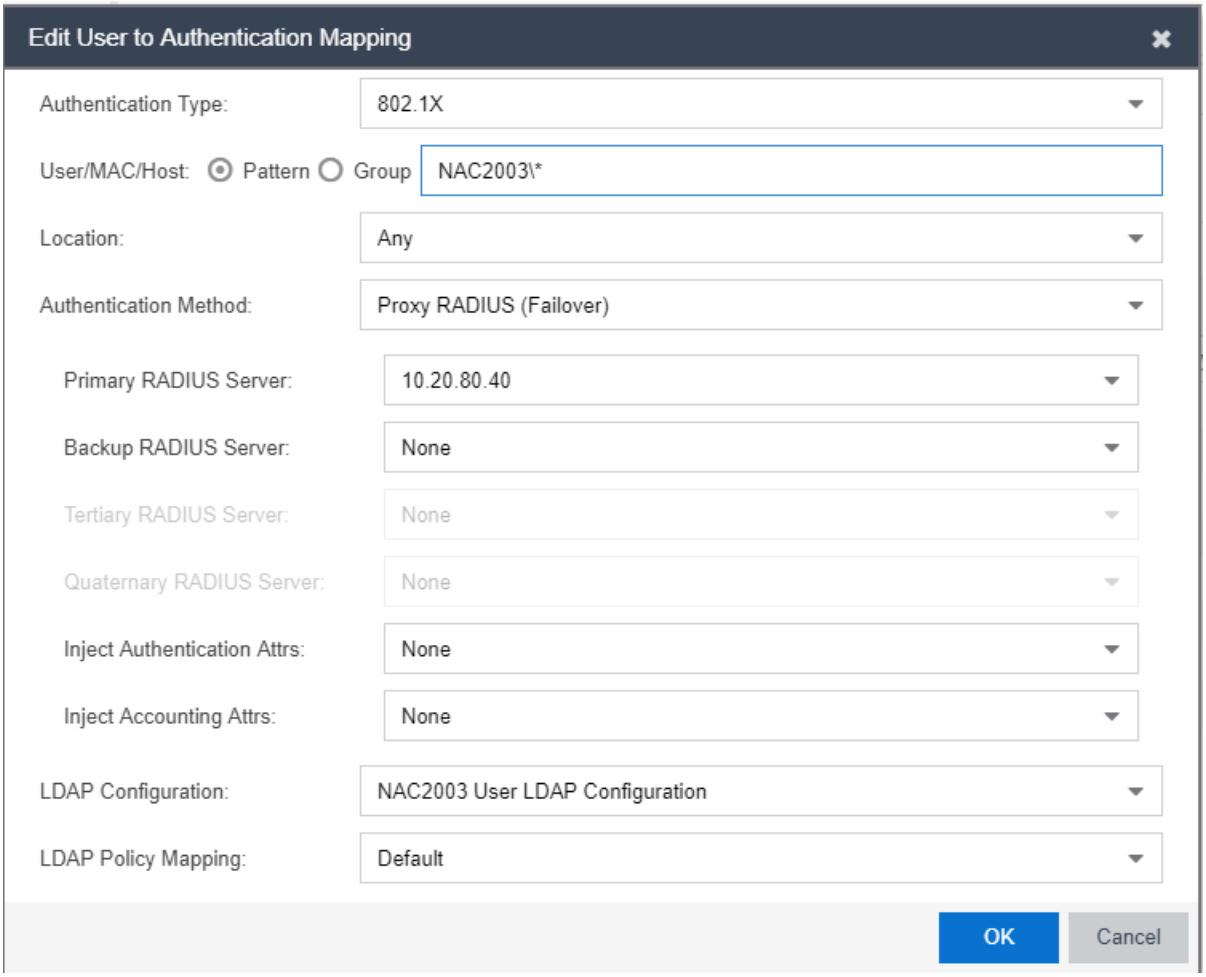


10. Create your second mapping rule to capture end user authentications using the sample below as a guide. In the example below, ***@nac2003.com** will capture all users logging in to the NAC2003 active directory domain when they authenticate

with their username in the format <username>@<domain>. Be sure to select the end user LDAP Configuration that you created. Click OK.



11. Create your third mapping rule to capture other end user authentications using the sample below as a guide. In the example below, NAC2003* will capture all users logging in to the NAC2003 active directory domain when they authenticate with their username in the format <domain>\<username>. Be sure to select the end user LDAP Configuration that you created. Click OK.



12. In the left-panel tree, click an AAA Configuration to open the Advanced AAA Configuration window. Use the Up and Down buttons (▲ Up ▼ Down) to move your new mappings above the "Any" mappings in the list of mappings. Click Save.

You can configure your LDAP policy mappings and/or LDAP user groups based on the attributes from either your host or user LDAP configurations.

Related Information

For information on related windows:

- Add User to Authentication Mapping Window
- AAA Configuration Window

How to Change the Assessment Agent Adapter Password

This Help topic provides instructions for changing the password on the assessment agent adapter on your network assessment servers, including agent-less, Nessus, or a third-party assessment agent (an assessment agent not supplied or supported by Extreme Management Center). The assessment agent adapter enables communication between the Extreme Access Control engine and the assessment servers, and the password is used by the assessment agent adapter to authenticate Extreme Access Control engine assessment requests.

This password must match the password specified in the Extreme Access Control Options as the Assessment Agent Adapter Credentials (Administration > Options > Identity and Access > Assessment Server). If you change the password on the assessment agent adapter, change assessment agent adapter credentials in the Extreme Access Control options as well, or connection between the engine and assessment servers is lost and assessments is not performed.

To change the assessment agent adapter password:

1. Go to the install directory for the assessment agent adapter on the assessment server. This can be a Nessus server or the Extreme Access Control engine if you are using on-board agent-less assessment. On an Extreme Access Control engine, the install directory is **/opt/nac/saint**.
2. Run the **sha1.sh** script (on an Extreme Access Control engine, the script is located in located in **/opt/nac/saint/util**) using the new password as the argument. The script produces a hash string that looks something like:
   9ba2db465ff11b0bdfd188f7ee87b10fc3a145dc
3. Open the **users.properties** file (on an Extreme Access Control engine, the file is located in **/opt/nac/saint/users.properties**) and replace the existing hash string with the new one:
   `admin=<new string>`
4. Restart the assessment agent adapter. On an Extreme Access Control engine, the command is `aglsctl restart`.

Related Information

For information on related tasks:

- How to Install the Assessment Agent Adapter on a Nessus Server
- How to Set Extreme Access Control Options - Assessment Server

For information on related windows:

- Manage Assessment Settings Window
- Extreme Access Control Options - Assessment Server

How to Set Extreme Access Control Options

Use the Options window (**Administration > Options**) to set options for Extreme Access Control. In the Options window, the right-panel view changes depending on what you have selected in the left-panel tree. Expand the Extreme Access Control folder in the tree to view all the different options you can set.

Instructions on setting the following Extreme Access Control options:

Advanced Settings

Use the Advanced Settings panel to configure advanced settings for Extreme Access Control. These settings apply to all users on all clients.

1. Select **Administration > Options** in Extreme Management Center. The Options window opens.
2. In the left-panel tree, expand the Extreme Access Control folder and select Advanced Settings.
3. Use the **Resource Allocation Capacity** option configure the Extreme Management Center resources allocated to end-system and configuration processing services. The greater the number of end-systems and engines in your Extreme Access Control deployment, the more resources it requires.

- Low - For low performance shared systems.
- Low-Medium - For medium performance shared systems, or low performance dedicated systems
- Medium - For medium performance shared systems, or medium performance dedicated systems.
- Medium-High - For high performance shared systems, or medium performance dedicated systems.
- High - For high performance dedicated systems.
- Maximum - For extremely high performance dedicated systems.

4. Use the Hybrid Mode option to enable Hybrid Mode for Layer 2 Controllers. Hybrid Mode allows a Layer 2 Extreme Access Control Controller engine to act as a RADIUS proxy for switches, like an Extreme Access Control Gateway engine. Select this option to enable Hybrid Mode for your Layer 2 Controllers at a global level. When the option is selected, the Configuration tab for a Layer 2 Controller displays an option to enable Hybrid Mode for that specific controller. Disabling Hybrid Mode at the global level when a controller has switches has a similar effect to deleting a gateway: the switches have the controller removed as a reference.
5. The Enable IPv6 Addresses for End-Systems option allows Extreme Access Control to collect, report, and display IPv6 addresses for end-systems in the end-systems table. When this option is changed, you must enforce your engines before the new settings take effect. In addition, end-systems needs to rediscover their IP addresses in order to reflect the change in the end-system 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 that have only IPv6 addresses are not supported. End-system functionality support varies for IPv6 end-systems. For complete information, see Extreme Access Control Tab Support in the Extreme Management Center Configuration Considerations Help topic.
6. Click Save or select the Autosave checkbox.

Assessment Server

Use the Assessment Server view to provide assessment agent adapter credentials. The options apply to all users on all clients.

The assessment agent adapter credentials are used by the Extreme Access Control engine when attempting to connect to network assessment servers, including Extreme Networks Agent-less, Nessus, or a third-party assessment server (an assessment server that is not supplied or supported by Extreme Management Center). The password is used by the assessment agent adapter (installed on the assessment server) to authenticate assessment server requests. Extreme Access Control provides a default password you can change, if desired. However, if you change the password here, you need to change the password on the assessment agent adapter as well, or connection between the engine and assessment agent adapter is lost and assessments are not performed. For instructions, see How to Change the Assessment Agent Adapter Password.

1. Select **Administration > Options**. The Options window opens.
2. In the left-panel tree, expand the Extreme Access Control folder and select Assessment Server.
3. Specify the assessment agent adapter credentials.
4. Click **Save** or select the **Autosave** checkbox.

Data Persistence

Use the Data Persistence view to customize how Extreme Management Center ages-out or deletes end-systems, end-system events, and end-system health results (assessment results) from the tables and charts in the End-Systems tab. These settings apply to all users on all clients.

1. Select **Administration > Options**. The Options window opens.
2. In the left-panel tree, expand the Extreme Access Control folder and select Data Persistence.
3. In the **Age End-Systems** section, enter the number of days the Data Persistence Check uses as criteria for aging end-systems. Each day, when the Data Persistence check runs, it searches the database for end-systems Extreme Management Center has not received an event for in the number of days specified (90 days by default). It removes those end-systems from the tables in the End-Systems tab.
4. If you select the **Remove Associated MAC Locks and Occurrences in Groups** checkbox, the aging check also removes any MAC locks or group memberships associated with the end-systems being removed. The **Remove Associated**

Registration Data checkbox is selected by default, so the aging check also removes any registration data associated with the end-systems being removed.

5. In the End-System Event Persistence section, select the checkbox if you want Extreme Management Center to store non-critical end-system events, which are events caused by an end-system reauthenticating. End-system events are stored in the database. Each day, when the Data Persistence check runs, it removes end-system events which are older than the number of days specified (90 days by default).
6. In the End-System Information Event section, select the checkbox if you want Extreme Management Center to generate an Extreme Access Control event when end-system information is modified.
7. In the Health Result Persistence section, specify how many health result (assessment results) summaries and details are saved and displayed in the End-Systems tab for each end-system. By default, the Data Persistence check saves the last 30 health result summaries for each end-system along with detailed information for the last five health result summaries per end-system.
   There are two additional options:
   - You can specify to only save the health result details for quarantined end-systems (with the exception of agent-based health result details, which are always saved for all end-systems).
   - You can specify to save duplicate health result summaries and detail. By default, duplicate health results obtained during a single scan interval are not saved. For example, if the assessment interval is one week, and an end-system is scanned five times during the week with identical assessment results each time, the duplicate health results are not saved (with the exception of administrative scan requests such as Force Reauth and Scan, which are always saved). This reduces the number of health results saved to the database. If you select this option, all duplicate results are saved.
8. Set the time you would like the Data Persistence Check to be performed each day.
9. In the Transient End-Systems section, configure the number of days to keep transient end-systems in the database before they are deleted as part of the nightly database cleanup task. The default value is 1 day. A value of 0 disables the deletion of transient end-systems. Transient end-systems are Unregistered end-systems and have not been seen for the specified number of days. End-systems are not deleted if they are part of an End-System group or there are MAC locks associated with them. Select the Delete Rejected End-Systems checkbox if you want end-systems in the

Rejected state to be deleted as part of the cleanup. You can also delete transient end-systems using the Tools > End-System Operations > Data Persistence option.

10. Click **Save** or select the **Autosave** checkbox.

End-System Event Cache

End-system events are stored daily in the database. In addition, the end-system event cache stores in memory the most recent end-system events and displays them in the End-System Events tab. This cache allows Extreme Management Center to quickly retrieve and display end-system events without having to search through the database. Use the End-System Event Cache view to configure the amount of resources used by the end-system event cache. This setting applies to all users on all clients.

1. Select **Administration > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Extreme Access Control folder and select End-System Event Cache.
3. Specify the parameters to use when searching for older events outside of the cache. (The search is initiated by using the **Search for Older Events** button in the End-System Events tab.) The search is ended when any one of the parameters is reached.

    - Maximum number of days to go back when searching
    - Maximum number of results to return from search
    - Maximum time to spend searching for events

4. Specify the number of events to cache. Keep in mind the more events you cache, the faster data is returned, but caching uses more memory.
5. The End-System Event Cache also keeps a secondary cache of events by MAC address. This means a particular end-system's events can be more quickly accessed in subsequent requests. Specify the number of MAC addresses kept in the secondary cache. Keep in mind that the more MAC addresses you cache, the more memory used. Also, note the secondary cache may includes events not in the main cache, but were retrieved by scanning the database outside the cache boundary.
6. Click **Save** or select the **Autosave** checkbox.

Enforce Warning Settings

Use the Enforce Warning Settings view to specify warning messages you don't want displayed during the Enforce engine audit.

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

These settings allow you to select specific warning messages that you do not want to have displayed in the audit results. This allows you to proceed with the Enforce without having to acknowledge the warning message. For example, you may have an Extreme Access Control configuration that always results in one of these warning messages. By selecting that warning here, it is ignored in future audit results and you no longer have to acknowledge it before proceeding with the Enforce.

1. Select Administration > Options in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Extreme Access Control folder and select Enforce Warnings. The Enforce Warnings view opens.
3. Select the checkbox in the Ignore column next to the warning messages you don't want displayed.
4. Click Save or select the Autosave checkbox.

Setting Features Options

Use the Features view to automatically create new Policy mappings and profiles. If you are not using these features, you can disable them to remove sections that pertain only to those features from certain Extreme Management Center windows.

Notification Engine Options

Use the Notification Engine view to define the default content contained in Extreme Access Control notification action messages. For example, with an email notification action, you can define the information contained in the email

subject line and body. With a syslog or trap notification action, you can specify certain information you want contained in the syslog or trap message. These settings apply to all users.

There are certain "keywords" that you can use in your email, syslog, and trap messages to provide specific information. Following is a list of the most common keywords used. For a complete list of available keywords for Extreme Access Control notifications, see the Keywords Help topic.

- $type - the notification type.
- $trigger - the notification trigger.
- $conditions - a list of the conditions specified in the notification action.
- $ipaddress - the IP address of the end-system that is the source of the event.
- $macaddress - the MAC address of the end-system that is the source of the event.
- $switchIP - the IP address of the switch where the end-system connected.
- $switchPort - the port number on the switch where the end-system connected.
- $username - the username provided by the end user upon connection to the network.

1. Select Administration > Options. The Options window opens.
2. In the left-panel tree, expand the Extreme Access Control folder and select Notification Engine. The Notification Engine view opens.
3. Use the fields to define the default content contained in notification action messages. For a definition of each field, see the Notification Engine view Help topic.
4. In the Advanced section, set parameters for the Action and Event queues processed by the Notification engine.
5. Click Save or select the Autosave checkbox.

Policy Defaults

Use the Policy Defaults view to specify a default policy role for each of the four access policies. These default policy roles display as the first selection in the drop-down lists when you create an Extreme Access Control profile. For example, if you specify an Assessment policy called "New Assessment" as the Policy Default, then "New Assessment" automatically displays as the first

selection in the Assessment Policy drop-down list in the New Extreme Access Control Profile window.

Extreme Management Center supplies seven policy role names from which you can select. You can add more policies in the Edit Policy Mapping window, where you can also define policy to VLAN associations for RFC 3580-enabled switches. Once a policy is added, it becomes available for selection in this view.

1. Select **Administration > Options**. The Options window opens.
2. In the left-panel tree, expand the Extreme Access Control folder and select Policy Defaults.
3. Select the desired policies.
    - The **Accept policy** is applied to an end-system when an end-system has been authorized locally by the Extreme Access Control Gateway and has passed an assessment (if an assessment was required), or the "Replace RADIUS Attributes with Accept Policy" option is used when authenticating the end-system.
    - The **Assessment policy** is applied to an end-system while it is being assessed (scanned).
    - The **Failsafe policy** is applied to an end-system when it is in an Error connection state. An Error state results if the end-system's IP address could not be determined from its MAC address, or if there was a scanning error and an assessment of the end-system could not take place.
    - The **Quarantine policy** is applied to an end-system if the end-system fails an assessment.
4. Click **Save** or select the **Autosave** checkbox.

Status Polling and Timeout

Use the Status Polling and Timeout view to specify polling and timeout options for Extreme Access Control engines. These settings apply to all users on all clients.

1. Select **Administration > Options**. The Options window opens.
2. In the left-panel tree, expand the Extreme Access Control folder and select Status Polling and Timeout.

3. In the **Extreme Access Control Appliance Enforce Timeout** section, specify the amount of time Extreme Management Center waits for an enforce response from the engine before determining the Extreme Access Control engine is not responding. During an enforce, an Extreme Access Control engine responds every second to report that the enforce operation is either in-progress or complete. Typically, you do not need to increase this timeout value, unless you are experiencing network delays that require a longer timeout value.
4. In the **Extreme Access Control Inactivity Check** section, you can enable a check to verify end-system Extreme Access Control activity is taking place on the network. If no end-system activity is detected, an Extreme Access Control Inactivity event is sent to the Extreme Access Control Events view. You can use the Alarms and Events tab to configure custom alarm criteria based on the Extreme Access Control Inactivity event to create an alarm, if desired.
5. In the **Status Polling** section, select the **Length of Timeout**, which specifies the amount of time Extreme Management Center waits when communicating with Extreme Access Control engines for status polling before determining contact failed. If Extreme Management Center does not receive a response from an engine in the defined amount of time, Extreme Management Center considers the engine to be "down" and the engine icon changes from a green up-arrow to a red down-arrow in the left-panel tree. The engine status refers to Messaging connectivity, not SNMP connectivity. This means that if the engine is "down," Extreme Management Center is not able to enforce a new configuration to it.
6. Specify the **Polling Interval**, which is the frequency Extreme Management Center polls the Extreme Access Control engines to determine engine status.
7. Click **Save** or select the **Autosave** checkbox.

Related Information

For information on related windows:

- Extreme Access Control Options

How to Set Up Registration in

The Extreme Networks Extreme Access Control Solution provides support for Registration which forces any new end-system connected on the network to provide the user's identity in a web page form before being allowed access to the network. Registration utilizes Registration Web Server functionality installed on an Extreme Access Control engine to allow end users to register their end-systems and automatically obtain network access without requiring the intervention of network operations. For more information on Registration and an overview of how it works, see the Registration section of the Concepts help file.

NOTE: For important information on web browser requirements for end-systems connecting through Extreme Management Center, refer to the Extreme Access ControlConfiguration Considerations Help topic.

This Help topic describes the specific steps that must be performed when deploying Registration on your network. The steps vary depending on whether you are using Extreme Access Control Gateway engines and/or Layer 2 Extreme Access Control Controller engines on your network. (Registration is not supported on the Layer 3 Extreme Access Control Controller engines.)

For Extreme Access Control Gateway engines you must:

- Identify the location in your network topology for the Extreme Access Control Gateway installation.
- Define the access policy for authorizing unregistered end-systems.
- Configure policy-based routing on your network.
- Configure Registration parameters in Extreme Management Center.

For Layer 2 Extreme Access Control Controller engines you must:

- Configure Registration parameters in Extreme Management Center.

The Registration Web Server is pre-installed on the Extreme Access Control engine. For instructions on installing and configuring a Extreme Access Control engine, please refer to your engine Installation Guide.

NOTE: It is important to add a DNS entry from the Fully Qualified Domain Name (FQDN) of the Extreme Access Control engine (both Extreme Access Control Gateways and Extreme Access Control Controllers) into the DNS servers deployed on the network so that the device running NAC Manager is able to resolve queries to these DNS servers. Otherwise, a short delay occurs in returning the Registration web page to end users on the network.

Information and instructions on:

Extreme Access Control Gateway Configuration

Perform the following steps when you are deploying Registration in a network that utilizes Extreme Access Control (Extreme Access Control) Gateway engines. These steps are not necessary if you are utilizing only Extreme Access Control Controller engines on your network.

Identifying Extreme Access Control Gateway Location

Although several Extreme Access Control Gateways may be deployed on the entire network depending on the number of connecting end-systems, only one Extreme Access Control Gateway is required to serve as the Registration Web Server. The location of this Extreme Access Control Gateway is important for the implementation of web redirection for unregistered end-systems on the network. The Extreme Access Control Gateway serving as the Registration Web Server must be installed on a network segment directly connected to a router or routers that exist in the forwarding path of HTTP traffic from unregistered end-systems. This is because policy-based routing is configured on this router or routers to redirect the web traffic sourced from unregistered end-systems to this Extreme Access Control Gateway. It is important to note that only the Extreme Access Control Gateway that you wish to serve as the Registration Web Server needs to be positioned in such a manner. All other Extreme Access Control Gateways may be positioned at any location on the network, with the only

requirement being that access layer switches are able to communicate to the gateways.

Typically, the Extreme Access Control Gateway serving as the Registration Web Server is positioned on a network segment directly connected to the distribution layer routers on the enterprise network, so that any HTTP traffic sourced from unregistered end-systems that are connected to the network's access layer can be redirected to that Extreme Access Control Gateway. As an alternative, the Extreme Access Control Gateway may be positioned on a network segment directly connected to the router providing connectivity to the Internet or internal web server farm. In this scenario, the HTTP traffic sourced from unregistered end-systems would be redirected to the Extreme Access Control Gateway before reaching the Internet or internal web servers.

Defining the Unregistered Access Policy

When you implement Registration, you assign the Unregistered Extreme Access Control Profile defined in Extreme Management Center (Extreme Management Center) as the Default Profile for all end-systems connected to the engine group. The Unregistered Extreme Access Control Profile specifies that end-systems are not assessed for security posture compliance (at this time) and authorizes end-systems on the network with the "Unregistered" access policy. With this configuration, end-systems are first forced to register to the network, and after successful registration, can be assessed for security posture compliance and subsequently quarantined or allowed network access.

Note that an end-system group may be configured to exempt certain devices from having to register to the network, based on authentication type, MAC address, or user name. For example, an end-system group for the MAC OUI of the printer vendor for the network can be configured to exempt printers from having to register for network access.

Creating the Unregistered Access Policy

The Unregistered access policy must allow unregistered end-systems access to ARP, DHCP, DNS, and HTTP; particularly HTTP communication to the Extreme Access Control Gateway implementing the Registration Web Server functionality. For a network composed of EOS policy-enabled switches in the access layer, you must create the appropriate network access services and rules for the Unregistered *policy role* in Extreme Management Center's Control >

Policy tab to meet these requirements, and enforce those changes to the policy-enabled switches. For a network composed of RFC 3580-enabled switches, you must ensure appropriate network services are allowed for the VLAN(s) associated to the Unregistered access policy.

For EOS policy-enabled Access Layer Switches

When configuring the Unregistered policy role (using Extreme Management Center's Policy tab) for EOS policy-enabled switches, there are two required configurations:

- A rule must be added that permits HTTP traffic (i.e. TCP destination port equaling 80) on the network.
- The rule must specify a class of service action that rewrites the ToS value of the HTTP traffic to a value of '*y*'. This value should match the decimal equivalent used in your policy-based routing that is used on the router.

If Assisted Remediation is already deployed with the Quarantine policy role appropriately configured for web redirection on EOS policy-enabled access layer switches, the simplest way to configure the Unregistered policy role in Extreme Management Center is to copy and paste the Quarantine policy role under the Roles tab in Extreme Management Center and rename this new policy role "Unregistered".

In addition, the Policy tab's Default Policy Domain includes an Unregistered role that is already configured with a service called Redirect Web Services, that includes an "Allow HTTP and Redirect" rule configured with the Extreme Access Control Web Redirect Class of Service.

Perform the following steps in Extreme Management Center to configure your Unregistered policy role.

NOTE: The Extreme Management Center Default Policy Domain includes an Extreme Access Control Web Redirect Class of Service you can use. Make sure that the ToS rewrite value is set to the appropriate value for your network. If you already created a Class of Service with ToS rewrite functionality for Assisted Remediation, you may use that same Class of Service for Registration and start with step number 3 below.

1. In Extreme Management Center, access the Administration > Options tab and select Policy Manager in the left-panel.

2. In the Default Class of Service Mode section, select **Role-Based Rate Limits/Transmit Queue Configuration** to enable the Role-based Class of Service mode on your network devices.
3. Create a new Class of Service that implements the ToS rewrite functionality:
    a. Open the Class of Service left-panel (**Control** > **Policy** tab > Class of Service).
    b. Right-click the Class of Service navigation tree and select Create CoS. The Create CoS window opens.
    c. Enter a name for the class of service (e.g. "Web Redirection").
    d. Click **OK**.
    e. Select the 802.1p Priority checkbox and use the drop-down menu to select the 802.1p priority to associate with the class of service.
    f. Select the **Edit** button next to the ToS field and enter a value (hex).
    g. The new Class of Service is automatically saved.
4. Use the Classification Rule Wizard to add an "Allow HTTP" rule to a service currently included in your Unregistered policy role.
    a. Select the service in the left-panel Roles/Services tab.
    b. From the menu bar, select **Tools > Classification Rule Wizard**.
    c. Enter a name for the rule (e.g. "Allow HTTP").
    d. Set the rule status to Enabled.
    e. Set the rule type to All Devices.
    f. Set the traffic classification layer to Layer 4.
    g. Set the traffic classification type to IP TCP Port Destination.
    h. Set the well-known values to HTTP (80).
    i. Do not enter an IP address value.
    j. Review the traffic description summary.
    k. For the Actions, select the CoS checkbox and the class of service you created in step 2 ("Web Redirection").
    l. Select Permit Traffic for the Access Control.
    m. Click **Finish** to complete the rule.
5. Enforce these policy configurations to your network devices.

For RFC 3580-compliant Access Layer Switches

A VLAN must be identified to which unregistered end-systems will be assigned upon connecting to the network. This may or may not be the same VLAN assigned to end-systems when they are being assessed or quarantined. The VLAN must provision network services to an unregistered end-system that allow the end-system to open a web browser; specifically HTTP, DHCP, ARP, and DNS. Furthermore, it is required that IP connectivity between the end-system and the NAC Gateway implementing the Registration Web Server functionality is operational.

The VLAN to which unregistered end-systems are assigned must be appropriately configured on all access layer switches where end-systems will be registering to the network. Access control lists may be configured at the default gateway router's interface for the unregistered VLAN to restrict particular types of traffic sourced from end-systems within this VLAN to other areas of the network; withstanding the previously described provisioning requirements for this VLAN.

For Both EOS policy-enabled and RFC 3580-compliant Access Layer Switches

Now that you have defined the Unregistered policy role in Policy Manager for EOS policy-enabled switches and/or the VLAN assigned to unregistered end-systems for RFC 3580-compliant switches, you must associate this policy role to the appropriate VLAN in NAC Manager.

1. In NAC Manager, click on the Manage NAC Profiles button in the toolbar. The Manage NAC Profiles window opens.
2. Select the Unregistered NAC Profile entry and click the **Edit** button. The Edit NAC Profile window opens.
3. Click the **Manage** button in the Policy Mappings section. The Edit Policy Mapping Configuration window opens.
4. Select the **Advanced** Radio button.
5. Select the Unregistered policy and click the **Edit** button. The Edit Policy Mapping window opens.
6. Use the drop-down list to select "Unregistered" as the Policy Role. (The drop-down list displays all the policy roles you have created and saved in your Policy Manager database.)
7. If only EOS policy-enabled switches are deployed in the access layer of the network, associate the Unregistered policy with the Default VLAN [1]. If RFC 3580-compliant

access layer switches are deployed, associate the "Unregistered" policy with the Unregistered VLAN you will be using in your network, adding the VLAN using the Add VLAN button, if necessary.

8. Click OK to close all the open windows. Close the Manage NAC Profiles window.

Your NAC Manager Unregistered access policy is now configured to allow unregistered end-systems the ability to communicate to the NAC Gateway serving as the Registration Web Server. In the next step, the authentication, authorization, and assessment of unregistered end-systems will be specified.

Configuring the Unregistered NAC Profile

Now that you have created the Unregistered access policy, you can customize the Unregistered NAC Profile. The Unregistered NAC Profile is defined by default in NAC Manager to specify that an unregistered end-system will not be assessed for security posture compliance and that it will be authorized on the network with the "Unregistered" policy. Therefore, unregistered end-systems will be immediately assigned to the "Unregistered" policy when connected to EOS policy-capable access layer switches and the "Unregistered" VLAN when connected to RFC 3580-compliant access layer switches, without being assessed. The authentication, assessment, and authorization settings of the Unregistered NAC profile may be changed as required by your organization. Once you have configured the Unregistered NAC Profile, it can be selected as the default profile for an engine group (as described in a later section) where end-systems will be required to register to the network.

To change the Unregistered NAC Profile, use the following steps.

1. In NAC Manager, click on the Manage NAC Profiles button in the toolbar. The Manage NAC Profiles window opens.
2. Select the Unregistered NAC Profile entry and click the Edit button. The Edit NAC Profile window opens.
3. Select the desired authentication, assessment, and configuration settings.
4. Click OK.

Configuring Policy-Based Routing

As described above, the NAC Gateway serving as the Registration Web Server must be located on a network segment directly connected to a router or routers

that exist in the transmission path of all traffic from any end-system that is not registered. This is because policy-based routing (PBR) must be configured on the routers to redirect the web traffic sourced from unregistered end-systems to that NAC Gateway.

If EOS policy-enabled switches are deployed on the network, this is done by configuring policy-based routing to forward all HTTP traffic with a ToS field of '*y*' to the next-hop address of the NAC Gateway serving as the Registration Web Server. If RFC 3580-enabled switches are deployed on the network, this is done by configuring policy-based routing to forward all HTTP traffic with the source IP address on the subnet(s)/VLAN(s) associated to the Unregistered access policy, to the next-hop address of the NAC Gateway serving as the Registration Web Server.

In addition, if you are adding multiple NAC Gateways for redundancy, the network needs to be configured for redundant policy-based routing as well.

For EOS policy-enabled Access Layer Switches

Let's consider an example where the Unregistered access policy is associated to a policy role on EOS policy-enabled switches that uses the "Allow HTTP" classification rule to assign HTTP traffic the "Web Redirection" class of service. This class of service rewrites the ToS field in the HTTP traffic to a value of 0x40 (or 64 base 10), equivalent to a DSCP value of 16. (The DSCP is the value defined in the six most significant bits of the 8-bit ToS field.) Furthermore, the Unregistered access policy is associated to VLANs 10, 20, and 30 on RFC 3580-enabled switches on the network which map to subnets 10.1.10.0/24, 10.1.20.0/24, and 10.1.30.0/24, respectively. The following steps describe how to configure policy-based routing on an N-Series router or Cisco IOS-based router when Registration is deployed for EOS policy-enabled access layer switches.

1. Configure an entry in the access-list 102 to identify HTTP traffic with a DSCP of 16.
   ```
   access-list 102 permit tcp any any eq 80 dscp 16
   ```
2. Use a route-map to configure the access-list 102 ACL to redirect HTTP traffic from end-systems to the next-hop IP address of the NAC Gateway serving as the Registration Web Server, where "xxx.xxx.xxx.xxx" is the IP addresses of the NAC Gateway. Note that multiple next hop IP addresses may be specified in the route-map if multiple NAC Gateways are serving as Registration Web Servers.
   ```
   route-map 101
   match ip address 102
   set next-hop xxx.xxx.xxx.xxx
   ```

3. Apply the route map for the PBR configuration to the routed interface receiving the HTTP traffic from unregistered end-systems by entering the routed interface configuration prompt and executing the following command.
   ip policy route-map 101

For RFC 3580-compliant Access Layer Switches

Let's consider an example where the Unregistered access policy is associated to VLANs 10, 20, and 30 on RFC 3580-enabled switches on the network which map to subnets 10.1.10.0/24, 10.1.20.0/24, and 10.1.30.0/24, respectively. The following steps describe how to configure policy-based routing on an N-Series router or Cisco IOS-based router when Registration is deployed for RFC 3580-compliant access layer switches.

1. Configure an entry in the access-list 102 to identify HTTP traffic sourced from subnets 10.1.10.0/24, 10.1.20.0/24, and 10.1.30.0/24.
   access-list 102 permit tcp 10.1.10.0.0.0.0.255 any eq 80
   access-list 102 permit tcp 10.1.20.0.0.0.0.255 any eq 80
   access-list 102 permit tcp 10.1.30.0.0.0.0.255 any eq 80
2. Use a route-map to configure the access-list 102 ACL to redirect HTTP traffic from end-systems to the next-hop IP address of the NAC Gateway serving as the Registration Web Server, where "xxx.xxx.xxx.xxx" is the IP addresses of the NAC Gateway. Note that multiple next hop IP addresses may be specified in the route-map if multiple NAC Gateways are serving as Registration Web Servers.
   route-map 101
   match ip address 102
   set next-hop xxx.xxx.xxx.xxx
3. Apply the route map for the PBR configuration to the routed interface receiving the HTTP traffic from unregistered end-systems by entering the routed interface configuration prompt and executing the following command.
   ip policy route-map 101

Setting up Redundancy on NAC Gateways

When adding multiple NAC Gateways for redundancy, the network needs to be configured for redundant policy-based routing as well. This is performed on the router in which policy-based routing is configured. Use the same commands described in the previous two sections except for the two following changes:

- In step 2, in addition to the single IP address set as the next-hop IP address, enter a list of IP addresses of the redundant NAC Gateways. For example:
  set next-hop xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx
- In step 3, when adding the ip policy route-map to the router interface, specify an additional command called "ip policy pinger on". This command will attempt to ping the first IP address that is specified in the next-hop to determine its availability. If it is not available, the next IP in the list of next-hops will be pinged and then used, if it is available.
  For example:
  ip policy route-map 101
  ip policy pinger on

With policy-based routing and the Unregistered NAC Profile configured, Registration settings can be specified and then enabled on the network, as described in the next section.

Configuring NAC Manager (for NAC Gateways and NAC Controllers)

Perform the following steps when you are deploying Registration in a network that utilizes NAC Gateway engines and/or Layer 2 NAC Controllers. (Registration is not supported on Layer 3 NAC Controller engines.)

Use the portal configuration section of the NAC Configuration window (in NAC Manager) to configure parameters for the Registration web pages served from the NAC engine. All NAC engines are initially assigned a default portal configuration. You can use this window to view and edit the default configuration or create new configurations to use. Once you have defined your portal configuration, you must enforce the NAC configuration to your engine(s).

Use the following steps to define your portal configuration and enforce it to the engine. These steps give you an overview of the required configuration. For more detailed information, see the NAC Configuration Window and Portal Configuration Help topics.

1. Verify that Registration/Web Access is enabled in the NAC Manager Features options accessed from Tools > Options in the NAC Manager menu bar.
2. Use the NAC Manager  toolbar button to open the NAC Configuration window.

3. In the left-panel tree, select the Features icon. Enable the registration, access, and assessment features you want for your network. For information on each available feature, see the Features section in the NAC Configuration Window Help topic.
4. In the left-panel tree, select the Portal icon. If needed, use the Portal Configuration drop-down menu in the right panel to select the configuration to configure or to create a new one.
5. Expand the Portal icon and select the portal configuration settings you want to edit:
    a. Click on Network Settings to view network web page parameters. Click on Look and Feel to view the common web page parameters. These parameters are shared by both the Remediation and the Registration web pages. You can edit and change these parameters; for a description of each parameter, see the Network Settings and Look and Feel sections of the Portal Configuration Help topic. Be aware that if you deploy both the assessment/remediation and registration features, any changes will affect the web pages for both features.
    b. Click on Common Settings where you can configure settings for the Registration web page. You can edit and change these parameters; for a description of each parameter, see the Common Registration Settings section of the Portal Configuration Help topic.
    c. Click on Administration where you can configure settings for the registration administration web page and grant access to the page for administrators and sponsors. For information on this tab, see the Administration section of the Portal Configuration Help topic.
    d. Depending on the registration, access, and assessment/remediation features you have selected for your network, there are additional views you can access where you can configure the settings and parameters for each type. For a description of each setting and parameter, see the Portal Configuration Help topic.
6. When you have finished making your changes to the portal configuration, click **Save** in the NAC Configuration window and then close the window.
7. Enforce the NAC configuration to the engine group.
8. To exempt certain end-systems or end users from having to register to the network, you can configure end-system groups based on authentication type, MAC address, or user name. For example, an end-system group for the MAC OUI of the printer vendor for the network can be configured to exempt printers from having to register for network access.

Registration is now enabled for all end-systems connecting to this engine group, with the exception of those end-systems and end users that have been exempted based on group membership.

Related Information

- Registration Concepts
- Portal Configuration
- Registration Administration

How to Configure Pre-Registration

This Help topic describes how to configure and use the Extreme Access Control pre-registration feature as a part of Secure Guest Access or Authenticated Registration. With pre-registration, guest users can be registered in advance and given a username and password, allowing for a more streamlined and simple registration process when the guest user connects to the network. This can be particularly useful in scenarios where guest users are attending a company presentation, sales seminar, or a training session.

Pre-registration allows IT to delegate control of the network registration process to less technical personnel such as company receptionists, administrative assistants, or training personnel. Using the pre-registration web portal, selected personnel can easily register guest users in advance of an event, and print out a registration voucher that provides the guest user with their appropriate registration credentials. The guest user then follows the instructions on the voucher to connect to the corporate network.

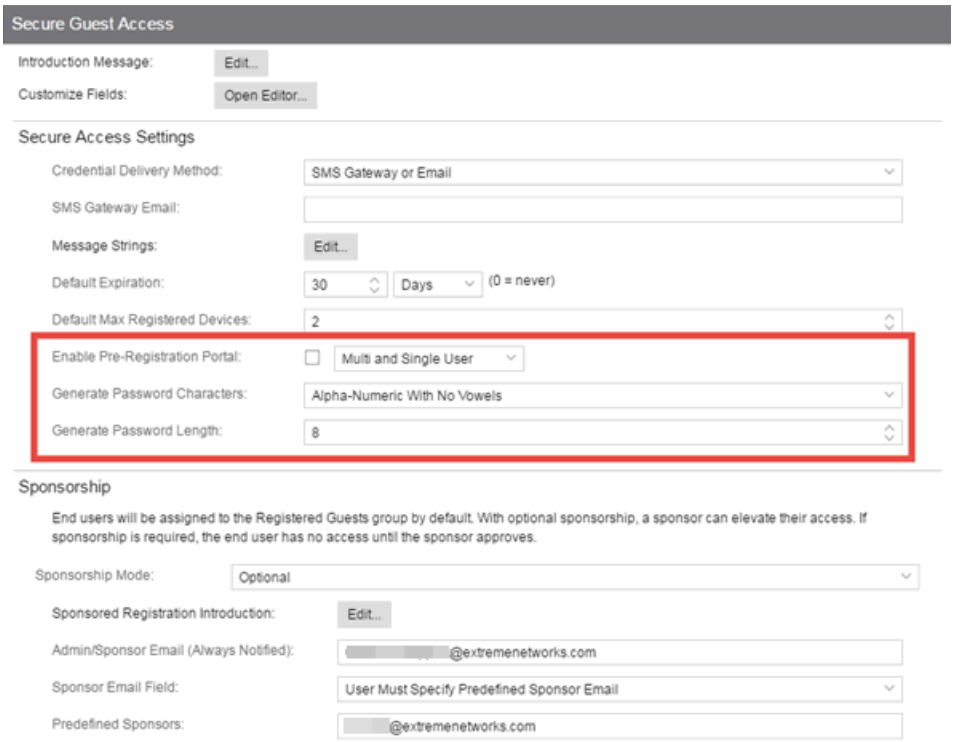
This topic includes information and instructions on:

Configuring Pre-Registration

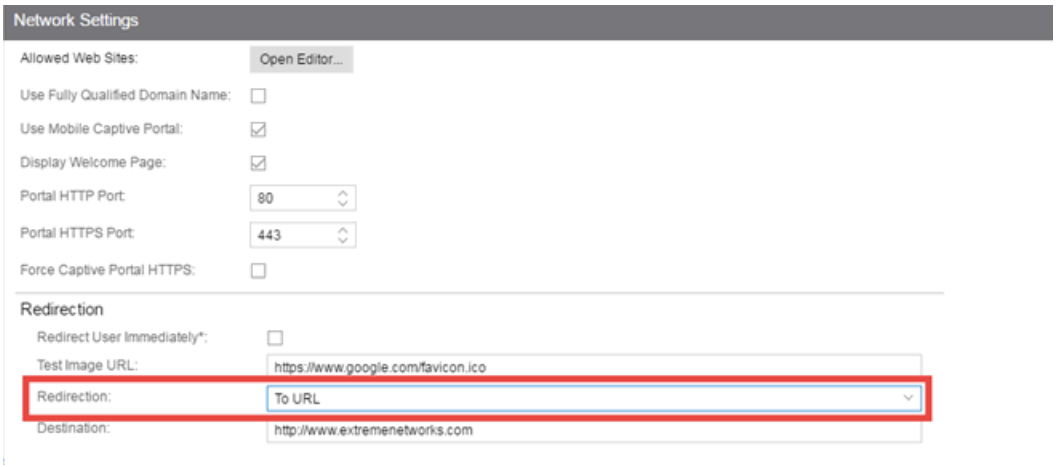
Following are instructions for configuring pre-registration in your portal configuration.

1. Open the **Control** > **Access Control** tab.
2. Select **Portal Configurations** > **Website Configuration** in the left-panel navigation tree.
3. Click Secure Guest Access or Authenticated Registration (depending on the access type you are configuring).

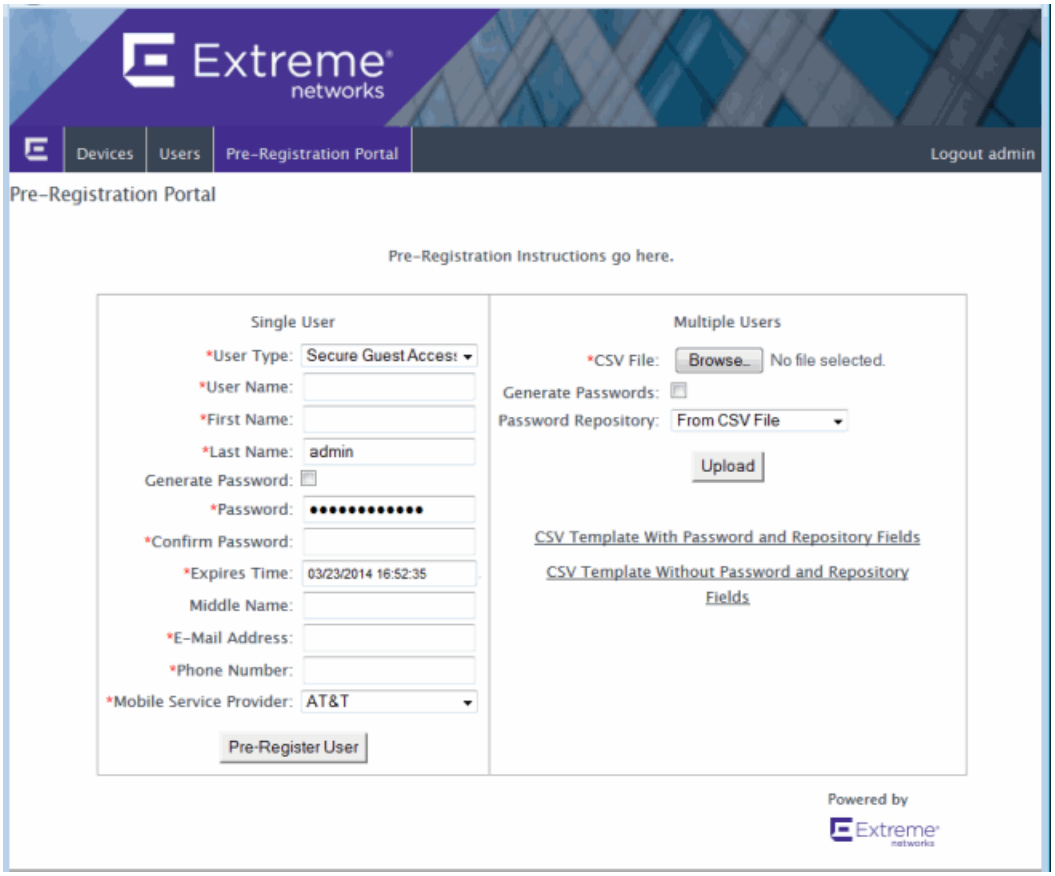
NOTE: If neither panel is available in the Website Configuration navigation tree, click Website Configuration in the left-panel and select the appropriate configuration.



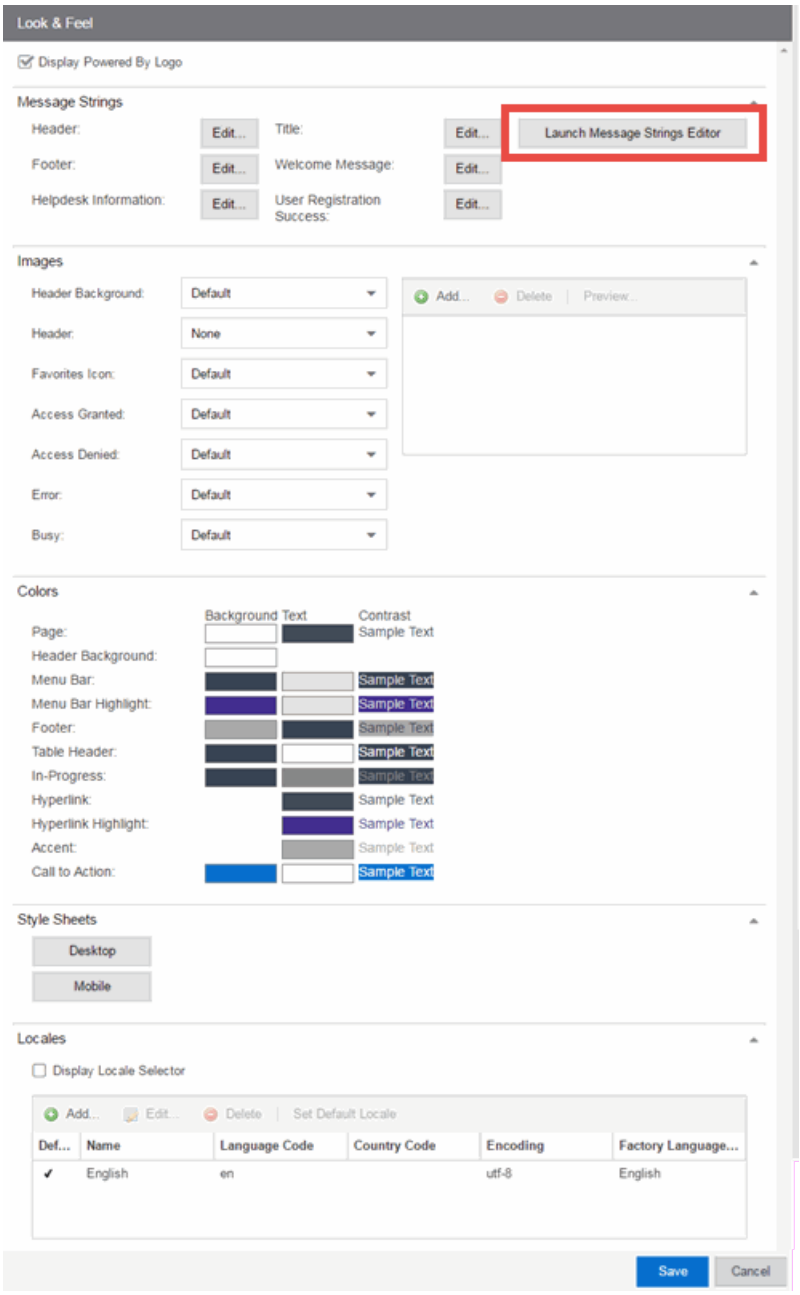
4. Select the **Enable Pre-Registration Portal** checkbox and specify whether personnel are able to register a single user, multiple users, or both single and multiple users.
5. Set the **Generate Password Characters** and **Generate Password Length** options. Extreme Access Control uses these options when generating passwords for guest users to use when connecting to the network. These settings are shared by Authenticated Registration and Secure Guest Access. Changing it for one access type also changes it for the other.
6. For Authenticated Registration, click on the Network Settings view to configure the connection URL specified on the Guest User Voucher (for example, www.ExtremeNetworks.com). Enter the URL in the **Redirection To URL** field. For Secure Guest Access, the Guest User Voucher provides instructions for connecting directly to the secure SSID.



7. Click **Save** to save your changes. Enforce your Extreme Access Control Configuration to your engines.
8. Access the Pre-Registration Portal by entering the following URL in a browser window:
   `https://<Extreme Access ControlEngineIP>/pre_registration`

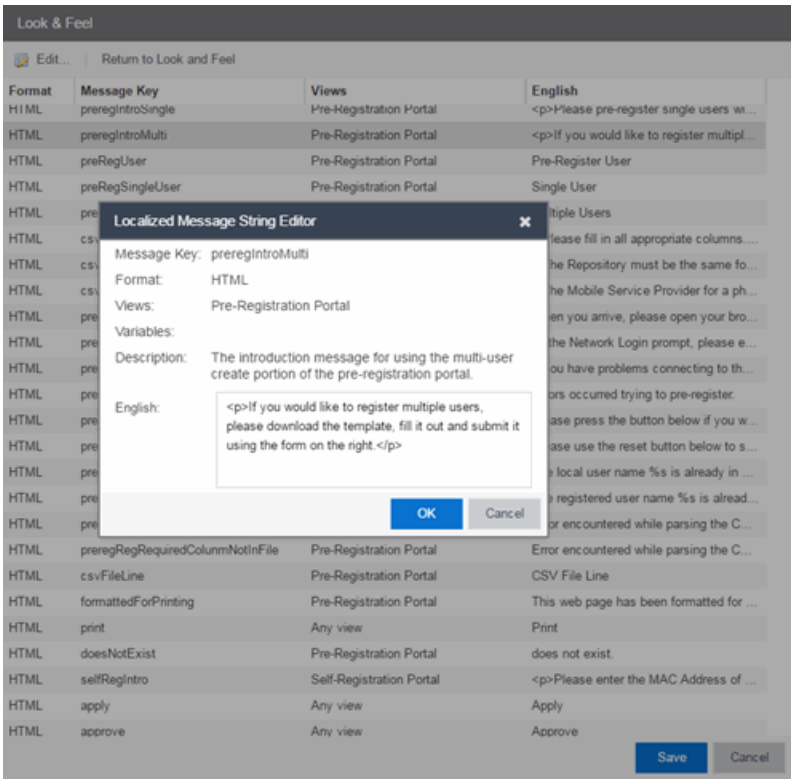


9. At the top of the portal web page are instructions for the people performing the pre-registrations. To modify and edit these instructions:
    a. In the **Control** > **Access Control** tab, select I&A Configurations > Portal in the left-panel navigation tree.
    b. Select a Portal Configuration and select Website Configuration > Look & Feel to open the Look & Feel panel.



c. Click on the Message Strings Launch Message Strings Editor button. The Message Strings Editor window opens.

d. Scroll down to the "preregIntroMulti" or "preregIntroSingle" message key and double-click that line. The Modify Localized Entry window opens.



e. Enter any changes or modifications you wish to make to the instructions, and click OK to close the window.

f. Enforce the changes to your engines.

g. Refresh the browser window to see the new instructions in the Pre-Registration Portal.

10. The following sections provides information on how to pre-register a single user (when you want to pre-register one user at time) or multiple users (when you have a larger group of users to pre-register).

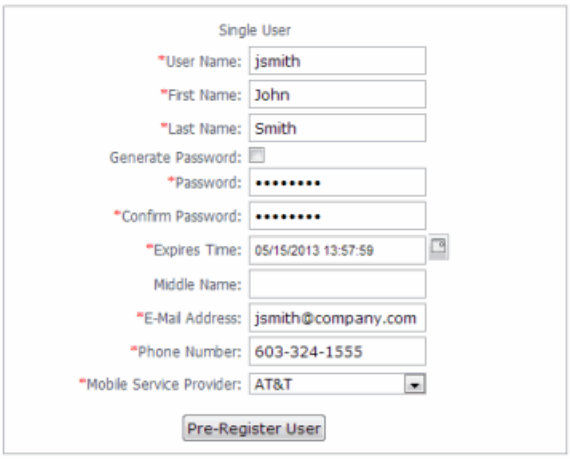
Pre-Registering Guest Users

After you have configured pre-registration, provide the URL for the Pre-Registration Portal (`https://<Extreme Access ControlEngineIP>/pre_registration`) to the personnel who are pre-registering guests. This may be network administrators or it may be personnel such as company receptionists, administrative assistants, or training personnel. (These users must be configured with administrative login privileges to access the web page).

The following sections provide steps for pre-registering single or multiple users in the Pre-Registration Portal.

Pre-Registering a Single User

Use the instructions in this section to pre-register a single end user using the Single User panel in the Pre-Registration Portal.



1. Enter the information for the guest user you want to pre-register. Fields with a red asterisk are required.
    - User Name — Enter the user name for the guest user when connecting to the network. Usernames must be unique and cannot already exist in the local password repository. Usernames are case sensitive. For example, "JSmith" and "jsmith" would be considered two different usernames.
    - First Name/Last Name — Enter the guest user's first and last name. The name is printed on the voucher along with their registration credentials.
    - Password/Confirm Password — Enter and confirm the password for the guest user connecting to the network. Select the Generate Password checkbox if you want Extreme Management Center to automatically generate a password for you.
    - Password Repository — When you pre-register the user, their credentials are automatically added to the local password repository specified here. Local Password Repositories are configured in the AAA Configuration window. (You only see this field if you have multiple repositories.)

- Expires Time — Select a registration expiration date from the calendar. The time is automatically set to 0:00:00, which is midnight. You can enter a specific time, if desired.

NOTE: You can add additional fields to be displayed here using the Manage Custom Fields window accessed from the Customize Fields link in the Edit Portal Configuration window's Authenticated Registration view or Secure Guest Access view. However the Pre-Registration web page always displays the First Name and Last Name fields even if they are not selected as visible/required in the Manage Custom Fields window. This is because it is important for the first and last name to be included on the pre-registration voucher printed out.

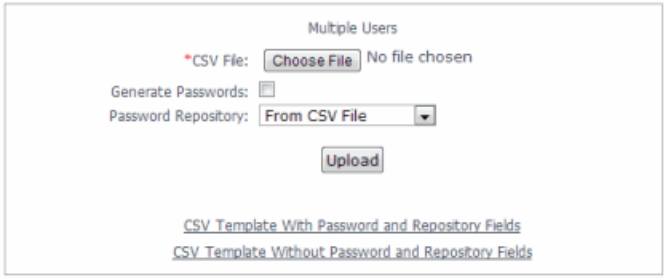
2. Click the Pre-Register User button to register the user. The user is added to the local password repository and added to the Registration Administration web page.
3. A voucher (see example below) is generated that provides registration instructions and the guest user's registration credentials. Print out this voucher to give to the guest user.

IMPORTANT: The voucher must be printed out immediately, as there is no way to go back and print out a voucher once you leave the web page. If you do not print out the voucher, the voucher needs to be created by hand. In the event that the "Generate Password" option was used, you need to modify the guest user password using the registration administration page or local repository administration.

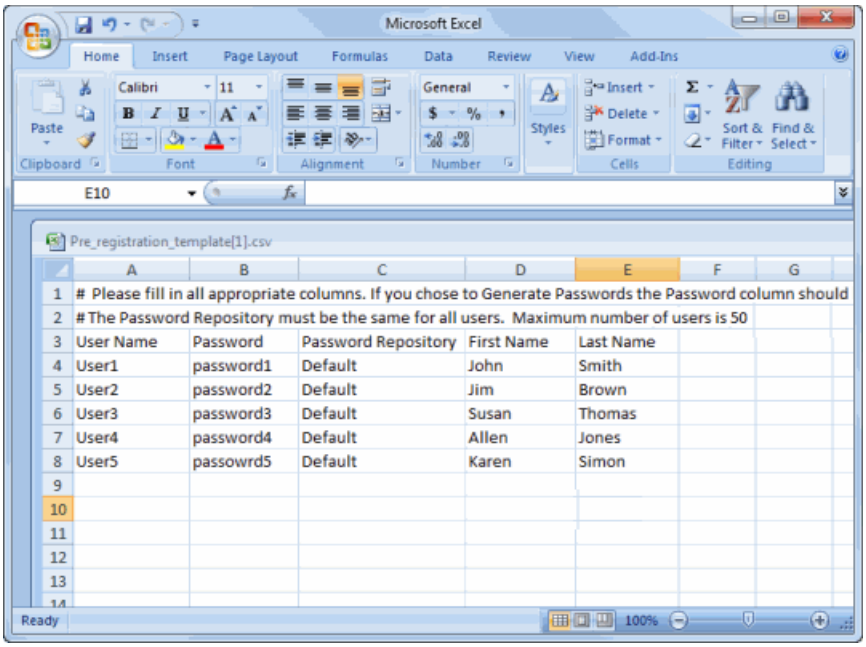
4. To register another user, you must re-access the Pre-Registration page by using the browser's back button or re-entering the URL.

Pre-Registering Multiple Users

Use the instructions in this section to pre-register multiple end users at one time using the Multiple Users panel in the Pre-Registration Portal. When pre-registering multiple users, create a CSV file to provide all the user credential information in table form. Then, upload the file to Extreme Management Center to perform the pre-registration.



1. Click the CSV Template link to open a template CSV file where you create your list of guest users to pre-register. You can use a CSV template that includes password and password repository fields or not, depending on your network requirements. Do not change any of the column headings in the file.



Following is an explanation of the columns that need to be filled in for each user, depending on the template you selected.

- User Name — Enter the username for the guest user connecting to the network. Usernames must be unique and cannot already exist in the local password repository. Usernames are case sensitive. For example, "JSmith" and "jsmith" would be considered two different usernames. (If you do try to pre-register existing usernames along with new usernames, you are notified of the error and given the option to continue registering the new names.)

- Password — Enter the password for the guest user connecting to the network. If you want Extreme Management Center to automatically generate end user passwords, leave the password column blank and select the **Generate Passwords** checkbox on the Multiple Users panel.
- Password Repository — When you pre-register the user, their credentials are automatically be added to the local password repository specified here. Local Password Repositories are configured in the AAA Configuration window. If you are using the Default repository, you can use the Password Repository drop-down menu (in the Multiple Users section) to select Default, and then you don't have to enter the Password Repository for each entry.
- First Name/Last Name — Enter the guest user's first and last name. The name is printed on the voucher along with their registration credentials.

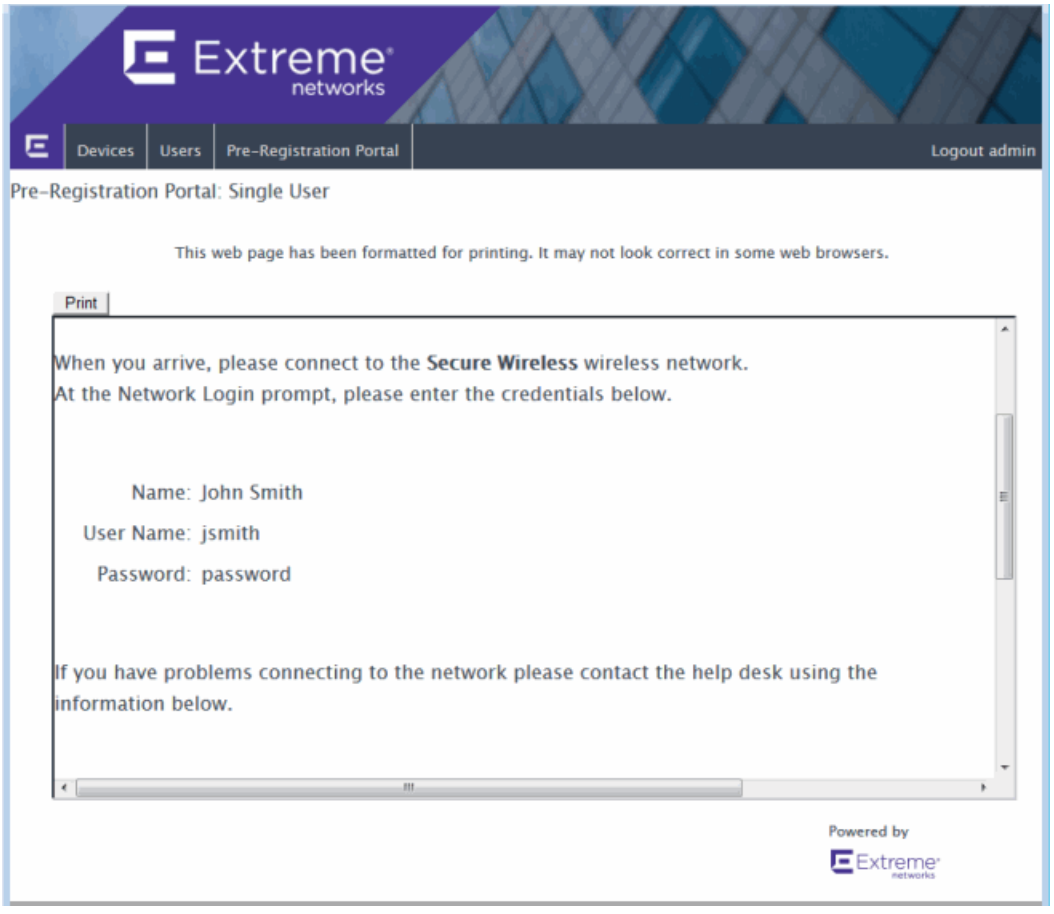
NOTE: You can add additional columns to be included in the template using the Manage Custom Fields window accessed from the Customize Fields link in the Edit Portal Configuration window's Authenticated Registration view and Secure Guest Access view, however, the template always displays the First Name and Last Name fields even if they are not selected as visible/required in the Manage Custom Fields window. This is because it is important for the first and last name to be included on the pre-registration voucher you print.

2. When you have finished entering the guest user information, save and close the file.
3. Back in the Multiple Users panel, enter the path and filename for the CSV file by using the **Browse** button to browse to the file on your system.
4. If your CSV file includes a Password Repository, use the Password Repository drop-down list to specify whether to use the default repository or the repository specified in the file.
5. Click the **Upload** button. Users are added to the local password repository and to the Registration Administration web page.
6. Individual vouchers (see an example below) are generated that provide registration instructions and the guest user's registration credentials for each guest user. Print out these vouchers to give to the guest users.

IMPORTANT: Vouchers must be printed out immediately, as there is no way to go back and print out a voucher once you leave the web page. If you do not print out the vouchers, the vouchers have to be created by hand. In the event that the "Generate Password" option is used, you need to modify the guest user passwords using the registration administration page or local repository administration.

7. To register another user, you must re-access the Pre-Registration Portal by using the browser's back button or re-entering the URL.

Sample Guest User Voucher



Related Information

- Portal Configuration

How to Enable RADIUS Accounting

This Help topic describes how to use RADIUS accounting to provide real-time end-system connection status in Extreme Management Center. RADIUS accounting collects various end-system session data that Extreme Management Center uses to determine connection status for each end-system session. This can be useful for compliance purposes, allowing you to determine both when an end-system session started and when it was terminated.

RADIUS accounting is also used to monitor switches for Auto Tracking, CEP (Convergence End Point), and Switch Quarantine authentication sessions, when used in conjunction with the Monitoring or Network Access switch authentication access types. (For more information, see the Auth. Access Type section of the Add/Edit Switch Window Help topics.)

You must be running Extreme Access Control engine version 4.0 or higher to take advantage of RADIUS accounting functionality in Extreme Management Center.

For Extreme Networks stackable and standalone devices (A-Series, B-Series, C-Series, D-Series, G-Series, and I-Series), Extreme Management Center uses a combination of SNMP and CLI (command line interface) to configure RADIUS accounting on the switch. Before enabling RADIUS accounting on these devices, please read through Considerations for Fixed Switching Devices below.

NOTES: RADIUS accounting is not supported on the Extreme Access Control Controller.

Use the following steps to enable RADIUS accounting:

1. Enable RADIUS accounting on your switches and controllers using the instructions appropriate for your devices.

   For Extreme Networks devices or ExtremeWireless Controller devices running firmware version 9.21.x.x or newer:

   a. If you are editing an existing device: In the right-panel Switches tab, select the devices you want to perform RADIUS accounting and click the Edit button. The Edit Switches in Extreme Access Control Appliance Group window opens. If you are adding a new device: Click Add in the right-panel Switches tab and

the Add Switches to Extreme Access Control Appliance Group window opens.

NOTE: Wireless Controllers must be running in Strict mode to use RADIUS accounting.

b. Set the RADIUS Accounting option to **Enabled**. Click **OK**.

c. Enforce to your engines.

For ExtremeWireless Controller devices running firmware versions older than 9.21.x.x:

a. RADIUS accounting must be enabled manually on the controller using the ExtremeWireless Assistant or the device CLI (command line interface).

b. Be sure to configure the Extreme Access Control engine IP address as the IP address of the RADIUS server. Refer to your wireless controller User Guide for instructions on enabling RADIUS accounting via the ExtremeWireless Assistant, or the CLI Reference Guide for the exact CLI command syntax to use.

For third-party switching devices:

a. RADIUS accounting must be enabled manually on the device using the device CLI (command line interface).

b. Be sure to configure the Extreme Access Control engine IP address as the RADIUS accounting server. Refer to your device documentation for the exact command syntax.

2. If you are doing RADIUS accounting in an Extreme Access Control environment where the primary RADIUS server is being used for redundancy in a single Extreme Access Control engine configuration (Basic AAA configuration only), then enable the Proxy RADIUS Accounting Requests option in the Edit RADIUS Server window.

   a. In the Edit Basic AAA Configurations window, use the Configuration Menu button in the Primary RADIUS Server field to open the Manage RADIUS Servers window.

   b. Select the RADIUS Server and click **Edit**.

   c. Enable the Proxy RADIUS Accounting Requests option. Click **OK**.

   d. Enforce to your engine.

With RADIUS accounting enabled, you now see real-time connection status in the Extreme Management Center **End-Systems** tab and Dashboard.

Considerations for Fixed Switching Devices

Extreme Management Center uses a combination of SNMP and CLI (command line interface) to configure RADIUS accounting on Extreme Networks stackable and standalone devices (A-Series, B-Series, C-Series, D-Series, G-Series, and I-Series). Due to a limitation on the SNMP interface, the configuration can be read via SNMP, but must be written to the device via CLI. Before enabling RADIUS accounting on these devices, read through the following considerations.

NOTE: These considerations do not apply to A4, B5, and C5 devices running firmware version 6.81 and higher. Those devices support RADIUS accounting configuration using SNMP.

- The devices must be assigned a Device Access profile that provides Write access and includes CLI credentials for Telnet or SSH. Profiles and CLI credentials are configured using the Authorization/Device Access tool's Profiles tab.
- Before you enforce a new RADIUS server configuration to your fixed switching devices, you should verify that your CLI credentials are configured according to the settings in your new configuration. This is because the Enforce process first writes the RADIUS server configuration to the switch using SNMP, and then writes the RADIUS accounting configuration to the switch using Telnet or SSH. If CLI credentials are not configured according to the new RADIUS server configuration, then the RADIUS accounting configuration are not written to the switches.

  For example, by default you can Telnet to a fixed switching device using username=admin (with no password or a blank password). But, if you configure a new RADIUS configuration with an Auth Access Type (or Realm Type)=Any, then you may need to change the Device Access for the switches to use the IAS credentials, in order for Extreme Management Center to successfully write the RADIUS accounting information to the switches during Enforce.

Fixed switches only allow one accounting server to be configured. If a primary and secondary Extreme Access Control gateway are configured for the switch, only the primary gateway's accounting configuration is written to the switch. If a secondary gateway is configured, a warning is displayed.

Considerations for ExtremeXOS Devices

Extreme Management Center uses CLI access to perform RADIUS accounting configuration operations on ExtremeXOS devices. CLI credentials for the device are obtained from the device profile and must be configured in the Authorization/Device Access tool.

Related Information

- Add Switches to Extreme Access Control Engine Group Window
- Edit Switches in Extreme Access Control Engine Group Window

How to Set Up Access Policies and Policy Mappings

Access policies define the appropriate level of access to network resources allocated to a connecting end-system based on the end-system's authentication and/or assessment results. There are four access policies defined in an Extreme Access Control profile: Accept policy, Quarantine policy, Failsafe policy, and Assessment policy. When an end-system connects to the network, it is assigned one of these access policies, as determined by the Extreme Access Control profile assigned to the matching Extreme Access Control rule and the end-system state.

In your Extreme Access Control profiles, each access policy is associated to a *policy mapping* that defines exactly how an end-system's traffic is handled when the access policy is applied.

A policy mapping specifies the policy role (created in the Policy tab) and other RADIUS attributes included as part of a RADIUS response to a switch. The RADIUS attributes required by the switch are defined in the Gateway RADIUS Attributes to Send field configured in the Edit Switch window. Policy mappings are configured in the Edit Policy Mapping Configuration window.

How you set up your access policies depends on whether your network utilizes Extreme Access Control Controller engines and/or Extreme Access Control Gateway engines. In addition, if your network utilizes Extreme Access Control Gateway engines, your setup depends on whether your network contains EOS switches that support Policy, third-party switches that support RFC 3580, or switches that support RADIUS attributes that are defined manually.

For Extreme Access Control Controllers:

If your network utilizes Extreme Access Control L2/L3 controller engines, the access policies specified in Extreme Access Control profiles are mapped to policy roles that are defined in a default policy configuration already configured on the controller. It is recommended that you review this default policy configuration using the Policy tab. To do this, you must create a policy domain in the Policy tab specifically for the Extreme Access Control Controller, assign the Extreme Access Control Controller to the domain, then import the policy configuration from the device into Policy tab. Review the policy roles and make

any rule changes required for your environment. When you have finished modifying the policy configuration, you must enforce it back to the Extreme Access Control Controller.

For Extreme Access Control Gateway Appliances:

If your network utilizes Extreme Access Control Gateway engines, the access policies specified in Extreme Access Control profiles are mapped to policy roles that must be created and defined in the Policy tab and enforced to the policy-enabled switches in your network. If you have RFC 3580-enabled switches in your network, Extreme Management Center lets you associate your policy roles to a VLAN ID or VLAN Name using the Policy Mappings panel. This allows your Extreme Access Control Gateway engines to send the appropriate VLAN attribute instead of a policy role to those switches that are RFC 3580-enabled.

Policy mappings have a Location option that allows different VLAN IDs to be returned for a policy based on the location the authentication request originated from. This is useful in networks that may have a VoIP/voice VLAN that is defined on multiple switches, but that VLAN maps to a unique VLAN ID on each switch. (For more information, see the section on Location in the Edit Policy Mapping Configuration Window Help topic.)

NOTE: If you have RFC 3580-enabled switches in your network, be sure to verify that the DHCP Resolution Delay Time option is set correctly in your Appliance Settings (Tools > Manage Advanced Configurations> Global and Appliance Settings). This option specifies the number of seconds an Extreme Access Control engine waits after an authentication completes before attempting to resolve the end-system's IP address. When modifying this delay, keep in mind that for RFC 3580 devices, the engine links down/up a port to force the end-system to get a new IP address when Extreme Management Center determines that the VLAN has changed. If the delay time specified is less than the amount of time the end-system needs to renew its IP address, then the Extreme Access Control engine may resolve the end-system's IP address incorrectly (to the previously held IP), or additional delay may be introduced as the resolution process attempts to resolve the address based on the configured retry interval. This is a problem when either registration or assessment is enabled: the registration process may never complete or may take an unacceptable amount of time to complete, or the Extreme Access Control engine could attempt to scan the incorrect IP address. Be sure to take into account the amount of time required for an end-system to get a new IP address when setting the delay time value.

Setting Up Your Access Policies

Before you begin working with the Access Control tab, use these steps to define the policy mapping criteria (policy roles, corresponding VLAN IDs, etc.) available for selection for each access policy.

1. For each Extreme Access Control profile, create a worksheet listing the four Extreme Access Control policies. For each access policy, associate a policy role (created in the Policy tab), and the policy role's corresponding VLAN ID, if you are using RFC 3580-enabled switches in your network. For a description of each access policy, and some guidelines for creating corresponding policy roles, see the section on Access Policies in the Concepts file.

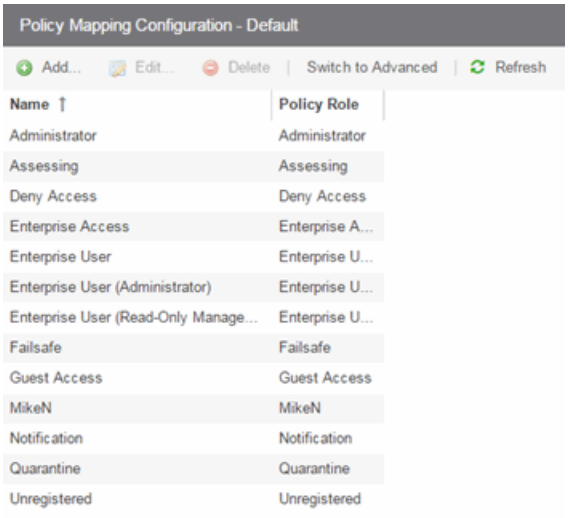
   NOTE: If your network uses Extreme Access Control Gateway engines with only RFC 3580-enabled switches, instead of listing policy roles, simply create a list of policy names that correspond to the VLANs you are using in your network. One tip is to use policy names that identify the corresponding VLAN name for ease of selection when you are creating your Extreme Access Control profiles.

   Here's an example of a worksheet for an Extreme Access Control profile that contains both policy-enabled and RFC 3580 switches:

Access Policy	Policy Role	VLAN ID
Accept Policy	Enterprise User	[2] Enterprise User VLAN
Quarantine Policy	Quarantine	[4] Quarantine VLAN
Failsafe Policy	Failsafe	[5] Failsafe VLAN
Assessment Policy	Assessing - Strict	[6] Assessing - Strict VLAN

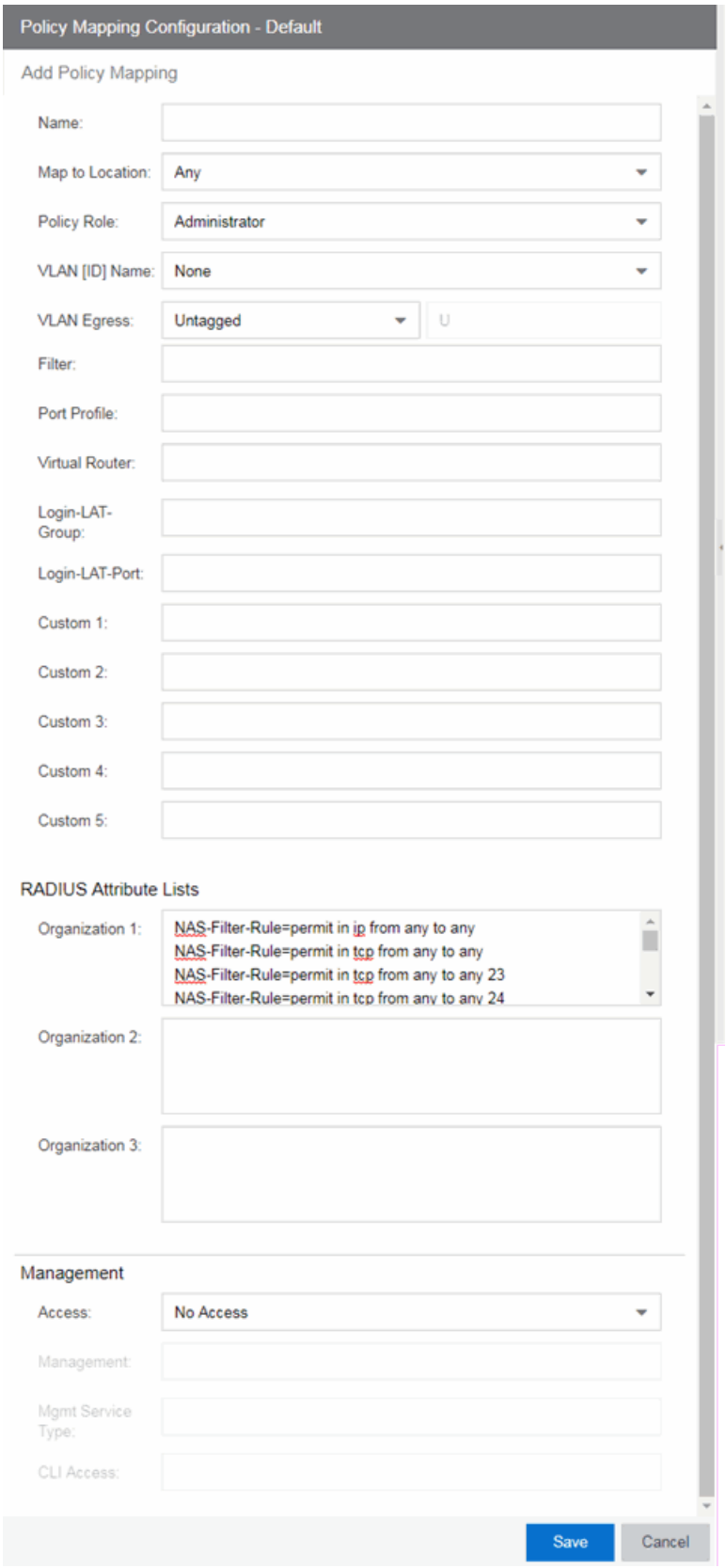
2. For Extreme Access Control Controllers, use the Policy tab to verify that the policy configuration contains the required policy roles, and that the configuration has been enforced to the Extreme Access Control Controller. See the instructions above.
3. For Extreme Access Control Gateways, verify each policy role listed on your worksheet is created in Extreme Management Center's Policy tab and enforced to the policy-enabled switches in your network. If you have RFC 3580-enabled switches in your network, verify that your VLANs have been created on the switches in your network.

4. Define the policy mappings that map each access policy to the appropriate policy role as specified in your worksheet.
    a. Select a policy mapping configuration from the Extreme Access Control Configurations > Extreme Access Control Profiles > Policy Mappings left-panel option.
    b. The Policy Mapping Configuration right-panel opens.



    c. Select between a Basic policy mapping and an Advanced policy mapping, depending on your network needs by selecting **Switch to Advanced** or **Switch to Basic** at the top of the panel. Typically, the Basic policy mapping configuration is used unless your devices require customization or when using locations in your mappings.

       Extreme Access Control provides a list of default policy mappings you can use. Be aware if you use one of the default mappings, you still need to verify that the policy role specified in the mapping is part of your Extreme Access Control Controller policy configuration and/or is created and enforced to the policy-enabled switches in your network via the **Policy** tab.
    d. To add a new policy mapping, click the **Add** button to open the Add Policy Mapping window.


Policy Mapping Configuration - Default
Add Policy Mapping
Name:
Map to Location:
Any
Policy Role:
Administrator
VLAN [ID] Name:
None
VLAN Egress:
Untagged
U
Filter:
Port Profile:
Virtual Router:
Login-LAT-Group:
Login-LAT-Port:
Custom 1:
Custom 2:
Custom 3:
Custom 4:
Custom 5:
RADIUS Attribute Lists
Organization 1:
NAS-Filter-Rule=permit in ip from any to any
NAS-Filter-Rule=permit in tcp from any to any
NAS-Filter-Rule=permit in tcp from any to any 23
NAS-Filter-Rule=permit in tcp from any to any 24
Organization 2:
Organization 3:
Management
Access:
No Access
Management:
Mgmt Service Type:
CLI Access:
Save
Cancel

For the new policy mapping, enter a mapping name and specify a policy role (created in the **Policy** tab) and other required RADIUS attributes included in the RADIUS response to a switch. Click **OK** to add the mapping. Note that the required RADIUS attributes for your switches are defined in the Gateway RADIUS Attributes to Send field configured in the Edit Switch window, as shown below.

e. Click **OK** to close the Edit Policy Mapping Configuration window.

5. In your Extreme Access Control profile, your policy mappings are available for selection when you define your Accept, Quarantine, Failsafe, or Assessment access policy.

Related Information

For information on related windows:

- Edit Policy Mapping Configuration Window
- Add/Edit Policy Mapping window
- Access Policies, Concepts

How to Configure Credential Delivery for Secure Guest Access

Secure Guest Access provides secure network access for wireless guests via 802.1x PEAP by sending a unique username, password, and access instructions for the secure SSID to guests via an email address or mobile phone (via SMS text). Use the instructions in this Help topic to configure the method used to send guests their credentials and access instructions for the secure SSID.

Configuration Steps

The Credential Delivery method is configured in your portal configuration. Depending on the method you specify, the appropriate custom fields must be configured for display on the Registration web page, so that end users can enter the required information.

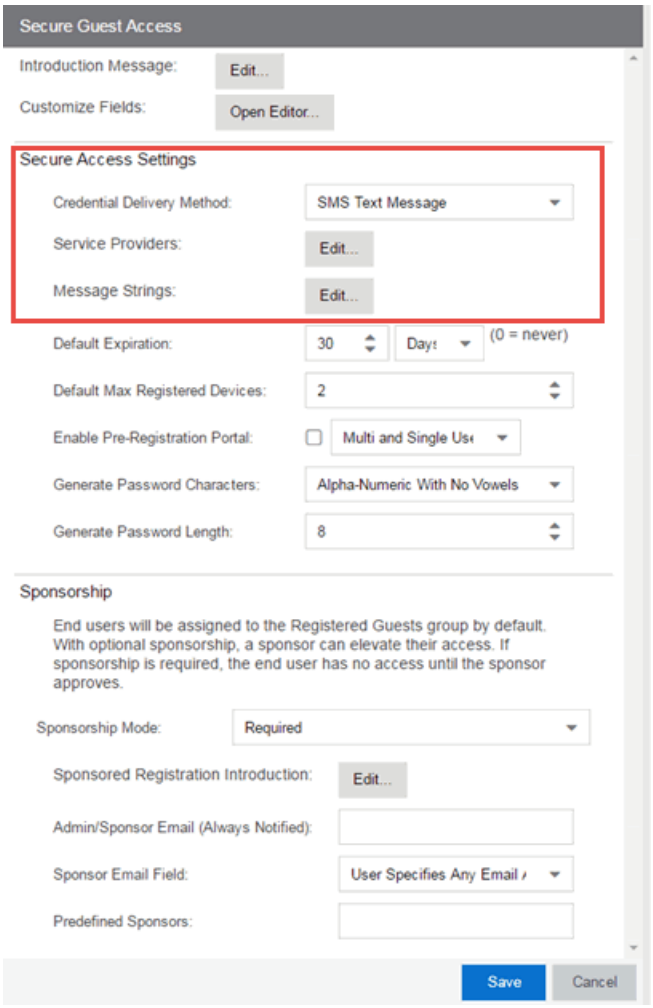
The following table provides a description of each credential delivery method and lists their custom field requirements.

User Verification Method	Description	Custom Field Requirement
Captive Portal	The credential information is displayed on the Registration web page.	There are no Custom Field requirements.
Email	The end user must enter a valid email address on the Registration web page.	The Email Address Custom Field must be set to **Required**.
SMS Gateway	The SMS Gateway provider must support SMTP API. The SMS Gateway provider converts the email to an SMS text message. The end user must enter a mobile phone number on the Registration web page.	The Phone Number Custom Field must be set to **Required**.

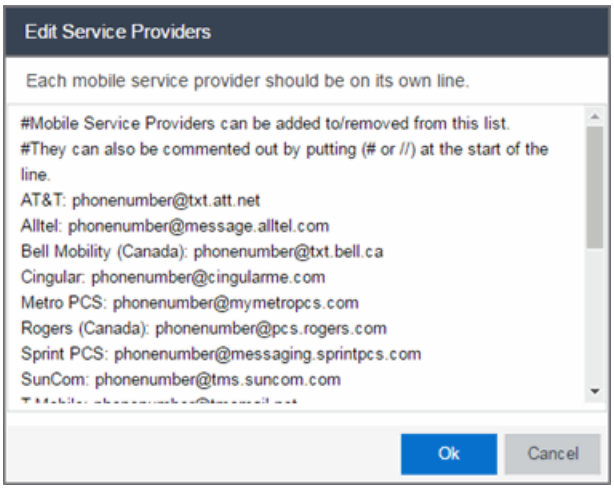
User Verification Method	Description	Custom Field Requirement
SMS Gateway or Email	The SMS Gateway provider must support SMTP API. The SMS Gateway provider converts the email to an SMS text message. The end user must enter a mobile phone number or email address on the Registration web page.	The Phone Number and Email Address Custom Fields must be set to **Visible**.
SMS Text Message	The mobile provider converts the email to an SMS text message. The end user must enter a valid mobile phone number on the Registration web page.	The Phone Number Custom Field must be set to **Required**.
SMS Text or Email	The mobile provider converts the email to an SMS text message. The end user must enter a valid mobile phone number or email address on the Registration web page.	The Phone Number and Email Address Custom Fields must be set to **Visible**.

Use the following steps to configure credential delivery for Secure Guest Access in your portal configuration.

1. In the **Access Control** tab, access the Portal Configuration. Click on the Secure Guest Access selection in the Portal Configuration tree. (If you don't see this selection, click Features in the tree and enable the Secure Guest Access feature.)
2. In the Secure Guest Access panel, use the drop-down menu to select the desired Credential Delivery Method (refer to the table above).



3. If you selected the **SMS Text Message** or the **SMS Text or Email** Credential Delivery method, click the Service Providers **Edit** button to configure the list of mobile service providers from which end users can select on the Registration web page. The Mobile Service Provider List provides a default list of providers that can be edited to include the appropriate service providers for your geographic location.



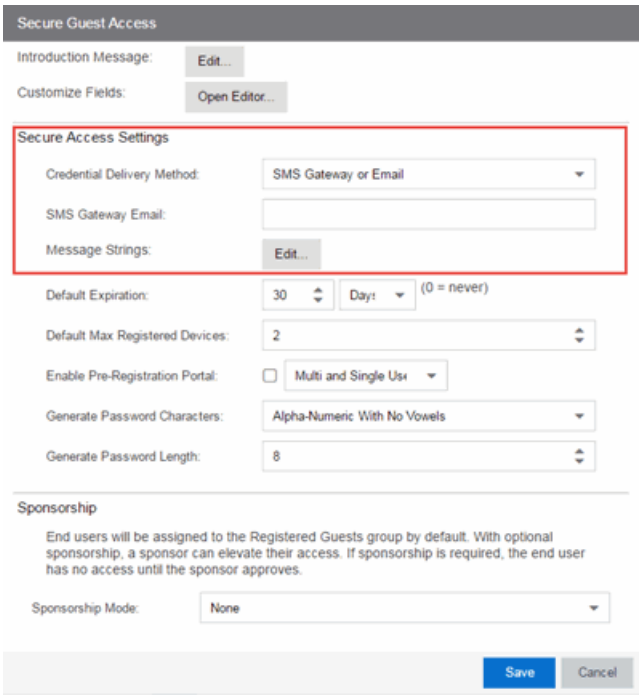
You can comment out entries by preceding each line with either a # or // to allow temporary editing of the file without removing the text.

The list requires one service provider entry per line, using the following format: <Provider>:phonenumber@<specificdomain>.

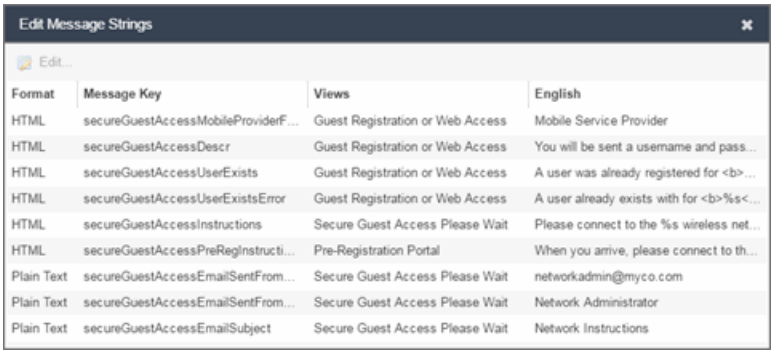
When the end user registers, they only see the <Provider> portion in the drop-down menu of providers on the Registration web page.

Click **OK** to close the window.

4. If you have selected the **SMS Gateway** or **SMS Gateway or Email** method, enter the SMS Gateway Email address provided by the SMS Gateway provider.



5. For all methods, click on the Message Strings **Edit** button to open the Message Strings Editor where you can customize the text displayed on the Registration web page and the messages sent to the end user.



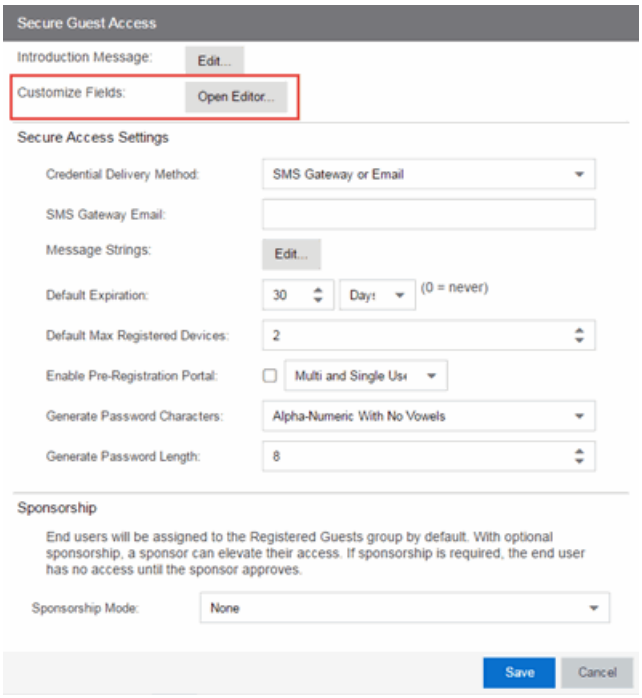
You need to modify different message strings sent to the end user, depending on the delivery method or methods you selected. Double-click on the message to open a window where you can edit the message text.

NOTE: When customizing message strings for text messaging (SMS Gateway or SMS Text Message) it is best to keep the message length as short as possible (under the maximum 160 characters limit). Some providers break long messages into multiple messages and other providers truncate the message, which could cause important information to be missing from the text message the guest receives.

- Email — This method uses the following strings:
  - secureGuestAccessEmailMsgBody — the default message shouldn't need to be changed.
  - secureGuestAccessEmailSentFromAddress — you need to change the default message to the appropriate email address for your company.
  - secureGuestAccessEmailSentFromName — the default message shouldn't need to be changed.
  - secureGuestAccessEmailSubject — the default message shouldn't need to be changed.
- SMS Gateway — Depending on your SMS Gateway provider and their required format, modify the following message strings using appropriate variables to customize the dynamic data such as phone number.
  - secureGuestAccessSMSMsgBody
  - secureGuestAccessSMSSubject
- SMS Text Message — This method uses the following strings. The default messages shouldn't need to be changed.
  - secureGuestAccessSMSMsgBody
  - secureGuestAccessSMSSubject

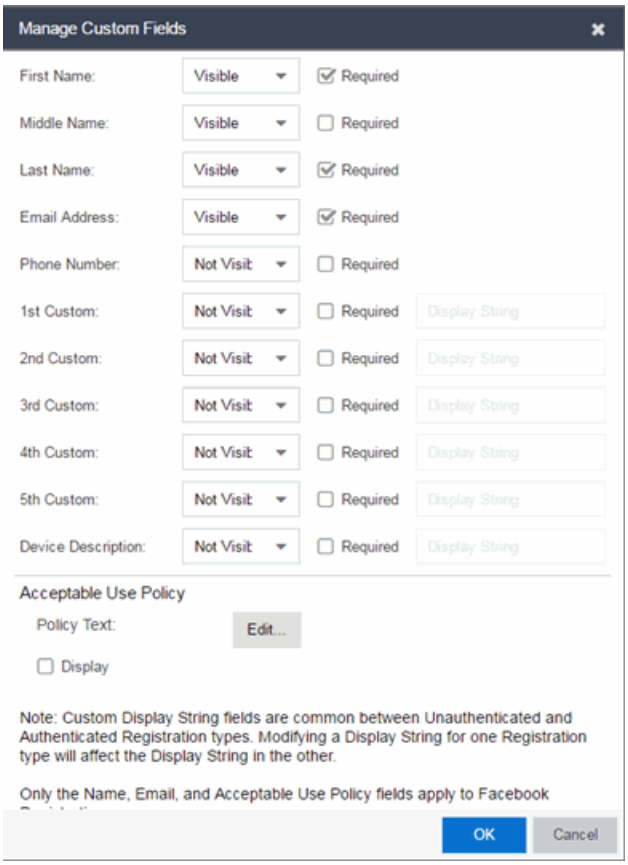
Click OK to close the window.

6. Click the Customize Fields Open Editor button to open the Manage Custom Fields window.



7. Set the appropriate custom fields to display on the Registration web page, depending on the delivery method you selected (refer to the table above). If you do not set these fields, Extreme Access Control automatically sets them for you based on your delivery method.

   These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing them for one access type also changes them for the others. For more information, see the Manage Custom Fields Window.

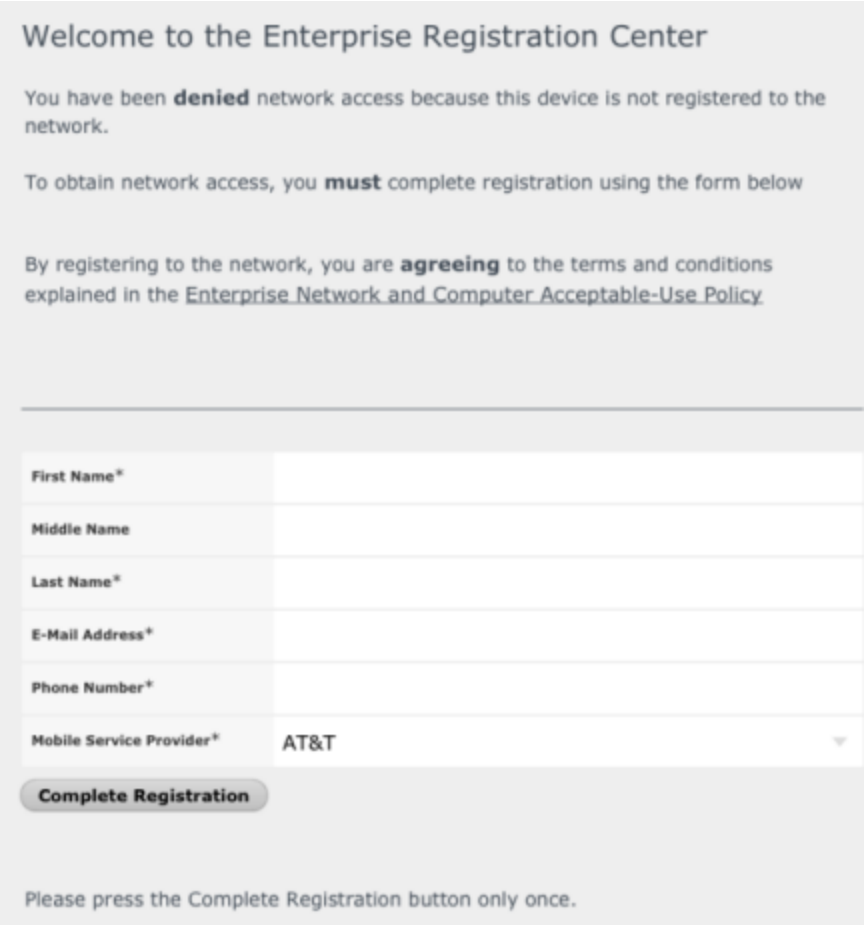


8. Click OK to close the window.
9. Back in the Portal Configuration, click Save to save your changes.
10. Enforce the new portal configuration to your engine(s).

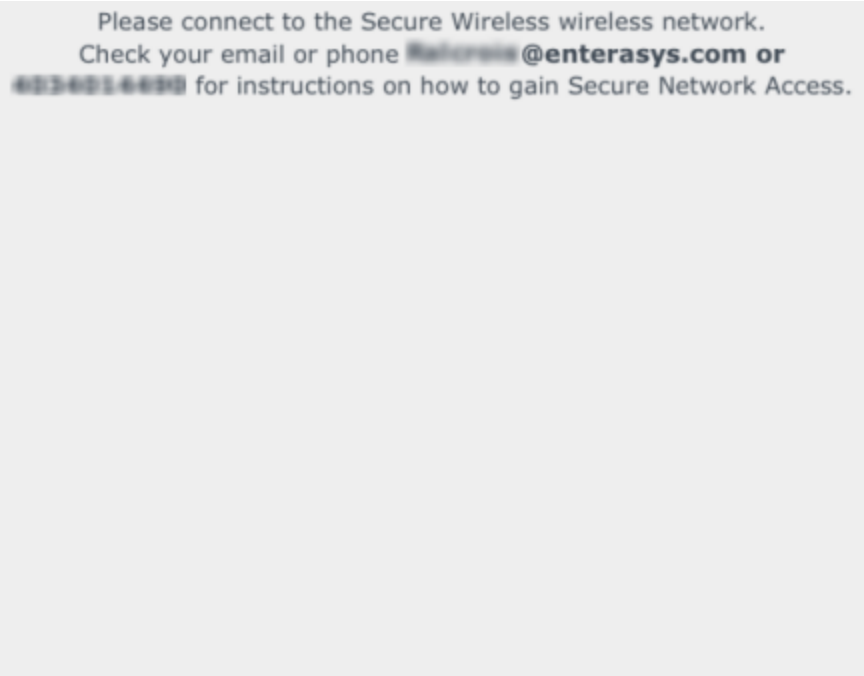
    Credential delivery is now configured for your secure guest access.

How Secure Guest Access Works

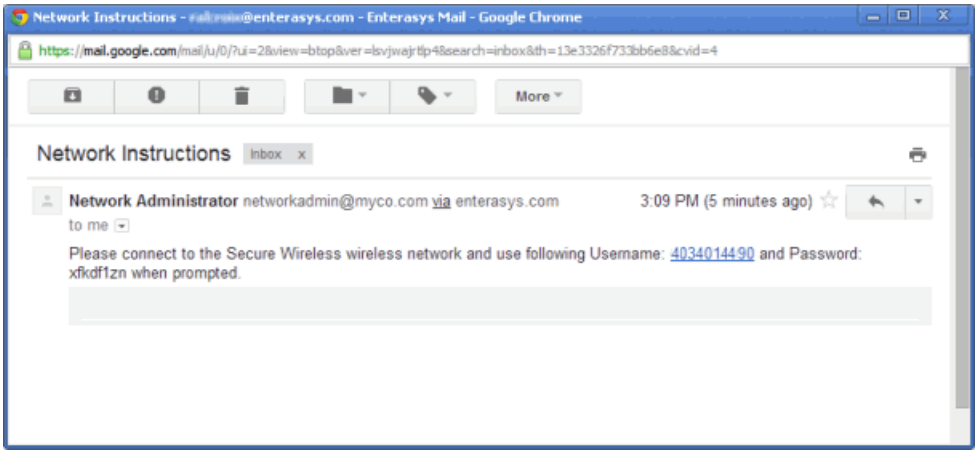
When a guest attempts to access the network, the Registration web page asks for their email address and/or phone number, and any other required/configured information.



When they click the Complete Registration button, they see the following screen that notifies them to check their email or phone for instructions on how to gain access to the network.



They are sent a username, password, and access instructions via an email or a phone text message.



When they connect to the Secure Wireless network, they will enter their username and password in this screen to gain access to the network.

Related Information

For information on related help topics:

- Portal Configuration

How to Configure Verification for Guest Registration

Guest registration requires end users to enter their name and contact information on a Registration web page in order to gain access to the network. However, in many cases, end users provide false names and contact information because they don't want their personal information to be used for other purposes. In those cases, network administrators do not have a way to contact the user in the event of an Acceptable Use Policy (AUP) violation or in the case of an emergency.

With verification, guest end users registering to the network are required to enter a verification code that is sent to their email address or mobile phone (via SMS text) before gaining network access. This ensures that network administrators have at least one way to contact the end user.

Configuration Steps

The verification feature is supported for both Guest Registration and Guest Web Access, and is configured using the Verification Method options in your portal configuration. Depending on the verification method you specify, the appropriate custom fields must be configured for display on the Registration web page, so that end users can enter the required information.

The following table provides a description of each verification method and lists their custom field requirements.

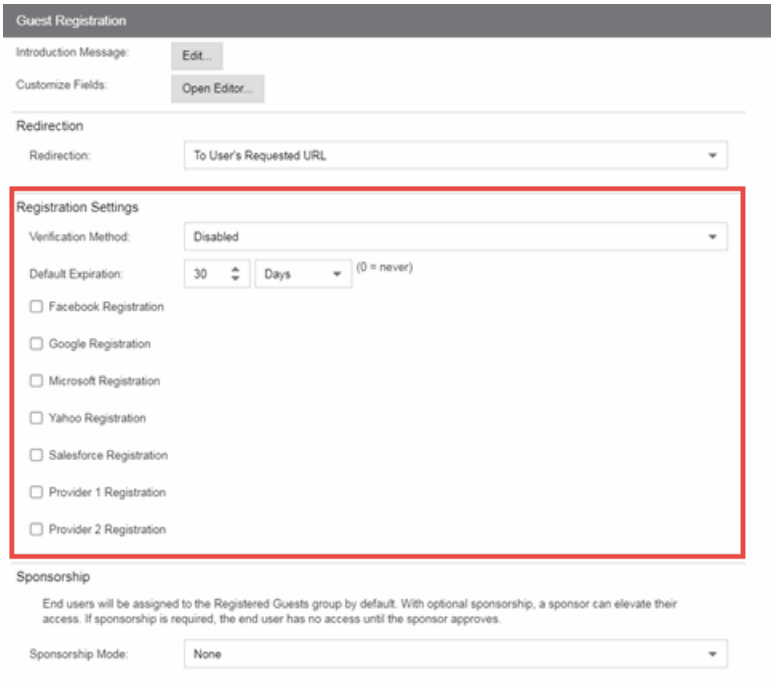
User Verification Method	Description	Custom Field Requirement
Email	The end user must enter a valid email address on the Registration web page or Guest Web Access login page.	The Email Address Custom Field must be set to **Required**.

User Verification Method	Description	Custom Field Requirement
SMS Gateway	The SMS Gateway provider must support SMTP API. The SMS Gateway provider converts the email to an SMS text message. The end user must enter a mobile phone number on the Registration web page or Guest Web Access login page.	The Phone Number Custom Field must be set to **Required**.
SMS Gateway or Email	The SMS Gateway provider must support SMTP API. The SMS Gateway provider converts the email to an SMS text message. The end user must enter a mobile phone number or email address on the Registration web page or Guest Web Access login page.	The Phone Number and Email Address Custom Fields must be set to **Visible**.
SMS Text Message	The mobile provider converts the email to an SMS test message. The end user must enter a valid mobile phone number on the Registration web page or Guest Web Access login page.	The Phone Number Custom Field must be set to **Required**.
SMS Text or Email	The mobile provider converts the email to an SMS test message. The end user must enter a valid mobile phone number or email address on the Registration web page or Guest Web Access login page.	The Phone Number and Email Address Custom Fields must be set to **Visible**.

Use the following steps to configure verification in your portal configuration.

1. In Extreme Management Center, access the Portal Configuration. Click on the Guest Registration or Guest Web Access selection in the Portal tree, depending on what access type your network is using. (If you don't see these selections, click Website Configuration in the tree and enable the appropriate feature.)

2. In the Guest Registration or Guest Web Access panel, use the drop-down menu to select the desired Verification Method (refer to the table above). The Guest Registration panel is shown below.



3. If you selected the SMS Text Message or the SMS Text or Email User Verification method, click the Service Providers link to configure the list of mobile service providers from which end users can select on the Registration web page or Guest Web Access login page. The Mobile Service Provider List provides a default list of providers that can be edited to include the appropriate service providers for your geographic location.

   You can comment out entries by preceding each line with either a # or // to allow temporary editing of the file without removing the text.

   The list requires one service provider entry per line, using the following format: <Provider>:phonenumber@<specificdomain>.

   When the end user registers, they will see only the <Provider> portion in the drop-down list of providers on the Registration web page.

   Click OK to close the window.

4. If you have selected the SMS Gateway or SMS Gateway or Email method, enter the SMS Gateway Email address provided by the SMS Gateway provider.
5. For all methods, click on the Message Strings link to open the Message Strings Editor where you can customize the text displayed on the Registration web page or Guest Web Access login page, and the messages sent to the end user.

   You need to modify different message strings sent to the end user, depending on the verification method or methods you selected. Double-click on the message to open a window where you can edit the message text.

   - Email - This method uses the following strings:
     - registrationVerificationEmailMsgBody - the default message shouldn't need to be changed.
     - registrationVerificationEmailSentFromAddress - you need to change the default message to the appropriate email address for your company.
     - registrationVerificationEmailSentFromName - the default message shouldn't need to be changed.
     - registrationVerificationEmailSubject - the default message shouldn't need to be changed.
   - SMS Gateway - Depending on your SMS Gateway provider and their required format, modify the following message strings using appropriate variables to customize the dynamic data such as phone number.
     - registrationVerificationSMSMsgBody
     - registrationVerificationSMSSubject
   - SMS Text Message - This method uses the following strings. The default messages shouldn't need to be changed.
     - registrationVerificationSMSMsgBody
     - registrationVerificationSMSSubject

   Click OK to close the window.
6. In the Web Page Customizations (Shared) section, click the Customize Fields link to open the Manage Custom Fields window.

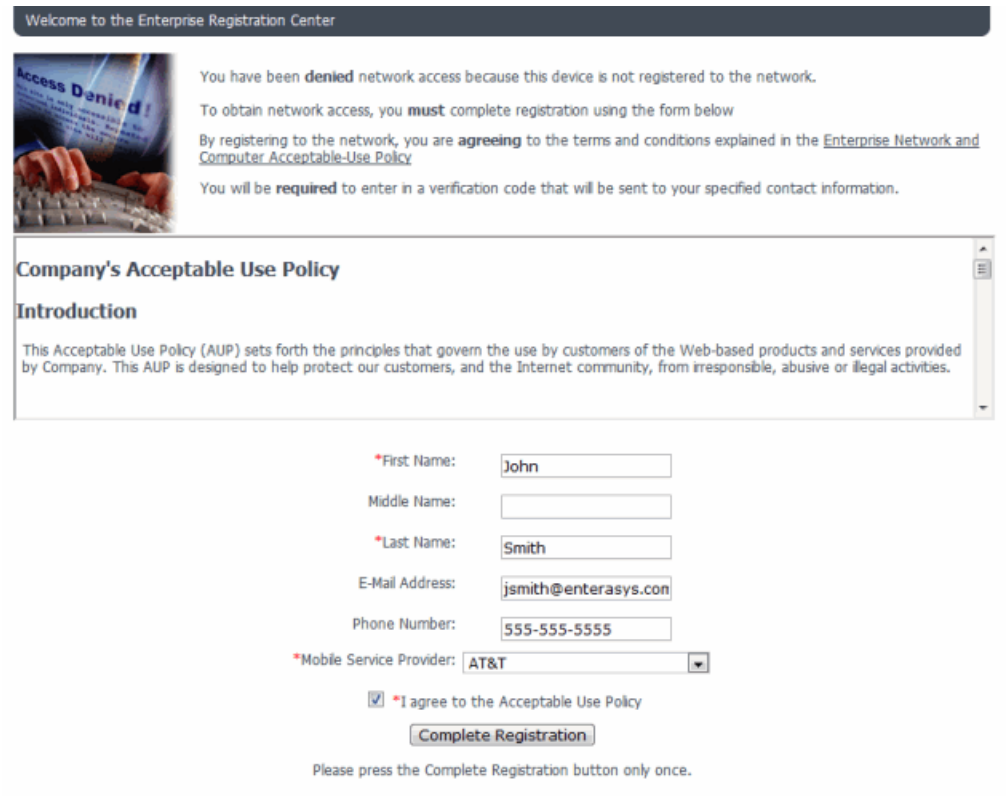
7. Set the appropriate custom fields to display on the Registration web page or Guest Web Access login page, depending on the verification method you selected (refer to the table above). When you save your portal changes, the correct configuration of the custom fields are verified. These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing them for one access type also changes them for the others. For more information, see the Manage Custom Fields Window.

   Click OK to close the window.

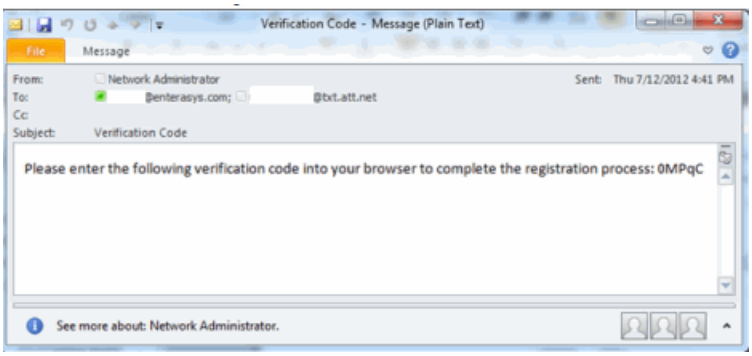
8. Back in the Portal Configuration, click Save to save your changes. Close the Portal Configuration window. Enforce the new portal configuration to your engine(s). Verification is now configured for your guest registration.

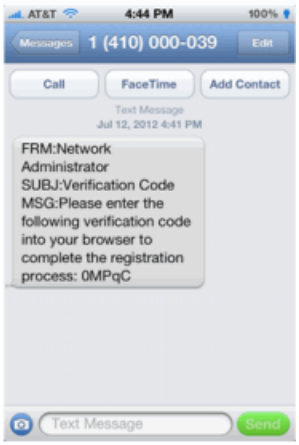
How User Verification Works

When a guest attempts to access the network, the Registration web page or Guest Web Access login page asks for their email address and/or phone number and mobile service provider, along with their normal contact information.

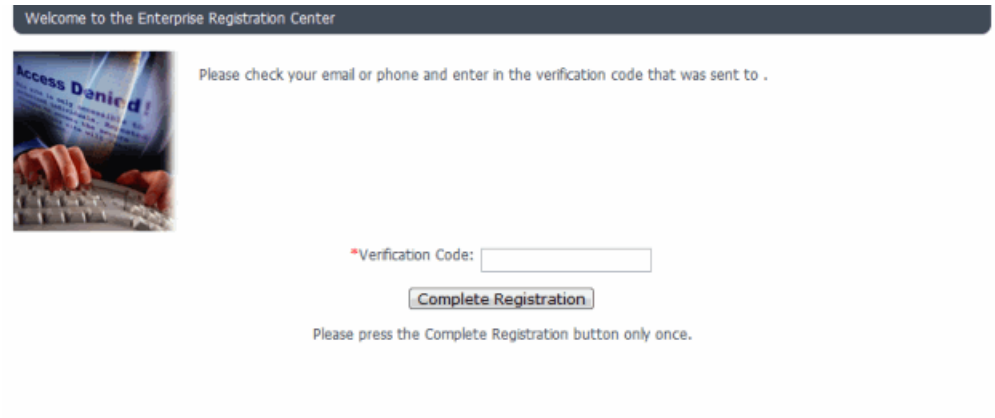


When they click the Complete Registration button, they are sent a verification code via an email or a phone text message.





The web page then prompts them for the code. When they enter the correct code that was generated for them and click the Complete Registration button, they are allowed access to the network. The verification code is valid for 15 minutes and cannot be reused once it is validated.



Related Information

For information on related help topics:

- Portal Configuration

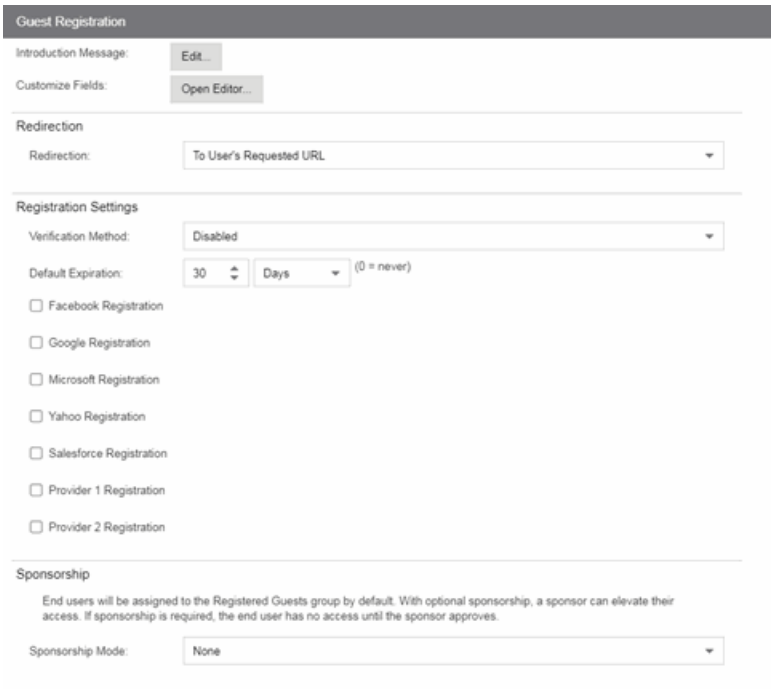
How to Configure Sponsorship for Guest Registration

This topic describes how to configure sponsorship for Guest Registration and Secure Guest Access. Sponsorship is configured as part of your portal configuration, and is accessed from the Guest Registration and Secure Guest Access views in the Portal section of the Portal Configuration panel.

With sponsored registration, end users are only allowed to register to the network when approved by a "sponsor," an internal trusted user to the organization. Sponsorship can provide the end user with a higher level of access than just guest access and allows the sponsor to fine-tune the level of access for individual end users. The end user registers and declares a sponsor's email address. The sponsor is notified and approves the registration, and can assign an elevated level of access, if desired.

To configure sponsorship:

1. Access the **Control** > **Access Control** tab.
2. In the left-panel tree, expand the **Access Control** Configurations > Portal and click on the Guest Registration view or the Secure Guest Access view (depending on the access type you are configuring). The screenshot below shows the Guest Registration view.



3. In the Sponsorship section, select the Sponsorship Mode required. Additional settings display when you select optional or required sponsorship.
    - None - Sponsorship is not required and the end user is assigned to the Registered Guests End-System Group.
    - Optional - The end user is assigned to the Registered Guests End-System Group until sponsored. At that time, the sponsor can assign elevated access, if desired.
    - Required - The end user has no access until the sponsor approves the registration. The end user is added to the Registration Pending Access end-system group and is presented the sponsorship pending page until approved.
4. Sponsored Registration Introduction - Click the Edit button to open a window where you can edit the introductory message displayed to the end user.
5. Admin/Sponsor Email - Enter the person or group to notify when an end user requests sponsorship, typically the network Extreme Access Control administrator, for example "IT@CompanyA.com." This email address is always notified, in addition to the sponsor email address entered by the end user when they register to the network.
6. Sponsor Email Field - Select an option for the sponsor email field on the registration web page.

- Do Not Display - The field is not displayed, and the end user is not required to enter a sponsor email address. In this case, only the admin/sponsor email address (defined above) is notified when the end user registers.
- Display Predefined Sponsor List - The end user must select a sponsor email from a list of predefined sponsors (defined below). The end user sees a drop-down menu of sponsor email addresses and select the appropriate sponsor.
- User Specifies Any Email as Sponsor - The end user can enter any email address as a sponsor's email address.
- User Must Specify Predefined Sponsor Email - The end user must enter an email address that matches one of the predefined sponsors (defined below).

7. Predefined Sponsors - Enter one or more sponsor email addresses. If you have selected Display Predefined Sponsor List as your Sponsor Email Field option (above), these addresses are presented to the end user as a drop-down menu, allowing them to select a sponsor email address. If you have selected User Must Specify Predefined Sponsor Email as your Sponsor Email Field option, then the sponsor email address entered by the end user must match an email address listed here. Email addresses can be separated by semi-colons (;) or commas (,) for example, jdoe@CompanyA.com;rsmith@CompanyA.com. Because commas are accepted separators, they should not be used in actual email addresses.
8. In the Portal Configuration window, click Save to save your changes. You need to enforce the new portal configuration to your engine(s).

Related Information

For information on related help topics:

- Portal Configuration

How to Implement Facebook Registration

This Help topic describes the steps for implementing guest registration using Facebook as a way to obtain end user information.

In this scenario, the Guest Registration portal provides the option to register as a guest or log into Facebook in order to complete the registration process. If the end user selects the Facebook option, Extreme Management Center OAuth to securely access the end user's Facebook account, obtain public end user data, and use that data to complete the registration process.

NOTE: Guest OAuth (e.g. Google, Yahoo) may not support native mobile browsers and display a "user agent" error. To access the network, use a standard browser application (e.g. Google Chrome).

Guest Registration using Facebook has two main advantages:

- It provides Extreme Management Center with a higher level of user information by obtaining information from the end user's Facebook account instead of relying on information entered by the end user.
- It provides an easier registration process for the end user. Extreme Management Center retrieves the public information from the end user's Facebook account and uses that information to populate the name and email registration fields.

This topic includes information and instructions on:

Requirements

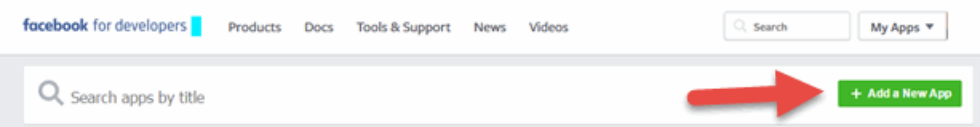
These are the configuration requirements for Facebook Registration.

- The Extreme Access Control engine must have Internet access in order to retrieve user information from Facebook.
- The Extreme Access Control Unregistered access policy must allow access to the Facebook site (either allow all SSL or make allowances for Facebook servers).
- A Unique Facebook application must be created on the Facebook Developers page (see instructions below).
- The Portal Configuration must have Facebook Registration enabled and include the Facebook Application ID and Secret (see instructions below).

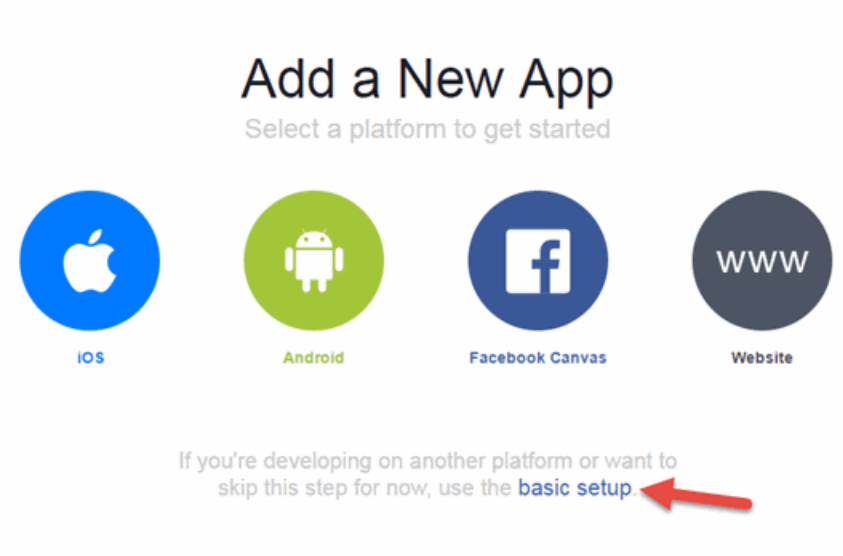
Creating a Facebook Application

When implementing guest registration using Facebook, you must first create a Facebook application. This generates an Application ID and Application Secret that are required as part of the Extreme Management Center OAuth process. Use the following steps to create a Facebook application.

1. Access the Facebook Developers page at https://developers.facebook.com/apps/. If you already have a Developers account you can log in, otherwise you must create a Developers account.
2. Once logged in, click the Add a New App button.



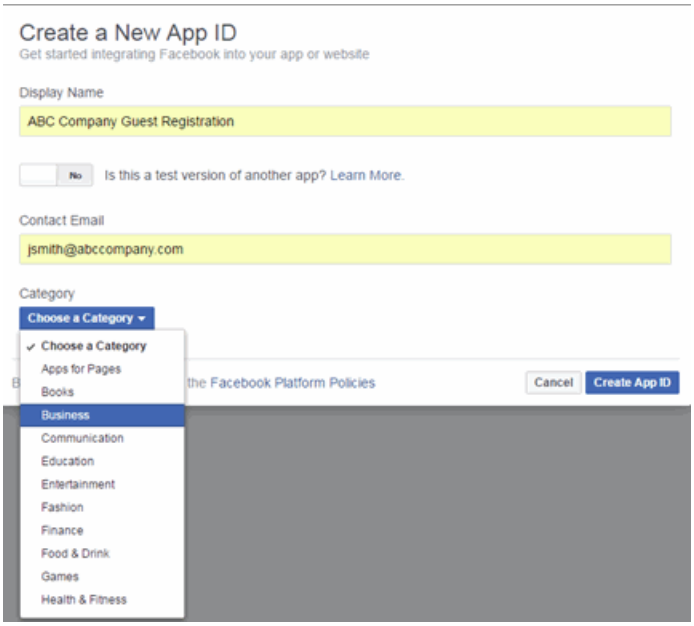
   The Add a New App window opens.
3. Click the basic setup link at the bottom of the window.



The Create a New App ID window opens.

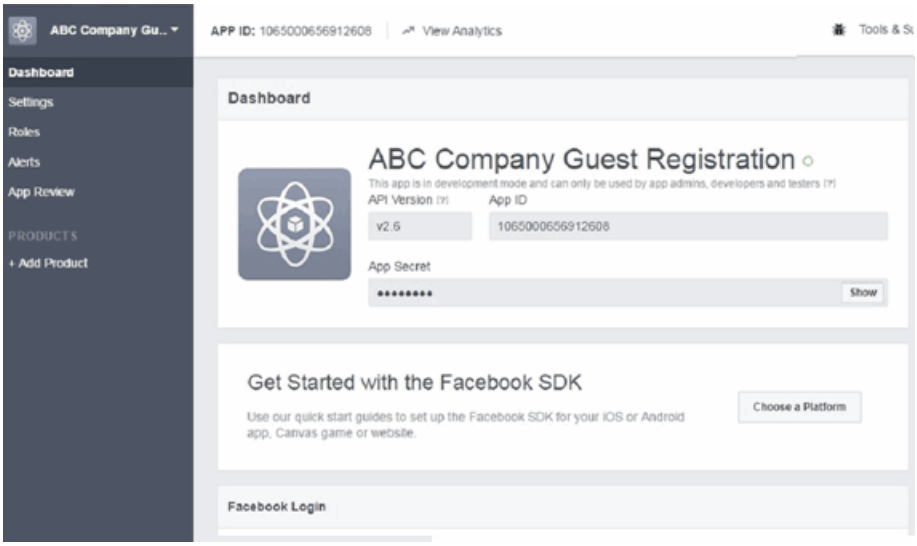
4. Enter a **Display Name**, enter a **Contact Email**, and select a **Category** for your app.

   The **Display Name** is the name of the app presented to the end-user when they grant Extreme Management Center access to their Facebook information and should clearly indicate what its purpose is, for example, Extreme Networks Guest Registration.



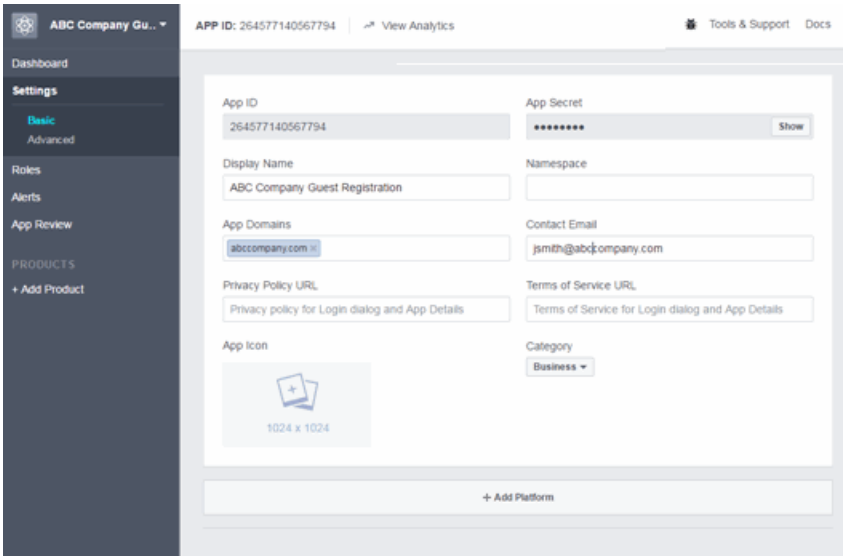
5. Click **Create App ID**.

   The Dashboard panel opens and displays information about the new app including an App ID and an App Secret.



6. Select **Settings** in the left panel.

   The Settings panel's **Basic** tab opens.

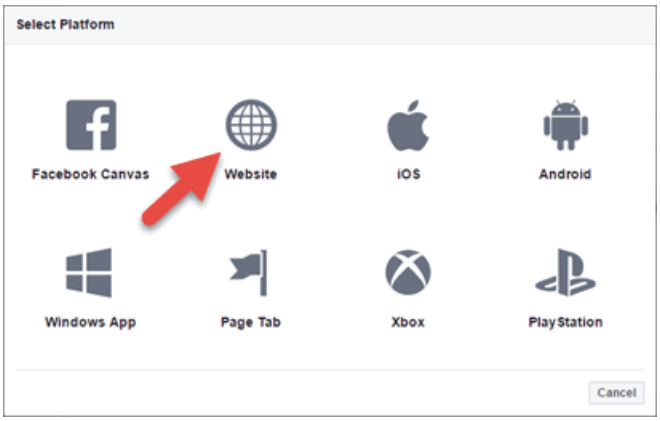


7. Enter in a valid domain name for the Extreme Access Control engines in the **App Domains** field. For example, if the Extreme Access Control engine to which users are

connecting is Extreme Access Control engine.AbcCompany.com, enter "abccompany.com" in the **App Domains** field.

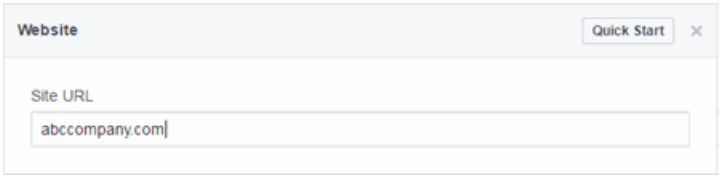
8. Click **Add Platform**.

   The Select Platform window opens.



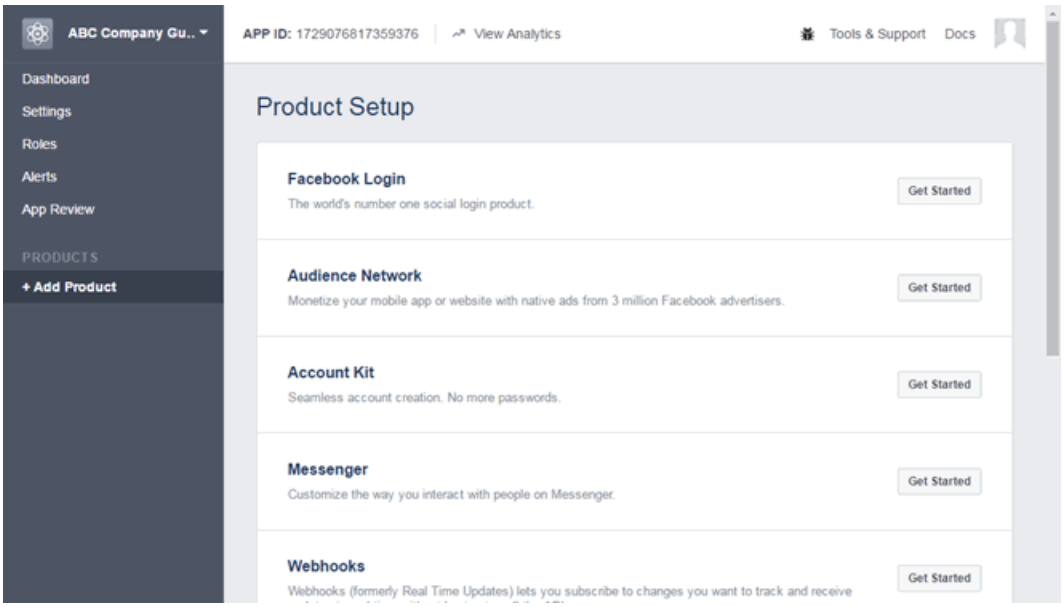
9. Select **Website**.

   The Website panel displays on the **Basic** tab.



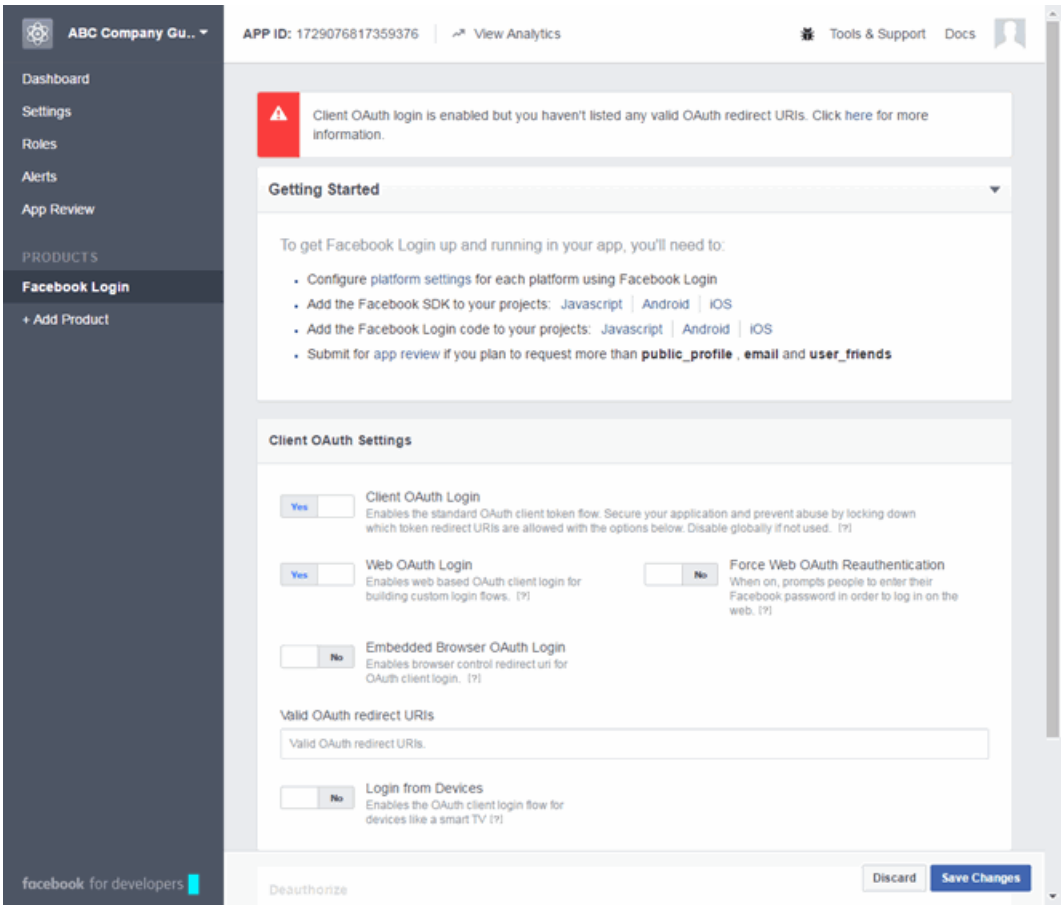
10. Enter the domain name you added in the **App Domains** field in step 7 in the **Site URL** field.
11. Click **Save Changes**.
12. Click **Add Product** in the left panel.

    The Product Setup panel opens.



13. Click the Facebook Login Get Started button.

    The Getting Started panel opens.



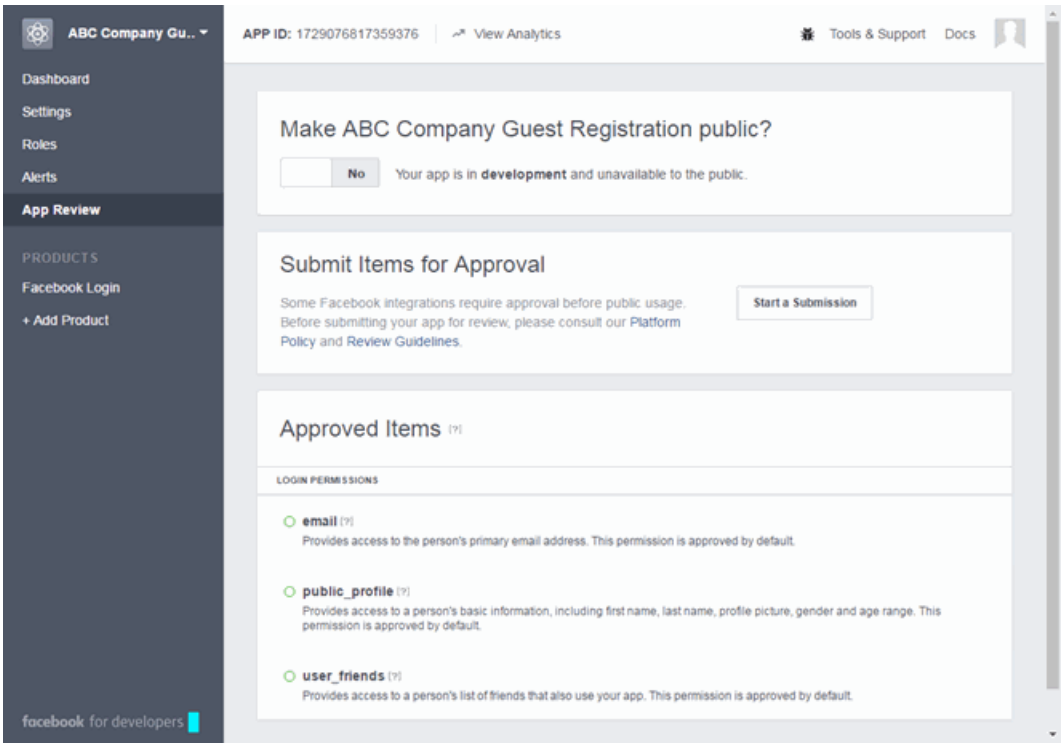
14. Enter the **Valid OAuth redirect URIs**. A redirect URI is required to redirect the user back to the engine with an Access Token Extreme Management Center uses to access the user account and retrieve the user data. The Redirection URI should be in the following format:

    https://<Extreme Access ControlengineFQDN>/fb_oauth

    A Redirection URI must be added for each Extreme Access Control engine where end users can register via Facebook.

15. Click **Save Changes**.
16. Select **App Review** in the left panel.

    The App Review panel opens.



17. Click the **No** button in the **Make *<Display Name>* public** field to change the button to **Yes**.

    A Confirmation window appears.

18. Click **Confirm**.

    The Approved Items section displays a list of default permissions that provide access to end user data. (For more information on setting permissions, see https://developers.facebook.com/docs/facebook-login/permissions#reference.)

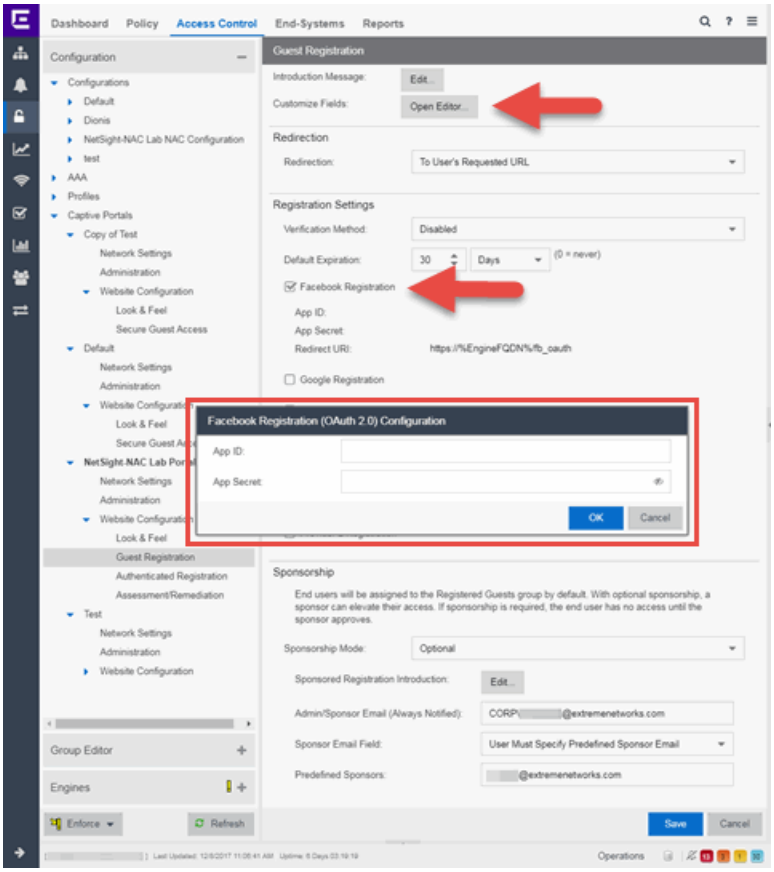
    Your application is created and ready to use.

    You need to add the App ID and App Secret to your portal configuration.

Portal Configuration

The Application ID and Application Secret assigned during the creation of the Facebook application must be provided in the Portal Configuration in order for the entire process to complete properly.

1. Open the **Control** > **Access Control** tab.
2. In the left-panel tree, expand the Extreme Access Control Configurations > Portal tree and select Guest Registration.



3. In the Customize Fields section, click the **Open Editor** button to open the Manage Custom Fields window where you can change registration portal fields. Facebook registration uses only the First Name, Last Name, and Email Address fields, and the Display Acceptable Use Policy (AUP) option. All other fields only apply to regular guest registration. If the Display AUP option is selected, the captive portal verifies that the AUP has been acknowledged before redirecting the user to Facebook.
4. Select the Facebook Registration checkbox.
5. Enter the Facebook App ID and Facebook App Secret.
6. Click **Save**. Warning messages display stating that Verification Method and Sponsorship are not used for Facebook registration, and that an FDQN is required will be enabled.
7. Enforce the new configuration to your engines.

How Facebook Registration Works

Once you have configured Facebook registration using the steps above, this is how the registration process works:

1. The end user attempts to access an external Web site. Their HTTP traffic is redirected to the captive portal.
2. In the Guest Registration Portal, the end user selects the option to register using Facebook.
3. The end user is redirected to the Facebook login. If Acceptable Use Policy option is configured, the captive portal verifies that the AUP has been acknowledged before redirecting the user to Facebook.
4. Once logged in, the end user is presented with the information that Extreme Management Center receives from Facebook.
5. The end user grants Extreme Management Center access to the Facebook information and is redirected back to the captive portal where they see a "Registration in Progress" message.
6. Facebook provides the requested information to Extreme Management Center, which uses it to populate the user registration fields.
7. The registration process completes and network access is granted.
8. The word "Facebook" is added to the user name so you can easily search for Facebook registration via the Registration Administration web page.

Special Deployment Considerations

Please read through the following deployment consideration prior to configuring Facebook Registration.

Wireless Clients

To allow traffic to your network via a wireless connection, create an L7 host record for the Unregistered Role on your Wireless Controller for `facebook.com`.

Networks using DNS Proxy

Facebook Registration for networks redirecting HTTP traffic to the captive portal using DNS Proxy requires additional configuration.

In order for Facebook Registration to work properly with DNS Proxy, all domains/URLs necessary to properly load the Facebook web page must be added to the Allowed URLs/Allowed Domains section of the captive portal configuration. Otherwise, the Extreme Access Control engine resolves DNS queries for these components to the Extreme Access Control engine IP causing the page to not load properly.

As of July 26, 2014, you must add the following domains in order for Facebook registration to work with DNS Proxy. These domains are subject to change and may vary based on location.

Facebook.com
fbstatic-a.akamaihd.net
fbcdn-profile-a.akamaihd.net
fbcdn-photos-c-a.akamaihd.net

Related Information

- Portal Configuration

How to Implement Google Registration

This Help topic describes the steps for implementing guest registration using Google as a way to obtain end user information.

In this scenario, the Guest Registration portal provides the option to register as a guest or log into Google in order to complete the registration process. If the end user selects the Google option, Extreme Management Center OAuth to securely access the end user's Google account, obtain public end user data, and use that data to complete the registration process.

NOTE: Guest OAuth (e.g. Google, Yahoo) may not support native mobile browsers and display a "user agent" error. To access the network, use a standard browser application (e.g. Google Chrome).

Guest Registration using Google has two main advantages:

- It provides Extreme Management Center with a higher level of user information by obtaining information from the end user's Google account instead of relying on information entered by the end user.
- It provides an easier registration process for the end user. Extreme Management Center retrieves the public information from the end user's Google account and uses that information to populate the name and email registration fields.

This topic includes information and instructions on:

Requirements

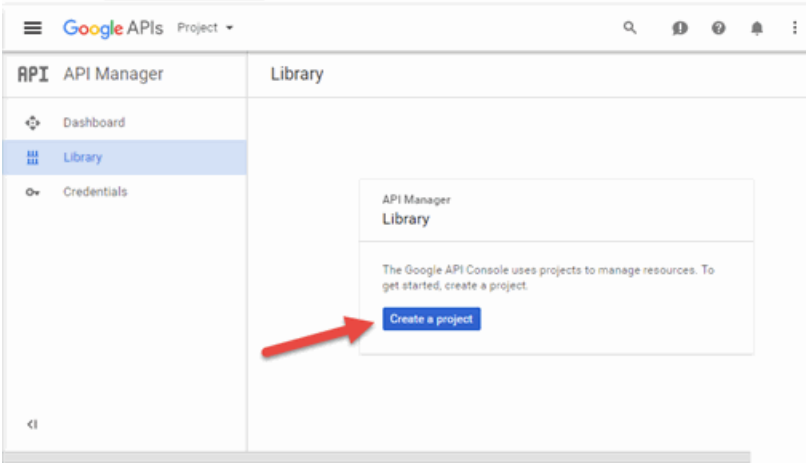
These are the configuration requirements for Google Registration.

- The Extreme Access Control engine must have Internet access in order to retrieve user information from Google.
- The Extreme Access Control Unregistered access policy must allow access to the Google site (either allow all SSL or make allowances for Google servers).
- The Extreme Access Control Unregistered access policy must allow access to HTTPS traffic to the Google OAuth servers.
- A Unique Google application must be created on the Google Developers page (see instructions below).
- The Portal Configuration must have Google Registration enabled and include the Google Application ID and Secret (see instructions below).

Creating a Google Application

When implementing guest registration using Google, you must first create a Google application. This generates an Application ID and Application Secret that are required as part of the Extreme Management Center OAuth process. Use the following steps to create a Google application.

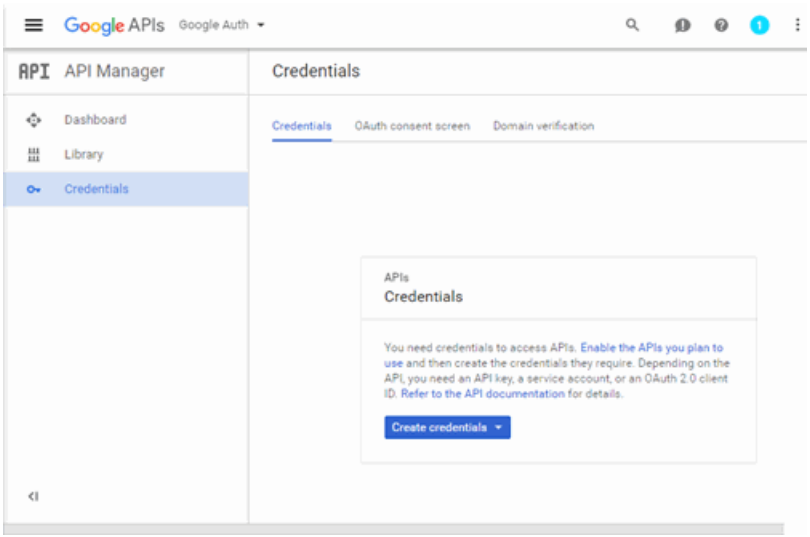
1. Access the Google Developers page at https://console.developers.google.com/projectselector/apis/library.
2. Log into your existing Developers account or create a new Developers account.
3. Click the **Create a project** button.



The New Project window opens.

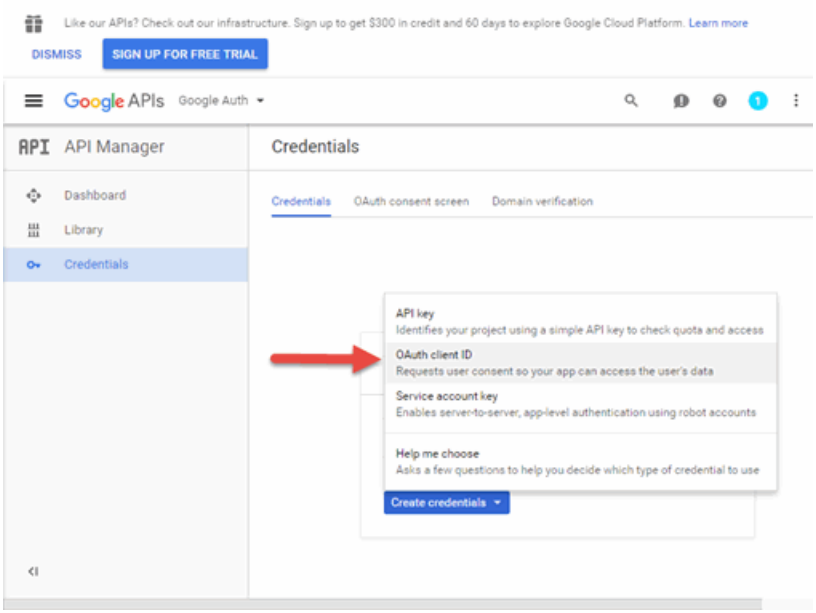
4. Enter a **Project name** and click **Create**.

5. Click the **Credentials** link in the left-panel.



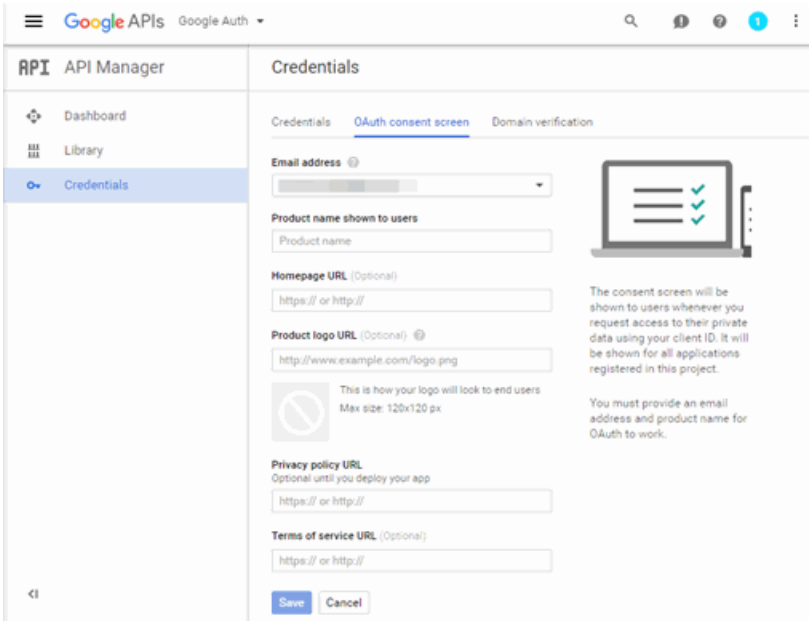
The Credentials panel opens.

6. Click the **Create credentials** button to open the drop-down menu and select **OAuth client ID**.



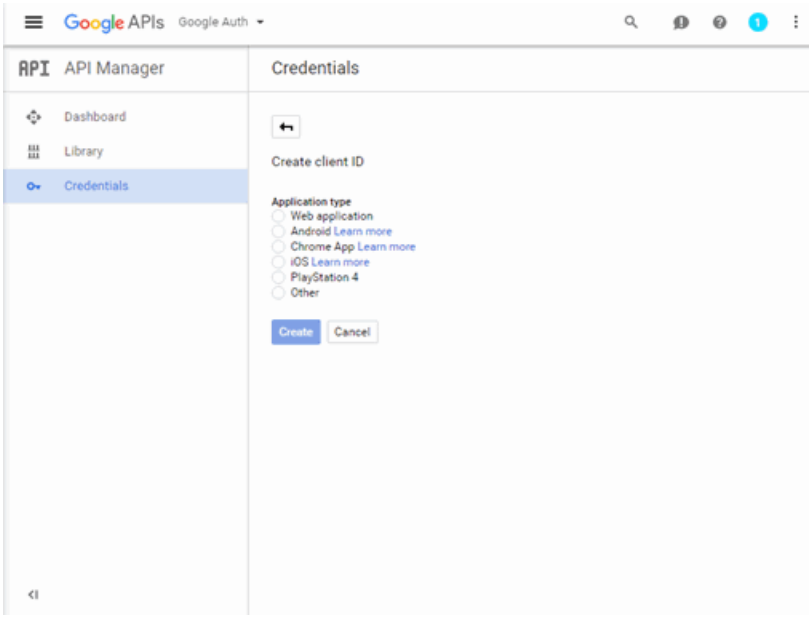
The Create client ID panel displays.

7. Click **Configure consent screen** to open the OAuth consent screen panel.



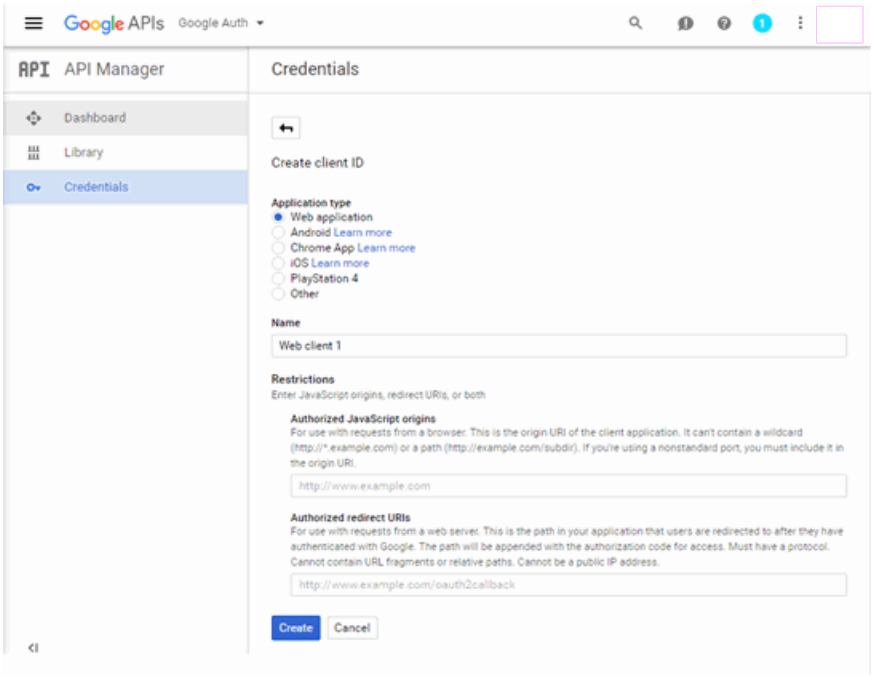
8. Select your email address, enter your product name, and enter the URL to any of the applicable resources for your company, then click **Save**.

   The Create client ID panel opens.



9. Select **Web application**.

The panel expands to display additional fields.



10. Enter a name for the application in the **Name** field. Use a name that clearly indicates what its purpose is, for example, Extreme Networks Guest Registration.
11. Enter an **Authorized redirect URI** in the following format `https://<AccessControlengineFQDN>/google_oauth`. Google uses the **Authorized redirect URI** to redirect the user back to the engine with an Access Token.

NOTES: Google OAuth APIs require your engine's FQDN resolves to a top level domain (.com, .net, .edu, .org, .mil, .gov, or .int. You cannot use a domain not classified as top level (e.g. MyGateway.MyCompany.Local) or the engines IP address, which may require you to reclassify your domain and hosts.

Use only lowercase when entering the host and domain suffix (e.g. .com).

---

12. Enter the **Authorized redirect URI** for any additional Extreme Access Control engines registering end-users via Google.
13. Click **Create**.

The **OAuth client** window appears, displaying your client ID and secret.

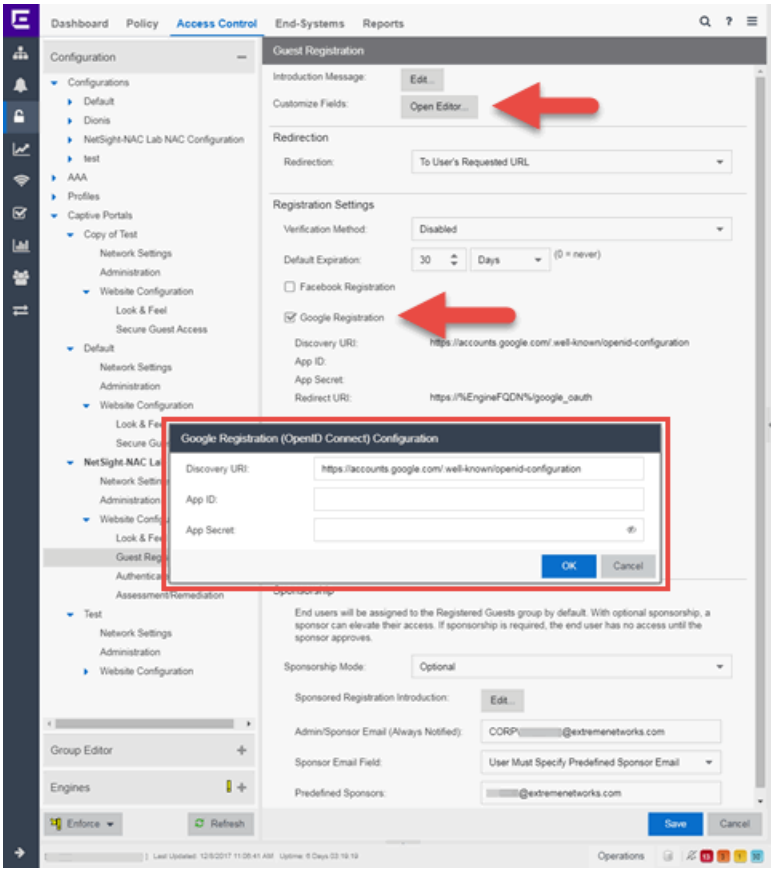
Your application is created and ready to use.

You need to add the client ID and client secret to your portal configuration.

Portal Configuration

The client ID and client secret assigned during the creation of the Google application must be provided in the Portal Configuration in order for the entire process to complete properly.

1. Open the Control > Access Control tab.
2. In the left-panel tree, expand the Configuration > Captive Portals > Website Configuration > and select Guest Registration.



3. In the Customize Fields section, click the **Open Editor** button to open the Manage Custom Fields window where you can change registration portal fields. Google registration uses only the First Name, Last Name, and Email Address fields, and the Display Acceptable Use Policy (AUP) option. All other fields only apply to regular guest registration. If the Display AUP option is selected, the captive portal verifies that the AUP has been acknowledged before redirecting the user to Google.
4. Select the **Google Registration** checkbox.
5. Click **Edit**.
6. Enter the client ID in the **Google App ID** field and the client secret in the **App Secret** field.
7. Click **Save**. Warning messages display stating that Verification Method and Sponsorship are not used for Google registration, and that an FDQN is required will be enabled.
8. Enforce the new configuration to your engines.

How Google Registration Works

Once you have configured Google registration using the steps above, this is how the registration process works:

1. The end user attempts to access an external Web site. Their HTTP traffic is redirected to the captive portal.
2. In the Guest Registration Portal, the end user selects the option to register using Google.
3. The end user is redirected to the Google login. If Acceptable Use Policy option is configured, the captive portal verifies that the AUP has been acknowledged before redirecting the user to Google.
4. Once logged in, the end user is presented with the information that Extreme Management Center receives from Google.
5. The end user grants Extreme Management Center access to the Google information and is redirected back to the captive portal where they see a "Registration in Progress" message.
6. Google provides the requested information to Extreme Management Center, which uses it to populate the user registration fields.
7. The registration process completes and network access is granted.
8. The word "Google" is added to the user name so you can easily search for Google registration via the Registration Administration web page.

Special Deployment Considerations

Please read through the following deployment consideration prior to configuring Google Registration.

To allow traffic to your network via a wireless connection, create an L7 host record for the Unregistered Role on your Wireless Controller for `accounts.google.com` and `gstatic.com`.

Networks using DNS Proxy

Google Registration for networks redirecting HTTP traffic to the captive portal using DNS Proxy requires additional configuration.

In order for Google Registration to work properly with DNS Proxy, all domains/URLs necessary to properly load the Google web page must be added to the Allowed URLs/Allowed Domains section of the captive portal configuration. Otherwise, the Extreme Access Control engine resolves DNS queries for these components to the Extreme Access Control engine IP causing the page to not load properly.

As of February 2017, you must add the following domains in order for Google registration to work with DNS Proxy. These domains are subject to change and may vary based on location.

Accounts.google.com

Related Information

- Portal Configuration

How to Implement Microsoft Registration

This Help topic describes the steps for implementing guest registration using Microsoft as a way to obtain end user information.

In this scenario, the Guest Registration portal provides the option to register as a guest or log into Microsoft in order to complete the registration process. If the end user selects the Microsoft option, Extreme Management Center OAuth to securely access the end user's Microsoft account, obtain public end user data, and use that data to complete the registration process.

NOTE: Guest OAuth (e.g. Google, Yahoo) may not support native mobile browsers and display a "user agent" error. To access the network, use a standard browser application (e.g. Google Chrome).

Guest Registration using Microsoft has two main advantages:

- It provides Extreme Management Center with a higher level of user information by obtaining information from the end user's Microsoft account instead of relying on information entered by the end user.
- It provides an easier registration process for the end user. Extreme Management Center retrieves the public information from the end user's Microsoft account and uses that information to populate the name and email registration fields.

This topic includes information and instructions on:

Requirements

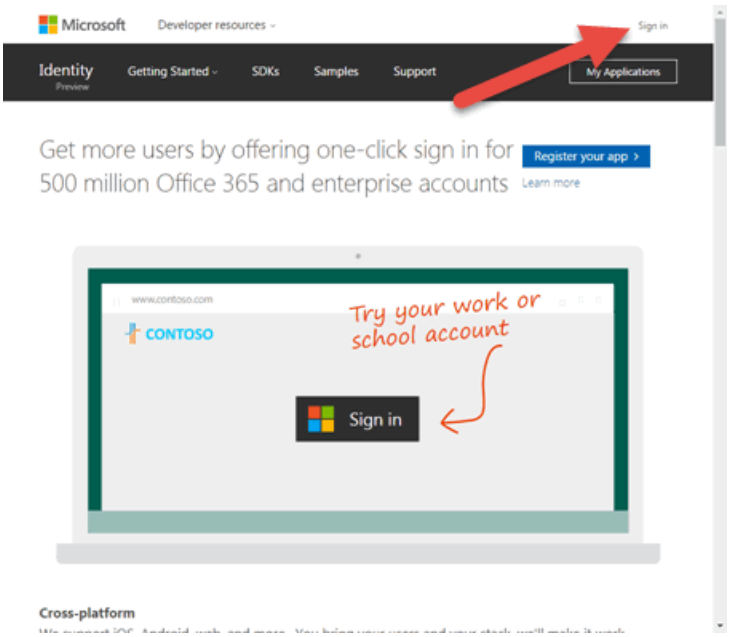
These are the configuration requirements for Microsoft Registration.

- The Extreme Access Control engine must have Internet access in order to retrieve user information from Microsoft.
- The Extreme Access Control Unregistered access policy must allow access to the Microsoft site (either allow all SSL or make allowances for Microsoft servers).
- The Extreme Access Control Unregistered access policy must allow access to HTTPS traffic to the Microsoft OAuth servers.
- A Unique Microsoft application must be created on the Microsoft Developers page (see instructions below).
- The Portal Configuration must have Microsoft Registration enabled and include the Microsoft Application ID and Secret (see instructions below).

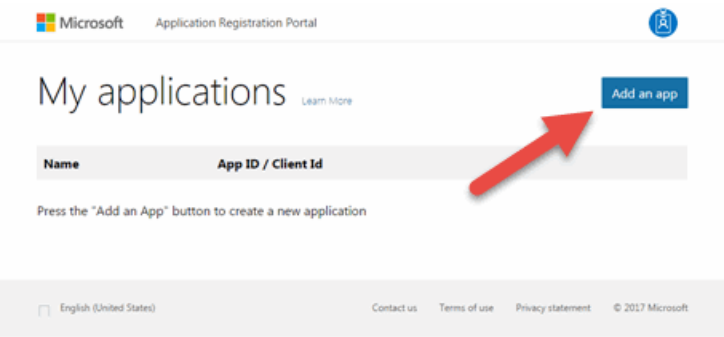
Creating a Microsoft Application

When implementing guest registration using Microsoft, you must first create a Microsoft application. This generates an Application ID and Application Secret that are required as part of the Extreme Management Center OAuth process. Use the following steps to create a Microsoft application.

1. Access the Microsoft Developers page at https://apps.dev.microsoft.com/#/appList.
2. Log into your existing account or create a new account by clicking the Sign in link in the top-right corner of the window.



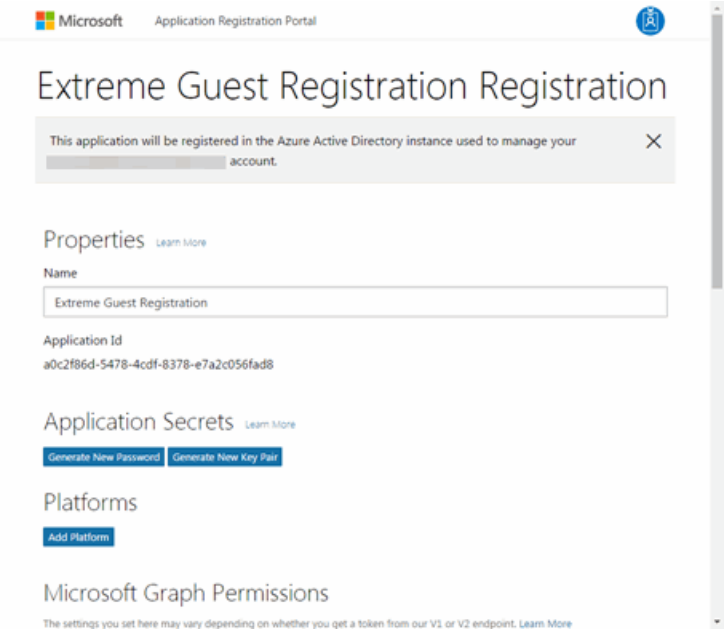
3. Click the **Add an app** button.



The New Application Registration window opens.

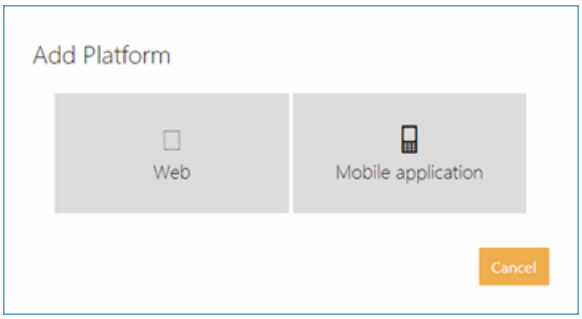
4. Enter a **Name** for the application. Use a name that clearly indicates it's purpose (e.g. Extreme Networks Guest Registration) and click **Create application**.

The Application Registration window opens.



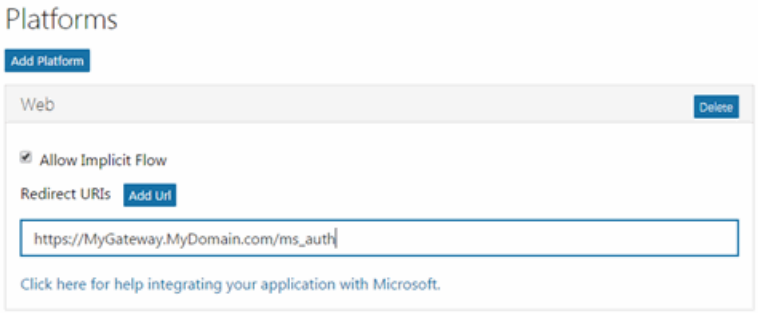
5. Click **Add Platforms** under Platforms.

The Add Platform window opens.



6. Click **Web**.

   Additional fields display under Platforms allowing you to configure a web platform.

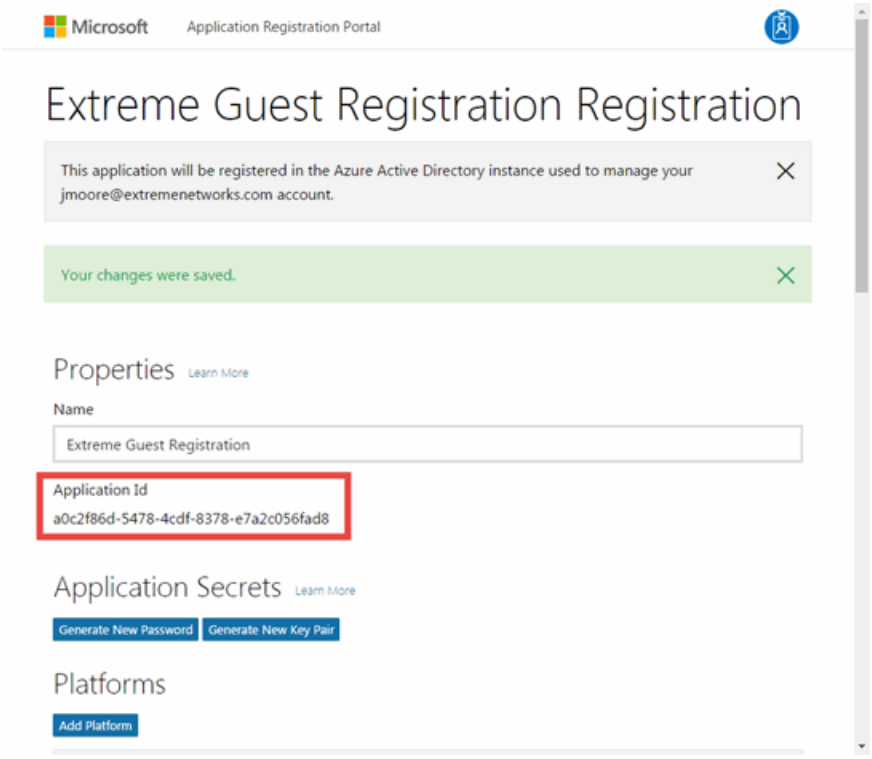


7. Enter a **Redirect URI** in the following format `https://<AccessControlengineFQDN>/ms_oauth`. Microsoft uses the **Redirect URI** to redirect the user back to the engine with an Access Token.

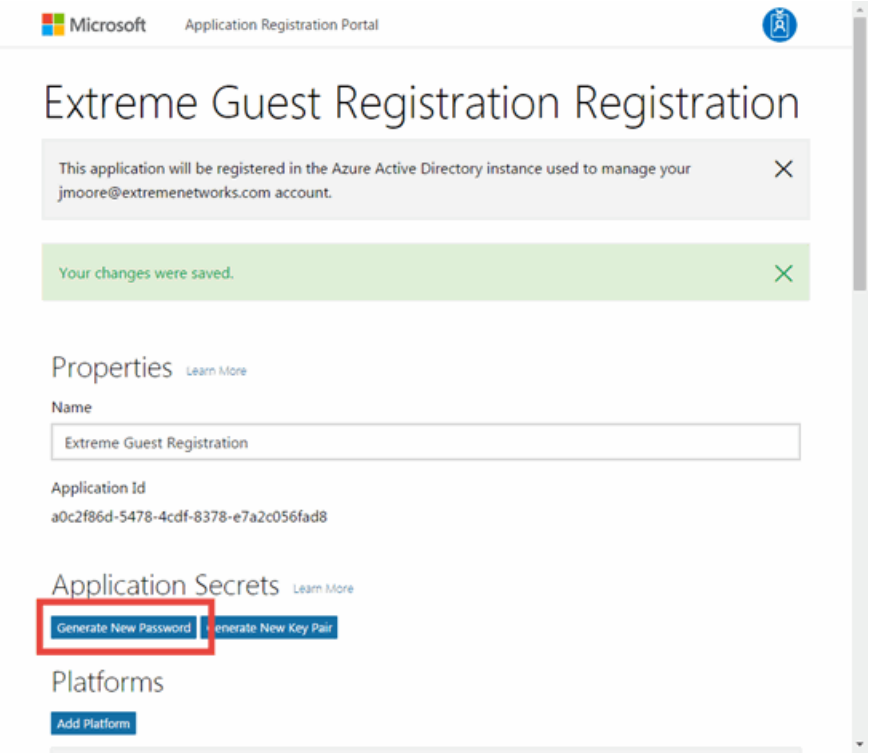
   NOTE: Microsoft applications can only use a limited set of redirect URI values.

8. Click **Add Url** to enter the **Redirect URI** for any additional Extreme Access Control engines registering end-users via Microsoft.

9. Copy the **Application Id** under Properties.



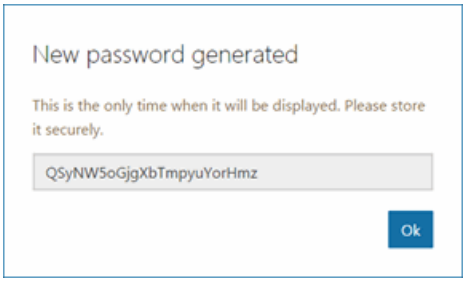
10. Click **Generate New Password** under Application Secrets.



The **New password generated** window displays.

11. Copy the application password.

IMPORTANT: Ensure you copy the password accurately. After the window is closed, you cannot access the password again.



12. Click **Save**.

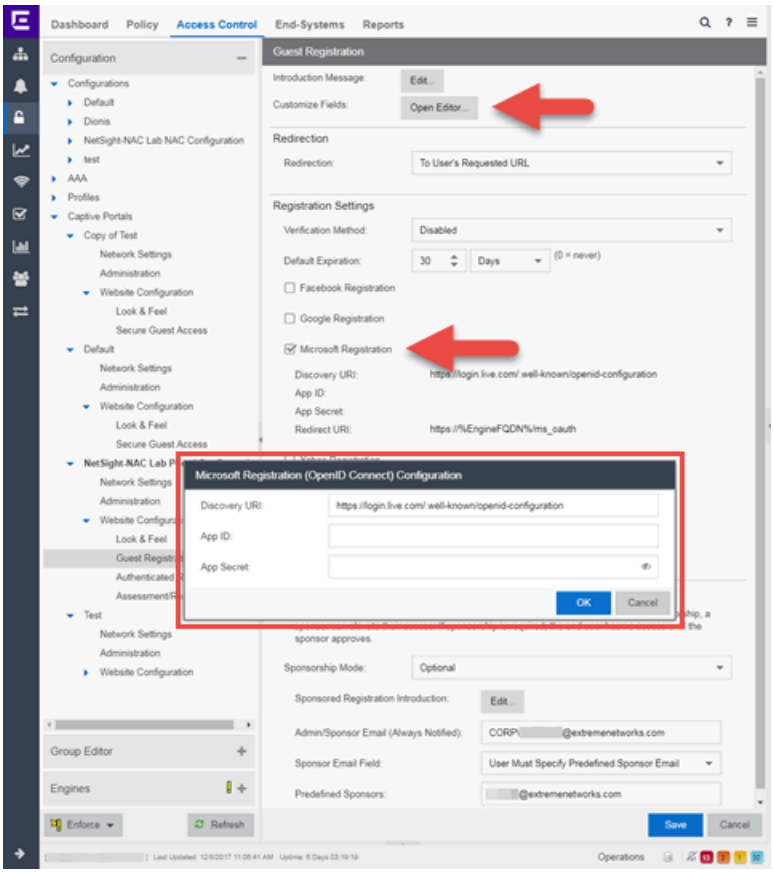
Your application is created and ready to use.

You need to add the **Application Id** and application password to your portal configuration.

Portal Configuration

The Application Id and application password assigned during the creation of the Microsoft application must be provided in the Portal Configuration in order for the entire process to complete properly.

1. Open the **Control** > **Access Control** tab.
2. In the left-panel tree, expand the Extreme Access Control Configurations > Portal tree and select Guest Registration.



3. In the Customize Fields section, click the **Open Editor** button to open the Manage Custom Fields window where you can change registration portal fields. Microsoft registration uses only the First Name, Last Name, and Email Address fields, and the Display Acceptable Use Policy (AUP) option. All other fields only apply to regular guest registration. If the Display AUP option is selected, the captive portal verifies that the AUP has been acknowledged before redirecting the user to Microsoft.
4. Select the **Microsoft Registration** checkbox.

5. Click **Edit**.
6. Enter the Application Id in the **Microsoft App ID** field and the application password in the **Microsoft App Secret** field.
7. Click **Save**. Warning messages display stating that Verification Method and Sponsorship are not used for Microsoft registration, and that an FDQN is required and will be enabled.
8. Enforce the new configuration to your engines.

How Microsoft Registration Works

Once you have configured Microsoft registration using the steps above, this is how the registration process works:

1. The end user attempts to access an external Web site. Their HTTP traffic is redirected to the captive portal.
2. In the Guest Registration Portal, the end user selects the option to register using Microsoft.
3. The end user is redirected to the Microsoft login. If Acceptable Use Policy option is configured, the captive portal verifies that the AUP has been acknowledged before redirecting the user to Microsoft.
4. Once logged in, the end user is presented with the information that Extreme Management Center receives from Microsoft.
5. The end user grants Extreme Management Center access to the Microsoft information and is redirected back to the captive portal where they see a "Registration in Progress" message.
6. Microsoft provides the requested information to Extreme Management Center, which uses it to populate the user registration fields.
7. The registration process completes and network access is granted.
8. The word "Microsoft" is added to the user name so you can easily search for Microsoft registration via the Registration Administration web page.

Special Deployment Considerations

Please read through the following deployment consideration prior to configuring Microsoft Registration.

To allow traffic to your network via a wireless connection, create an L7 host record for the Unregistered Role on your Wireless Controller for `login.live.com` and `auth.gfx.ms`.

Networks using DNS Proxy

Microsoft Registration for networks redirecting HTTP traffic to the captive portal using DNS Proxy requires additional configuration.

In order for Microsoft Registration to work properly with DNS Proxy, all domains/URLs necessary to properly load the Microsoft web page must be added to the Allowed URLs/Allowed Domains section of the captive portal configuration. Otherwise, the Extreme Access Controlengine resolves DNS queries for these components to the Extreme Access Control engine IP causing the page to not load properly.

As of February 2017, you must add the following domains in order for Microsoft registration to work with DNS Proxy. These domains are subject to change and may vary based on location.

Login.live.com

Related Information

- Portal Configuration

How to Implement Yahoo Registration

This Help topic describes the steps for implementing guest registration using Yahoo as a way to obtain end user information.

In this scenario, the Guest Registration portal provides the option to register as a guest or log into Yahoo in order to complete the registration process. If the end user selects the Yahoo option, Extreme Management Center OpenID to securely access the end user's Yahoo account, obtain public end user data, and use that data to complete the registration process.

NOTE: Guest OAuth (e.g. Google, Yahoo) may not support native mobile browsers and display a "user agent" error. To access the network, use a standard browser application (e.g. Google Chrome).

Guest Registration using Yahoo has two main advantages:

- It provides Extreme Management Center with a higher level of user information by obtaining information from the end user's Yahoo account instead of relying on information entered by the end user.
- It provides an easier registration process for the end user. Extreme Management Center retrieves the public information from the end user's Yahoo account and uses that information to populate the name and email registration fields.

This topic includes information and instructions on:

Requirements

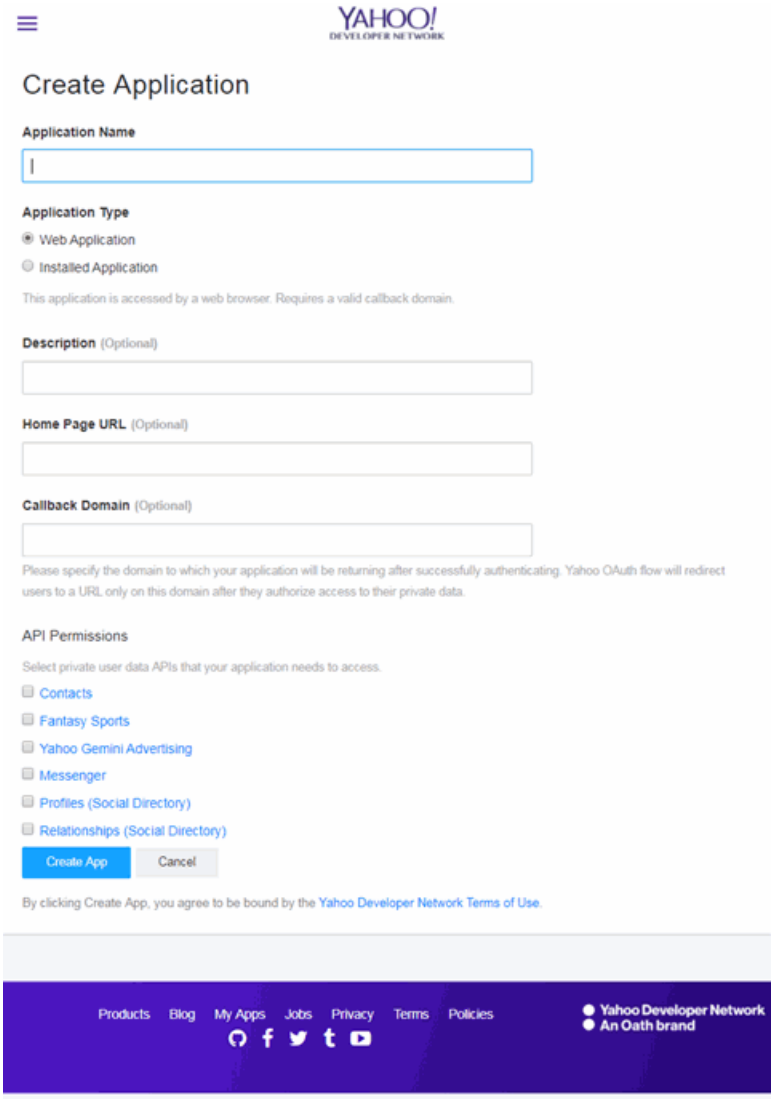
These are the configuration requirements for Yahoo Registration.

- The Extreme Access Control engine must have Internet access in order to retrieve user information from Yahoo.
- The Extreme Access Control Unregistered access policy must allow access to the Yahoo site (either allow all SSL or make allowances for Yahoo servers).
- The Extreme Access Control Unregistered access policy must allow access to HTTPS traffic to the Yahoo OpenID servers.
- A Unique Yahoo application must be created on the Yahoo Developers page (see instructions below).
- The Portal Configuration must have Yahoo Registration enabled and include the Yahoo Application ID and Secret (see instructions below).

Creating a Yahoo Application

When implementing guest registration using Yahoo, you must first create a Yahoo application. This generates an Application ID and Application Secret that are required as part of the Extreme Management Center OpenID process. Use the following steps to create a Yahoo application.

1. Log into your existing account or create a new account.
2. Access the Create Application page at https://developer.yahoo.com/apps/create/.



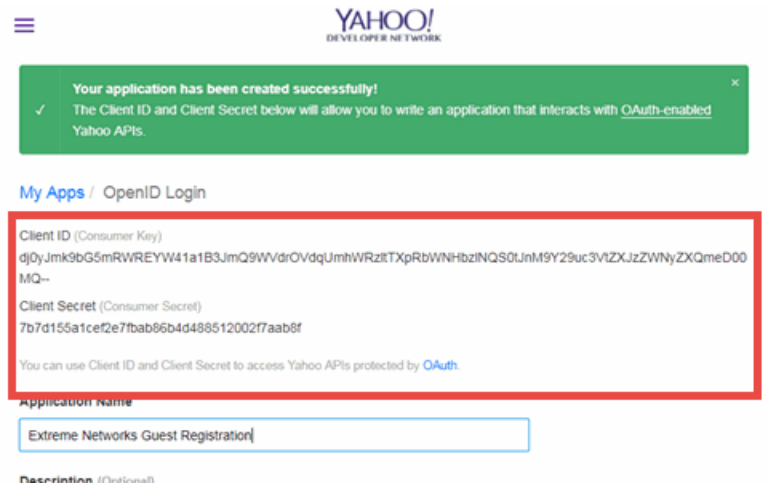
3. Enter a name for the application in the **Application Name** field. Use a name that clearly indicates what its purpose is, for example, Extreme Networks Guest Registration.
4. Select **Web Application** for the **Application Type**.
5. Enter an **Callback Domain** in the following format `https://<AccessControlengineFQDN>`. Yahoo uses the **Callback Domain** to redirect the user back to the engine with an Access Token.

NOTES: Yahoo OAuth APIs require your engine's FQDN resolves to a top level domain (.com, .net, .edu, .org, .mil, .gov, or .int. You cannot use a domain not classified as top level (e.g. MyGateway.MyCompany.Local) or the engines IP address, which may require you to reclassify your domain and hosts.

Use only lowercase when entering the host and domain suffix (e.g. .com).

6. Click Create App.

   The Client ID and Client Secret display at the top of the window.



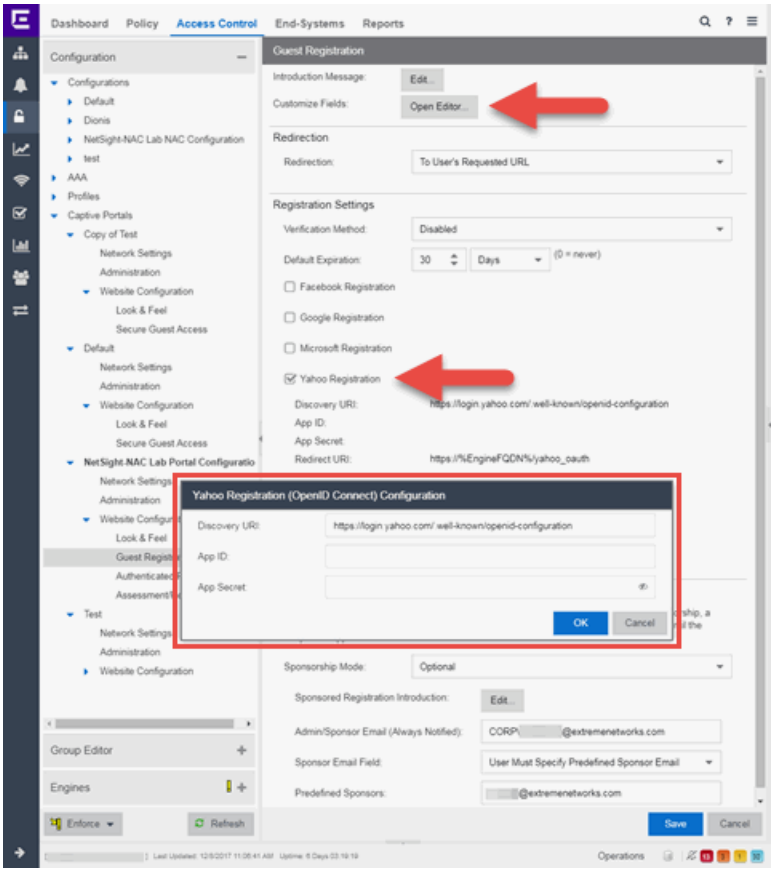
   Your application is created and ready to use.

   You need to add the client ID and client secret to your portal configuration.

Portal Configuration

The client ID and client secret assigned during the creation of the Yahoo application must be provided in the Portal Configuration in order for the entire process to complete properly.

1. Open the Control > Access Control tab.
2. In the left-panel tree, expand the Configuration > Captive Portals > Website Configuration > and select Guest Registration.



3. In the Customize Fields section, click the **Open Editor** button to open the Manage Custom Fields window where you can change registration portal fields. Yahoo registration uses only the First Name, Last Name, and Email Address fields, and the Display Acceptable Use Policy (AUP) option. All other fields only apply to regular guest registration. If the Display AUP option is selected, the captive portal verifies that the AUP has been acknowledged before redirecting the user to Yahoo.
4. Select the **Yahoo Registration** checkbox.
5. Click **Edit**.
6. Enter the Client ID in the **App ID** field and the Client Secret in the **App Secret** field.
7. Click **Save**. Warning messages display stating that Verification Method and Sponsorship are not used for Yahoo registration, and that an FDQN is required will be enabled.
8. Enforce the new configuration to your engines.

How Yahoo Registration Works

Once you have configured Yahoo registration using the steps above, this is how the registration process works:

1. The end user attempts to access an external Web site. Their HTTP traffic is redirected to the captive portal.
2. In the Guest Registration Portal, the end user selects the option to register using Yahoo.
3. The end user is redirected to the Yahoo login. If Acceptable Use Policy option is configured, the captive portal verifies that the AUP has been acknowledged before redirecting the user to Yahoo.
4. Once logged in, the end user is presented with the information that Extreme Management Center receives from Yahoo.
5. The end user grants Extreme Management Center access to the Yahoo information and is redirected back to the captive portal where they see a "Registration in Progress" message.
6. Yahoo provides the requested information to Extreme Management Center, which uses it to populate the user registration fields.
7. The registration process completes and network access is granted.
8. The word "Yahoo" is added to the user name so you can easily search for Yahoo registration via the Registration Administration web page.

Special Deployment Considerations

Please read through the following deployment consideration prior to configuring Yahoo Registration.

To allow traffic to your network via a wireless connection, create an L7 host record for the Unregistered Role on your Wireless Controller for `login.yahoo.com`.

Networks using DNS Proxy

Yahoo Registration for networks redirecting HTTP traffic to the captive portal using DNS Proxy requires additional configuration.

In order for Yahoo Registration to work properly with DNS Proxy, all domains/URLs necessary to properly load the Yahoo web page must be added to the Allowed URLs/Allowed Domains section of the captive portal configuration. Otherwise, the Extreme Access Controlengine resolves DNS queries for these components to the Extreme Access Controlengine IP causing the page to not load properly.

As of February 2017, you must add the following domains in order for Yahoo registration to work with DNS Proxy. These domains are subject to change and may vary based on location.

login.yahoo.com

Related Information

- Portal Configuration

How to Implement Salesforce Registration

This Help topic describes the steps for implementing guest registration using Salesforce as a way to obtain end user information.

In this scenario, the Guest Registration portal provides the option to register as a guest or log into Salesforce in order to complete the registration process. If the end user selects the Salesforce option, Extreme Management Center uses OpenID to securely access the end user's Salesforce account, obtain public end user data, and use that data to complete the registration process.

NOTE: Guest OAuth (e.g. Google, Yahoo) may not support native mobile browsers and display a "user agent" error. To access the network, use a standard browser application (e.g. Google Chrome).

Guest Registration using Salesforce has two main advantages:

- It provides Extreme Management Center with a higher level of user information by obtaining information from the end user's Salesforce account instead of relying on information entered by the end-user.
- It provides an easier registration process for the end user. Extreme Management Center retrieves the public information from the end user's Salesforce account and uses that information to populate the name and email registration fields.

This topic includes information and instructions on:

Requirements

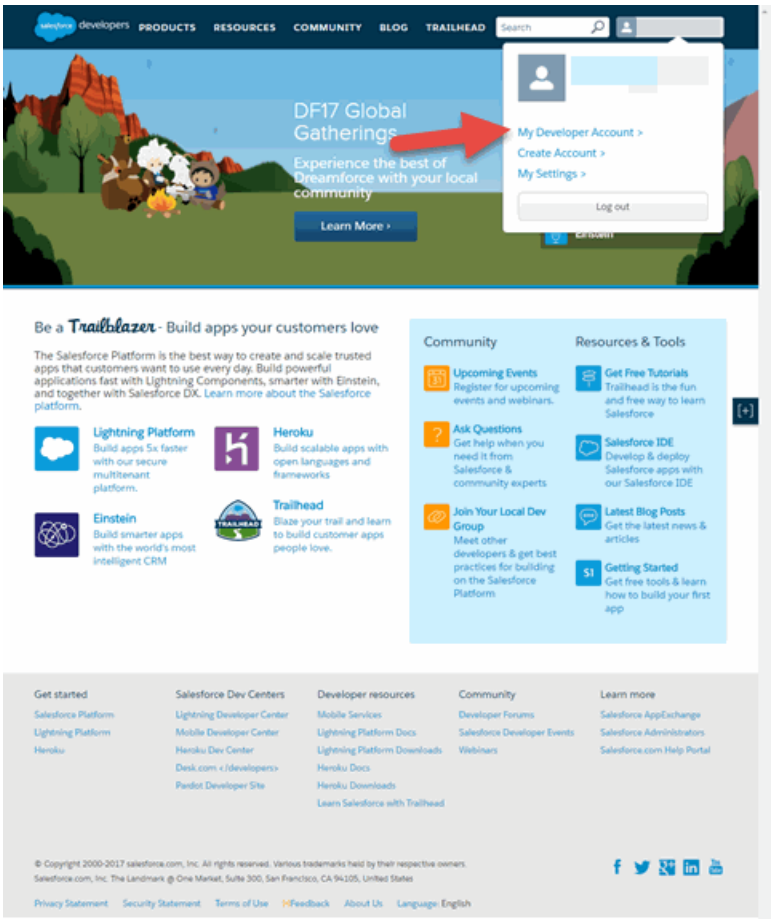
These are the configuration requirements for Salesforce Registration.

- The Extreme Access Control engine must have Internet access in order to retrieve user information from Salesforce.
- The Extreme Access Control Unregistered access policy must allow access to the Salesforce site (either allow all SSL or make allowances for Salesforce servers).
- The Extreme Access Control Unregistered access policy must allow access to HTTPS traffic to the Salesforce OpenID servers.
- A Unique Salesforce application must be created on the Salesforce Developers page (see instructions below).
- The Portal Configuration must have Salesforce Registration enabled and include the Salesforce Application ID and Secret (see instructions below).

Creating a Salesforce Application

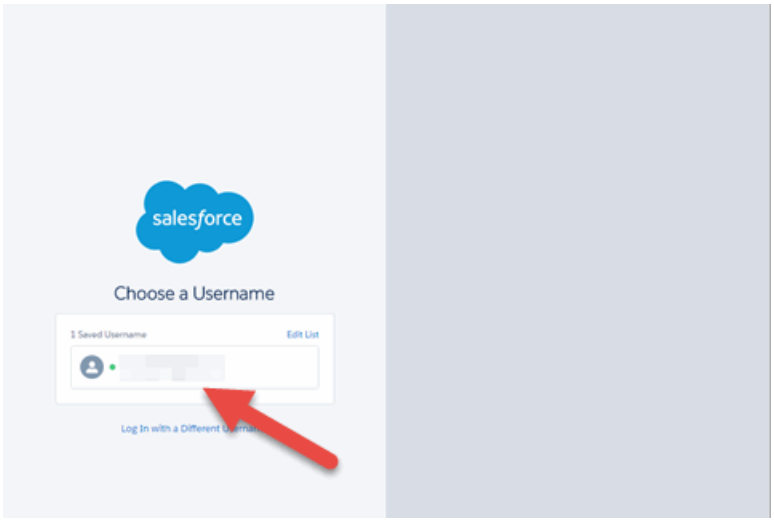
When implementing guest registration using Salesforce, you must first create a Salesforce application. This generates an Application ID and Application Secret that are required as part of the Extreme Management Center OpenID process. Use the following steps to create a Salesforce application.

1. Access the Salesforce Developers page at https://developer.salesforce.com/signup.
2. Log into your existing Developers account or create a new Developers account.
3. Click the My Developer Account button from the profile drop-down menu.



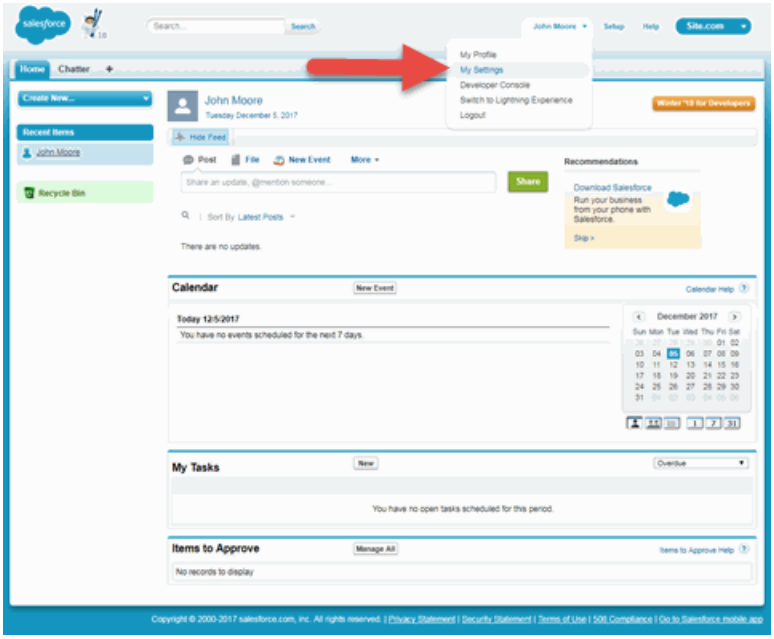
The Developer Account login window opens.

4. Click your account.



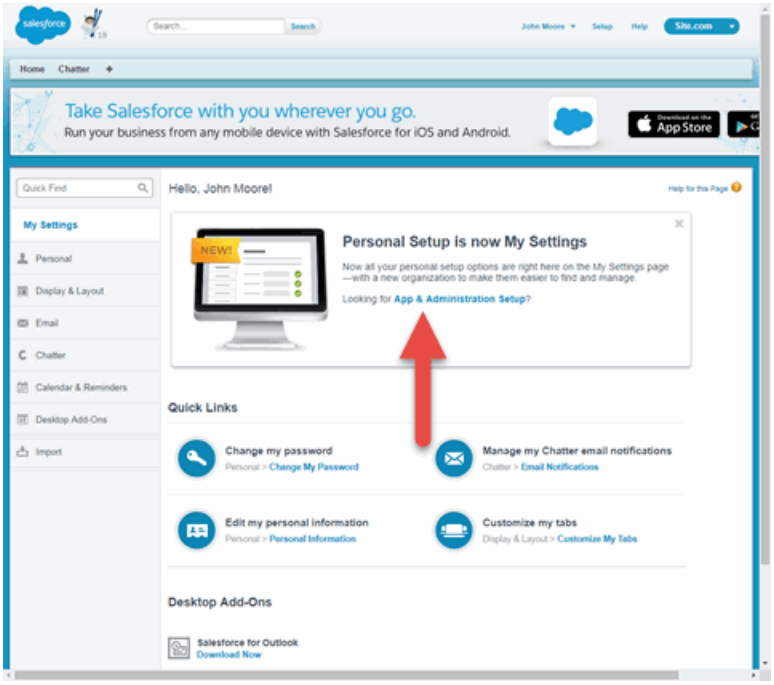
The **Developer Home** window opens.

5. Select **My Settings** from the Profile drop-down menu.



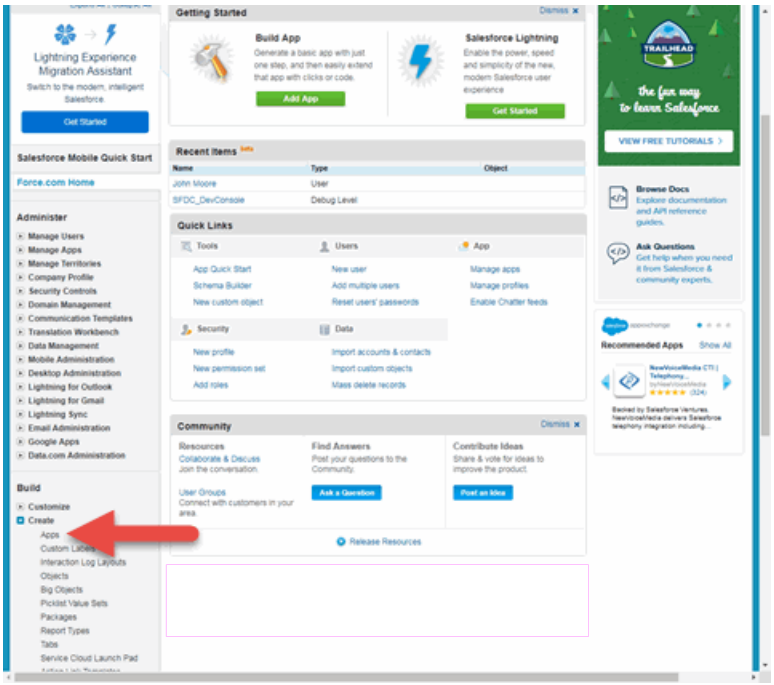
The **My Settings** window opens.

6. Click **App & Administration Setup**.



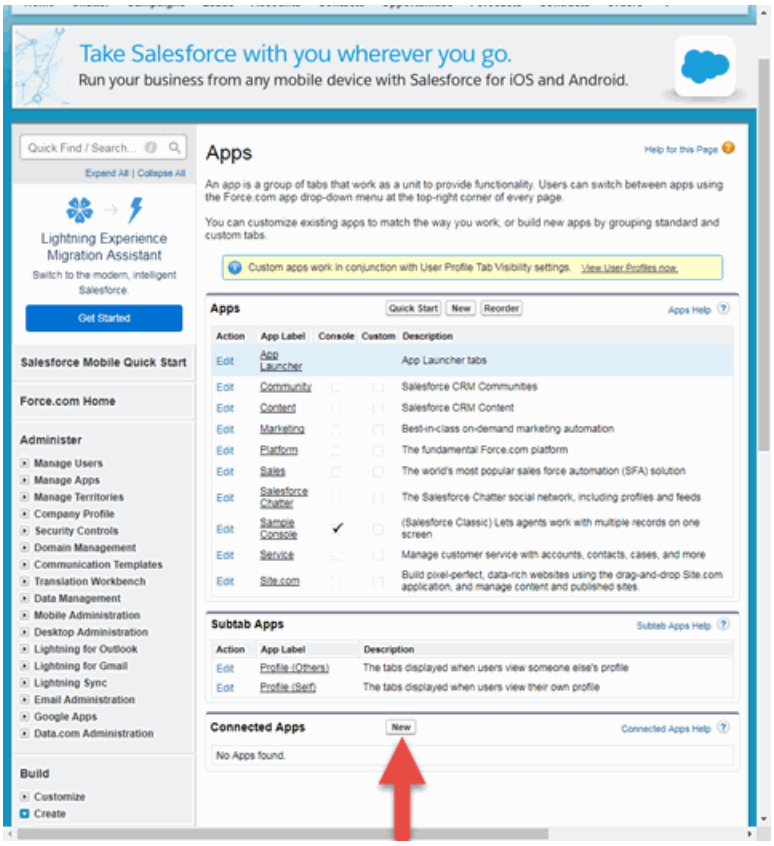
The App & Administration Setup window opens.

7. Click Apps from within the Build > Create menu.



The Apps window opens.

8. Click the **New** button in the Connected Apps section.



The New Connected App window opens.

9. Enter a **Connected App Name**, **API Name**, **Contact Email**, and select the **Enable OAuth Settings** checkbox.

   The API (Enable OAuth Settings) section of the window expands to display additional fields.

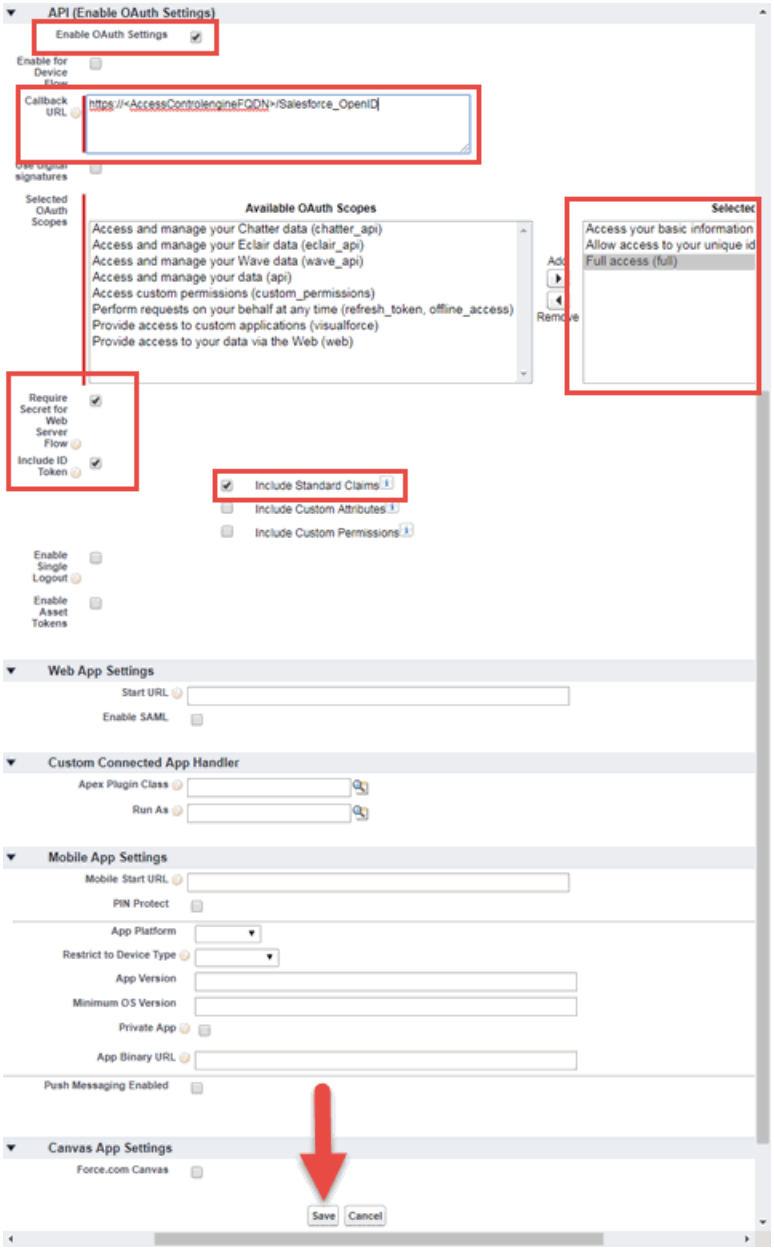
10. Select **Enable OAuth Settings**.

11. Enter a **Callback URL** in the following format `https://<AccessControlengineFQDN>/Salesforce_oauth`. Salesforce uses the **Authorized redirect URI** to redirect the user back to the engine with an Access Token.

NOTES: Salesforce OpenID APIs require your engine's FQDN resolves to a top level domain (.com, .net, .edu, .org, .mil, .gov, or .int. You cannot use a domain not classified as top level (e.g. MyGateway.MyCompany.Local) or the engines IP address, which may require you to reclassify your domain and hosts.

Use only lowercase when entering the host and domain suffix (e.g. .com).

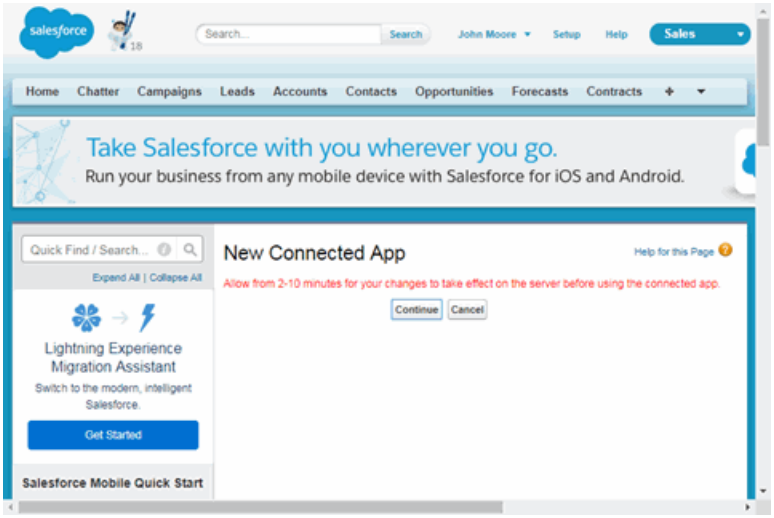
12. Select Access your basic information (id, profile, email, address, phone), Full access (full), and Allow access to your unique identifier (openid), then click the Add icon in the Selected OAuth Scopes section of the window to add the scopes to the Selected OAuth Scopes list.
13. Select the Require Secret for Web Server Flow, Include ID Token and Include Standard Claims checkboxes.



14. Click **Save**.

    Your application is created and ready to use.

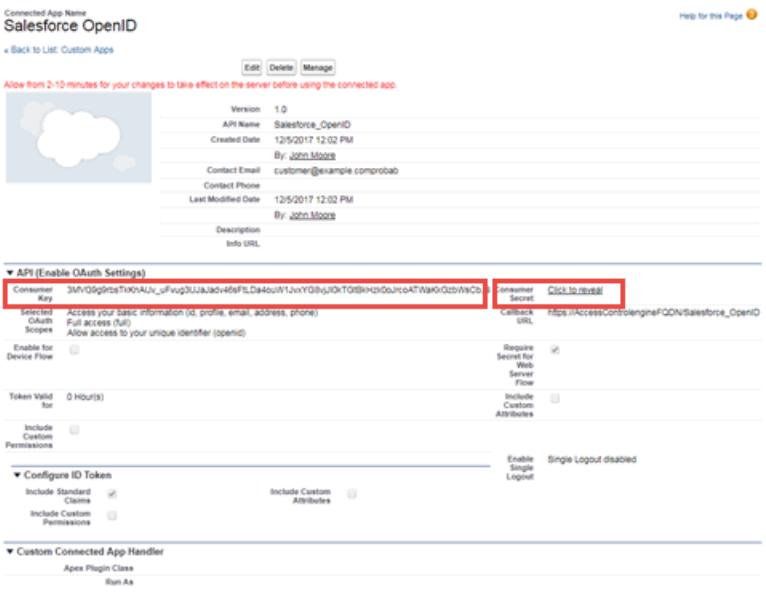
    The **New Connected App** window opens.



15. Click **Continue**.

    The **Connected App** window opens.

16. Click the **Click to reveal** link in the **Consumer Secret** field and copy the **Consumer Secret** and **Consumer Key**.

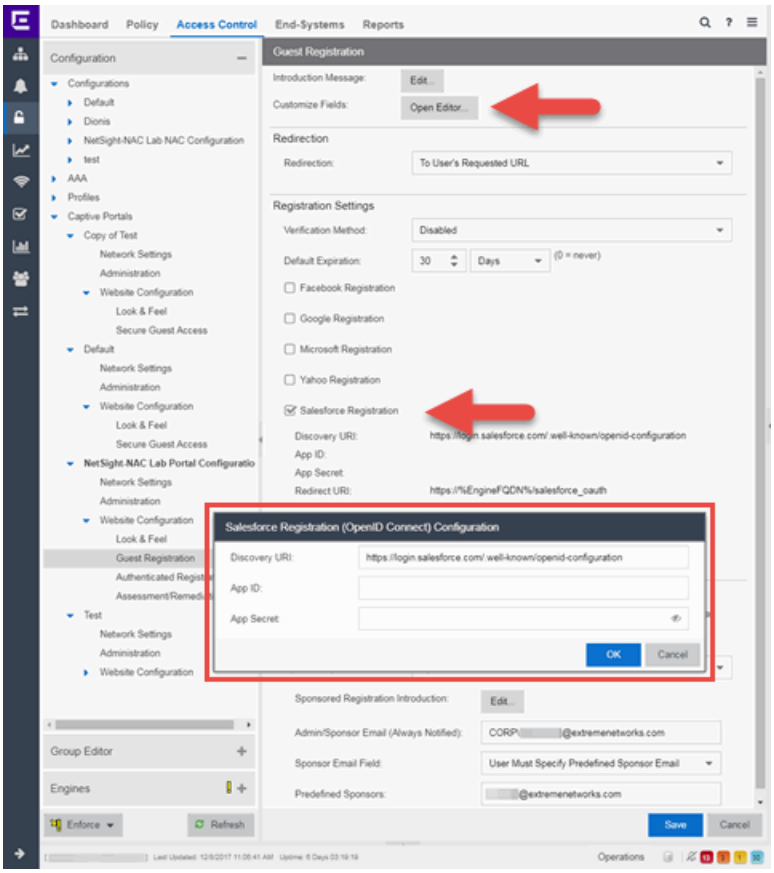


You need to add the Consumer Key and Consumer Secret to your portal configuration.

Portal Configuration

The client ID and client secret assigned during the creation of the Salesforce application must be provided in the Portal Configuration in order for the entire process to complete properly.

1. Open the **Control** > **Access Control** tab.
2. In the left-panel tree, expand the Extreme Access Control Configurations > Portal tree and select Guest Registration.



3. In the Customize Fields section, click the **Open Editor** button to open the Manage Custom Fields window where you can change registration portal fields. Salesforce registration uses only the First Name, Last Name, and Email Address fields, and the Display Acceptable Use Policy (AUP) option. All other fields only apply to regular guest registration. If the Display AUP option is selected, the captive portal verifies that the AUP has been acknowledged before redirecting the user to Salesforce.
4. Select the **Salesforce Registration** checkbox.

5. Enter the Consumer Key in the App ID field and the Consumer Secret in the App Secret field.
6. Click Save. Warning messages display stating that Verification Method and Sponsorship are not used for Salesforce registration, and that an FDQN is required will be enabled.
7. Enforce the new configuration to your engines.

How Salesforce Registration Works

Once you have configured Salesforce registration using the steps above, this is how the registration process works:

1. The end user attempts to access an external Web site. Their HTTP traffic is redirected to the captive portal.
2. In the Guest Registration Portal, the end user selects the option to register using Salesforce.
3. The end user is redirected to the Salesforce login. If Acceptable Use Policy option is configured, the captive portal verifies that the AUP has been acknowledged before redirecting the user to Salesforce.
4. Once logged in, the end user is presented with the information that Extreme Management Center receives from Salesforce.
5. The end user grants Extreme Management Center access to the Salesforce information and is redirected back to the captive portal where they see a "Registration in Progress" message.
6. Salesforce provides the requested information to Extreme Management Center, which uses it to populate the user registration fields.
7. The registration process completes and network access is granted.
8. The word "Salesforce" is added to the user name so you can easily search for Salesforce registration via the Registration Administration web page.

Special Deployment Considerations

Please read through the following deployment consideration prior to configuring Salesforce Registration.

To allow traffic to your network via a wireless connection, create an L7 host record for the Unregistered Role on your Wireless Controller for `login.Salesforce.com`.

Networks using DNS Proxy

Salesforce Registration for networks redirecting HTTP traffic to the captive portal using DNS Proxy requires additional configuration.

In order for Salesforce Registration to work properly with DNS Proxy, all domains/URLs necessary to properly load the Salesforce web page must be added to the Allowed URLs/Allowed Domains section of the captive portal configuration. Otherwise, the Extreme Access Control engine resolves DNS queries for these components to the Extreme Access Control engine IP causing the page to not load properly.

As of February 2017, you must add the following domains in order for Salesforce registration to work with DNS Proxy. These domains are subject to change and may vary based on location.

login.Salesforce.com

Related Information

- Portal Configuration

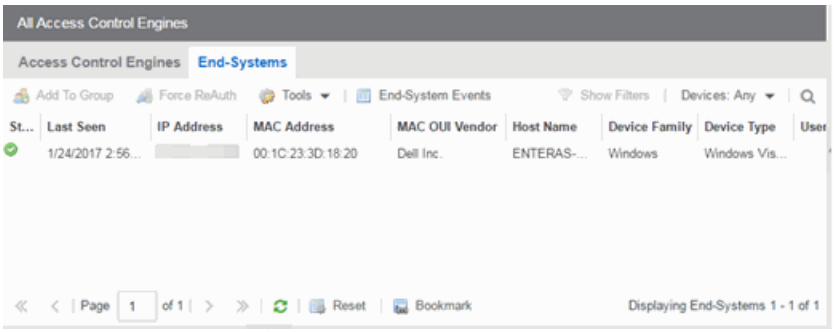
End-Systems

The End-Systems tab presents end-system connection information for a single Extreme Access Control engine, all Extreme Access Control engines, or all the engines in an engine group, depending on what you select in the left-panel tree. You can also monitor end-system events and view the health results from an end-system's assessment.

The End-Systems tab is the first tab displayed when accessing the Control > Access Control tab. A high-level overview of the functionality found in the Extreme Access Control tab is also available.

To access this tab, select a single Extreme Access Control engine, the All Extreme Access Control Engines folder, or an engine group in the left-panel tree, then click the **End-Systems** tab in the right panel.

Use the table options and tools to filter, sort, and customize table settings. Access the options by clicking the down arrow in the right corner of any column header.



End-Systems

This table displays the last known connection state for each end-system that has attempted connection.

State

The end-system's connection state:

- Scan — The end-system is currently being scanned.
- Accept — The end-system is granted access with either the Accept policy or the attributes returned from the RADIUS server.
- Quarantine — The end-system is quarantined because the assessment failed.
- Reject — The end-system was rejected because the assigned Extreme Access Control profile was set to Reject, the MAC Locking test failed, or the RADIUS server was reachable but rejected the authentication request.
- Disconnected — All sessions for the end-system are disconnected. This state is only applicable for end-systems connected to switches that have RADIUS accounting enabled.
- Error — Indicates one of nine problems:
  - the MAC to IP resolution failed, if assessment is enabled
  - the MAC to IP resolution timed out, if assessment is enabled
  - all RADIUS servers are unreachable

- the RADIUS request was non-compliant
- all assessment servers are unavailable
- the assessment server can't reach the end-system
- no assessment servers are configured
- the assessment server is not compatible with the current version of Extreme Access Control
- the username and password configured in the Assessment Server panel of the Extreme Access Control options (Administration > Options > Extreme Access Control > Assessment Server) are incorrect for the assessment server.

MAC Address

The end-system's MAC address. MAC addresses can be displayed as a full MAC address or with a MAC OUI (Organizational Unique Identifier) prefix.

MAC OUI Vendor

The vendor associated with the MAC OUI.

IP Address

The end-system's IP address.

Switch IP

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

Switch Port

The port alias (if defined) followed by the switch port number to which the end-system connected. If the end-system is connected to a Layer 2 Extreme Access ControlController engine, this is the Extreme Access Control Controller PEP (Policy Enforcement Point) port. However, for Layer 3 Extreme Access Control Controller engines this column is blank.

If you add or update the port alias on the switch, you must enforce the Extreme Access Control engine in order for the new information to be displayed in the End-Systems table.

If you don't want the port alias displayed, remove the PORT_DESCRIPTION_FORMAT variable from the /opt/nac/server/config/config.properties file. If this variable is removed, only the switch port number is displayed.

Username
The username used to connect.

Hostname
The end-system's hostname.

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

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

Authentication Type
Identifies the latest authentication method used by the end-system to connect to the network. (For Layer 3 Extreme Access Control Controller engines, this column displays "IP.")

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 Extreme Access Control Controller engines, this column displays the policy assigned to the end-system for its authorization.

Profile
The name of the Extreme Access Control profile that was assigned to the end-system when it connected to the network.

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

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

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.

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

State Description
This column provides more details about the end-system state.

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

First Seen
The first time the end-system was seen by the Extreme Access Control engine.

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

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

Extreme Access Control Engines/Source IP
The Extreme Access Control engine to which the end-system is connecting.

Engine Group
This column is only displayed if you have multiple engine groups. It displays what engine group the Extreme Access Control engine was in when the end-system event was generated. For example, if the engine was in Engine Group A when an end-system connected, but then later the engine was moved to Engine Group B, this column would still list Engine Group A for that end-system's entry.

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

All Authentication Types
This column displays all the authentication methods the end-system has used to authenticate. The authentication types are listed in order of precedence from highest to lowest: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking. View details about each authentication session (such as the Extreme Access Control profile that was assigned to the end-system for each authentication type) in the End-System Events tab.

RFC3580 VLAN

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

Score

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

Top Score

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

Actual Score

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

Custom 1

Use this column to add additional information you want to display. To add or edit custom information, right-click on the table and select Edit Custom Information. You can add information for up to four Custom columns. The columns for Custom 2, Custom 3, and Custom 4 are hidden by default. To display these columns, click the down arrow to the right of the table header and select Columns > Column 2, Column 3, or Column 4.

Groups

Displays any end-system and/or user groups to which the end-system belongs.

Zone

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

Actions

TIP: These actions are also available from the right-click menu off an end-system entry in the table.

Force Reauth

Forces the selected end-system to re-authenticate. End-systems authenticated to a VPN device are disconnected from the VPN.

Force Reauth and Scan

Forces the selected end-system to re-authenticate and undergo an assessment (scan). (End-systems authenticated to a VPN device are disconnected from the VPN.) The assessment only takes place if scanning is enabled in the Extreme Access Control profile assigned to the end-system.

Add to Group

Lets you add the selected end-system to a specific end-system or user group. If the end-system is a registered device, it can be added to a registration group. After adding an end-system to a group, any rules created that involved that group apply to the end-system as well. Changes to end-system group membership do not require an enforce and are synchronized with engines immediately. Changes do not affect the end-system until the next authentication or assessment occurs.

Lock MAC

Opens the Add MAC Lock window where you can lock the MAC address of the selected end-system to a switch or switch and port.

Show Details

Opens the End-System Details tab where you can view summary information for the end-system selected in the table.

Delete

Deletes the selected end-system entries from the table and also deletes the associated end-system events. You are given the option to delete any custom information, group assignment, MAC locks, and registration and web authentication associated with the end-systems.

The Force Delete of End-System option completely deletes the end-system from Extreme Management Center, regardless of whether the end-system reauthentication is successful when the delete is executed. The option is deselected by default. When deselected, it prevents possible synchronization conditions where the authentication session remains active on the switch even though the end-system has been deleted from Extreme Management Center. These conditions can occur when there are underlying issues that prevent the end-system reauthentication from completing properly.

NOTES: The Delete operation does not remove an end-system from the Blacklist group. Blacklist is a special group that requires end-systems to be manually removed using the Edit End-System Group window.

Deleting an end-system from the table also deletes the user's current authentication. If the user is connected to the network at the time of the delete, they are forced to re-authenticate.

Menu Buttons

The menu at the top of the window contains most of the options available via a right-click previously mentioned in the Actions section above, as well as the End-System Events button, described below.

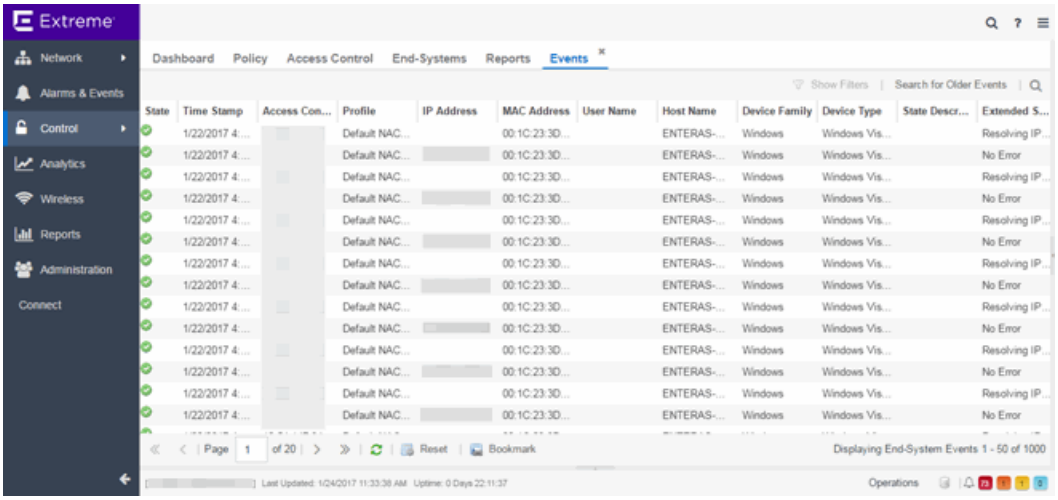
End-System Events

Opens the End-System Events tab where you can view information about events for the end-system selected in the table.

End-System Events Tab

This tab displays historical connection information for the end-system selected in the table above. End-system events are stored daily in the database. In addition, the end-system event cache stores in memory the most recent end-system events and displays them here in this tab. This cache allows Extreme Management Center to quickly retrieve and display end-system events without having to search through the database. You can configure parameters for the event cache (such as the number of events to display) using the End-System Event Cache options in the Extreme Access Control Options view (Administration > Options > Extreme Access Control > End-Systems Event Cache).

NOTE: The End-System Events tab displays events up to the most recent delete event for the end-system, if one exists. If you want to see events that happened prior to the most recent delete event, use the Search for Older Events button.



State

The end-system's connection state:

- Scan — The end-system was scanned.
- Accept — The end-system was granted access with either the Accept policy or the attributes returned from the RADIUS server.
- Quarantine —The end-system was quarantined because the assessment failed.
- Reject — The end-system was rejected because the assigned Extreme Access Control profile was set to Reject, the MAC Locking test failed, or the RADIUS server was reachable but rejected the authentication request.
- Disconnected — This end-system session was disconnected, however other sessions for the end-system may still be active. For example, the end-system may have a disconnected session with an authentication type of 802.1X, but still have an active MAC authentication session. This state is only applicable for end-systems connected to switches that have RADIUS accounting enabled.
- Error — Indicates one of nine problems:
  - the MAC to IP resolution failed
  - the MAC to IP resolution timed out
  - all RADIUS servers are unreachable
  - the RADIUS request was non-compliant
  - all assessment servers are unavailable
  - the assessment server can't reach the end-system
  - no assessment servers are configured
  - the assessment server is not compatible with the current version of Extreme Management Center
  - the username and password configured in the Assessment Server panel of the Extreme Access Control options (Administration > Options > Extreme Access Control > Assessment Server) are incorrect for the assessment server

Time Stamp

The date and time the end-system connected.

IP Address

The end-system's IP address.

Switch IP

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

Switch Nickname

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

Switch Port

The switch port number to which the end-system is connected. If the end-system is connected to a Layer 2 Extreme Access Control Controller engine, this is the Extreme Access Control Controller PEP (Policy Enforcement Point) port. However, for Layer 3 Extreme Access Control Controller engines this column is blank.

Username

The username used to connect.

Hostname

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.

Authentication Type

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

Authorization

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

Profile

The name of the Extreme Access Control 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 provides information as to the reason a policy is applied to the end-system or the reason the end-system is rejected.

Extended State

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

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.

Switch Location

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

Engine Group

This column is only displayed if you have multiple engine groups. It displays what engine group the Extreme Access Control engine is in when the end-system event was generated. For example, if the engine began in Engine Group A when an end-system connected, then the engine is moved to Engine Group B, this column still lists Engine Group A for that end-system's entry.

Zone

Displays the end-system zone to which the end-system is assigned. For additional information, see End-System Zones.

Search for Older Events

This button lets you search for older events stored in the database outside of the end-system events cache. The maximum search parameters for this extended search are configured in the End-System Event Cache options in the Extreme Access Control Options view (Administration > Options > Extreme Access Control > End-System Event Cache). The search is ended when any one of the parameters is reached.

- Maximum number of results to return from search
- Maximum time to spend searching for events (in seconds)
- Maximum number of days to go back when searching

Related Information

For information on related topics:

- Add MAC Lock Window
- End-System Details Tab

Add/Edit MAC Lock

Use this window to add a new locked MAC address or edit the settings for an existing locked MAC address. MAC Locking lets you lock a MAC address to a specific switch or port on a switch so that the end-system can only access the network from that port or switch. If the end-system tries to authenticate on a different switch/port, it is rejected or assigned a specific policy. You can add or edit MAC locks from the End-Systems tab.

NOTE: MAC Locking to a specific port on a switch is based on the port interface name (e.g. fe.5.1). If a switch board is moved to a different slot in a chassis, or if a stack reorders itself, this name changes and breaks the MAC Locking settings.

MAC Address

Enter the MAC address that you want to lock.

Switch IP

Enter the IP address of the switch on which you want to lock the MAC address.

Lock to Switch and Port

Select this checkbox if you want to lock the MAC address to a specific port on the switch, and enter the port interface name.

Failed Action

Select the action to take when this MAC address tries to authenticate on a different port and/or switch:

- Reject - The authentication request is rejected.
- Use Policy - Use the drop-down list to select the policy that you want applied. This policy must exist in the **Policy** tab and be enforced to the switches in your network.

Related Information

For information on related windows:

- End-Systems Tab

ExtremeAnalytics Overview

The Analytics tab allows you to view and customize its dashboard and browser, as well as ExtremeAnalytics reports, fingerprints, and application flow data. You can also manage and configure your Application Analytics engines.

Additionally, the Menu icon (☰) at the top right of the screen provides links to additional information about your version of Extreme Management Center.

NOTE: ExtremeAnalytics reports and application flow data is not available unless an Application Analytics engine is configured and you are a member of an authorization group assigned the Extreme Management Center ExtremeAnalytics Read Access or Read/Write Access capability. The Read Access capability allows the ability to access the Analytics tab and view the ExtremeAnalytics reports. The Read/Write capability adds the ability to configure Application Analytics engines and NetFlow Collecting devices. It also adds the ability to create and modify fingerprints.

Viewing ExtremeAnalytics application data requires certain access requirements and prerequisites. Both the ExtremeAnalytics feature and the Analytics tab require the Extreme Management Center Advanced (NMS-ADV) license. Contact your sales representative for information on obtaining an Extreme Management Center Advanced license.

Dashboard

The Dashboard tab displays an overview of application usage on your network through a series of graphs. It allows you to view network activity statistics based on client/server, application, industry, IP reputation, and response time for the specified Application Analytics engine. Many of the reports are links to more detailed pages.

Browser

The Browser tab lets you query information about recent network activity stored in the Extreme Management Center database and display results in various grid and chart report formats. Using the Browser, you can create custom queries

based on selected options including a data target, statistic type, and other search criteria.

Application Flows

You can choose from the View drop down menu to show you several options in the Application Flows table, including the latest flows from the specified Application Analytics engine, the worst network and application response times, classified and unclassified flows, and flows during a specified time frame. The table presents bidirectional flow data (aggregate flows) or unidirectional flow data (base flows).

Fingerprints

A fingerprint is a description of a pattern of network traffic which can be used to identify an application. The Fingerprints view provides detailed information about fingerprints used by ExtremeAnalytics to identify application flows. You can choose to view in-use and customized fingerprint data.

Configuration

The Configuration view provides detailed information on the Application Analytics engines you configure. It also lets you add and enforce your engines, access engine reports and diagnostics, and configure network locations. You must be a member of an authorization group assigned the Extreme Management Center Application Analytics Read/Write Access capability to view the Configuration tab.

Reports

In the Reports tab, you can access a selection of reports that provide detailed information on application usage on your network, as well as network activity statistics based on application, user name, client, and location. For many of the reports, you can click on an item in the report to view details or right-click an item to select from other focused reports.

Related Information

- Dashboard View Overview
- Browser View
- Application Flows View
- Fingerprints View
- Configuration View
- Reports View

ExtremeAnalytics Licensing

ExtremeAnalytics licensing allows deployment flexibility by granting flow rate and flow client capacity to an entire deployment, regardless of the number of Application Analytics engines. The NMS Advanced license (NMS-ADV) grants a basic flow rate and flow client capacity. Additional ExtremeAnalytics licenses can then be added to extend that capacity, if needed.

The table below shows the different ExtremeAnalytics licenses, and the flow rate capacity and flow client capacity granted by that license. The flow rate capacity is the number of flows per minute (FPM) that can be processed across all Application Analytics engines with a maximum of 3,000,000 FPM. The flow client capacity is the total number of application flow clients that can be reported system-wide.

License Name	Flow Rate Capacity	Flow Client Capacity
NMS-ADV-XXX	3,000 FPM	100 clients
PV-FPM-50K	50,000 FPM	Unlimited clients
PV-FPM-100K	100,000 FPM	Unlimited clients
PV-FPM-500K	500,000 FPM	Unlimited clients
PV-FPM-1M	1,000,000 FPM	Unlimited clients
PV-FPM-3M	3,000,000 FPM	Unlimited clients

ExtremeAnalytics licensing is enforced through Extreme Management Center. The capacity allowed by each license is applied to the entire deployment and is calculated by adding together the usage numbers for each individual Application Analytics engine in the deployment. The capacity is checked on a continual basis. If the flow rate capacity is exceeded, an event is logged in the ExtremeAnalytics event log and a notification is displayed at the bottom of the Extreme Management Center screen. If the flow client capacity is exceeded when using an NMS-ADV license, the client data for the clients beyond the capacity is not persisted.

NOTE: The **Max End-Systems** field in the Application Analytics Engine Advanced Configuration panel allows you to limit the clients from a single Application Analytics engine persisted in the Extreme Management Center database. This limits the amount of data stored on one engine.

Using Licenses to Establish Flow Rate Capacity

The following example shows how you can select ExtremeAnalytics licenses to achieve a desired flow rate capacity for your deployment.

The NMS-ADV license provides a basic flow rate capacity of 3,000 flows per minute. If you add additional ExtremeAnalytics licenses, the flow rate capacity is increased by the amount provided by the added licenses, up to the system-wide maximum of 3 million flows per minute.

For example, if you add the PV-FPM-100K license, then you would have a total flow rate capacity of 103,000.

3,000 + 100,000 = 103,000 FPM

If you then add the PV-FPM-50K license, you would have a total flow rate capacity of 153,000.

3,000 + 100,000 + 50,000 = 153,000 FPM

Getting Started with ExtremeAnalytics

This topic provides information to help you get started using Extreme Management Center Application Analytics to view network application data in the Analytics tab. It includes information on Application Analytics access requirements, configuring the Application Analytics engine, enabling NetFlow flow collection, and configuring network locations.

ExtremeAnalytics Access Requirements

Both the ExtremeAnalytics feature and the Analytics tab require the Extreme Management Center Advanced (NMS-ADV) license. Contact your sales representative for information on obtaining an Extreme Management Center Advanced license.

In order to view the Analytics tab, you must be a member of an authorization group assigned the Extreme Management Center Application Analytics Read Access or Read/Write Access capability. The Read Access capability allows the ability to access the Analytics tab and view the Application Analytics reports.

The Read/Write capability adds the ability to configure Application Analytics engines and NetFlow Collecting devices. It also adds the ability to create and modify fingerprints.

Application Analytics Engine Configuration

The Application Analytics engine provides the engine to monitor and classify layer 7 application information based on data from CoreFlow switches and reports that information to Extreme Management Center, where it is managed and displayed in the Analytics tab.

The Application Analytics engine must be installed and running on your network. For instructions, see the Application Analytics Engine Installation Guide.

Following installation, the Application Analytics engine must be added to Extreme Management Center and enforced via the Configuration tab in the Analytics tab.

Enable Flow Collection

Because the Analytics tab displays reports based on NetFlow or Application Telemetry (sflow) flow data, you must enable your network devices that act as the flow sensors, and enable flow collection for their device interfaces. You must also configure your flow sensor devices to send their flow information to the Application Analytics engine. In addition, the device interfaces you enable for flow collection must match the interfaces configured for analysis by the engine.

Configure Network Locations

In order to take full advantage of the reporting features in Application Analytics, it is recommended that you configure network locations. Defining network locations will provide additional client flow data in your Application Analytics reports as well as increase your options when specifying report search criteria.

A network location is a set of IP address ranges that identify a portion of your network. You can create a single network location that identifies which IP address ranges belong to the resources in your network or you can create multiple locations to identify different buildings, sites, or geographical areas of

your network. Application Analytics uses the defined network locations to identify the portion of the network where the application flow client resides.

Related Information

- Configuration - Analytics
- Network Locations

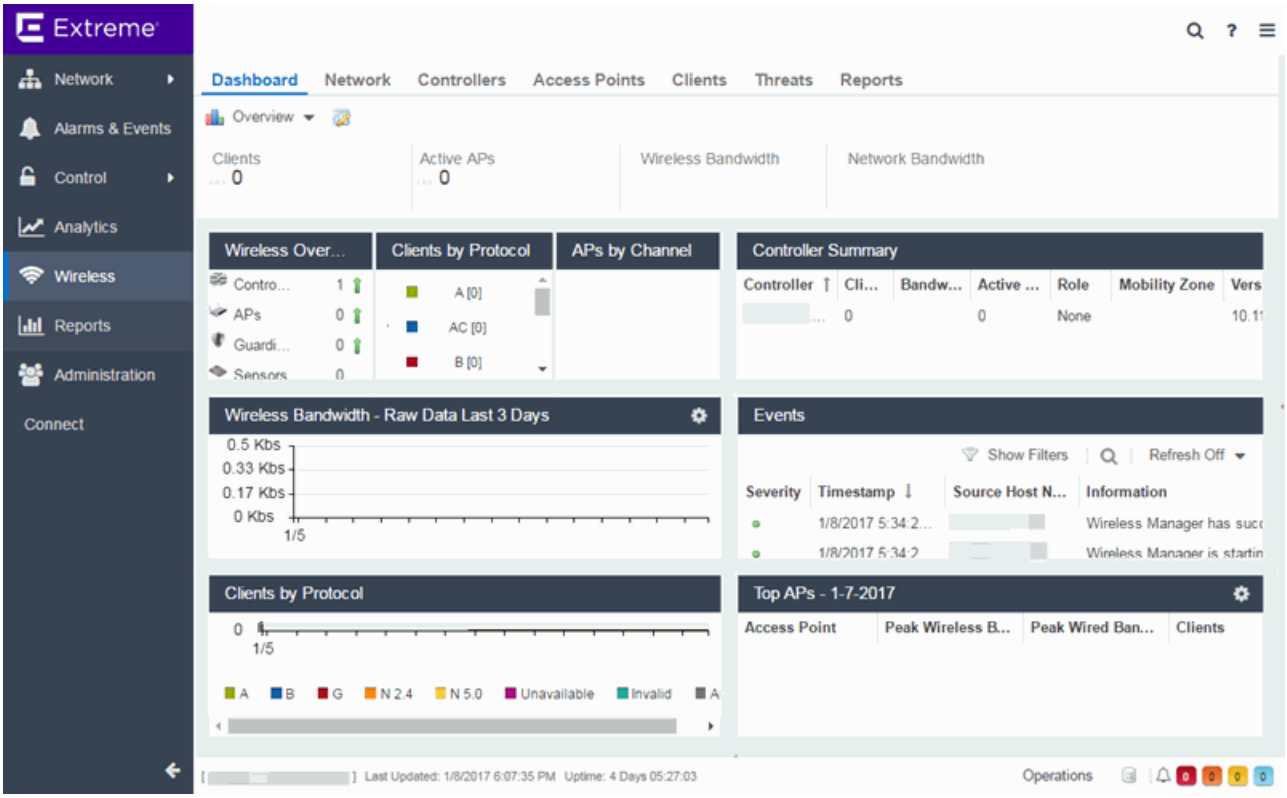
Configuring Enhanced Netflow for Extreme Analytics and Extreme Wireless Controller Version 10.21

When adding a Wireless Controller as a flow source in Extreme Management Center, 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.

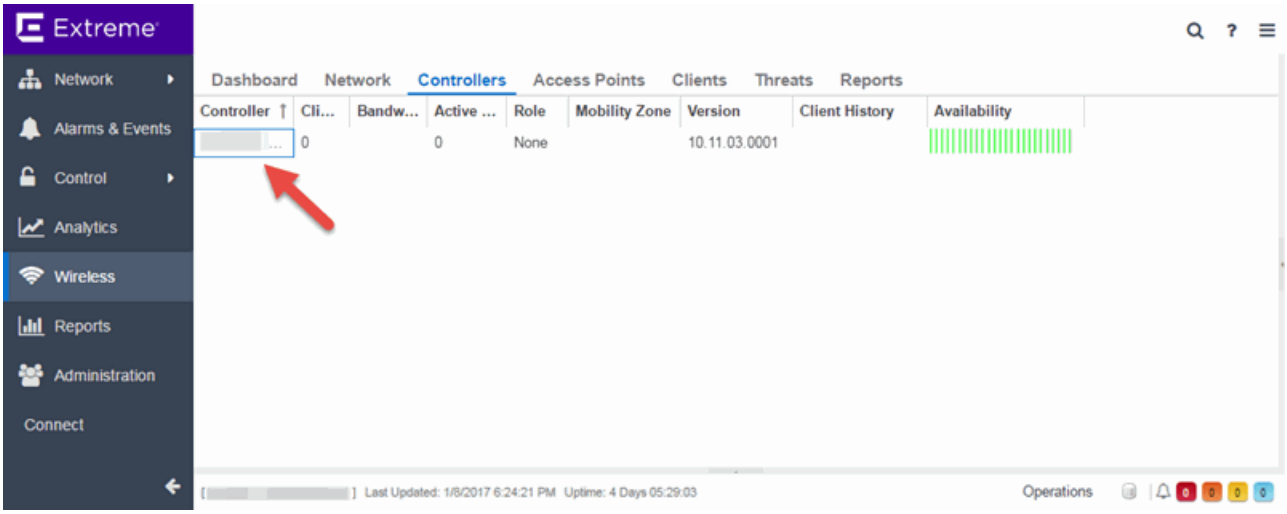
NOTE: Wireless Controllers on which a firmware version lower than 10.21 is installed still require the mirror port be configured.

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

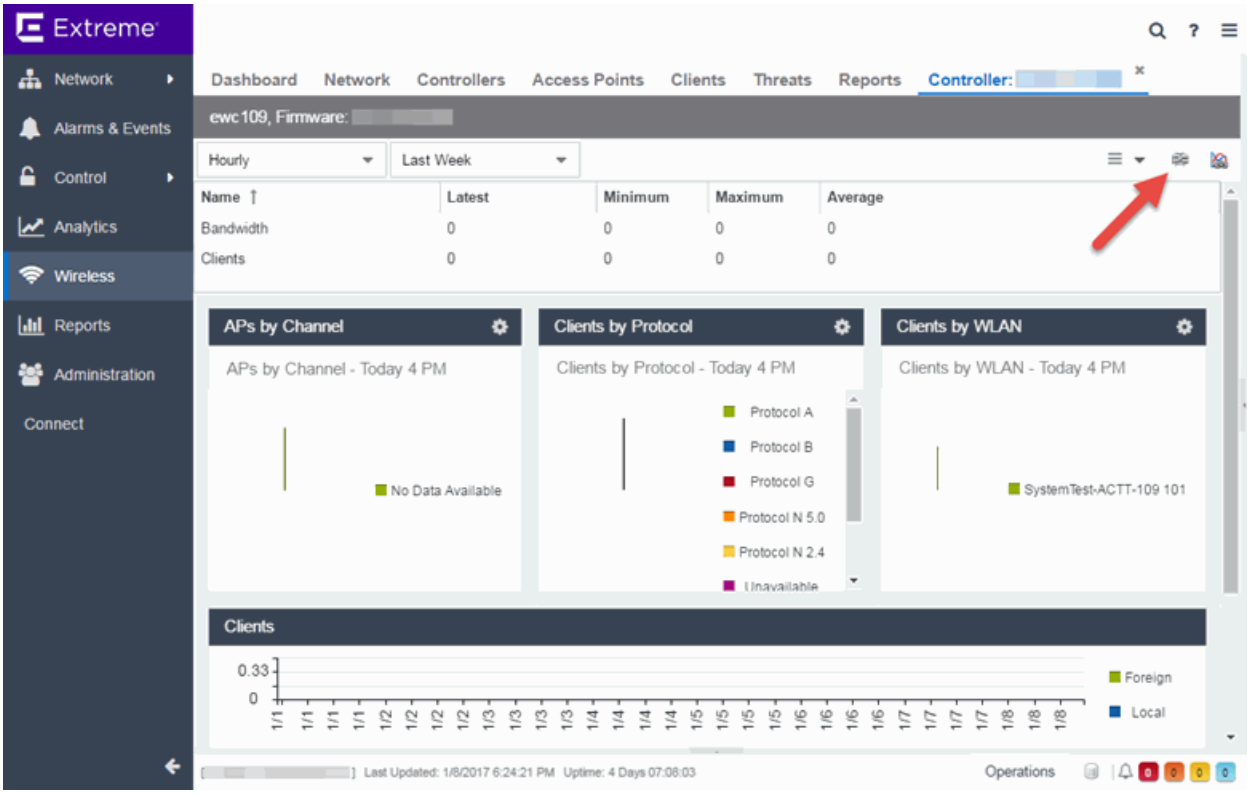
1. Access the **Wireless** tab in Extreme Management Center.
   The Wireless tab opens.



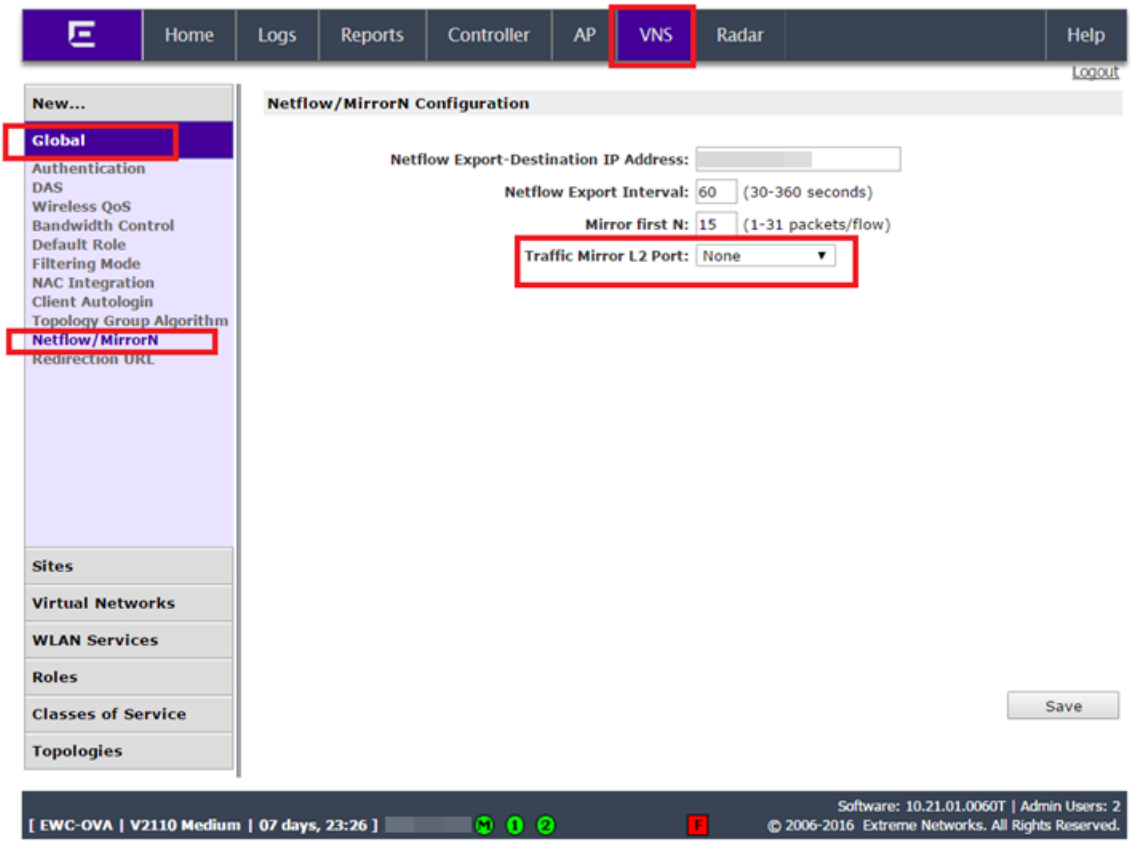
2. Select the **Controllers** tab.
   The Controllers tab opens.



3. Click the **IP address** for the controller, located in the **Controller** column.
   The Wireless Controller Summary page opens.



4. Click the **WebView** icon ( ) at the top right of the Wireless Controller Summary page.
   The WebView opens for the controller.
5. Click the **VNS** tab.
   The **VNS** tab opens.

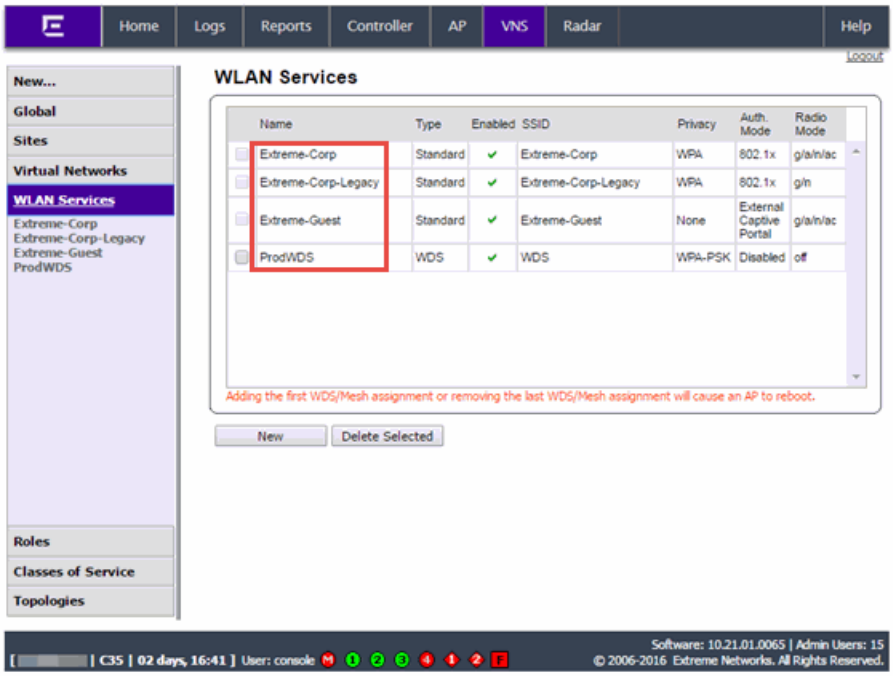


6. Select **Netflow/MirrorN** from the left-panel.
   The Netflow/MirrorN Configuration page opens.
7. Select **None** from the **Traffic Mirror L2 Port** drop-down menu.
8. Click the **Save** button.

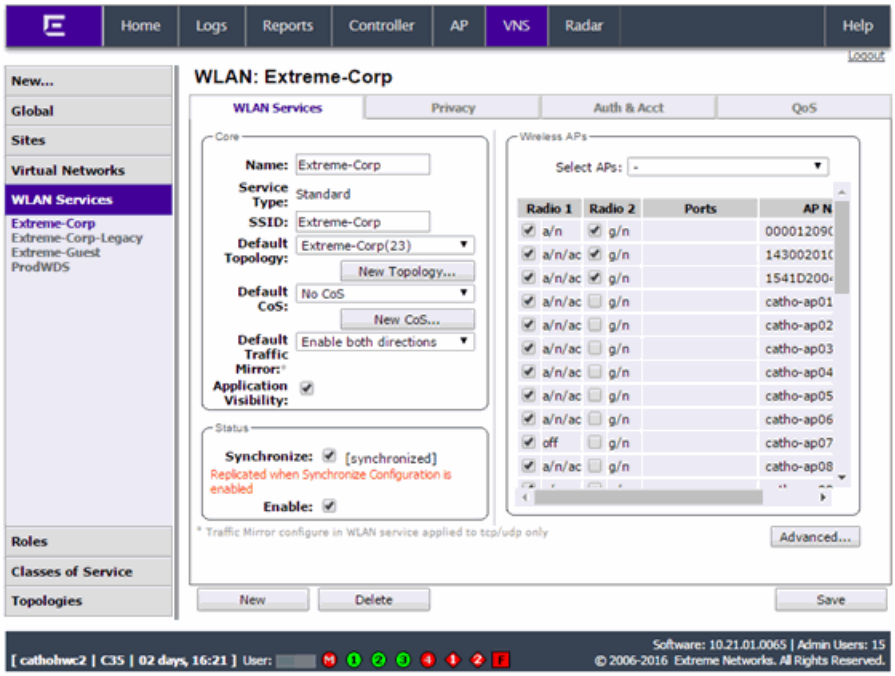
NOTE: The Mirror Port in the Wireless Control Flow Sources section of the **Analytics** > **Configuration** > **Configuration** tab is not available once the **Traffic Mirror L2 Port** is disabled.

---

9. Select **WLAN Services** from the left-panel.
   The WLAN Services page opens.

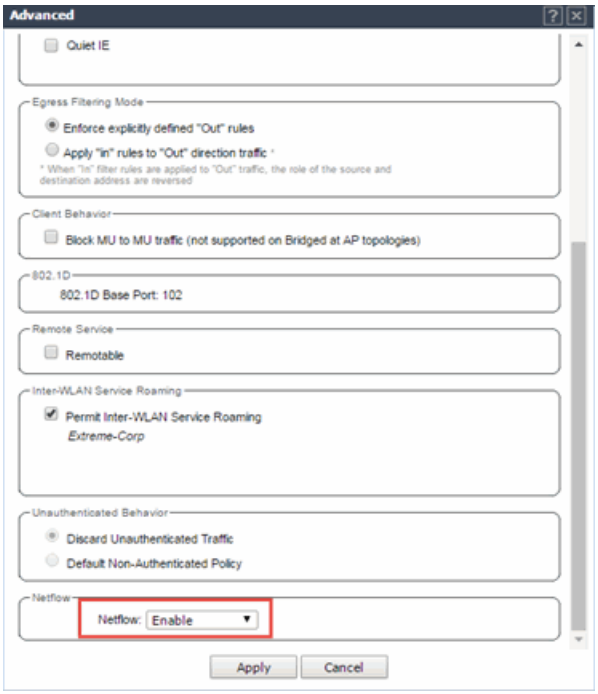


10. Click a wireless LAN in the table.
    The WLAN page opens for the selected wireless LAN.



11. Click the **Advanced** button.
    The **Advanced** window opens.

12. Scroll to the bottom of the window and ensure the **Netflow** drop-down menu is set to **Enable**.



13. Click the **Apply** button.

The wireless controller is now configured.

NOTE: **Rx Packets** and **Rx Bytes** may 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 may be blank. This is a known issue and will be addressed in a future release.

Related Information

For information on related topics:

- Wireless

Network Locations

In order to take full advantage of the reporting features in ExtremeAnalytics, you must first configure network locations. Defining network locations identify IP ranges for certain end-systems in your network, provides client flow data in your ExtremeAnalytics reports, and provides additional options for working with report search criteria. Locations can be imported or exported as a CSV formatted file. Additionally, configuring the location of your Application Analytics engine provides ExtremeAnalytics with improved flow data.

Configuring network locations is useful if you have already reserved certain IP address ranges for certain physical locations on your network. Create network locations that correspond to these reserved IP ranges. The network locations are then used to identify the portion of the network where the application flow source resides by matching the client's IP address to the ranges included in each network location. Create multiple locations to identify different buildings, sites, or geographical areas of your network. Even if you have no such policies, you can create a single network location that identifies which IP address ranges belong to resources in your network.

A location is defined with a name, description, and one or more IP address ranges specified by an IP address/mask. When a client's IP address matches any IP address/mask in a location, the client is determined to have that location. If the client matches the address/mask of several locations, the location with the most specific mask (the highest CIDR value) is used.

The name of the network location that matches the client's IP address is listed in the Location column of the Application Flows table in the Analytics tab. This allows you to search, sort, and filter flow data according to location. ExtremeAnalytics uses this data to provide a summary of the data for locations, which can be viewed as either an hourly or high-rate report in the Analytics Browser.

You must be a member of an authorization group that has been assigned the Extreme Management Center ExtremeAnalytics Read/Write Access capability in order to manage network locations. For additional information, see Getting Started with Application Analytics.

This Help topic provides the following information about managing Extreme Management Center network locations:

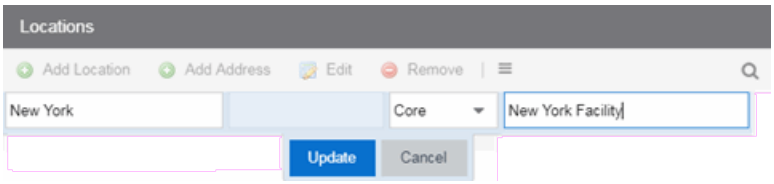
Managing Locations

Locations are created and managed in the Configuration view of the **Analytics** tab.

Adding Locations

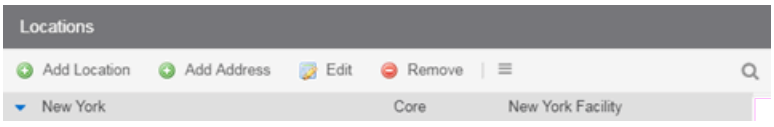
To add a location:

1. Access the **Analytics** tab and select the **Configuration** tab.
2. In the left-panel tree, select **Locations**.
3. In the right-panel **Locations** tab, click the **Add Location** button and enter a name for the new location in the first text box. If desired, enter a role for the location in the drop-down menu and a description in the text box.

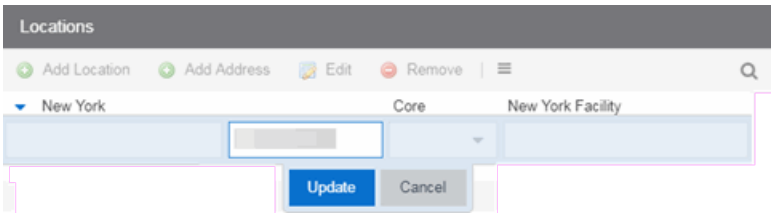


4. Click **Update**.

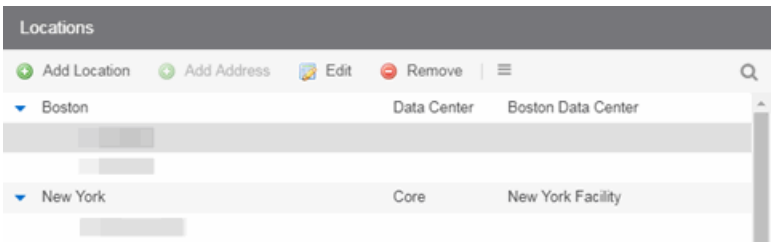
   The new location is added.



5. Select the location in the list, click the **Add Address** button, and enter an IP address/mask in the field in CIDR notation.



6. Click **Update**. The IP address/mask is added to the list under the location. Repeat steps 5 and 6 to add as many IP addresses/masks as necessary. The following image shows the Locations panel with multiple locations defined.



Editing Locations

To edit a location name, description, or address/mask:

1. Access the Extreme Management Center **Analytics** tab and select the Configuration view.
2. In the left-panel tree, expand System and select **Locations**.
3. In the right-panel Locations view, select the location name, role, description, or address/mask that you want to edit.
4. Click the **Edit** button and make the desired changes to the location name, description, or address/mask. You can also double-click on a name, description, or address/mask to make the desired changes, instead of using the **Edit** button.
5. Click **Update**.

Removing Locations

To remove a location or address/mask:

1. Access the **Analytics** tab and select the Configuration view.
2. In the left-panel tree, expand System and select **Locations**.

3. In the right-panel Locations view, select the location name or address/mask that you want to remove.
4. Click the **Remove** button.

Importing Locations

To import locations from a CSV file:

1. Access the Extreme Management Center **Analytics** tab and select the Configuration view.
2. In the left-panel tree, expand System and select **Locations**.
3. In the right-panel Locations view, click the **Gear** button (≡) and select **Import from CSV**.
   The Import Locations window appears.
4. Click the **Select File** button and navigate to the folder in which the CSV file is located.
5. Select the CSV file and click **Open**.
6. Click one of the following options in the Import Options section of the window to determine how Extreme Management Center handles existing locations:
   a. Select **Discard all locations and import new ones** to replace all locations currently listed in the Locations view with the locations imported from the CSV file.
   b. Select **Import locations, overwriting existing locations** to replace existing locations currently listed in the Locations view with locations imported from the CSV file, but leave all other locations in the Locations view unchanged.
   c. Select **Import locations, but do not change existing locations** to add new locations to the Locations view, but prevent existing locations currently listed in the Locations view from being overwritten by locations imported in the CSV file.
7. Click **Import**.
   The locations are imported to the Extreme Management Center.

Exporting Locations

To export locations and save them as a CSV file:

1. Access the Extreme Management Center **Analytics** tab and select the Configuration view.
2. In the left-panel tree, expand System and select **Locations**.
3. In the right-panel Locations view, click the **Menu** button (≡) and select() **Export to CSV**.
   The CSV file is saved to the web browsers default download location.

Searching Locations

To search for a specific location or address/mask in the Locations view, enter the location name or address/mask in the **Search** field and press **Enter**. The search results are displayed in the view.

Related Information

For information on related ExtremeAnalytics topics:

- Getting Started with ExtremeAnalytics
- Analytics Tab

How to Deploy ExtremeAnalytics in an MSP or MSSP Environment

This Help topic presents instructions for deploying ExtremeAnalytics within an MSP (Managed Service Provider) or MSSP (Managed Security Service Provider) environment. It includes the following information:

Configuring Extreme Management Center Behind a NAT Router

If the Extreme Management Center server is located behind a NAT (Network Address Translation) router, use the following steps to add an entry to the nat_config.txt file that defines the real IP address for the Extreme Management Center server. This allows the Extreme Management Center server to convert the NAT IP address received in the Application Analytics engine response to the real IP address used by the Extreme Management Center server. Not adding the real IP address for the Extreme Management Center server to the nat_config.txt file results in the Application Analytics engine incorrectly displaying a state of IMPARED (orange) rather than UP (green).

NOTE: The text in the nat_config.text file refers to a remote IP address and a local IP address. For this configuration, the NAT IP address is the remote IP address and the real IP address is the local IP address.

1. On the Extreme Management Center server, add the following entry to the `<install directory>/appdata/nat_config.txt` file.
   `<NAT IP address>=<real IP address>`
2. Save the file.
3. If the Extreme Management Center Management server IP address is not configured to use the NAT IP address of the Extreme Management Center server, perform the following steps:
   a. Enter the following command at the engine CLI:
      `/opt/appid/configMgmtIP <IP address>`

Where *<IP address>* is the NAT IP address of the Extreme Management Center server.
Press Enter.

b. Restart the appidserver once the new IP address is configured by typing:
`appidctl restart`
Press Enter.

4. On the Extreme Management Center server, add the following text to the *<install directory>*`/appdata/NSJBoss.properties` file. In the second to last line, specify the hostname of the Extreme Management Center server.

NOTE: The Application Analytics engine functions as a client computer independent of the server. Both engines and clients must be able to resolve the hostname you specify.

```
# In order to connect to a NetSight server behind a NAT fi
rewall or a
# NetSight server with multiple interfaces you must define
 these two
# variables on the Extreme Management Center
server. The java.rmi.server.hostname
# should be the hostname
(not the IP) if multiple IPs are being used
# so that each client can resolve the hostname to the corr
ect IP that
# they want to use as the IP to connect to.
java.rmi.server.hostname=<hostname of NetSight server>
java.rmi.server.useLocalHostname=true
```

5. Save the file.
6. Add the Extreme Management Center server hostname to your DNS server, if necessary.

NOTE: Application Analytics engines, remote Extreme Management Center clients, and any Extreme Access Control engines must be able to connect to Extreme Management Center using this hostname.

Related Information

For information on related windows:

- Application Analytics Engine Advanced Configuration Panel

Application Analytics Application Data Collection

The Application Analytics engine provides an application data collection function that collects and records information about network utilization. It includes:

- General Usage Collection — High-level application-centric data, collected hourly and in five-minute intervals.
- Extended Application Collection — Detailed data about all end-systems in the network, collected hourly.

Application data collection is based on network flow information. Network utilization for various objects in the network (called targets) is measured, collected, and used to create application data reports in Extreme Management Center.

NOTE: Ensure at least 4GB of swap space is available for flow storage or impaired functionality may occur. Use the `free` command to verify the amount of available RAM on your Linux system.

This Help topic describes application data collection, including collection targets, statistics, and intervals. It also describes the different collectors used to perform the collection, as well as the sources for flow information.

Data Collection Overview

Application data collection is performed by the Application Analytics engine. The engine collects flow records from switches in your network. It then augments the collected flow data with detailed application information derived by network packet inspection, resulting in rich analytical data.

For example, if a NetFlow record reports 100 bytes transferred from client Workstation 1 to server Host A, then the collection process would add 100 bytes to the tally for Workstation 1, and 100 bytes to the separate tally for Host A. If the flow is identified as traffic for the Payroll application, then 100 bytes would be added to another tally for Payroll as well. And finally, 100 bytes is added to another tally for the entire network. At the end of a collection interval, the totals for client Workstation 1, server Host A, the Payroll application, and the entire network are written to the database.

Data from network flows is collected in an aggregated form for a period of time (called a collection interval), and then stored in the Extreme Management Center database. Extreme Management Center uses this data to provide reports that show how your network is being utilized.

To conserve space on your Extreme Management Center server hard drive, your Application Analytics engines only collect total flow records when the server hard drive drops below 10 GB of free space. If the Extreme Management Center server hard drive drops an additional 1 GB (under 9 GB of free space), your Application Analytics engines stop collecting all flow data.

NOTE: To change the differential threshold (the additional amount of free space reduction after which all records stop being collected), edit the RM_FREE_SPACE_MINIMUM_ALLOW_SUMMARY_KB value in the NSJBOSS.properties file. The value is set to 1,000,000 KB by default, so Application Analytics stops collecting all records when free space reaches 10GB - 1,000,000 KB = 9 GB.

Collection Targets

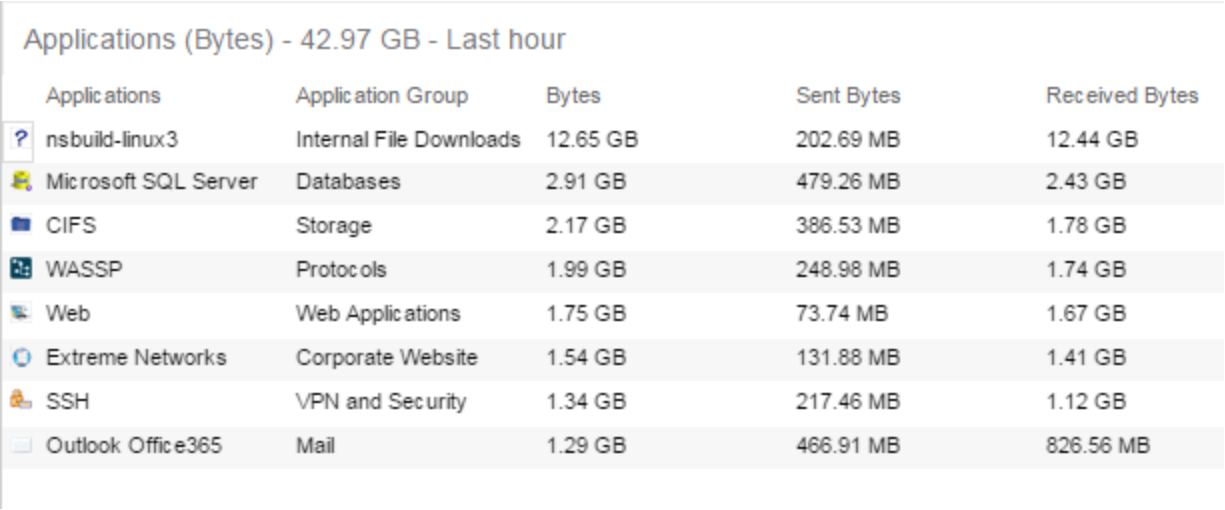
Flow data is collected on objects in your network called targets. Some targets are physical, such as clients and servers, and some are logical, such as applications.

An Application Analytics engine can track the following target types:

- Client — The end-point of a flow that has the client role for that connection.
- Server — The end-point of a flow that has the server role for that connection.
- Application — An application in Application Analytics, identified through layer 7 analysis (for example, Facebook).
- Application Group — Application categories, such as Cloud Computing or Social Networking.
- Location — The client's physical location on the network, based on its IP address. Network locations are used by Application Analytics to identify the physical location for the client of an application flow. For additional information, see Using Locations to Collect In-Network Traffic.
- Device Family — The kind of device determined for a client, such as Windows or iOS.
- Profile — An Extreme Access Control profile assigned to a client.

In some cases, the engine can also track combinations of targets. For example, it can track the total number of bytes transferred from Workstation 1 for the Payroll application separately from Workstation 2 for Payroll, and from Workstation 1 for Facebook. These target and sub-target pairs provide for Extreme Management Center drill-down reports, for example, reports to show the top Payroll clients or the top applications for Workstation 1.

This report shows the top 10 applications seen on the network (based on bandwidth) during the last hour.



Applications (Bytes) - 42.97 GB - Last hour

Applications	Application Group	Bytes	Sent Bytes	Received Bytes
nsbuild-linux3	Internal File Downloads	12.65 GB	202.69 MB	12.44 GB
Microsoft SQL Server	Databases	2.91 GB	479.26 MB	2.43 GB
CIFS	Storage	2.17 GB	386.53 MB	1.78 GB
WASSP	Protocols	1.99 GB	248.98 MB	1.74 GB
Web	Web Applications	1.75 GB	73.74 MB	1.67 GB
Extreme Networks	Corporate Website	1.54 GB	131.88 MB	1.41 GB
SSH	VPN and Security	1.34 GB	217.46 MB	1.12 GB
Outlook Office365	Mail	1.29 GB	466.91 MB	826.56 MB

Collection Statistics

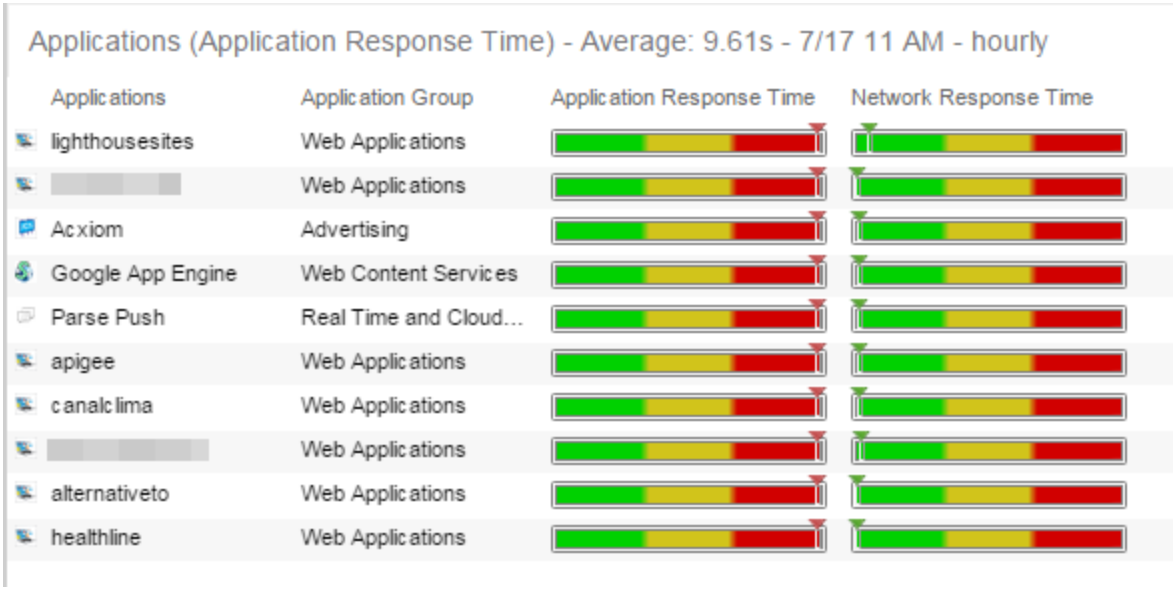
Collection statistics are quantitative data that can be collected for a target. This includes statistics directly reported in NetFlow records, such as bytes transferred, as well as information that can be derived indirectly, such as the number of unique clients seen using an application.

An Application Analytics engine can track the following statistics:

- Bytes — The number of bytes transferred in both directions, between the client and the server. Also known as bandwidth. You can track sent and received bytes as well as total bytes.
- Flows — The number of NetFlow records sent by the switch to report the traffic between the client and the server. You can track inbound and outbound flows as well as total flows.
- Clients — The number of unique clients associated with the target.
- Applications — The number of unique applications associated with the target.

- Network Response Time — The average amount of time to create a connection.
- Application Response Time — The average amount of time for a server to respond to a request.

This report shows the average application response times for the top 10 applications during the last hour.

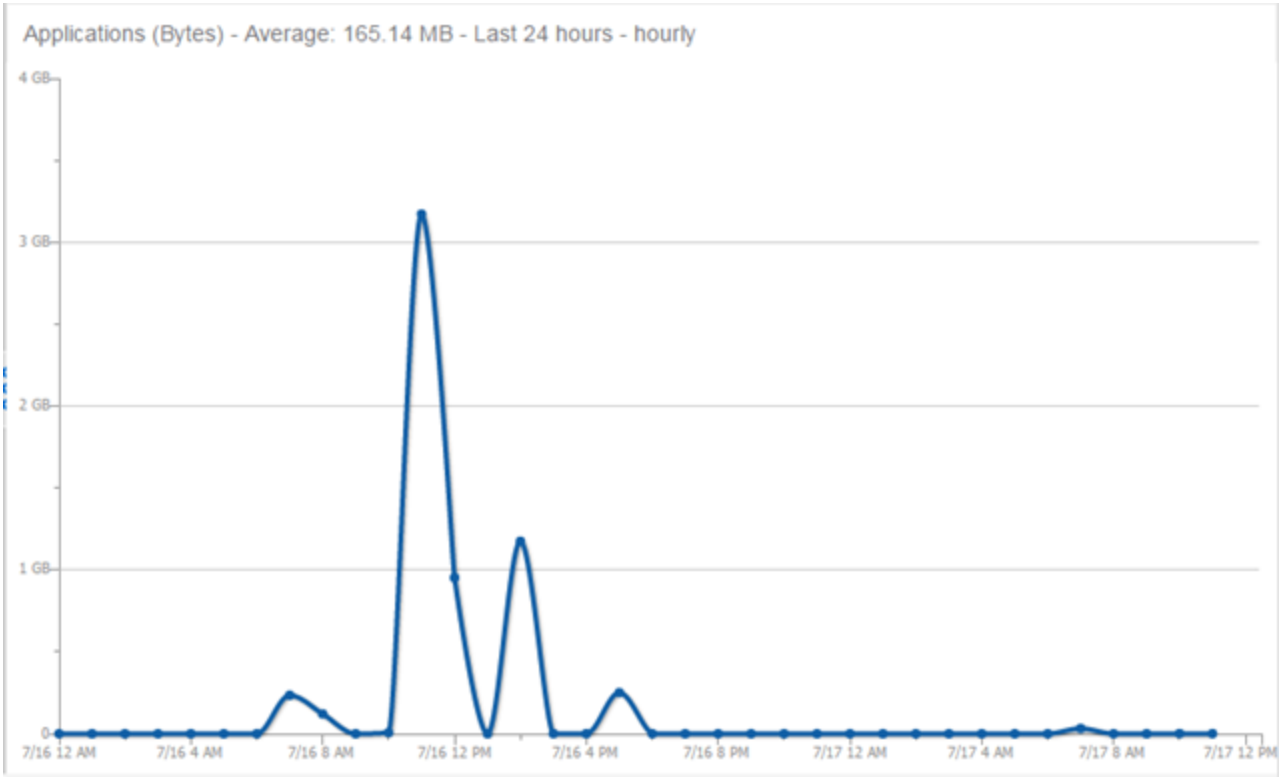


Collection Intervals

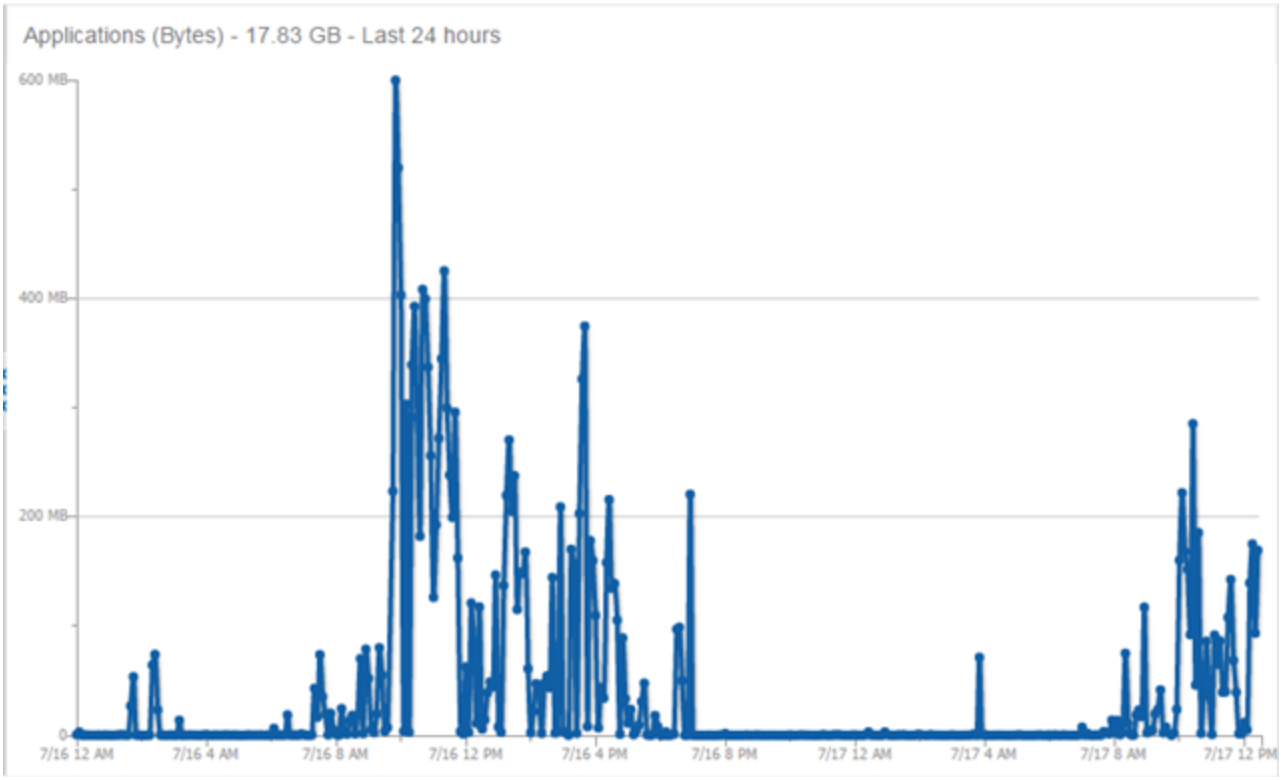
The Application Analytics engine collects and aggregates flow data for a period of time called an interval. At the end of the interval, the engine writes the totals to the Extreme Management Center database and a new interval begins, with new totals collected starting at zero.

Some statistics are collected and written to the database on an hourly interval. Other statistics are collected at a high-rate interval of every five minutes, providing for a more detailed picture of how traffic changes over time.

This report shows application bandwidth over 24 hours based on an hourly interval.



This report shows application bandwidth over 24 hours based on a high-rate interval.



All statistics can be collected over multiple intervals and averaged. When viewing report data, it is important to know the interval used for any average that is displayed.

Certain statistics, such as bytes and flows, can be collected over multiple intervals to provide a total over time, while other statistics, such as client count, cannot. To illustrate, the number of bytes seen in two hours would be the total of the number of bytes seen in each hour. However, the number of unique clients seen in two hours would not be the total of the number of unique clients seen in each hour, as some clients were probably seen in both hours.

Using Locations to Collect In-Network Traffic

While flow data collection can aggregate data for all flow traffic that is visible, it may be more useful to aggregate data for *in-network* flows only. These are flows used by clients that are located in your internal network. By collecting data for only in-network flows, the overhead of aggregating data over an interval can be reduced.

You can define your internal network by configuring Application Analytics locations. A location is a set of IP masks that defines a well-known portion of your internal network. You can define a single location that identifies your entire internal network. If you have already reserved certain IP address ranges for certain physical locations on your network, you can create multiple network locations that correspond to these reserved IP ranges. Multiple locations can be created to identify different buildings, sites, or geographical areas of your network. Any IP that matches any location is considered to be in-network. If you define multiple locations, you will be able to analyze data broken down by location.

Data Collector Types

There are two kinds of data collectors used in Application Analytics.

- General Usage Collectors — These are hourly and high-rate collectors that record the top targets during an interval. Many types of targets and target-pairs are supported.
- End-System Details Collector — This is an hourly collector that attempts to capture and record data for all in-network clients and servers that it detects. All traffic collected is tagged with location, profile, device family, and other attributes.

Data from these collectors is stored separately in the database. The collector data used in a report depends on the nature of the report. Higher-level information, such as top applications during an hour, will be based on general usage collector data, since it is relatively inexpensive to access. End-system details data might be used when data for a specific client or server is needed, or when the information requested is highly specific, for example, top applications used by Android devices in the London location.

General Usage Collectors

General usage collectors collect data about all instances of a target for the interval, and then record only the most significant targets (typically, the 100 most significant targets).

When the top targets are calculated for a collection interval, several different statistics can be used as a basis for choosing the most significant entries. For example, collectors can record the top applications based on bytes, and also

record the top applications based on number of clients. For each type of target collected, there are different sets of bases used.

General usage collectors operate at both hourly and high-rate intervals. They can collect data from all flows or from in-network flows only.

Hourly General Usage Collectors

The following table describes the hourly data collected by the general usage collectors.

Target	Sub-Target	Bases	Traffic Used
Total			In-Network Flows/ All Flows
Application		Bytes Received Bytes Transmitted Bytes Flows Receive Flows Transmit Flows Clients Network Response Time Application Response Time	In-Network Flows
Application	Client	Bytes	In-Network Flows
Application Group		Bytes Flows Clients	In-Network Flows

Target	Sub-Target	Bases	Traffic Used
Client		Bytes Received Bytes Transmitted Bytes Flows Receive Flows Transmit Flows Applications Network Response Time Application Response Time	All Flows
Device Family		Bytes Flows Clients	In-Network Flows
Location		Bytes Flows Clients Network Response Time Application Response Time	In-Network Flows
Profile		Bytes Received Bytes Transmitted Bytes Flows Receive Flows Transmit Flows Network Response Time Application Response Time	In-Network Flows

Target	Sub-Target	Bases	Traffic Used
Threat		Bytes Flows Application Response Time Network Response Time Received Bytes Sent Bytes Inbound Flows Outbound Flows	In-Network Flows
Threat	Threat End-System Pair	Bytes Flows Application Response Time Network Response Time Received Bytes Sent Bytes Inbound Flows Outbound Flows	In-Network Flows
Server		Bytes Received Bytes Transmitted Bytes Flows Receive Flows Transmit Flows Network Response Time Application Response Time	All Flows
Application	Device Family	Bytes Flows Clients	In-Network Flows
Application	Profile	Bytes Flows Clients	In-Network Flows

High-Rate General Usage Collectors

The following table describes the high-rate data collected by the general usage collectors.

Target	Sub-Target	Bases	Traffic Used
Total			In-Network Flows/ All Flows
Application		Bytes Flows Clients	In-Network Flows
Application Group		Bytes Flows Clients	In-Network Flows
Device Family		Bytes Flows Clients	In-Network Flows
Location		Bytes Flows Clients	In-Network Flows
Profile		Bytes Flows Clients	In-Network Flows

End-System Details Collector

The end-system details collector tracks client/application target pairs.

Unlike general usage collectors, this collector attempts to record data for all in-network clients and servers it sees during the hour. For each client or server, it records data for up to 10 applications, plus an "other" category to capture the remaining traffic. Information such as location, device family, and profile are also recorded for each end-system.

The large number of targets recorded each hour and the amount of detail recorded for each one, can result in a large volume of data being stored in the database. In order to prevent disk space from being over-utilized, there is a total limit of 50,000 clients which can be recorded each hour across all Application

Analytics engines. There is also a 25,000 client limit per engine for most license types. However, if you have an NMS-ADV license without any Application Analytics license, the per-hour total limit is 100 clients across all Application Analytics engines.

Flow Information Sources

The Application Analytics engine uses NetFlow or SFlow records from the switches and wireless controllers in your network as a source for flow data. Information such as IP addresses, ports, and bytes transferred comes from this flow data source.

This data is augmented with additional layer 7 application information produced by the Application Analytics engine through deep packet inspection. Information such as application name and network response time comes from this source.

There is additional information that can be obtained from sources other than NetFlow/SFlow records and deep packet inspection.

NOTE: Most of these sources rely on Extreme Access Control data. If Extreme Access Control is part of your network configuration, then Extreme Access Control integration can be enabled (see instructions below) to provide access to these sources. Location data is obtained from network locations configured in Application Analytics.

The following is a list of information that can obtained from different sources:

- Hostname — The client or server's hostname can be derived using Extreme Access Control. Extreme Access Control integration must be enabled.
- Location — The location for a flow is the location of the client in the flow. Client and server locations are derived from the network locations configured in Application Analytics. If a client does not match a location, then the location is empty. If a flow has a location, the flow is considered to be in-network. For additional information, see Using Locations to Collect In-Network Traffic.
- Detailed Location — Detailed location information is derived from the switch and port information resolved for the client end-system. Extreme Access Control Integration must be enabled.
- Device Family — The device family is a general description of the operating system detected in the client, for example, Windows, Linux, or Android. The device family is

derived from network packet inspection. The device family can also be provided by Extreme Access Control, if Extreme Access Control integration is enabled.

- Profile — The client's profile is derived from the Extreme Access Control profile assigned to the client end-system. Extreme Access Control integration must be enabled.
- Username — The client's username is derived from network packet inspection. The username can also be provided by Extreme Access Control, if Extreme Access Control integration is enabled.

It is possible that different sources may provide different values for the same information. For example, network packet inspection may provide the device family name of Window 7, whereas Extreme Access Control may provide the device family name of Windows.

Enabling ExtremeControl Integration

If your network configuration includes ExtremeControl, ExtremeControl data can be integrated with flow data to provide additional information. Extreme Access Control integration is only useful if you are collecting flows for end-systems managed by ExtremeControl.

When ExtremeControl integration is enabled, if a client in a flow matches an end-system in ExtremeControl, then:

- The client hostname in the flow is derived from the end-system.
- The device family in the flow is derived from the end-system.
- The username in the flow is derived from the end-system.
- The profile in the flow is derived from the end-system's ExtremeControl profile.
- The detailed location in the flow is derived from end-system data.

If a server in a flow matches an end-system in ExtremeControl, then:

- The server hostname in the flow is derived from the end-system.

To enable ExtremeControl integration on the Application Analytics engine:

1. If the ExtremeControl distributed end-system cache is not enabled on the Extreme Management Center server, you must enable it using the following steps.

a. Select **Administration > Options** from the menu bar to open the **Access Control Options** window.
b. Click on **Advanced Settings**.
c. In the End-System Mobility section, select the **Enable distributed end-system cache** option.
d. Click the **Reload** button to reload the cache configuration on the Extreme Management Center server. Click **OK**.

2. Enable ExtremeControl Integration on each Application Analytics engine where you want to use ExtremeControl data.
   a. Access the **Analytics** tab.
   b. Expand each Application Analytics engine and select Advanced Configuration. In the right panel under Configuration Options, select the **Enable Extreme Access Control Integration** option.
   c. If your Extreme Access Control engines are using Communication Channels, you must select the **Extreme Access Control Communication Channel** option and enter the channel name. The Application Analytics engine is only able to access end-systems in its channel.
   d. Click **Save**.
   e. Enforce your Application Analytics engines.

Reports

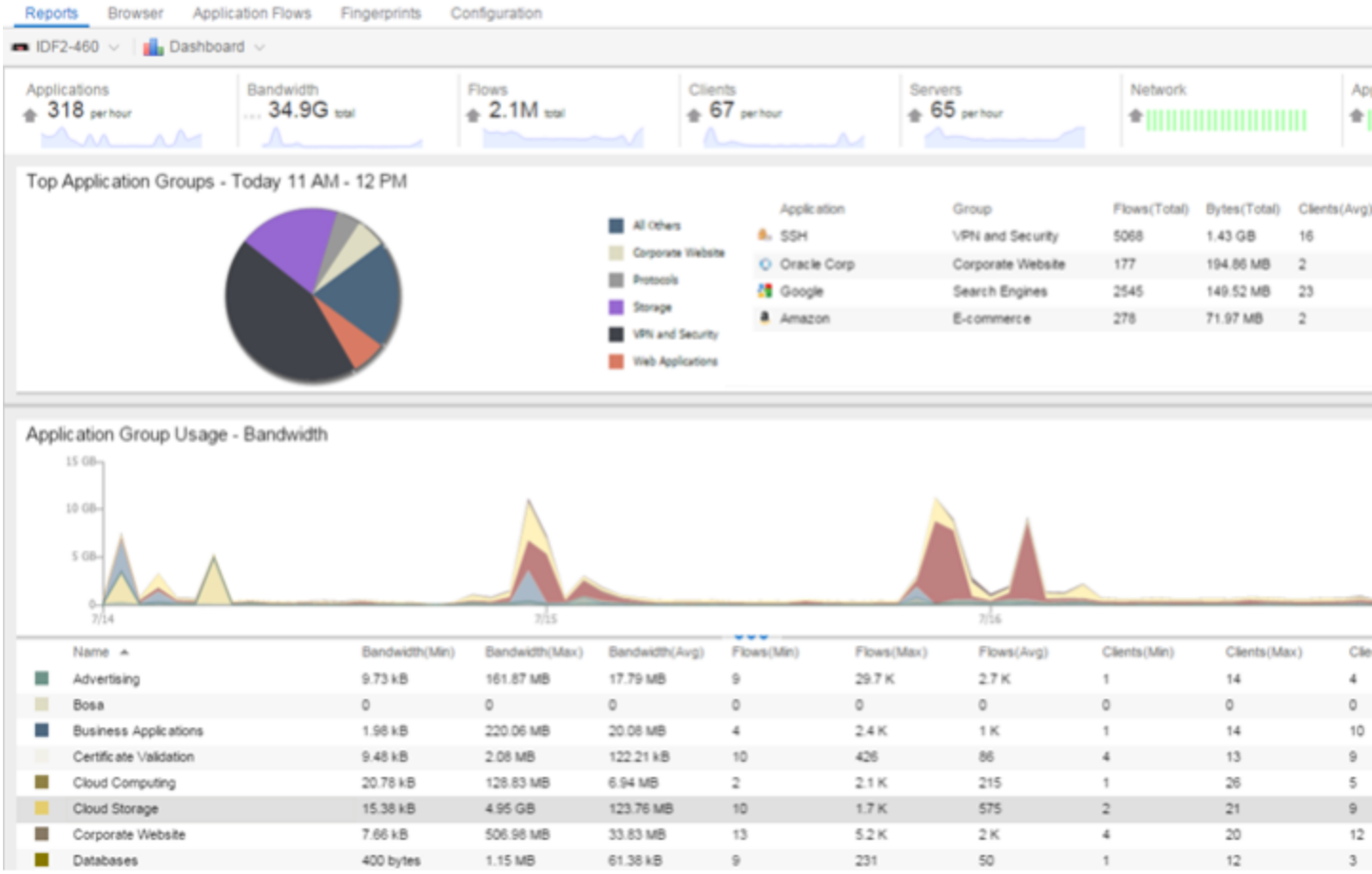
Data gathered from flow usage collection is the basis of many reports in the Extreme Management Center's **Analytics** tab. Once collection is enabled, these reports begin to exhibit data.

For additional information, see Analytics Tab.

Dashboard Report

The following screen-shot shows the main Dashboard report. It contains data produced by the hourly General Usage collectors, and displays data for a specific hour. Across the top are the hour's totals. Below them are Top Application Groups, as a chart, and Top Applications, as a table, for the same hour. There is also Application Group Usage over the last 3 days, as a chart and as a table.

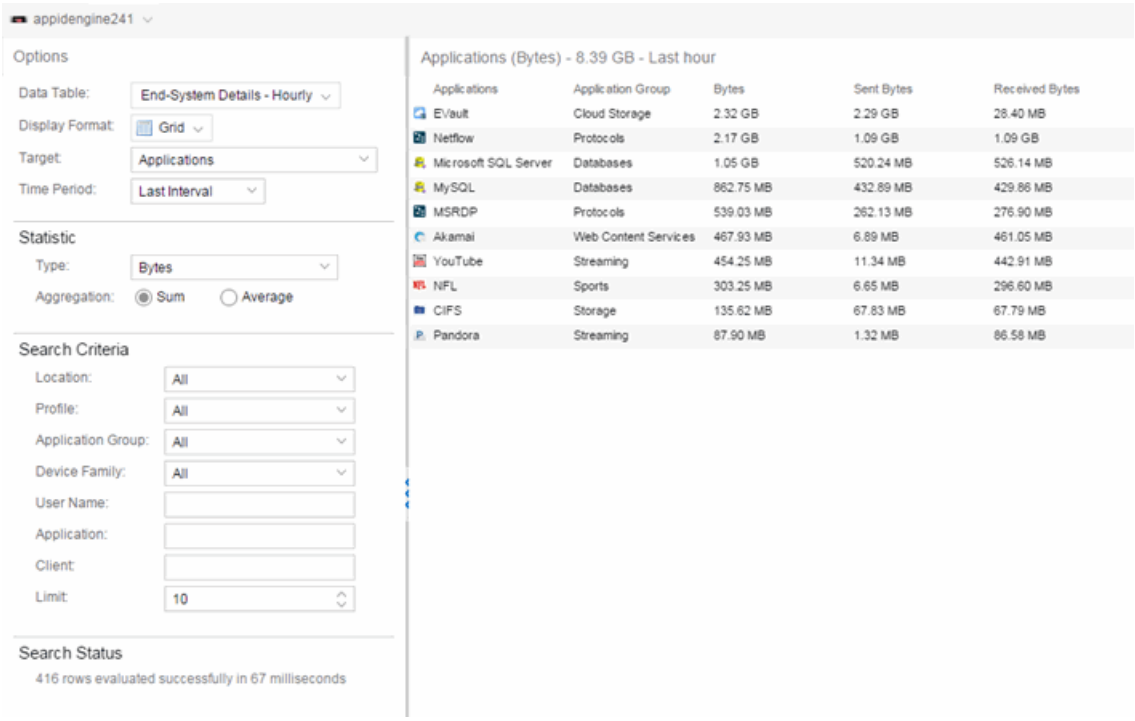
Note that data from different Application Analytics engines is maintained separately. If you have more than one Application Analytics engine, you need to select which engine to view, using the engine menu in the top-left corner.



Browser Reports

The Browser provides special reports that lets you select the targets, statistics, and collection interval for your report, as well as define search criteria to further filter report data. Using the Browser, you can create custom queries that provide greater flexibility in defining what data to display and how to display it. When you create a Browser report, you select which type of network activity data to use: end-system details (always hourly), application data hourly, or application data high-rate. For additional information, see Applications Browser.

The following screen-shot shows an example of a Browser report showing application/device family bandwidth usage for the last hour.



Related Information

For information on related Application Analytics topics:

- Getting Started with ExtremeAnalytics
- Analytics Tab
- Network Locations

ExtremeAnalytics Dashboard

Accessible from the **Analytics** tab in Extreme Management Center, the **Dashboard** view displays an overview of application usage on your network, as well as network activity statistics through a series of real-time reports. The Dashboard is flexible and customizable - you can choose the reports and the design of the page to meet your specific needs. Many of the reports are links to more detailed pages.

The Dashboard includes a drop-down menu with links to additional report dashboards:

- Insights
- Client/Server
- Applications Browser
- High-Rate Application Collector
- Industry
- Application Map
- Response Time
- Network Service
- Tracked Applications

Several report pages can be launched in the **Reports > Reports Designer** view in Extreme Management Center by clicking the **Launch in Report Designer** icon ( ).

Insights Dashboard Reports

The Insights dashboard provides you with graphs that display real-time network and application usage and service data, and tools that you can use to customize the dashboard using drag-and-drop capabilities.

Five ring charts display real-time Engines, Disk Usage, Flow Rate, Network, and Application usage and service data. The ring charts are links to additional data. The Network and Application charts link to the Network Service and Response Time report dashboards, respectively, which are also accessible from the **Dashboard** drop-down menu.

The Application Group dashboard allows you to drag and drop only the graphs you want on your dashboard. Each graph is a real-time preview and many are linked to additional detail reports. You can also choose whether the graphs in the Application Group area are organized in columns or rows in the Application Group area.

Client/Server Dashboard Reports

This dashboard displays reports on clients and servers seen on the network over the last 24 hours. It also displays reports on top clients by bandwidth, flow, or number of applications, and top servers by bandwidth or flow.

Click on the Info icon (ℹ) at the top right of the dashboard page to read a description of each report.

Applications Browser Dashboard Report

The Application Browser Dashboard displays bubble maps for top applications by bytes and flows, top profiles by bytes, and top locations by bytes. Hovering over a bubble displays bandwidth use or the number of flows. Use the drop-down menus to change the start date and time for the reports.

Drill-down for more information by clicking on an application bubble to open a new graph of clients, flows, and usage data for that application. In that graph, click on a client link to view application data for that client.

High-Rate Application Collector Dashboard Report

The High-Rate Application Collector Dashboard shows the number of clients, flows and bytes collected during the high-rate collection interval for the time period configured at the top of each section. Click the arrows to the left and right of each graph to adjust the time period.

Click on the Info icon (ℹ) at the top right of the dashboard page to read a description of each report.

Industry Dashboards

- The Enterprise Dashboard displays application information specific to the Enterprise network including social applications, storage applications and cloud, business

applications and email, and network applications and protocols.

- The Education Dashboard displays application information specific to the campus network including learning management systems, P2P, streaming, and social applications.
- The Healthcare Dashboard focuses on applications used in the healthcare environment including patient care, medical applications, and HIPAA.
- The Venue Dashboard displays data grouped according to sports, social media, news and weather applications, as well as software update applications.

Application Map

The Application Map provides a global overview of top application groups by location, displayed in the **Network** tab World map. The application data is displayed in pie charts and is based on application data for ExtremeAnalytics locations linked to the **Network** tab map.

For information on configuring the Extreme Management Center World map to show application data, see Show Application Data in the Advanced Map Features section of the *Extreme Management Center User Guide*.

NOTE: By default, the Application Map displays theExtreme Management Center World map. You can specify a different map to use by changing the Application Dashboard Map option. On the **Configuration** tab, select the **System > Advanced** options in the left-panel and select a new Application Dashboard Map in the right-panel.

Response Time Dashboard

The Response Time Dashboard presents the response time in milliseconds of application data grouped by different criteria, selected from the drop-down menu. The data is displayed as a line graph, which is updated periodically.

Network Service Dashboard

The Network Service Dashboard displays the response time of network services for the top five worst-performing locations as well as the overall average of all locations. The data for each network service at a location is displayed as a bar and line graph, which is updated periodically.

Tracked Applications Dashboard

The Tracked Applications Dashboard displays the response time of the applications you configure in the **Tracked Applications** field on the **Analytics** > **Configuration** > Configuration tab. The data for each network service at a location is displayed as a bar and line graph, which is updated periodically. You can choose to organize the graphs in either columns (IIII) or rows (⊞).

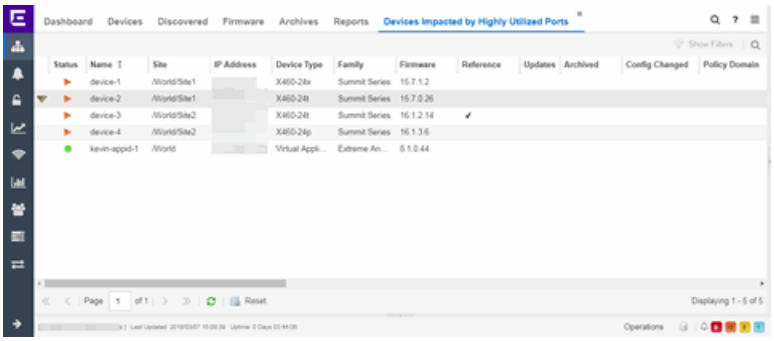
Related Information

- ExtremeAnalytics tab

ExtremeAnalytics Insights Dashboard

Accessible from the Analytics tab in Extreme Management Center, the Insights Dashboard displays an overview of application usage on your network, as well as network activity statistics based on client/server, application, industry, IP reputation, and response time.

The Insights Dashboard provides you with graphs that display real-time network and application usage and service data, and tools that you can use to customize your dashboard using drag-and-drop capabilities.

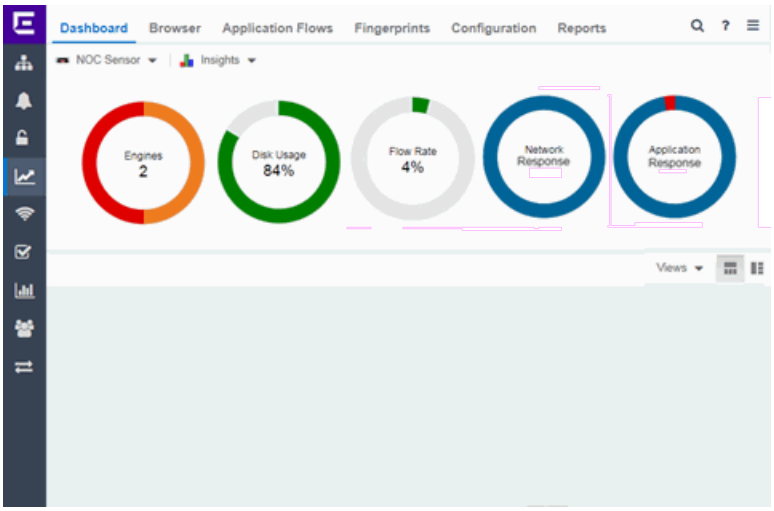


Insights

The Insights Dashboard displays ring charts and a customizable Application Group Dashboard. You can collapse and expand the ring charts and Application Group Dashboard for flexible display capabilities.

Ring Chart

Five ring charts display real-time Engines, Disk Usage, Flow Rate, Network, and Application usage and service data:

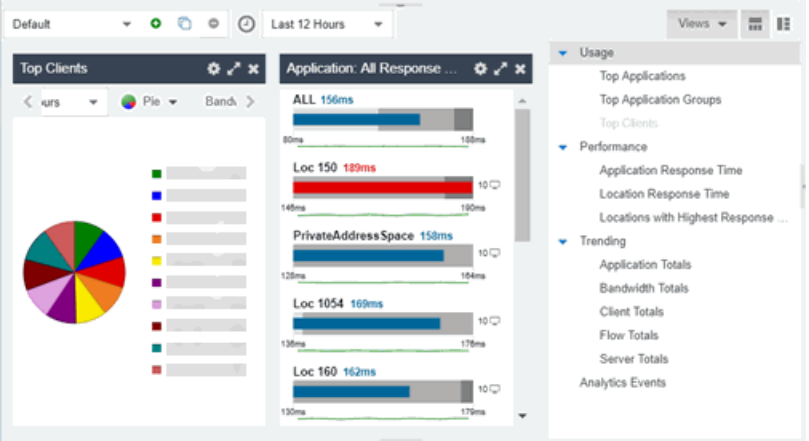


- Engines — The number at the center of the ring chart indicates how many engines are represented by the chart. The colors in the graph indicate the states of the configured engines. Hover over a ring color to display a tooltip with the status of that engine. Click the graph to display overview and status details.
- Disk Usage — The number at the center of the ring chart indicates the percentage of Disk Usage. The colors in the graph display the percentage of disk usage being used. Hover over the ring color to display a tooltip with usage percentage and units of space details.

  Click the graph to open the Configuration tab, where you can configure the information displayed in the Insights Dashboard.
- Flow Rate — The number at the center of the ring chart indicates the flow rate percentage. The colors in the graph indicate the flow rates for the different engines being used. Hover over a ring color to display a tooltip with status, percentage and rate details for each engine. Click the graph to open the Licenses tab.
- Network Response — The colors in the graph indicate the network response time for the application/location. Hover over a ring color to display a tooltip with status details and the number of networks at that status. Click a color in the graph to open the Network Service dashboard, which displays network service details.
- Application Response — The colors in the graph indicate the application response time for the application/location. Hover over a ring color to display a tooltip with response time details and the number of applications within the expected response time range. Click a color in the graph to open the Response Time dashboard, which displays network and application response time charts and details.

Custom Dashboard

The Custom Dashboard is a customizable space for viewing graphs that you select from the **Views** drop-down menu. The buttons at the top right of the Applications Group dashboard () allow you to save and copy your dashboard.



Related Information

- Analytics Tab
- How to Use the Application Group Dashboard

How to Create an ExtremeAnalytics Insights Custom Dashboard

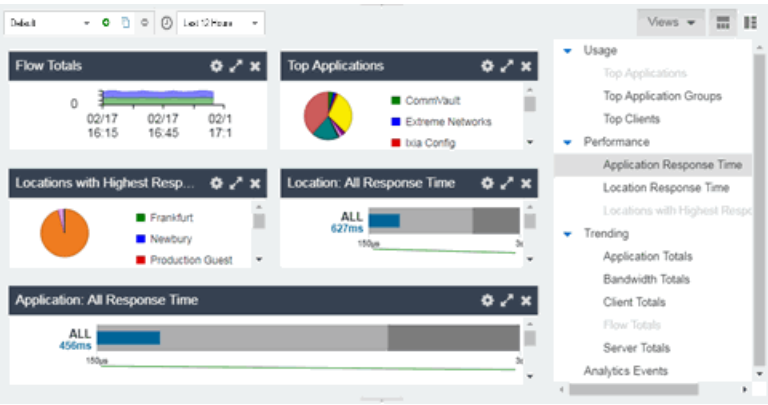
The **Dashboard** > **Insights** view in Extreme Management Center provides you with graphs that display real-time network and application usage and service data, and tools that you can use to customize the dashboard using drag-and-drop capabilities.

The Custom dashboard in the **Insights** view allows you the flexibility to create your graphs and reports preview area. Choose the graphs you want to view, the data that is displayed in the graphs, and how the graphs are displayed. You can collapse and expand the Custom dashboard for flexible display capabilities.

Custom Dashboard

The Custom dashboard is a flexible space for viewing graphs that you select from the Views drop-down menu. The buttons at the top right of the Custom dashboard ( ) allow you to save and copy your dashboard.

- Click the **Create** button ( ) to create a new, empty dashboard where you can drag and drop the graphs you select from the Views drop-down menu. The Create Dashboard window opens to allow you to name your new dashboard. Click the **Save** button to save the dashboard, which is available to all users in your network.
- Click the **Copy** button ( ) to copy the current dashboard, which you can customize by adding new graphs from the Views drop-down menu. Once you have edited the copied dashboard, click the **Save** button to save the new dashboard, which is available to all users in your network.



1. Click the **Views** button at the far right and select from the graphs in the drop-down menu.
2. Drag and drop the graph(s) to the open area to the left. Once in place, the link will display as a real-time preview of the graph.
3. Choose the orientation of your dashboard by clicking either the row ( ) or column ( ) button.
4. Hover over the data to display a tooltip with usage data.
5. Click the **Gear** button ( ) in each graph to further modify your Application Group graphs data:
    - **Top** — Choose the number of top applications, application groups or clients (depending on the graph) to be displayed in the graph

- Range — Adjust the time frame of the data depicted in the graph by choosing from the drop-down menu. The Custom Time option allows you to choose any start time, and the Custom Range option allows you to choose any start and end times.
- Graph style — Select from pie, word cloud, tree map or bubble map graph styles in the drop-down menu.
- Data — Select from Bandwidth, Flows, Clients data types from the drop-down menu.

Graphs

These graphs are available to be added as real-time previews to your Custom dashboard:

Usage

Top Applications — Displays usage data for the top applications. Click any color in the graph to display an encrypted web detail page for that application.

Top Application Groups — Displays usage data for the top application groups. Click any color in the graph to display an encrypted web detail page for that group.

Top Clients — Displays usage data for the top clients. Click any color in the graph to display application and application group detail page for that client.

Performance

Application Response Time — Displays response times for all applications. You can also create response time reports for individual applications and locations that you define.

Location Response Time — Displays response times for all locations. You can also create response time reports for individual applications and locations that you define.

Locations with Highest Response Time — Displays locations with the highest response times. Click any color in the graph to display network and application response time reports for that location.

Trending

Application Totals — Displays the total number of applications based on the date, time, and duration you choose. Click any color in the graph to display an application detail page.

Bandwidth Totals — Displays bandwidths for the application in a line graph based on the date, time and duration you choose. Click any data point in the graph to display a Top Applications by Bandwidth detail page.

Client Totals — Displays the total number of clients for the application based on the date, time, and duration you choose. Click any data point in the graph to display a Top Clients detail page.

Flow Totals — Displays the total number of outbound and inbound flows for the application based on the date, time, and duration you choose. Click any data point in the graph to display a Top Applications by Flows detail page.

Server Totals — Displays the total number of servers for the application based on the date, time, and duration you choose. Click any data point in the graph to display a Top Servers detail page.

Analytics Events

Analytics Events - This report displays the event log filtered to show only the events related to ExtremeAnalytics

---

Related Information

- ExtremeAnalytics tab
- ExtremeAnalytics Insights Dashboard

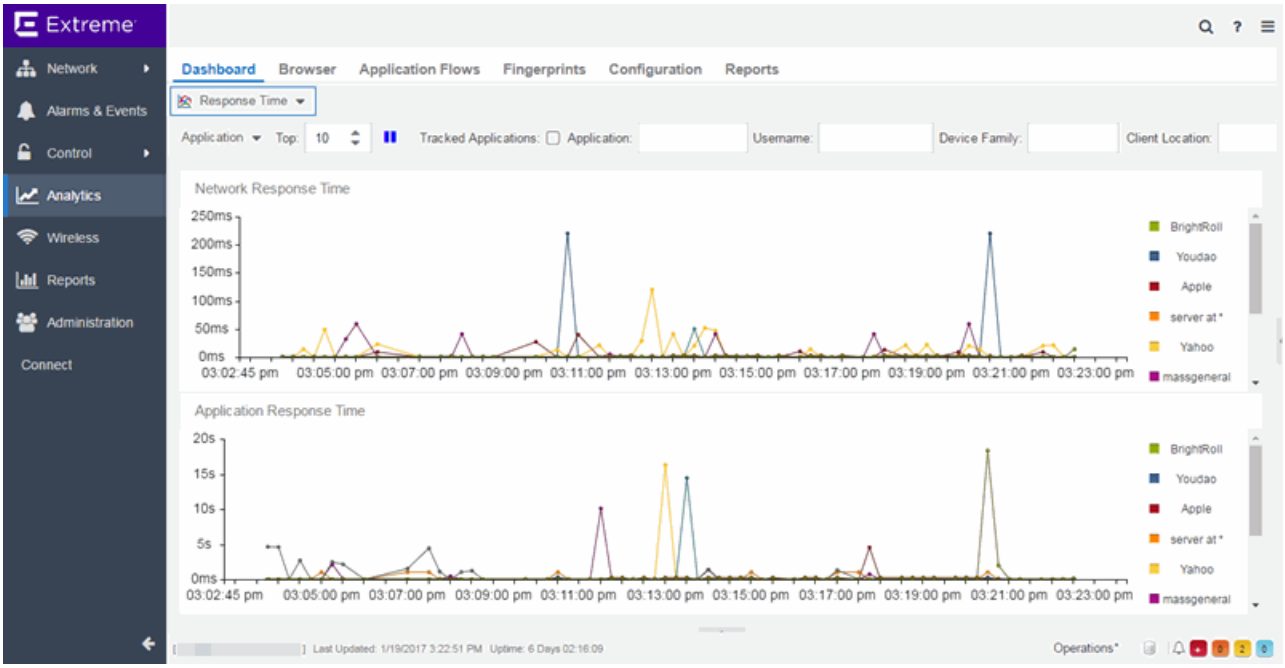
ExtremeAnalytics Response Time Dashboard

The Response Time Dashboard displays the network and application response time data for the slowest targets on your network based on response time for the last 20 minutes. Extreme Management Center allows you to view response

time data for a variety of filters, including application, device family, and username.

The dashboard also allows you to select the number of targets for which the response time is displayed. Additionally, the Response Time Dashboard allows you to filter based on certain criteria and view flow data specific to the data you select.

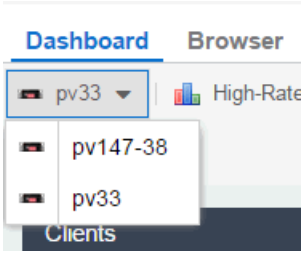
To access the Response Time Dashboard, open the **Analytics** > **Dashboard** tab and select **Response Time** in the dashboard drop-down menu.



Overview

The Response Time Dashboard contains two graphs, one displays the network response time and the other displays the application response time. Data is updated every 15 seconds and displays data over the last 20 minutes.

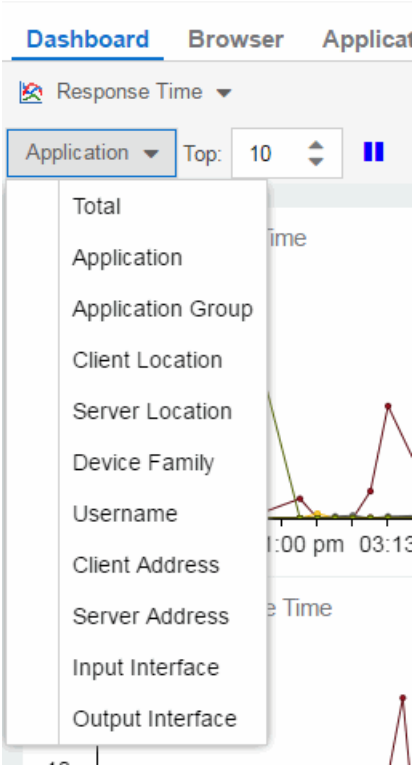
If you have multiple Application Analytics engines, use the **Engine** drop-down menu to select an engine to use as the source for the report data.



The toolbar at the top of the window allows you to display data based on criteria you select and updates the two graphs.

Application

The Application drop-down menu allows you to group the data in the Response Time Dashboard by the following criteria:



Top

The Top field allows you to limit the results in the graphs to display only the top results based on the number you enter.

For example, you can configure the graphs to display the top 3 slowest applications by response time.

Tracked Applications

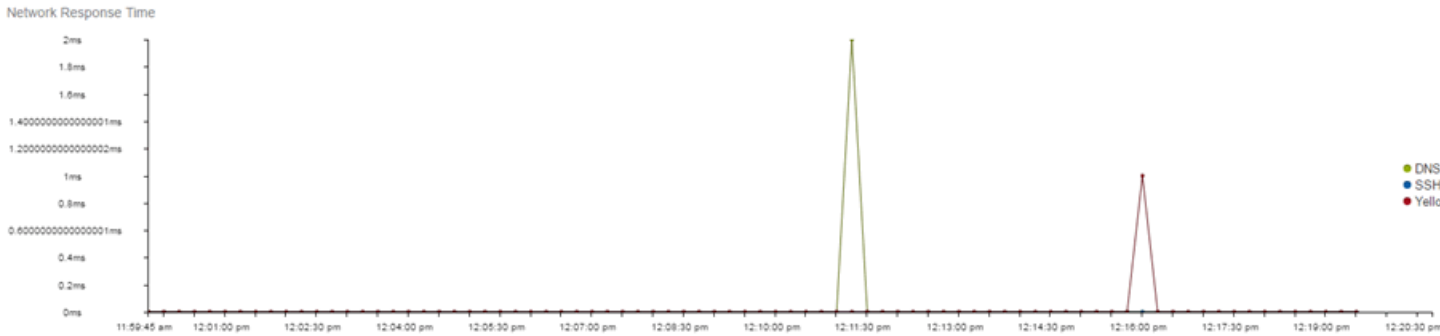
Click the **Tracked Applications** box to add response time results for tracked applications to the Network Response Time and Application Response Time graphs.

Filters

You can also use the filter options at the top of the window to search for specific criteria. Using these fields allow you to limit the data to Tracked Applications, Application, Username, Device Family, Client Location, and Server Location. Entering a value in one of these fields filters the results displayed in the graphs below. Clear the data by clicking the **Clear** (⊗) button to the right of the filter options.

Network Response Time Graph

The Network Response Time graph displays the response time (in milliseconds) the TCP request took to complete for the Top N slowest Targets. The data in this graph depends on the criteria you select in the toolbar at the top of the window and can be filtered to match specific criteria. Extreme Management Center displays data collected by the Application Analytics engine over the previous 20 minutes updated every 15 seconds. Use the **Pause** button in the toolbar to stop the graph from updating. Clicking the **Unpause** button resumes the updates and refreshes the graph with the most up-to-date data.



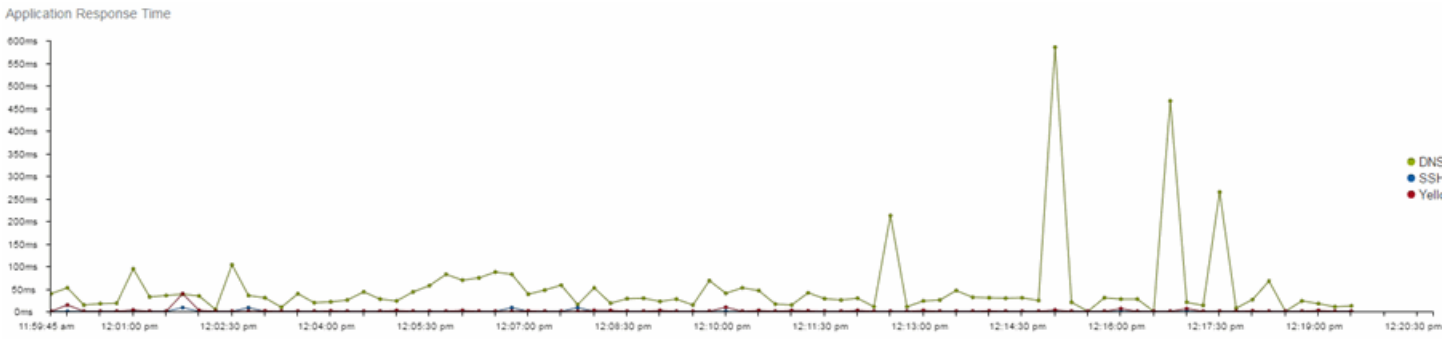
Hover over a point in the graph to see a pop-up with details about that application at that moment in time.

Clicking on a point opens a flow data table for that Target at that time at the bottom of the window, limited to match any filters you applied. Right-click a row in the flow to see additional options for working with that flow.

Click the Arrow button (⌄⌄⌄) at the top of the flow data table to collapse the table and click the Arrow button (⌃⌃⌃) on the collapsed table to expand the table again.

Application Response Time Graph

The Application Response Time graph displays the response time (in milliseconds) the application request took to complete for the Top N slowest Targets. The data in this graph depends on the criteria you select in the toolbar at the top of the window and can be filtered to match specific criteria. Extreme Management Center displays data collected by the Application Analytics engine over the previous 20 minutes updated every 15 seconds. Use the Pause button in the toolbar to stop the graph from updating. Clicking the Unpause button resumes the updates and refreshes the graph with the most up-to-date data.



Hover over a point in the graph to see a pop-up with details about that application at that moment in time.

Clicking on a point opens a flow data table for that Target at that time at the bottom of the window, limited to match any filters you applied. Right-click a row in the flow to see additional options for working with that flow.

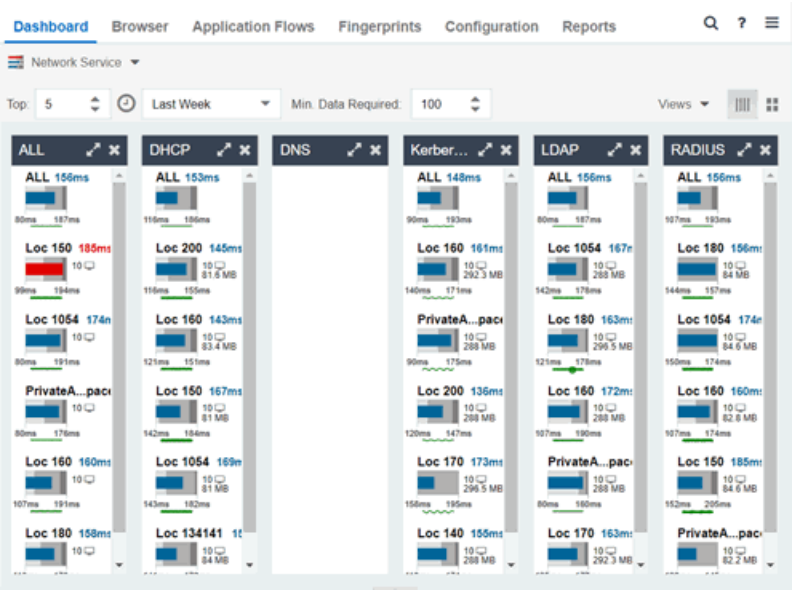
Click the Arrow button (⌄⌄⌄) at the top of the flow data table to collapse the table and click the Arrow button (⌃⌃⌃) on the collapsed table to expand the table again.

Related Information

- ExtremeAnalytics tab

ExtremeAnalytics Network Service Dashboard

To access the Network Service Dashboard, open the **Analytics** > **Dashboard** tab and select **Network Service** in the dashboard drop-down menu.



Overview

The Network Service Dashboard contains two graphs for each network service: the Expected Response Time bar graph displays the average response time over the selected time period and the Historical Response Time line graph displays the individual response times over that period for each location.

Select the number of locations displayed in each column in the **Top** field.

Use the **Time Period** drop-down menu to display the date and time range for which data is displayed. Selecting **Custom** displays additional fields allowing you to indicate a **Start Date** and time and an **End Date** and time.

Use the Minimum Required Response Time Dashboard Data Points to configure the minimum amount of data Extreme Management Center requires before displaying a given application or location pair. The data below this threshold is not reliable and may set off a false alarm, however, you can adjust how much data is required based on the individual needs of your network.

The Network Service Dashboard displays the performance (in response time) of your network services. Each column in the dashboard represents a service:

- ALL
- DHCP
- DNS
- Kerberos
- LDAP
- RADIUS

The top graphs for each service displays the average response time of all of the locations for that service, while the following rows indicate the top worst performing locations for that service.

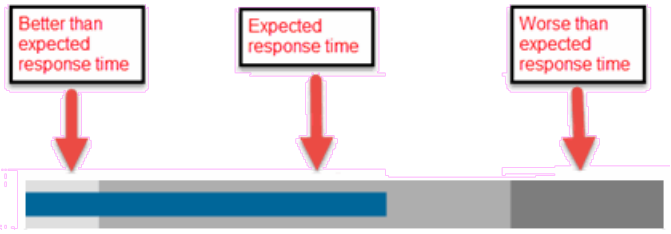
You can display or hide any of the application columns using the Views drop-down menu. You can also click the X at the top of a column to hide the column from the dashboard. Click the Single Row icon ( ) to display all columns in a single row, or click the Double Row icon ( ) to display the columns in two rows.

The worst performing locations are defined as those whose response time is the slowest when compared to the expected response time observed over the selected time period. For example, a location with an average RADIUS authentication response time of 40 ms over the past seven days that displayed a slowest response time of 50 ms would rank as a better performing location than a location with an average RADIUS authentication response time of 5 ms over the same period that displayed a slowest response time of 30 ms.

Expected Response Time

The Expected Response Time bar graph displays the range of response times, the most recently measured response time, and the expected response time for a network service a specific location (or all locations) during the date range you configure in the Date Range drop-down menu. The value displayed on the far

right of the graph is the slowest response time observed during the selected time period. The vertical green bar indicates the most recently observed response time for the network service.



Hover over the Expected Response Time graph to display a pop-up with the response time for the network service as well as the date and time the measurement occurred. The Expected Response Time bar graphs also display the client count, represented by a number and a monitor icon (10), and a client byte count observed as of the most recent measured minute. The client count is the number of clients using the service at the location. The client byte count indicates the amount of storage being utilized by clients. The data used for the client count, the client byte count, and the reported response time are from the same recently observed minute.

NOTE: Client counts and client byte counts are not provided for the bar graphs that display the average response time of all the locations for that service.

Extreme Management Center uses a standard deviation of the values gathered as response times to determine the expected response time for a network service at a location. In the bar graph, the medium gray color indicates a response time that falls within the "expected" range. A response time in the light gray range is better than expected, while a response time in the dark gray is worse than expected.

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

Clicking the Expected Response Time bar graph opens the Response Time dashboard (which is also accessible from the **Analytics** > Dashboard tab) filtered to display the network service. If you click the network service for a particular location, the Response Time dashboard also filters to that location.

Historical Response Time

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

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

This is the data set from which Extreme Management Center creates the Expected Response Time graph. The wider the expected 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.

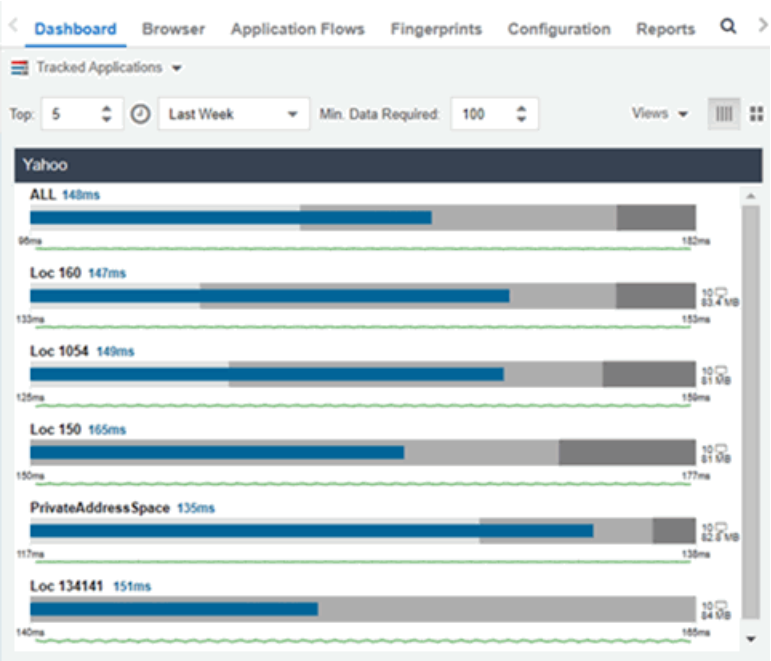
Related Information

- ExtremeAnalytics tab

ExtremeAnalytics Tracked Applications Dashboard

The Tracked Application dashboard displays the performance (in response time) of your network for applications you configure in the **Tracked Applications** field on the **Analytics** > **Configuration** > Configuration tab.

To access the Tracked Application dashboard, open the **Analytics** > **Dashboard** tab and select **Tracked Applications** in the dashboard drop-down menu.



Overview

The Tracked Applications dashboard contains two graphs for each application, one displays the average response time over the selected time period and the other displays the individual response times over that period for each location. Data is updated every minute and can be manually refreshed by clicking the **Refresh** button ( ).

Select the number of locations displayed in each column in the **Top** field. The Tracked Applications dashboard can display up to 25 locations.

Use the **Time Period** drop-down menu to display the date and time range for which data is displayed. Selecting **Custom** displays additional fields allowing you to indicate a **Start Date** and time and an **End Date** and time.

Use the **Minimum Required Response Time Dashboard Data Points** to configure the minimum amount of data Extreme Management Center requires before displaying a given application or location pair. The data below this threshold is not reliable and may set off a false alarm, however, you can adjust how much data is required based on the individual needs of your network.

Each column in the dashboard represents an application. The top row displays the average response time of all of the locations for that application, while the following rows indicate the top worst performing locations for that application.

You can display or hide any of the application columns using the **Views** drop-down menu. You can also click the **X** at the top of a column to hide the column from the dashboard. Click the **Single Row** icon ( ) to display all columns in a single row, or click the **Double Row** icon ( ) to display the columns in two rows.

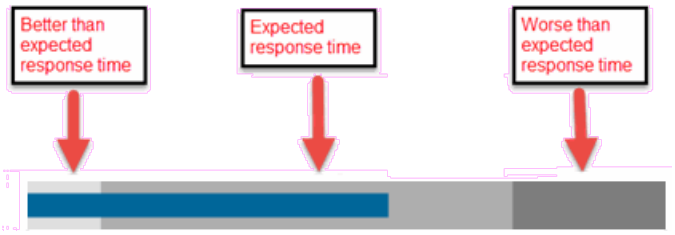
Click the **Maximize** icon ( ) to expand a single application column.

The worst performing locations are defined as those whose response time is the slowest when compared to the expected response time observed over the selected time period. For example, a location with an average Microsoft Office 365 authentication response time of 40 ms over the past seven days that displayed a slowest response time of 50 ms would rank as a better performing location than a location with an average Microsoft Office 365 authentication response time of 5 ms over the same period that displayed a slowest response time of 30 ms.

Expected Response Time

The Expected Response Time bar graph displays the range of response times, the most recently measured response time, and the expected response time for an application a specific location (or all locations) during the date range you configure in the Date Range drop-down menu. The value displayed on the far right of the graph is the slowest response time observed during the selected time period. The vertical blue or red bar indicates the most recently observed 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 response time for the application as well as the date and time the measurement occurred. The Expected Response Time bar graphs also display the client count, represented by a number and a monitor icon (10), and a client byte count observed as of the most recent measured minute. The client count is the number of clients using the service at the location. The client byte count indicates the amount of storage being utilized by clients. The data used for the client count, the client byte count, and the reported application response time are from the same recently observed minute.

NOTE: Client counts and client byte counts are not provided for the bar graphs that display the average application response time of all the locations for that service.

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

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

Clicking the Expected Response Time bar graph opens the Response Time dashboard filtered to display the application. If you click the application for a particular location, the Response Time dashboard also filters to that location.

Historical Response Time

The Historical Response Time line graph shows all of the 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 response time at which you are looking. Additionally, a pop-up with the date, time, and response time appears for that point.

This is the data set from which Extreme Management Center creates the Expected Response Time graph. The wider the expected 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

- ExtremeAnalytics tab

ExtremeAnalytics Browser

The Browser lets you query information about recent network activity stored in the Extreme Management Center database and display results in various grid and chart report formats. Using the Browser, you can create custom queries that provide greater flexibility in defining what data to display and how to display it. You can access the Browser from the Extreme Management Center Analytics tab.

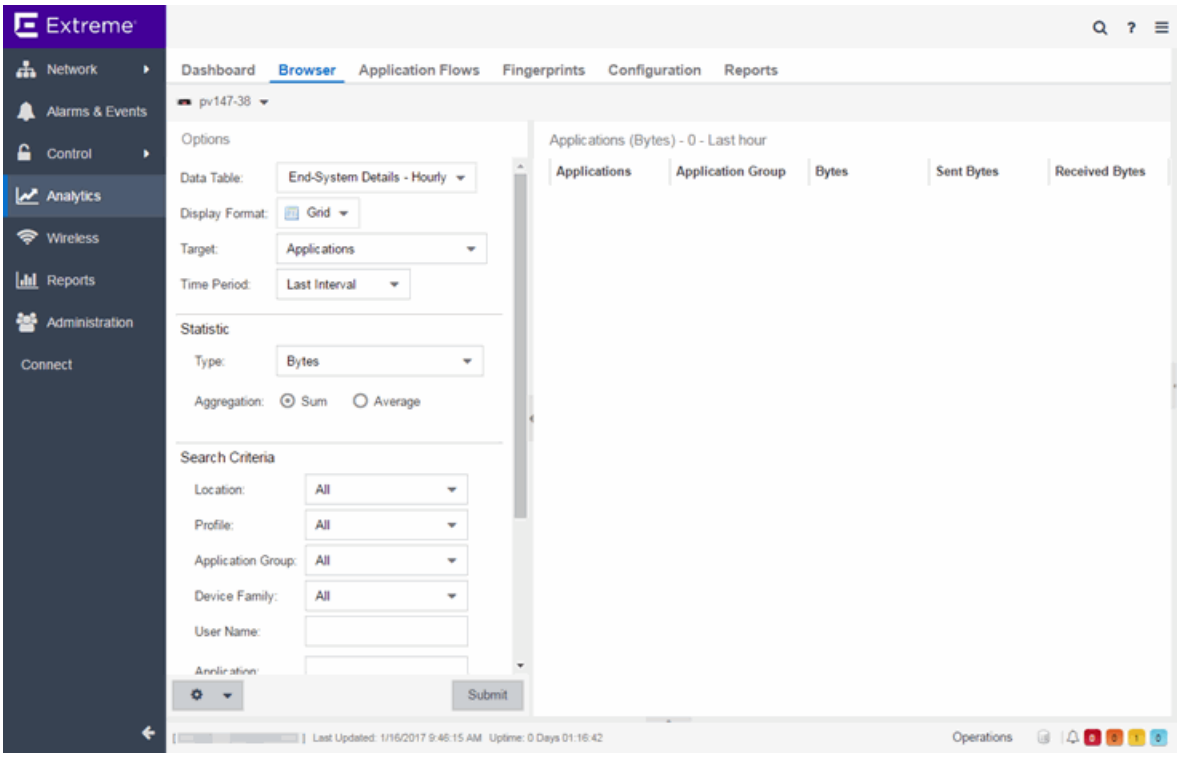
Overview

The Browser allows you to generate reports in several different formats using data based on selected options including a data target, statistic type, start time, and other search criteria.

For example, you can display application response time for the last hour or the last three days. You can view the results as a grid or a chart. You can filter the results to display data for a specific application or location.

If you have multiple Application Analytics engines, use the **Engine** drop-down menu to select an engine to use as the source for the report data. Then, select the desired options on the left side of the Browser view and click **Submit**. The report is displayed on the right side of the view. Click on an item in the report to view details or right-click an item to select from other focused reports.

After you have generated a report, use the **Gear** menu ( ) (at the bottom left of the options panel) to (Save) save it to the Report Designer to use as a custom component, ( ) bookmark the report, or ( ) export it as a CSV file.



Data Aggregation

Network data displayed in a report is aggregated from your network by the Application Analytics engine and sent to Extreme Management Center. The data gathering process begins with the Application Analytics engine, which monitors network activity on the switch or controller you configure using a traffic mirror and NetFlow or application telemetry. The traffic mirror gathers the first (N) packets of a flow to determine the application in use, while NetFlow (a flow-based data collection protocol) provides information about the amount of data sent and received for the application. The engine holds this information in its cache and transmits the aggregated data to Extreme Management Center every five minutes to update the High-Rate data table information and every hour to update the hourly data table information. Creating a report in the Applications Browser displays the information sent from the Application Analytics engine to Extreme Management Center based on the criteria you select.

NOTE: Information held in the Application Analytics engine's cache is not saved. Restarting the Application Analytics engine before the data in the memory cache is sent to Extreme Management Center results in the loss of that information.

Options

Following are definitions of the different options available when creating your custom query.

Data Table
: Select which type of network activity data to query. The correct data table to use depends on the nature of the report.

- End-System Details - Hourly — End-system data collected every hour. Used when data for a specific client or server is needed, or when the information requested is highly specific, for example top applications used by Android devices in the London location.
- Application Data - Hourly — Application data collected every hour. Used for higher level information, such as top applications during an hour.
- Application Data - High-Rate — Application data collected at a higher rate (every five minutes). Used for a more detailed picture of how traffic changes over time.
- Application Telemetry - Hourly — Application Telemetry flow data collected every hour.

Display Format
: Select the display format for the report: Grid, Chart Over Time, Word Cloud, Tree Map, or Bubble Map.

Target
: Network traffic information is collected on objects in your network called targets. Some targets are physical, such as clients and servers, and some are logical, such as applications. Select the type of target that you want information about. Available targets vary depending on the selected data table. If you want information on a specific target, specify that target in the Search Criteria options.

- Applications — An application in Application Analytics is identified through layer 7 analysis of network traffic. For example, an application can be identified as Facebook.
- Application/Client — Information about applications used by clients, or about clients using an application.
- Application/Device Family — Information about applications used by device families, or about device families using an application.

- Application/Interface — Information about the applications used by interfaces.
- Application/Profile — Information about applications used by profiles, or about profiles using an application.
- Application Groups — Application categories, such as Cloud Computing or Social Networking, which are implied by the application.
- Device Family — The kind of device determined for a client, such as Windows or iOS. Device information is only available for some network traffic.
- Interface/Applications — Information about interfaces used by applications.
- Application-Interface Pair/Client — Displays the applications and interfaces used by clients.
- Interface/Client — Information about the interfaces used by clients.
- Locations — Network locations are used by Application Analytics to identify the physical location for the client of an application flow. A network location is a set of IP address ranges that identify a portion of your network. Multiple locations can be created to identify different buildings, sites, or geographical areas of your network.
- Profiles — A profile assigned to a client. Profile information is only collected under certain circumstances.
- Threat — Displays a list of the threat classifications that occurred during the Time Period you select.
- Threat/Threat End-System Pair — Displays a list of the threat classifications broken down by the IP addresses of the end-systems involved in the flow (the trusted and untrusted hosts) that occurred during the Time Period you select.
- Clients — The end-point of a flow which has the client role for that connection.
- Servers — The end-point of a flow which has the server role for that connection.
- Total — The total values for all detected traffic for the interval used by the data table (hourly or high-rate).

Statistic

Statistics are quantitative data that can be collected for the selected target. Available statistics vary depending on the selected target. Select the desired statistic for the report:

- Bytes — The number of bytes transferred in both directions, between the client and the server. Also known as bandwidth.
- Flows — The number of NetFlow records sent by the switch to report the traffic between the client and the server.

- Application Response Time — The average amount of time for a server to respond to a request.
- Network Response Time — The average amount of time to create a connection.
- Received Bytes — The number of bytes received by clients. This may be an estimated number of bytes if you are using an Application Telemetry flow.
- Sent Bytes — The number of bytes sent by clients. This may be an estimated number of bytes if you are using an Application Telemetry flow.
- Inbound Flows — The number of NetFlow records sent by the switch to report the server-to-client traffic. This is a rough indication of the duration of client connections.
- Outbound Flows — The number of NetFlow records sent by the switch to report the client-to-server traffic. This is a rough indication of the duration of client connections.
- Clients — The number of unique clients that have been seen associated with the target.
- Servers — The number of unique servers that have been seen associated with the target.
- Application Count — The number of unique applications seen for the selected target.

For byte, flow, and application count statistics, if you select a time range that is larger that the interval, specify whether you want the data aggregated as a summation of all the values for that statistic or as an average of all the values for that statistic.

Start Time

Select the start time (duration) for the report: Last Interval, Today, Yesterday, Last 24 Hours, Last 3 Days, or Last Week. You can also specify a custom start time and end time for the report. The Last Interval is the most recent recorded data covering a time period determined by the selected Data Table.

Search Criteria

Defining search criteria allows you to further filter the report data. Available criteria will vary depending on the selected data table and target. If you select either of the Application Data tables, you can only filter based on the selected target. For example, if you select Locations as your target, you can only filter on defined locations. If you select the End-System Details data table, you can filter on additional criteria. For example, if you select Locations as your target, you can filter on defined locations as well as flows for iOS devices.

You can enter a partial term in the text field or use the SQL wildcard "%" (as a substitute for multiple characters) or "_" (as a substitute for a single character) for multiple matches. For example, for the Device Family name, you could enter "iPhone %" to match iPhone 3, 4, and 5.

NOTE: Values entered in the text fields that contain multiple, non-alphanumeric characters may cause issues with the returned results. If this happens, alternate values should be used.

- Location — Select a network location to match or select All. If a location has been added to a map, you will also see a selection for that map. If you select custom, you can enter a partial location name or use the SQL wildcard characters to match one or more locations.
- Profile — Select an Extreme Access Control profile to match or select All. If you select custom, you can enter a partial profile name or use the SQL wildcard characters to match one or more profiles. Profile information is only collected under certain circumstances.
- Application Group — Select an application group to match or select All. If you select custom, you can enter a partial application group name or use the SQL wildcard characters to match one or more groups.
- Device Family — Select the operating system family to match or select All. If you select custom, you can enter a partial device family name or use the SQL wildcard characters to match one or more families. Device information is only available for some network traffic.
- User Name — Enter a client's username to match. Username information is only available for some network traffic.
- Application — Enter an application name to match.
- Client — Enter a client's IP address or hostname to match.
- Engine — Select the Application Analytics engine for which you are generating the report.
- Limit — Select the number of results to return, for example, 10 clients.

Display Options

If you have selected Chart Over Time as your report display format, you can select whether to display the data as a line or an area, and also select the color to use in the chart.

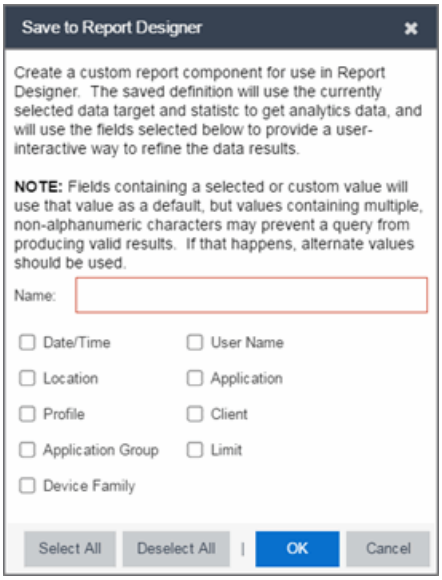
Bookmark

After you have generated a report, click the Gear menu ( ) in the lower left corner to save the options you have currently set. A new window opens for the current report with a link that can be bookmarked in your browser. You can then use the bookmark whenever you want the same search options.

Save to Report Designer

Click the Gear menu ( ) in the lower left corner to access the Save to Report Designer window. This window lets you save the currently defined report to use as a custom component in the Report Designer. The custom component uses the target, statistic, and start time currently defined in the Browser.

Enter a name for the custom component and select any search criteria that you want displayed in the component panel. The search criteria is displayed as fields in the component panel, providing a custom interface that lets you further refine report data. If no search criteria are selected, the saved component only uses the target, statistic, and start time definitions when requesting data, creating a view-only report.



Export to CSV

Click the Gear menu ( ) in the lower left corner and click ( ) to export the report data as a CSV file. The currently defined report opens in a spreadsheet, which can then be saved.

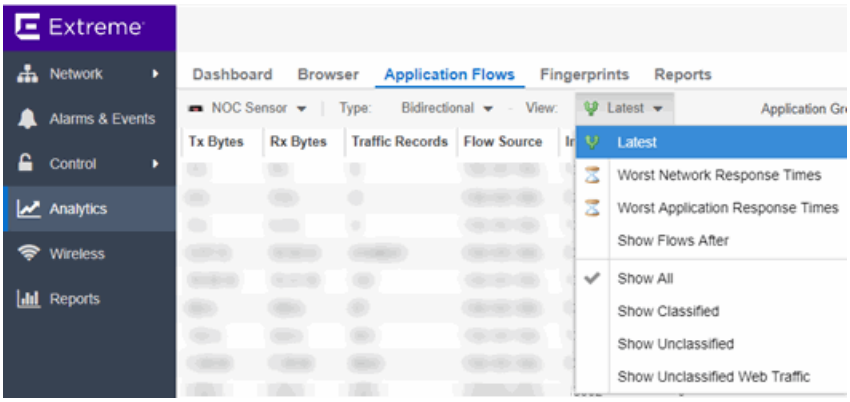
Related Information

- ExtremeAnalytics tab

ExtremeAnalytics Application Flows Tab Overview

The Application Flows table presents bidirectional flow data (aggregate flows) or unidirectional flow data (base flows).

If you have multiple Application Analytics engines, use the **Engine** menu to select an engine to use as the source for the flow data. Use the **Type** menu to select whether to display bidirectional or unidirectional flow data.



By default, the table displays the latest flows collected. Use the **View** menu to select different display options. The available options vary depending the flow type (bidirectional or unidirectional) selected.

- Latest — Displays the latest flows collected by the specified engine.
- Worst Network Response Times — Sorts the flows based on the worst TCP response time and displays the flows with the worst time at the top of the chart.
- Worst Application Response Times — Sorts the flows based on the worst application response time and displays the flows with the worst time at the top of the chart.
- Show Flows After — Allows you to select a start date and time for the flows displayed.
- Show All — Show all flows.
- Show Classified — Show only flows classified by an application fingerprint.
- Show Unclassified — Show only flows not classified by an application fingerprint.
- Show Unclassified Web Traffic — Show only web traffic that has not been classified by an application fingerprint.

Use the Application Group menu to filter the table by application group.

The Search field at the top right of the table can be used to filter specific flow information. For example, searching on "snmp" or "10.20.30.131/24" filters the table so only flow data related to SNMP or the given subnet is displayed. You can enter one or more filters simultaneously, separated by semicolons. Individual components of a filter is separated by commas. For complete instructions on how to use the Flow Search, rest your cursor on the Search field and read the tooltip (click on the "more" link in the tooltip). Press the Reset button at the bottom left of the window to clear the Search results and refresh the table.

You can also use the Search field to search for a specific application, user name, or IP address from your filtered results:

1. Click a user name or IP address from the filtered search results to launch PortView, which provides a detailed topology context for the user.
2. Enter meta= before the term for which you are searching includes all variations of that search term in the result set. For example, entering meta=extreme returns extremenetworks.com, www.extremenetworks.com, extreme.boston.com, and any other flows that include the word "extreme".
3. Right-click on a flow to access a menu of options including the ability to:
    - Add a new custom fingerprint based on the flow selected in the table.
    - Show all fingerprints associated with the application in the selected flow.
    - Create a UDP or TCP rule using the IP port.
    - Search Extreme Management Center maps for the selected flow client.
    - Open a Flow Details report for the selected flow (bidirectional flows only).
    - Access a variety of reports for the flow.

Use the Refresh drop-down menu at the top right of the window to specify an interval (in seconds) at which the flows data automatically refreshes. To stop auto refresh, select the Refresh Off option.

Bidirectional Flows

The Application Flows tab includes a table that displays bidirectional flow data stored in memory. It provides aggregated flow data for a given client, server, server port, application, and protocol. All matching flows are aggregated to show the flow count, total duration, amount of data transmitted, and additional

information. The bidirectional report presents flow data for real-time troubleshooting purposes, and is not designed for historical long-term flow collection.

Unidirectional Flows

The Application Flows tab includes a table that displays unidirectional flow data stored in memory. It provides the raw non-aggregated flow data received from the flow sensors on the network. It presents flow data for real-time troubleshooting purposes, and is not designed for historical long-term flow collection.

Report Features

The Application Flows table (bidirectional and unidirectional) includes the following features:

Create Policy Rule

Right-click on a flow in the table and select Create Policy Rule to open the Create Policy Rule window, which allows you to create a UDP or TCP rule using the IP port. You can also enter a Rule Name, if applicable. In the Policy Manager domain that you select, two services are created, each with their own rule: one that is server-based and one that is client-based. For example, for an SNMP flow, the following two rules would be created:

- Client Traffic - To Server Port: snmp[161]
- Server Traffic - From Server Port: snmp[161]

Optionally, the IP address of the flow can be used when creating the rule, which would add the IP address to the rule name, for example:

- Client Traffic - To Server Port: snmp[161](10.20.30.131)
- Server Traffic - From Server Port: snmp[161](10.20.30.131)

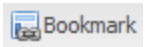
These are simplified rules that have no associated action and are not added to any roles. You must use Policy Manager to configure actions for the rules and assign them to the appropriate role.

Interactive Tables

Manipulate table data in several ways to customize the view for your own needs:

- Click on the column headings to **perform an ascending or descending sort** on the column data.
- **Hide or display different columns** by clicking on a column heading drop-down arrow and selecting the column options from the menu.
- **Filter data in each column** by clicking on a column heading drop-down arrow and using the Filters option on the menu.

The sort and filter functionality for these two tables behaves differently than for other Extreme Management Center tables. In these tables, Max Rows are considered for display, and then sorting and filtering is applied to these rows. In other tables, sorting and filtering is applied to the entire table, and then Max Rows of the result is displayed. For example, if the Max Rows value is set to 50 and you create a filter for a specific IP address, only those 50 rows will be filtered for the IP, not all the flows maintained in memory on the server.

Bookmark Report 

Use the **Bookmark** button to save the search, sort, and filtering options you have currently set. It opens a new window for the current report with a link that can be bookmarked in your browser. You can then use the bookmark whenever you want the same search, sort, and filtering options.

Related Information

- Application Analytics tab

ExtremeAnalytics Application Flows Tab Bidirectional Flow Table

This table displays bidirectional flow data that is stored in memory. It provides aggregated flow data for a given client, server, server port, application, and protocol. All matching flows are aggregated to show the flow count, total duration, amount of data transmitted, and additional information. The bidirectional report presents flow data for real-time troubleshooting purposes, and is not designed for historical long-term flow collection.

By default, the top 100 entries are displayed in the table. However, you can change this value using the Max Rows field at the bottom of the view.

Text at the bottom of the table shows:

- The CSV Export icon - allows you to save report data to a CSV file and to provide report data in table form
- Aggregate Flows data - uses an X number of days, hh:mm:ss format and includes Current Load and Peak Load calculations in flows per second

Following are definitions for the table columns:

Flow Summary
: Rest the cursor over the first column in the table and click the arrow to open the Flow Summary window. Flow summary information can include response times, Uniform Resource Identifier, and header data for the flow. In the Flow Summary window, use the Menu icon to access additional functionality, such as the ability to modify the application fingerprint or create a policy rule.

Flows
: The number of base flows included in the aggregate flow. Click on a link in the Flows column to open a Flow Details tab that displays the individual flows that contributed to the aggregate flow.

Client Address
: The IP address or hostname of the system where the flow originated. Click on the Client address link to open a PortView for the client (if it is in the database) or a PortView for the switch configured as the NetFlow sensor.

Server Address
The IP address or hostname of the server handling the flow.

Server Port
Either the TCP or UDP port on the server handling the flow.

Application
The name of the application as identified by the Application Analytics engine using the Fingerprint database.

Application Group
The flow application group to which the application belongs.

Application Info
Additional information about the flow provided by the Application Analytics engine. Hover over the flow and a table of the information displays.

Type
The content type of a flow, such as sound, video, or text. Click on the **Type** icon to open the flow's URI.

Network Response
The response time (in milliseconds) that it took for the TCP request to complete.

Application Response
The response time (in milliseconds) that it took the application request to complete.

Location
The name of the network location that matches the client's IP address.

Detailed Location
The client's switch IP and switch port (wired), or controller IP, AP, and SSID (wireless).

Device Family
The operating system family for the client end-system.

User
The username used when the client system connected.

Profile
The Extreme Management Center profile assigned to the client end-system.

Threat
: Indicates if the flow contains potential threat activity from IP addresses known to be suspicious. IP addresses can be flagged as suspicious for a variety of reasons, including forced IP anonymity through the use of a Tor exit node, being listed as a threat by the Emerging Threats project, or classified as suspicious by internet users.

Protocol
: The connection type protocol used by the flow.

Last Seen Time
: The last time a unidirectional (base) flow was aggregated into this bidirectional flow.

Duration
: The duration of a bidirectional (aggregate) flow is the sum of the durations of the unidirectional (base) flows that make up the bidirectional flow. The duration of a bidirectional flow may be greater than or less than the period of time indicated by the First Seen and Last Seen Time. This is because there may be times during that time period when no flow is active or when several flows are active at the same time.

NOTE: Bidirectional flows may be greater than the period of time between the First Seen and Last Seen Time columns because they display the sum of all flow records for a client and a server on a server port. For a flow that lasts for 60 seconds, there are two flow records (a client to server flow and a server to client flow), so the total duration may exceed 60 seconds. Multiple simultaneous connections from the client to the same server port (e.g. multiple browser windows open to a web-based email client) can also increase the duration.

Rate
: The average bandwidth for the flow based on the total flow duration. Because bandwidth calculations are based on the total duration (not on the First Seen and Last Seen Time), they represent the average throughput for each flow considered separately, not as an aggregate.

Tx Packets
: The number of packets transmitted for this flow. For flows collected via Application Telemetry, this number may be estimated.

Rx Packets
: The number of packets received for this flow. For flows collected via Application Telemetry, this number may be estimated.

Tx Bytes
: The number of bytes transmitted for this flow. For flows collected via Application Telemetry, this number may be estimated.

Rx Bytes
: The number of bytes received for this flow. For flows collected via Application Telemetry, this number may be estimated.

Traffic Records
: The number of records received in each flow.

Flow Source
: The IP address of the NetFlow source switch, Application Telemetry source switch, or wireless controller sending the NetFlow data to the NetFlow collector.

Input Interface
: The interface receiving the flow on the NetFlow sensor.

Output Interface
: The interface transmitting the flow on the NetFlow sensor.

Client TOS
: The DSCP (Diffserv Codepoint) value for the client to server flow. The TOS/DSCP value is used to configure quality of service for network traffic.

Server TOS
: The DSCP (Diffserv Codepoint) value for the server to client flow. The TOS/DSCP value is used to configure quality of service for network traffic.

TTL
: The TTL (IP Time to Live) value of the flow. The TTL field indicates the maximum number of router hops the packet can make before being discarded. The TTL field is set by the packet sender and reduced by every router on the route to its destination. When the value hits zero, the packet is dropped.

Related Information

- ExtremeAnalyticstab

ExtremeAnalytics Application Flows Tab Unidirectional Flow Table

This table displays unidirectional flow data stored in memory. It provides the raw, non-aggregated flow data received from the flow sensors on the network. It presents flow data for real-time troubleshooting purposes, and is not designed for historical long-term flow collection.

Hover over an application in the table to display switch data, which is an accumulation of multiple switches into single flow record, as well as the path that flow has taken.

By default, the top 100 entries are displayed in the table. However, you can change this value using the Max Rows field at the bottom of the view.

Text at the bottom of the table shows Base Flows, using X number of days, hh:mm:ss format, and including Current Load and Peak Load calculations in flows per second.

Following are definitions for the table columns:

Flow Summary
: Rest the cursor over the first column in the table and click the arrow to open the Flow Summary window for a specific flow. Flow summary information can include response times, Uniform Resource Identifier, and header data for the flow. In the Flow Summary window, use the Gear menu to access additional functionality such as the ability to modify the application fingerprint or create a policy rule.

Client/Server Flows
: Identifies whether the flow is a Client Flow or a Server Flow. The client/server direction of a flow is calculated by the Application Analytics engine. Hover over the icon to see a tooltip with more information.

Source Address
: The IP address or hostname of the system where the flow originated. Click on the Source address link to open a PortView for the client or server (if it is in the database) or a PortView for the switch configured as the NetFlow sensor.

Source Port
: Either the TCP or UDP port on the client/server handling the flow.

Destination Address
: The IP address or hostname of the system that received the flow.

Destination Port
: Either the TCP or UDP port on the system that received the flow.

Application
: The name of the application as identified by the Application Analytics engine using the Fingerprint database.

Application Group
: The flow application group to which the application belongs.

Application Info
: Additional information about the flow provided by the Application Analytics engine.

Type
: The content type of a flow, such as sound, video, or text. Click on the **Type** icon to open the flow's URI.

Network Response
: The response time (in milliseconds) that it took for the TCP request to complete.

Application Response
: The response time (in milliseconds) that it took the application request to complete.

Location
: The network location where the flow originated.

Detailed Location
: The client's switch IP and switch port (wired), or controller IP, AP, and SSID (wireless).

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

User
: The username used when the client system connected.

Profile
: The Extreme Access Control profile assigned to the client end-system.

Protocol
: The connection type protocol used by the flow.

Last Seen Time
: The last time the flow was seen.

Duration
: The amount of time that the flow was active.

Rate
: The average bandwidth for the flow based on the flow duration.

Packets
: The number of packets in this flow. For flows collected via Application Telemetry, this number may be estimated.

Bytes
: The number of bytes in this flow. For flows collected via Application Telemetry, this number may be estimated.

NetFlow Records
: The number of NetFlow records for this flow.

Flow Source
: The IP address of the NetFlow source switch, Application Telemetry source switch, or wireless controller sending the Flow data to the Flow collector.

Input Interface
: The interface receiving the flow on the Flow sensor.

Output Interface
: The interface transmitting the flow on the Flow sensor.

TOS
: The DSCP (Diffserv Codepoint) value for the flow. The TOS/DSCP value is used to configure quality of service for network traffic.

TTL
: The TTL (IP Time to Live) value of the flow. The TTL field indicates the maximum number of router hops the packet can make before being discarded. The TTL field is set by the packet sender and reduced by every router on the route to its destination. When the value hits zero, the packet is dropped.

Related Information

- ExtremeAnalytics tab

ExtremeAnalytics Fingerprints Overview

The Fingerprints view provides detailed information about fingerprints used by ExtremeAnalytics to identify application flows. A fingerprint is a description of a pattern of network traffic which can be used to identify an application. They can be created based on flow, application or application group,, or a destination address. For applications such as Facebook and Google, multiple fingerprints are included to capture the different ways these applications can be used.

Fingerprints are created and stored on the Extreme Management Center server. When a fingerprint is changed or enabled, a flag is raised on the Application Analyticsengine to show it needs enforcing. Access the Browser from the Extreme Management Center Analytics tab.

There are two types of fingerprints: system fingerprints and custom fingerprints.

System fingerprints are provided by Extreme Management Center. They cannot be deleted; however, they can be modified or disabled. When a system fingerprint is modified, it results in a new custom fingerprint that overrides the original system fingerprint.

Custom fingerprints are either new user-defined fingerprints or modifications of system fingerprints. Custom fingerprints can be deleted. If a custom fingerprint was overriding a system fingerprint, then deleting the custom fingerprint will reload the original system fingerprint.

Related Information

- ExtremeAnalytics tab

ExtremeAnalytics Custom Fingerprints

Custom fingerprints are either new user-defined fingerprints or modifications of system fingerprints. Custom fingerprints can be deleted. If a custom fingerprint was overriding a system fingerprint, then deleting the custom fingerprint will reload the original system fingerprint.

The Fingerprints view is divided into a left-panel tree and a table with six columns. The left-panel tree displays all the application groups and the fingerprints assigned to that group. The table on the right displays detailed information for each fingerprint. You can filter the information displayed in the table by selecting a single application group or fingerprint in the left-panel.

Fingerprint Table

The Fingerprint table displays detailed fingerprint information. Above the table, in the top left corner, is a Menu icon ≡, where you can access various system and fingerprint actions.

If you have multiple Application Analytics engines, an **Engine** menu is available that allows you to select an engine to use as the source for the fingerprint Matches data.

Use the **In Use** checkbox to filter the table to only show fingerprints that have had a match for the selected engine. Use the **Customized** checkbox to filter the table to display only custom fingerprints.

Menu

Use the **Menu icon** ≡ to access the following system and fingerprint actions. (You must have a fingerprint selected to enable the **Fingerprint** menu options.) Most of the options are also available by right-clicking on a fingerprint.

- Create Fingerprint — Add a new fingerprint.
- Modify Fingerprint — Change a fingerprint's description.
- Reset Fingerprint Counters — Reset the Matches counters.
- Delete Custom Fingerprint — Delete custom fingerprints, which can be identified by a ✓ in the Custom column.
- Fingerprint Definition — View the XML definition for a fingerprint.

Column Definitions

Following are definitions for the table columns. All columns are sortable in ascending and descending order and can be filtered by text or numeric values.

Application

Name of the application this fingerprint detects. Click on an **Application** link to view client, flow, and usage information for that specific application.

Fingerprint

Name of the fingerprint.

Confidence

Reliability of this fingerprint. Higher confidence fingerprints override lower confidence fingerprints when determining a match for a traffic flow. The values are from 1 to 100, with 100 being absolutely reliable.

Custom

A check mark ✔ indicates the fingerprint is a custom (user-defined) fingerprint. It is custom if it is a new fingerprint that has been added, a system fingerprint that has been modified, or a system fingerprint that has been disabled.

Application Group

The group this fingerprint's application belongs to. Application groups organize fingerprints into different types of applications such as Web applications or Business applications. You can sort the **Application Flows** view by application group, making it easier to view data for a specific type of flow. An application may only belong to one application group.

Matches

The total number of times a traffic flow has matched this fingerprint for the selected engine. A match is an occurrence of the Application Analytics engine making a final determination that a flow matches a fingerprint after all refinements are completed. The corresponding flow in the opposite direction, if there is one, is also matched. See Notes below.

NOTES:

- Matches are stored and displayed per engine. If you have multiple engines, use the **Engine** menu to select an engine to use as the source for the Hits and Matches data.
- If a flow generates hits on multiple fingerprints, and one fingerprint has a higher confidence than another fingerprint, a hit is counted for each fingerprint, but a match is only recorded for the final, highest confidence fingerprint.
- If you need to reset the Matches counters, use the **Reset Fingerprint Counters** option from the **Menu** icon (≡).

Type

The fingerprint type refers to how the fingerprint determines a match.

- FlexFire — These fingerprints execute specific matching algorithms encoded into the engine. Disabling the fingerprint disables the specific code that implements the fingerprint.
- PCRE — These fingerprints search using Perl Compatible Regular Expressions (PCRE).
- Port-based — These fingerprints search for traffic on a specific port (typically, server-only ports). These are very low-confidence fingerprints and are generally just used for wider coverage.
- Web-App Rule — These fingerprints search for a specific hostname in the URI of web requests.
- SSL Name — These fingerprints search for values in the SSL common name.
- Http Host — These fingerprints search for values in the HTTP hostname.
- Decoder — These fingerprints extract protocol metadata from a flow that is provided when we generate a match on that flow.
- General — Any fingerprint that isn't included in one of the other types. Typically, these fingerprints search for a straight pattern, or for a specific port and/or IP address with custom fingerprints (excluding custom Web-App Rule fingerprints).

Enabled

A ✔ indicates the fingerprint is enabled. When a fingerprint is enabled, it will be used to identify applications. When it is disabled, it will be ignored.

Last Modified

Date that the fingerprint was last modified.

Created
: Date that the fingerprint was created.

Description
: Description of the fingerprint.

Related Information

- ExtremeAnalytics tab

Delete Custom Fingerprints

ExtremeAnalytics uses fingerprints to identify to which application a network traffic flow belongs. A fingerprint is a description of a pattern of network traffic which can be used to identify an application. Extreme Management Center provides thousands of system fingerprints with the ExtremeAnalytics feature. In addition, you can modify these fingerprints and create new custom fingerprints.

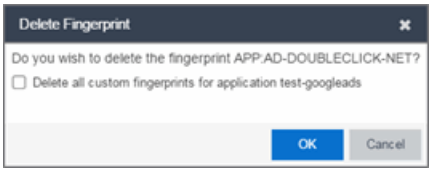
Deleting a Custom Fingerprint

Delete a custom fingerprint from the Fingerprints tab. A custom fingerprint is either a new user-defined fingerprint, a modification of a system fingerprint, or a disabled fingerprint. (Custom fingerprints can be identified by a ✔ in the Custom column.)

When you delete a custom fingerprint, it is removed entirely. If you delete a custom fingerprint overriding a system fingerprint, the original system fingerprint is reloaded. System fingerprints that have not been modified cannot be deleted, however, they can be disabled.

Use these steps to delete a custom fingerprint:

1. Select the **Analytics** tab in Extreme Management Center and then select the Fingerprints view
2. Right-click on the desired custom fingerprint in the Fingerprints table and select **Delete Custom Fingerprint**. The Delete Fingerprint window opens.



3. You can delete only the selected fingerprint or select the option to delete all custom fingerprints that match the application name of the selected fingerprint.
4. Click **OK**. If a custom fingerprint overrides a system fingerprint, then deleting the custom fingerprint reloads the original system fingerprint.
5. Enforce to push the change to your engines.

Related Information

- ExtremeAnalytics tab

Custom Fingerprint Examples

The Application Analytics feature uses fingerprints to identify to which application a network traffic flow belongs. A fingerprint is a description of a pattern of network traffic which can be used to identify an application. Extreme Management Center provides thousands of system fingerprints with the Application Analytics feature. In addition, you can create new custom fingerprints.

For additional information, see Getting Started with Application Analytics.

This Help topic provides examples of three different types of custom fingerprints you can create:

- Fingerprints Based on a Flow
- Fingerprints Based on an Application or Application Group
- Fingerprints Based on a Destination Address

For additional information, see Add and Modify Fingerprints.

Fingerprints Based on a Flow

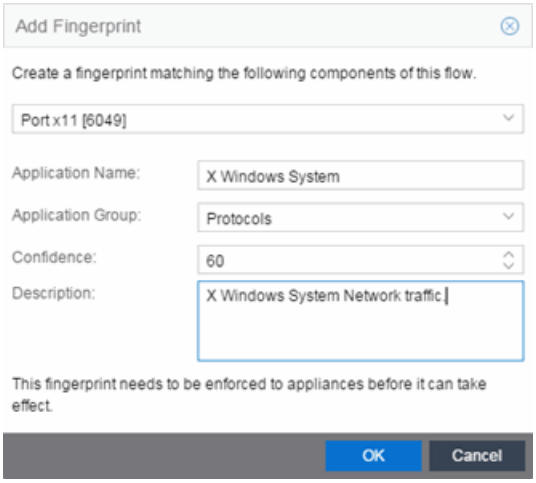
This example demonstrates how to create a custom fingerprint based on X Window System network traffic.

In the Extreme Management Center Flows table (with the Show Unclassified View selected) you notice several flows that had an X Window System source port 6049. Since these flows are not currently identified with a fingerprint, you can create a fingerprint for those flows based on the port that x11 traffic normally runs over.

Use the following steps to create the fingerprint.

1. Select the **Analytics** tab.
2. Select the **Application Flows** tab.
3. In the table, select the **Show Unclassified View**.
4. Right-click on a flow with the **x11 Source Port** and select **Fingerprints** > **Add Fingerprint**.

5. The Add Fingerprint window opens.



6. Use the drop-down list to select matching Portx11 [6049].
7. Set the Application Name to X Window System.
8. Set the Application Group to Protocols.
9. Set the Confidence level to 60 (the default). A fingerprint with a confidence higher than 60 can supersede this fingerprint, if it also matches the flow.
10. Click OK to create the fingerprint.
11. Enforce to push the new fingerprint to your engines.

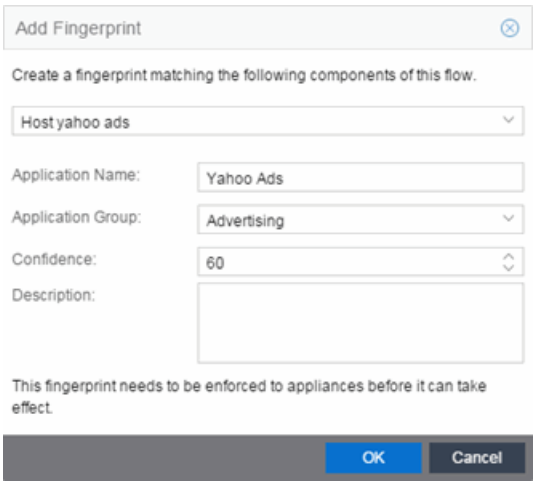
Fingerprints Based on an Application or Application Group

This example demonstrates how to create a fingerprint for some unclassified web traffic.

In the Extreme Management Center Application Flows table (with the Show Unclassified Web Traffic View selected) you noticed several flows for the "yahoo ads" application that are part of the Web Applications group. You want to create a fingerprint that provides an application and application group specifically for this traffic, instead of letting it default to the Web Applications group. The new fingerprint categorizes "yahoo ads" flows into the Yahoo Ads ld application and the Advertising application group.

Use the following steps to create the fingerprint.

1. Select the Analytics tab in Extreme Management Center.
2. Select the Application Flows tab.
3. In the table, select the **Show Unclassified Web Traffic View**.
4. Right-click on a flow with the yahoo ads application and select **Fingerprints** > **Add Fingerprint**.
5. The Add Fingerprint window opens.



6. Use the drop-down menu to select matching the "yahoo ads" host.
7. Set the **Application Name** to **Yahoo Ads**.
8. Set the **Application Group** to **Advertising**.
9. Set the **Confidence** level to **60** (the default). A fingerprint with a confidence higher than 60 can supersede this fingerprint, if it also matches the flow.
10. Click **OK** to create the fingerprint.
11. Enforce to push the new fingerprint to your engines.

Fingerprints Based on a Destination Address

In both of the previous examples, you created a new custom fingerprint to cover a case where no appropriate fingerprint existed. You may also want to create a new fingerprint for traffic flows already identified as one application, but should be categorized as something else.

For example, let's say you have a Git repository on your network. Git repositories (a source code management system used in software development) are

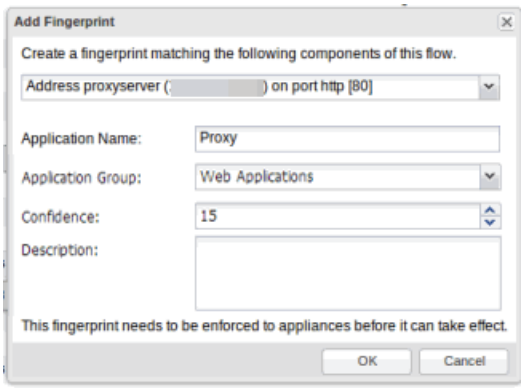
frequently accessed via SSH on port 22 (the standard TCP port assigned for SSH traffic). In this case, the SSH traffic flows is identified using the system SSH port-based fingerprint.

But what if you would like to more closely monitor who is accessing the Git repository? If you know you are running the Git server on a certain system (10.20.117.102 port 22, for our example), you can create a custom fingerprint to identify the Git traffic flows.

The fingerprint is based on one of the SSH flows using the IP address/port of the Git server and have a higher confidence than the system port-based fingerprint. The higher confidence fingerprint will override the lower confidence fingerprint when determining a match for the traffic flow.

Use the following steps to create the fingerprint.

1. Select the Analytics tab in Extreme Management Center.
2. Select the Application Flows tab.
3. In the table, right-click on an SSH port-based flow with the Git server destination address and select **Fingerprints** > **Add Fingerprint**.
4. The Add Fingerprint window opens.



5. Use the drop-down menu to select matching the Git server IP address and port.
6. Set the **Application Name** to **Git**.
7. Select an **Application Group** that makes the most sense for your network. It might be **Web Collaboration**, **Databases**, **Business Applications**, or **Storage**. You can also create a new **Application Group** using the **Create Custom Application Group** option available from the gear menu in the Fingerprint Details tab. (You would need to do this before you create the custom fingerprint.)

8. Set the Confidence level to 60, which is a higher confidence than the current fingerprint which is set at 10.
9. Click OK to create the fingerprint.
10. Enforce to push the new fingerprint to your engines.

Related Information

For information on related Application Analytics topics:

- Analytics Tab
- Add and Modify Fingerprints

Create Custom Fingerprints Based on Flow

The ExtremeAnalytics feature uses fingerprints to identify to which application a network traffic flow belongs. A fingerprint is a description of a pattern of network traffic which can be used to identify an application. Extreme Management Center provides thousands of system fingerprints with the ExtremeAnalytics feature. In addition, you can create new custom fingerprints.

Creating Fingerprints Based on a Flow

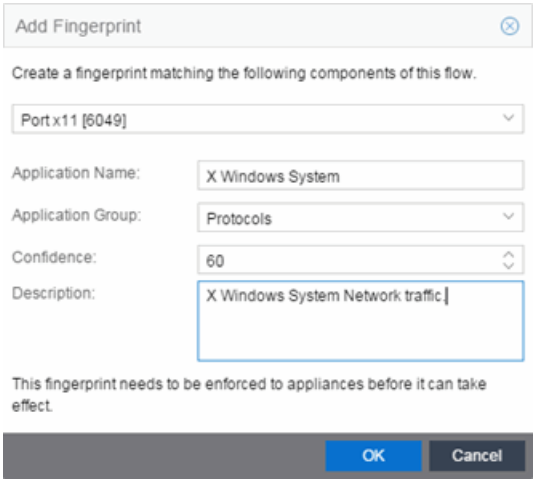
This example demonstrates how to create a custom fingerprint based on X Window System network traffic.

In the Extreme Management Center Flows table (with the Show Unclassified View selected) you notice several flows that had an X Window System source port 6049. Since these flows are not currently identified with a fingerprint, you can create a fingerprint for those flows based on the port that x11 traffic normally runs over.

Use the following steps to create the fingerprint.

1. Select the Analytics tab.
2. Select the Application Flows tab.
3. In the table, select the **Show Unclassified View**.
4. Right-click on a flow with the **x11 Source Port** and select **Fingerprints** > **Add Fingerprint**.

5. The Add Fingerprint window opens.



6. Use the drop-down list to select matching **Portx11 [6049]**.
7. Set the **Application Name** to **X Window System**.
8. Set the **Application Group** to **Protocols**.
9. Set the **Confidence** level to **60** (the default). A fingerprint with a confidence higher than 60 can supersede this fingerprint, if it also matches the flow.
10. Click **OK** to create the fingerprint.
11. Enforce to push the new fingerprint to your engines.

Related Information

- ExtremeAnalytics tab

Create Custom Fingerprints Based on Destination Address

The ExtremeAnalytics feature uses fingerprints to identify to which application a network traffic flow belongs. A fingerprint is a description of a pattern of network traffic which can be used to identify an application. Extreme Management Center provides thousands of system fingerprints with the ExtremeAnalytics feature. In addition, you can create new custom fingerprints.

Creating Fingerprints Based on a Destination Address

Often, you will create a new custom fingerprint to cover a case where no appropriate fingerprint existed. However, you may also want to create a new fingerprint for traffic flows already identified as one application, but should be categorized as something else.

For example, let's say you have a Git repository on your network. Git repositories (a source code management system used in software development) are frequently accessed via SSH on port 22 (the standard TCP port assigned for SSH traffic). In this case, the SSH traffic flows is identified using the system SSH port-based fingerprint.

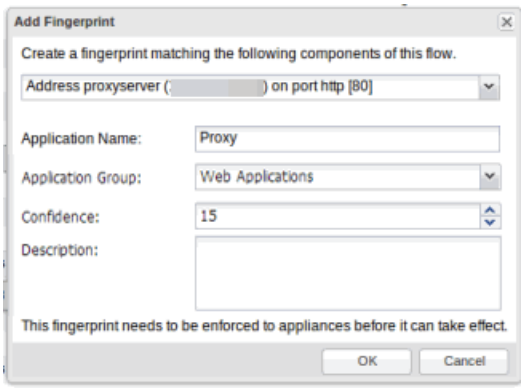
But what if you would like to more closely monitor who is accessing the Git repository? If you know you are running the Git server on a certain system (10.20.117.102 port 22, for our example), you can create a custom fingerprint to identify the Git traffic flows.

The fingerprint is based on one of the SSH flows using the IP address/port of the Git server and have a higher confidence than the system port-based fingerprint. The higher confidence fingerprint will override the lower confidence fingerprint when determining a match for the traffic flow.

Use the following steps to create the fingerprint.

1. Select the Analytics tab in Extreme Management Center.
2. Select the Application Flows tab.

3. In the table, right-click on an SSH port-based flow with the Git server destination address and select **Fingerprints** > **Add Fingerprint**.
4. The Add Fingerprint window opens.



5. Use the drop-down menu to select matching the Git server IP address and port.
6. Set the **Application Name** to **Git**.
7. Select an **Application Group** that makes the most sense for your network. It might be **Web Collaboration**, **Databases**, **Business Applications**, or **Storage**. You can also create a new **Application Group** using the **Create Custom Application Group** option available from the gear menu in the Fingerprint Details tab. (You would need to do this before you create the custom fingerprint.)
8. Set the **Confidence** level to **60**, which is a higher confidence than the current fingerprint which is set at 10.
9. Click **OK** to create the fingerprint.
10. Enforce to push the new fingerprint to your engines.

Related Information

- ExtremeAnalytics tab

Create Custom Fingerprints Based on Application or Application Group

The ExtremeAnalytics feature uses fingerprints to identify to which application a network traffic flow belongs. A fingerprint is a description of a pattern of network traffic which can be used to identify an application. Extreme Management Center provides thousands of system fingerprints with the ExtremeAnalytics feature. In addition, you can create new custom fingerprints.

Creating Fingerprints Based on an Application or Application Group

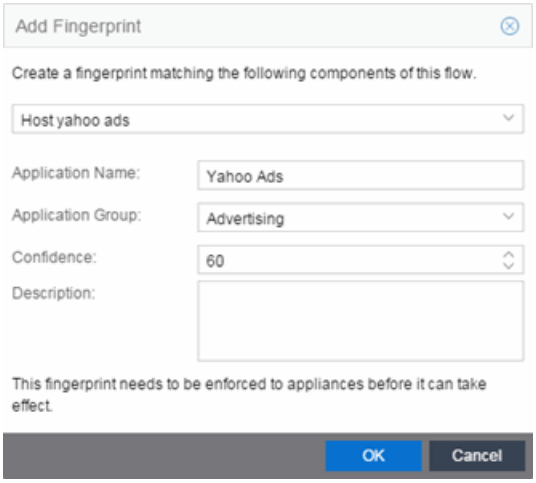
This example demonstrates how to create a fingerprint for some unclassified web traffic.

In the Extreme Management Center Application Flows table (with the Show Unclassified Web Traffic View selected), several flows for the "yahoo ads" application are part of the Web Applications group. The following instructions will allow you to create a fingerprint that provides an application and application group specifically for this traffic, instead of letting it default to the Web Applications group. The new fingerprint categorizes "yahoo ads" flows into the Yahoo Ads ld application and the Advertising application group.

Use the following steps to create the fingerprint.

1. Select the Analytics tab in Extreme Management Center.
2. Select the Application Flows tab.
3. In the table, select the Show Unclassified Web Traffic View.
4. Right-click on a flow with the yahoo ads application and select Fingerprints > Add Fingerprint.

5. The Add Fingerprint window opens.



6. Use the drop-down menu to select matching the "yahoo ads" host.
7. Set the **Application Name** to **Yahoo Ads**.
8. Set the **Application Group** to **Advertising**.
9. Set the **Confidence** level to **60** (the default). A fingerprint with a confidence higher than 60 can supersede this fingerprint, if it also matches the flow.
10. Click **OK** to create the fingerprint.
11. Enforce to push the new fingerprint to your engines.

Related Information

- ExtremeAnalytics tab

ExtremeAnalytics Configuration View

The Configuration view provides detailed information on the Application Analytics engines you configure. It also lets you add and enforce your engines, access engine reports and diagnostics, and configure network locations. You must be a member of an authorization group assigned the Extreme Management Center Application Analytics Read/Write Access capability to view the Configuration tab.

Use the left panel in the Configuration view to access various engine administrative options and reports. This Help topic provides information on the following operations available in the left panel:

- Overview
- Locations
- Fingerprints
- Licenses
- Status
- Configuration
- Appliances

Overview

View a list of configured engines and their engine statistics. Access the following options from the Menu icon (≡) (for some of the options, you must first select an engine in the list):

Add Engine
Adds a new Application Analyticsengine to Extreme Management Center.

Delete Engine
Delete the selected engine.

Enforce Engine
Enforce the selected engine.

Poll Engine
Poll the selected engine.

Restart Collector Process
Restarts the Application Analytics engine's collector process.

Enforce All Engines —
Enforces all of the Application Analytics engines added to Extreme Management Center.

Locations

View a list of network locations. Use the Add Location, Add Address, Edit and Remove buttons to configure and manage these locations (for some of the options, you must first select an engine in the list). Click the Menu icon (≡) to export to or import from a CSV file.

Fingerprints

View data for the application fingerprints in use.

Fingerprints

Statistic	Value
Fingerprints found	9927
Fingerprints customized	36
Fingerprints enabled	9921
Fingerprints utilizing PCREs	2565
Applications	8085
Feature: Decoder fingerprints	18
Feature: FlexFire fingerprints	209
Feature: HTTP Host fingerprints	42
Feature: Port-Based fingerprints	5693
Feature: WebAppRule fingerprints	2502
Feature: General fingerprints	1463

Use the Menu icon (≡) to access the following system fingerprint actions:

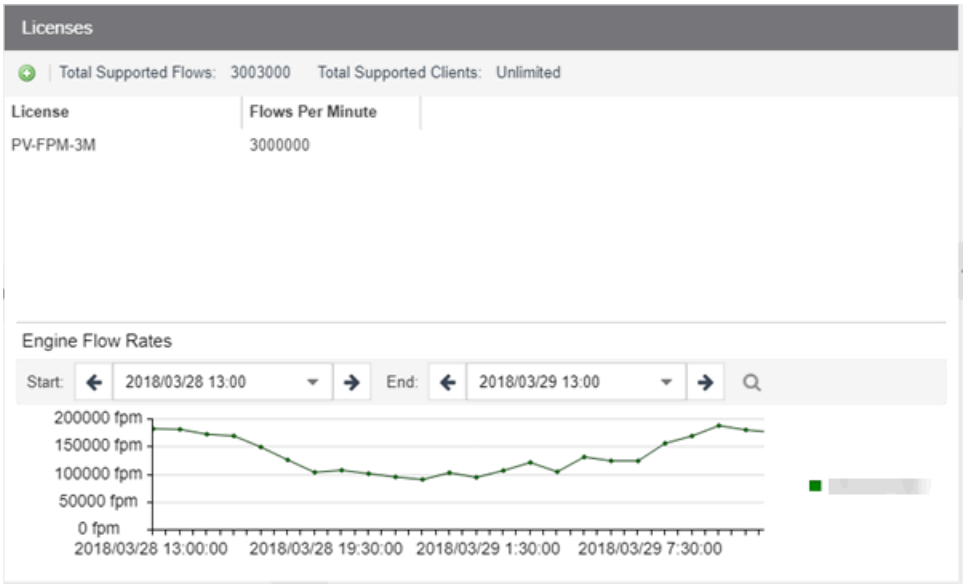
Update Fingerprints
Perform a manual one-time update of the fingerprint database.

Fingerprint Update Settings

Schedule fingerprint updates to be performed automatically on a daily or weekly basis.

Licenses

The Licenses window displays data for each license listed, including Total Supported Flows, Total Supported Clients and Flows per Minute. Click the Add button ( ) to add an Application Analytics flow capacity increase license.



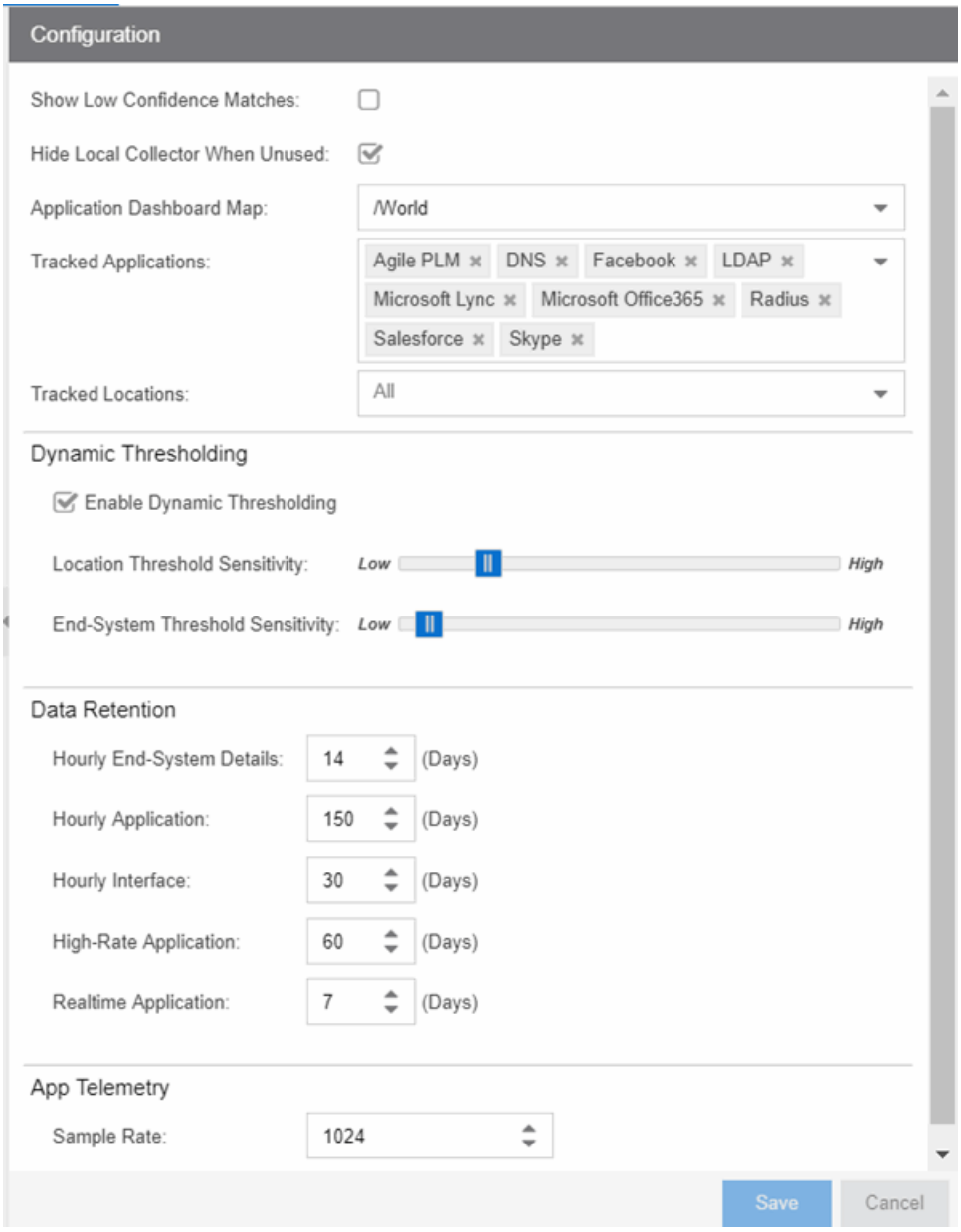
You can select the duration for the Engine Flow Rates report by specifying the start time and end time for the report. Click on Help Tips to read a description of the various sections.

Status

View a collection of Application Analytics system statistics, including Disk Usage and Approximate Row Counts, as well as Distinct Locations, Device Families, and Profiles.

Configuration

Use the Configuration window to configure the application information displayed in the Analytics tab.



Show Low Confidence Matches

Check the box to display flows for which Extreme Management Center has low confidence.

Hide Local Collector When Unused

Check the box to hide local collector information when not in use.

Application Dashboard Map

Select from the drop-down menu the map from which to draw application dashboard data.

Tracked Applications

Select the applications to track in the Analytics tab.

Tracked Locations

Select the locations to track in the Analytics tab.

Dynamic Thresholding

The Dynamic Thresholding section of the window allows you to indicate whether to enable dynamic threshold functionality for the Network Service and Tracked Applications dashboards.

When this functionality is enabled, the expected range for application response time is calculated based on past observed response times and a dynamic threshold is assigned. An alarm occurs when any network service or tracked application has a response time measured above its dynamic threshold.

The sliders allow you to adjust the sensitivity of the dynamic threshold by increasing or decreasing the size of the expected response time range. Selecting a lower sensitivity means more time is required for an alarm to occur. Alarms are displayed on the Alarms & Events > Alarms tab.

Data Retention

Use this section of the tab to configure the amount of time Extreme Management Center saves flow data.

App Telemetry

This section allows you to configure the default sample rate ExtremeAnalytics uses when configuring ExtremeXOS devices on which Application Telemetry is enabled.

Engines

View engine status information, configure web credentials, and configure advanced options for an individual engine.

Status

View engine status including flow collector, application sensor, CPU and memory, flow sources, and diagnostic information. Click on Help Tips to read a description of the various reports.

Web Credentials

Configure web credentials for an engine

Configuration

The Advanced Configuration panel lets you configure advanced options for the selected Application Analyticsengine:

- Set privacy levels.
- Add and enforce Engines.
- Enable Extreme Access Control Integration.
- Add advanced configuration properties.
- Enable sensor modules and sensor module logging.
- Add or remove devices as Application Telemetry flow sources.

Related Information

- ExtremeAnalytics tab
- Advanced Configuration View
- Add or Enforce Engines in Configuration View
- Add or Remove Devices as Application Telemetry Sources

ExtremeAnalytics Reports

The **Analytics** tab lets you view and customize ExtremeAnalytics reports and application flow data, as well as manage and configure your Application Analytics engines.

NOTE: ExtremeAnalytics reports and application flow data is not available unless an Application Analytics engine is configured and you are a member of an authorization group assigned the Extreme Management Center ExtremeAnalytics Read Access or Read/Write Access capability.

Reports

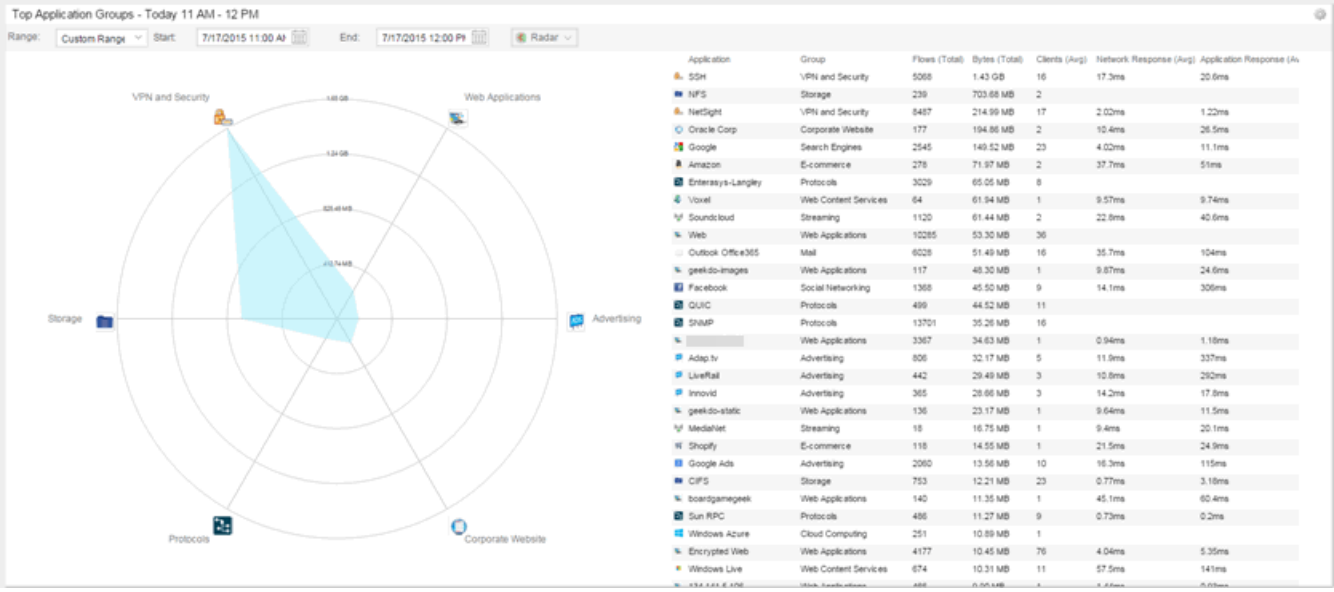
In the **Reports** tab, you can access a selection of reports that provide detailed information on application usage on your network, as well as network activity statistics based on application, user name, client, and location. For many of the reports, you can click on an item in the report to view details or right-click an item to select from other focused reports.

If you have multiple Application Analytics engines, use the **Engine** drop-down menu to select an engine to use as the source for the report data. Then use the Report drop-down menu to the right to access the different reports:

- Analytics Events
- Bandwidth for a Client Over Time
- Interface Top Applications Tree Map
- Locations Using Most Bandwidth
- Most Popular Applications
- Most Used Applications for a Client
- Most Used Applications for a User Name
- Network Activity by Location
- Network Activity by Client
- Network Activity by Application
- Slowest Application by Location
- Top Applications Group Radar

- Top Applications Radar
- Top Applications Tree Map
- Top Clients by Interface
- Top Interfaces by Application
- Top N Applications
- Top N Clients
- Top N Servers

In most of the reports, use the **Gear** button (on the right side of the view) to display a **Start Time** option that allows you to change the length of the reporting period displayed. Depending on the report, you can also change the type and/or format of the data reported, and the number of results to return.



Some of the reports are based on a specific object (target), such as a user name, client, application, or location. In those reports, enter the required information and then click the **Submit** button to generate the report. You can enter a partial value in the text field or use the SQL wildcard "%" (as a substitute for multiple characters) or "_" (as a substitute for a single character) to generate a report with multiple matches.

NOTE: Values entered in the text fields that contain multiple, non-alphanumeric characters may cause issues with the returned results. If this happens, use alternate values.

Related Information

- ExtremeAnalytics tab

ExtremeAnalytics Report Descriptions

The **Analytics** tab lets you view and customize ExtremeAnalytics reports and application flow data, as well as manage and configure your Application Analytics engines.

NOTE: ExtremeAnalytics reports and application flow data is not available unless an Application Analytics engine is configured and you are a member of an authorization group assigned the Extreme Management Center ExtremeAnalytics Read Access or Read/Write Access capability.

Report Descriptions

In the Reports tab, you can access a selection of reports that provide detailed information on application usage on your network, as well as network activity statistics based on application, user name, client, and location. For many of the reports, you can click on an item in the report to view details or right-click an item to select from other focused reports.

If you have multiple Application Analytics engines, use the **Engine** drop-down menu to select an engine to use as the source for the report data. Then use the Report drop-down menu to the right to access the different reports:

- Analytics Events
- Bandwidth for a Client Over Time
- Interface Top Applications
- Locations Using Most Bandwidth
- Most Popular Applications
- Most Used Applications for a Client
- Most Used Applications for a User Name
- Network Activity by Location
- Network Activity by Client
- Network Activity by Application
- Slowest Application by Location
- Top Applications Group Radar

- Top Applications Radar
- Top Applications Tree Map
- Top Applications for Interface
- Top Clients by Interface
- Top Interfaces by Application
- Top N Applications
- Top N Clients
- Top N Servers

Analytics Events

This report displays the event log filtered to show only the events related to ExtremeAnalytics.

Bandwidth for a Client Over Time

This report displays the bandwidth used by the specified client, provided as a line chart showing average bytes used over time. Enter a client's IP address or hostname and then click the **Submit** button to generate the report.

Interface Top Applications Treemap

This report displays the top applications for the top switch interfaces (devices) with application telemetry enabled.

NOTE: You need to first enable the application telemetry feature on ExtremeXOS switches from the **Analytics > Configuration** tab.

Locations Using the Most Bandwidth

This report displays the network locations with the highest bandwidth, provided as a bubble map.

Most Popular Applications

This report displays the applications used the most, based on the number of unique client IP addresses associated with them. Click on an application name to open a report showing the top clients for that application. Click on a client from the report to display an End-System Applications Summary for that client

Most Used Applications for a Client

This report displays the applications used the most by the specified client, based on bandwidth. Enter a client's IP address or hostname and then click the **Submit** button to generate the report.

Most Used Applications for a User Name

This report displays the applications used the most by the specified user, based on bandwidth. Enter a client's user name and then click the **Submit** button to generate the report.

Network Activity by Location

This report displays network traffic statistics and application and network response time for each network location.

Network Activity by Client

This report displays network traffic statistics for the specified client. Enter a client's IP address or hostname and then click the **Submit** button to generate the report.

Network Activity by Application

This report displays network traffic statistics for the specified application. Enter an application name and then click the **Submit** button to generate the report.

Slowest Applications by Location

This report displays the applications with the highest application response times for the specified location. Select a network location from the drop-down menu to match or select All and then click the **Submit** button to generate the report. If a location has been added to a map, you also see a selection for that map. If you select custom, you can enter a partial location name or use the SQL wildcard characters to match one or more locations.

Top Applications Group Radar

In the **Top Applications Group Radar** report, the info bar provides an overview of application group usage in a radar format. Use the **Start** calendar to select the start date and time and the format to display.

Top Applications Radar

In the **Top Applications Radar** report, the info bar provides an overview of application usage in a radar format. Use the **Start** calendar to select the start date and time and the format to display.

Top Applications TreeMap

This report displays hierarchical data on application bandwidth usage, grouped by application group and displayed in sets of colored nested rectangles. This design allows you to easily see patterns of bandwidth usage that might otherwise be difficult to spot. Click on an application group to zoom in and view data for that group. Hover over an application cell to view bandwidth for a particular application. Right-click on an application cell to access additional reports for that application.

Use the **Gear** button to change the start date and time to display. Set the scale to Linear to view the data scaled proportionately; set the scale to Log to make smaller rectangles of data more visible. Use the combo box to change how the data is displayed: by bandwidth, client count, or flow count.

Top Applications for Interface

This report displays the top applications for a specified interface (device) with application telemetry enabled (wildcards allowed).

NOTE: You need to first enable the application telemetry feature on ExtremeXOS switches from the **Analytics > Configuration** tab.

Top Clients by Interface

This report displays the top clients for a specified switch interface (device) with application telemetry enabled (wildcards allowed).

NOTE: You need to first enable the application telemetry feature on ExtremeXOS switches from the **Analytics > Configuration** tab.

Top Interfaces by Application

This report displays the top interfaces (device) for a specified application with application telemetry enabled (wildcards allowed).

NOTE: You need to first enable the application telemetry feature on ExtremeXOS switches from the **Analytics > Configuration** tab.

Top N Applications

This report displays application information, provided as a bar graph. Use the fields in the menu to configure the information displayed in the report:

- **Top N** — Select the number of clients displayed in the chart.
- **Start** — Select the start date and time.
- **# Hours** — Select the amount of time for which data is displayed from the date and time selected in **Start**.
- **Statistic** — Select the statistic by which the top clients are listed.
  - Bandwidth
  - Flows
  - Client Count

Top N Clients

This report displays client information, provided as a bar graph. Use the fields in the menu to configure the information displayed in the report:

- **Top N** — Select the number of clients displayed in the chart.
- **Start** — Select the start date and time.
- **# Hours** — Select the amount of time for which data is displayed from the date and time selected in **Start**.
- **Statistic** — Select the statistic by which the top clients are listed.
  - Bandwidth
  - Flows
  - Number of Applications

Top N Servers

This report displays server information, provided as a bar graph. Use the fields in the menu to configure the information displayed in the report:

- **Top N** — Select the number of clients displayed in the chart.
- **Start** — Select the start date and time.

- # Hours — Select the amount of time for which data is displayed from the date and time selected in Start.
- Statistic — Select the statistic by which the top clients are listed.
  - Bandwidth
  - Flows

Related Information

- ExtremeAnalytics tab

Add and Modify Fingerprints

Application Analytics uses fingerprints to identify to which application a network traffic flow belongs. A fingerprint is a description of a pattern of network traffic which can be used to identify an application. Extreme Management Center provides thousands of system fingerprints with the Application Analytics feature. In addition, you can modify these fingerprints and create new custom fingerprints.

For additional information, see Getting Started with Application Analytics.

This Help topic provides the following information:

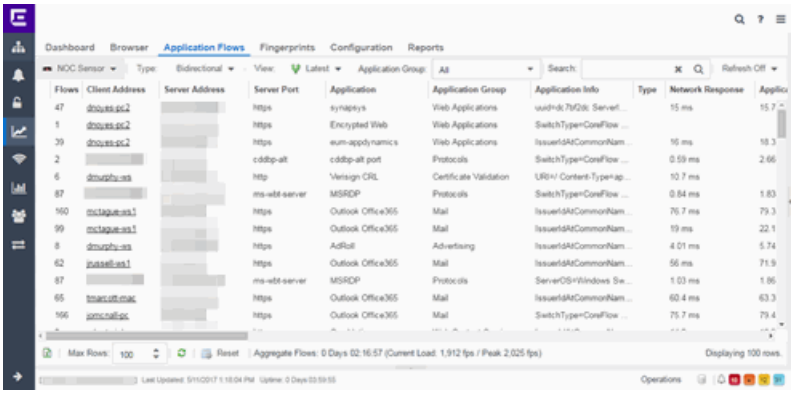
- Adding a Fingerprint
- Modifying a Fingerprint
- Enabling or Disabling a Fingerprint
- Deleting a Custom Fingerprint
- Updating Fingerprints

In order to add and modify fingerprints, you must be a member of an authorization group assigned the Extreme Management Center Application Analytics Read/Write Access capability.

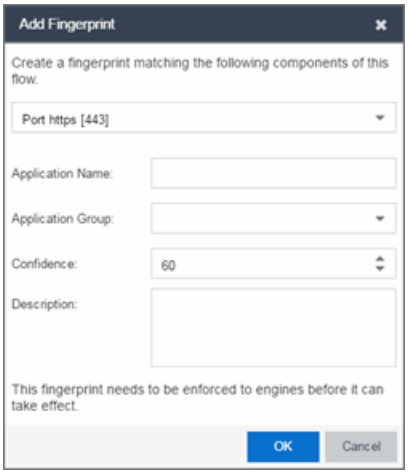
Adding a Fingerprint

Use the following steps to add a new custom fingerprint based on an existing flow in the Applications Flows view.

1. Select the **Analytics** tab and then select the **Application Flows** view.



2. Select the flow in the table that you want to base your new custom fingerprint on.
3. Right-click on the flow and select the Fingerprints > Add Fingerprint option. The Add Fingerprint window opens.



4. Use the drop-down list to select the flow components on which to base the fingerprint. The options vary depending on the fingerprint you initially selected.
    - Port <port number> — Creates a fingerprint that identifies traffic either coming from or going to the specified port.
    - Address <IP address> on port <port number> — Creates a fingerprint that identifies traffic either coming from or going to this IP address on the specified port.
    - Address <IP address> with mask on port <port number> — Creates a fingerprint that identifies traffic either coming from or going to the specified subnet on the specified port. For example, an IP address of 192.168.0.0 with a

mask of 16 would result in all traffic either coming from or going to the 192.168 subnet on the specified port to be identified by the fingerprint.

- Host <host name> — Creates a fingerprint that identifies a specific hostname in the URI of web traffic.
- HTTP Header — Creates a fingerprint that identifies traffic containing specified HTTP header information, if HTTP header information is included in the flow's metadata.

Note that there may be two port number or IP address options listed: one for the flow's source port/IP address and one for the flow's destination port/IP address.

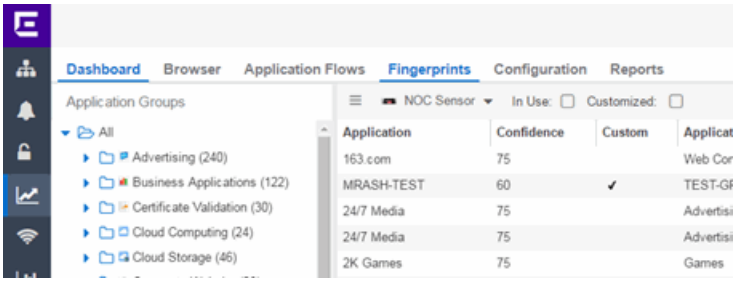
5. If you selected an IP address with mask option, you need to specify a subnet of IP addresses. Enter the IP CIDR mask, which is a mask on the flow IP, with 0-32 for IPv4 and 0-128 for IPv6.
6. Enter the name of the application for which the fingerprint is defined.
7. Use the drop-down menu to select the application group to which the application belongs. If none of the existing groups are appropriate, you can enter a new group name and the new group is automatically created.
8. Select the fingerprint's confidence level. The confidence level defines the reliability of this fingerprint. Higher confidence fingerprints override lower confidence fingerprints, if multiple fingerprints match a flow. Values are 1-100, with 100 being absolutely reliable.
9. Enter a description of the fingerprint, if desired.
10. Click Save. The new fingerprint is created on the Extreme Management Center server.
11. Enforce to push the new fingerprint to your engines.

TIP: You can also create a custom fingerprint from the Fingerprints tab. Click the Menu icon and select Create Fingerprint. The Add Fingerprint window opens where you can select all the flow components you want for the fingerprint. The new fingerprint is not based on an existing fingerprint and you need to enter values for all required fields such as IP or Hostname, Application Name, and Application Group. The new fingerprint must be enforced to engines before it can take effect.

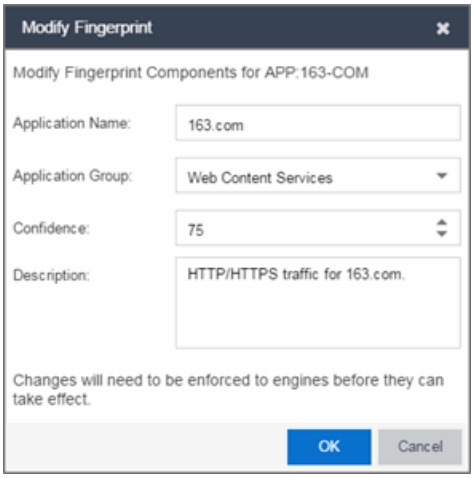
Modifying a Fingerprint

Modify a fingerprint's application name, application group, confidence level, and description from the Fingerprints tab.

1. Select the **Analytics** > **Fingerprints** tab.



2. Right-click on the desired fingerprint and select **Modify Fingerprint** from the menu. The Modify Fingerprint window opens.



3. Make the desired changes:
   - **Application Name** — The name of the application that the fingerprint detects. If you change the application name, you are prompted to select whether to change the application name for only the currently selected fingerprint or for all fingerprints that have that same application name.

     NOTE: If you change both the Application Name and Application Group:
     If the new **Application Name** matches an existing name, the application group

changes to the new group for all fingerprints with that new name, regardless of whether you choose to change the name for only the selected fingerprint or for all fingerprints with that name.

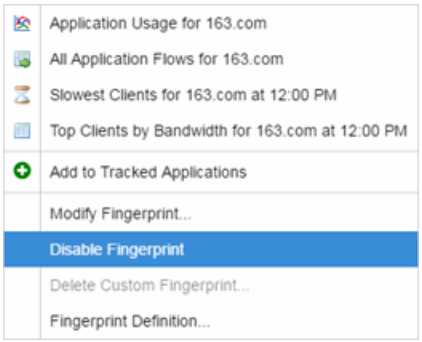
- Application Group — Organizes fingerprints into different types of applications such as Web applications or Business applications. You can sort the Application Flows view by application group, making it easier to view the data. If you change the application group for a fingerprint, it changes the group for all fingerprints with that same application name. If none of the existing groups are appropriate, you can create a new group by entering a new group name.
- Confidence — Defines the reliability of this fingerprint. Higher confidence fingerprints override lower confidence fingerprints, if multiple fingerprints match a flow. Values are 1-100, with 100 being absolutely reliable. The confidence level only applies to the currently selected fingerprint.
- Description — A description of the fingerprint. The description only applies to the currently selected fingerprint.

4. Click OK.
5. Enforce to push the change to your engines.

Enabling or Disabling a Fingerprint

Enable or disable a fingerprint from the Fingerprints tab. When a fingerprint is enabled, it is used to identify applications. When it is disabled, it is ignored.

1. Select the Analytics > Fingerprints tab.
2. Right-click on the desired fingerprint in the Fingerprints table and select either Enable Fingerprint or Disable Fingerprint.



3. Enforce to push the change to your engines.

NOTE: If you disable a system fingerprint, it becomes a custom fingerprint. If you then enable the fingerprint, it remains a custom fingerprint. Deleting the custom fingerprint reloads the original system fingerprint.

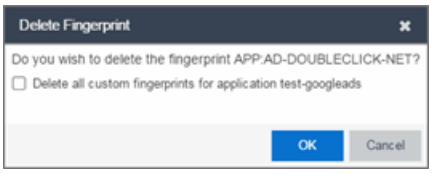
Deleting a Custom Fingerprint

Delete a custom fingerprint from the Fingerprints tab. A custom fingerprint is either a new user-defined fingerprint, a modification of a system fingerprint, or a disabled fingerprint. (Custom fingerprints can be identified by a ✔ in the Custom column.)

When you delete a custom fingerprint, it is removed entirely. If you delete a custom fingerprint overriding a system fingerprint, the original system fingerprint is reloaded. System fingerprints that have not been modified cannot be deleted, however, they can be disabled.

Use these steps to delete a custom fingerprint:

1. Select the Analytics tab in Extreme Management Center and then select the Fingerprints view
2. Right-click on the desired fingerprint in the Fingerprints table and select Delete Custom Fingerprint. The Delete Fingerprint window opens.



3. You can delete only the selected fingerprint or select the option to delete all custom fingerprints that match the application name of the selected fingerprint.
4. Click OK. If a custom fingerprint overrides a system fingerprint, then deleting the custom fingerprint reloads the original system fingerprint.
5. Enforce to push the change to your engines.

Updating Fingerprints

New and updated fingerprints are provided via a fingerprint update website. Perform a one-time manual update of the fingerprint database or configure a

scheduled update to be performed automatically from the Configuration tab. Custom fingerprints are not overwritten when an update is performed.

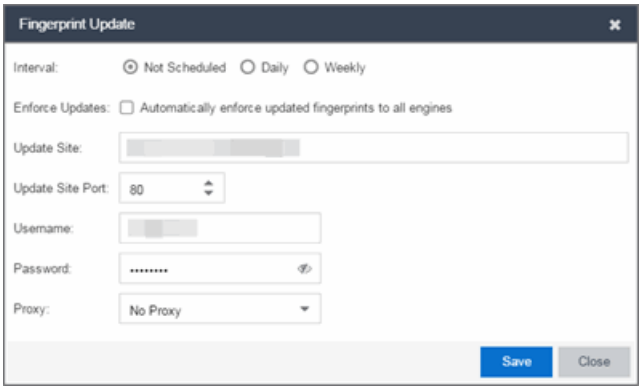
When a fingerprint update is performed, the fingerprint update server is checked for newer fingerprints than what is available on the Extreme Management Center server. If there are newer fingerprints, they are downloaded, and the fingerprint definitions are updated with any new fingerprint definition files. You need to enforce your engines following an update to push the updated fingerprints to the engines.

Perform a Fingerprint Update

Perform a manual one-time update of the fingerprint database. To access the update website, you need to create an Extranet account at ExtremeNetworks.com and define a username and password for the account. You need the username and password in order to perform updates.

1. Select the **Analytics** tab in Extreme Management Center and then select the **Configurations** view.
2. In the left-panel tree, expand the System folder and select **Fingerprints**.
3. Click the **Menu** icon (≡) and select **Update Fingerprints**. If you have already configured your Fingerprint Update settings, the update is performed immediately.

   If you have not configured your settings, the Fingerprint Update window opens.



   a. Leave the **Interval** selection as **Not Scheduled**.
   b. Select the **Enforce Updates** checkbox to automatically update fingerprints on all engines. Not selecting this checkbox requires you to update each engine manually.

c. The **Update Site** field displays the default path to the official fingerprint update site. Typically, this field does change unless for security reasons the system does not have access to the internet and an internal update site must be used.

d. The **Update Site Port** is the port on the update site to which the update connects. The port cannot be changed unless you are using a custom update site.

e. Enter the credentials used to access the fingerprint update website. These are the username and password credentials you defined when you created an Extranet account at ExtremeNetworks.com.

f. If your network is protected by a firewall, you need to configure proxy server settings to use when accessing the website. In the **Proxy** field, select **Use Proxy** or **Use Proxy with Credentials** and enter your proxy server address and port ID. (Consult your network administrator for this information.) If your proxy server requires authentication, enter the proxy username and password credentials. The credentials you add here must match the credentials configured on the proxy server.

g. Click **Save**. The Fingerprint Update is performed immediately.

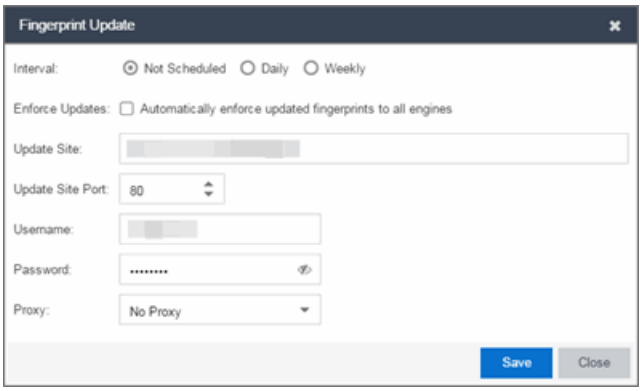
4. If you did not select the **Enforce Updates** checkbox, enforce to push the changes to your engines when the update is complete.

Schedule Fingerprint Updates

You can schedule fingerprint updates performed automatically on a daily or weekly basis.

To access the update website, you need to create an Extranet account at ExtremeNetworks.com and define a username and password for the account. You need the username and password in order to schedule updates.

1. Select the **Analytics** tab in Extreme Management Center and then select the Configuration view.
2. In the left-panel tree, expand the System folder and select **Fingerprints**.
3. Click on the **Menu** icon (≡) and select Fingerprint Update Settings. The Fingerprint Update window opens.



4. Select the update interval which defines how frequently the update is performed: Daily or Weekly.
5. If you have selected Weekly, select the day of the week you would like the update performed.
6. Enter the scheduled time you would like the update performed.
7. Select the Enforce Updates checkbox to automatically update fingerprints on all engines. Not selecting this checkbox requires you to update each engine manually.
8. The Update Site field displays the default path to the official fingerprint update site. Typically, this field does not change unless for security reasons the system does not have access to the internet and an internal update site must be used.
9. The Update Site Port is the port on the update site to which the update connects. The port cannot be changed unless you are using a custom update site.
10. Enter the credentials used to access the fingerprint update website. These are the username and password credentials you defined when you created an Extranet account at ExtremeNetworks.com.
11. If your network is protected by a firewall, configure proxy server settings to use when accessing the website. In the Proxy field, select Use Proxy or Use Proxy with Credentials and enter your proxy server address and port ID. (Consult your network administrator for this information.) If your proxy server requires authentication, enter the proxy username and password credentials. The credentials you add here must match the credentials configured on the proxy server.
12. Click Save.
13. If you did not select the Enforce Updates checkbox, enforce to push the changes to your engines when the update is complete.

Related Information

For information on related Application Analytics topics:

- Analytics Tab
- Custom Fingerprint Examples

Add Fingerprints

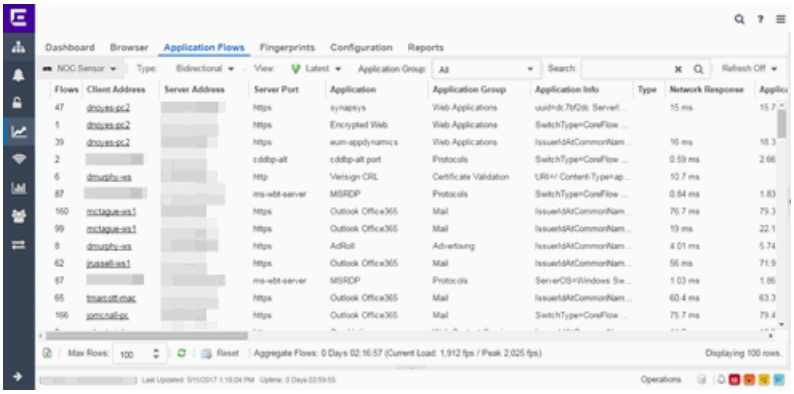
ExtremeAnalytics uses fingerprints to identify to which application a network traffic flow belongs. A fingerprint is a description of a pattern of network traffic which can be used to identify an application. Extreme Management Center provides thousands of system fingerprints with the ExtremeAnalytics feature. In addition, you can modify these fingerprints and create new custom fingerprints.

In order to add and modify fingerprints, you must be a member of an authorization group assigned the Extreme Management Center Application Analytics Read/Write Access capability.

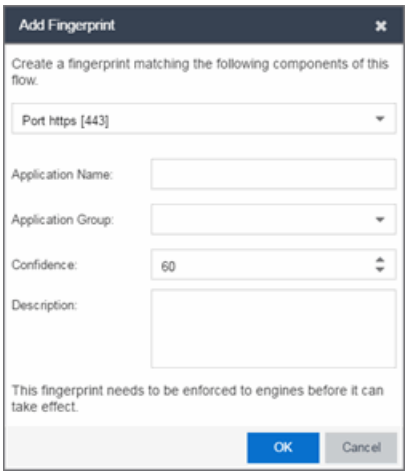
Add a Fingerprint

Use the following steps to add a new custom fingerprint based on an existing flow in the Applications Flows view. You can also create a new fingerprint based on an application or application group, or on a destination address.

1. Click **Analytics > Application Flows** view.



2. Select the flow in the table that you want to base your new custom fingerprint on.
3. Right-click on the flow and select the **Fingerprints** > **Add Fingerprint** option. The Add Fingerprint window opens.



4. Use the drop-down list to select the flow components on which to base the fingerprint. The options vary depending on the fingerprint you initially selected.
    - Port <port number> — Creates a fingerprint that identifies traffic either coming from or going to the specified port.
    - Address <IP address> on port <port number> — Creates a fingerprint that identifies traffic either coming from or going to this IP address on the specified port.
    - Address <IP address> with mask on port <port number> — Creates a fingerprint that identifies traffic either coming from or going to the specified subnet on the specified port. For example, an IP address of 192.168.0.0 with a mask of 16 would result in all traffic either coming from or going to the 192.168 subnet on the specified port to be identified by the fingerprint.
    - Host <host name> — Creates a fingerprint that identifies a specific hostname in the URI of web traffic.
    - HTTP Header — Creates a fingerprint that identifies traffic containing specified HTTP header information, if HTTP header information is included in the flow's metadata.

    Note that there may be two port number or IP address options listed: one for the flow's source port/IP address and one for the flow's destination port/IP address.

5. If you selected an IP address with mask option, you need to specify a subnet of IP addresses. Enter the IP CIDR mask, which is a mask on the flow IP, with 0-32 for IPv4 and 0-128 for IPv6.

6. Enter the name of the application for which the fingerprint is defined.
7. Use the drop-down menu to select the application group to which the application belongs. If none of the existing groups are appropriate, you can enter a new group name and the new group is automatically created.
8. Select the fingerprint's confidence level. The confidence level defines the reliability of this fingerprint. Higher confidence fingerprints override lower confidence fingerprints, if multiple fingerprints match a flow. Values are 1-100, with 100 being absolutely reliable.
9. Enter a description of the fingerprint, if desired.
10. Click **Save**. The new fingerprint is created on the Extreme Management Center server.
11. Enforce to push the new fingerprint to your engines.

TIP: You can also create a custom fingerprint from the Fingerprints tab. Click the **Menu** icon and select **Create Fingerprint**. The Add Fingerprint window opens where you can select all the flow components you want for the fingerprint. The new fingerprint is not based on an existing fingerprint and you need to enter values for all required fields such as **IP** or **Hostname**, **Application Name**, and **Application Group**. The new fingerprint must be enforced to engines before it can take effect.

Related Information

- ExtremeAnalytics tab

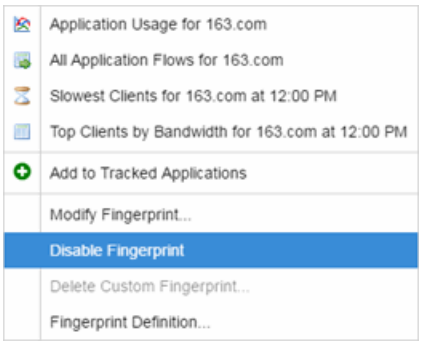
Enable or Disable Fingerprints

ExtremeAnalytics uses fingerprints to identify to which application a network traffic flow belongs. A fingerprint is a description of a pattern of network traffic which can be used to identify an application. Extreme Management Center provides thousands of system fingerprints with the ExtremeAnalytics feature. In addition, you can modify these fingerprints and create new custom fingerprints.

Enabling or Disabling a Fingerprint

Enable or disable a fingerprint from the Fingerprints tab. When a fingerprint is enabled, it is used to identify applications. When it is disabled, it is ignored.

1. Select the **Analytics** > **Fingerprints** tab.
2. Right-click on the desired fingerprint in the Fingerprints table and select either **Enable Fingerprint** or **Disable Fingerprint**.



3. Enforce to push the change to your engines.

NOTE: If you disable a system fingerprint, it becomes a custom fingerprint. If you then enable the fingerprint, it remains a custom fingerprint. Deleting the custom fingerprint reloads the original system fingerprint.

Related Information

- ExtremeAnalytics tab

Modify Fingerprints

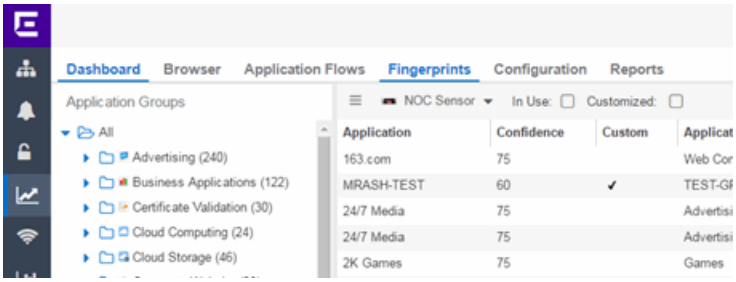
ExtremeAnalytics uses fingerprints to identify to which application a network traffic flow belongs. A fingerprint is a description of a pattern of network traffic which can be used to identify an application. Extreme Management Center provides thousands of system fingerprints with the ExtremeAnalytics feature. In addition, you can modify these fingerprints and create new custom fingerprints.

In order to add and modify fingerprints, you must be a member of an authorization group assigned the Extreme Management Center Application Analytics Read/Write Access capability.

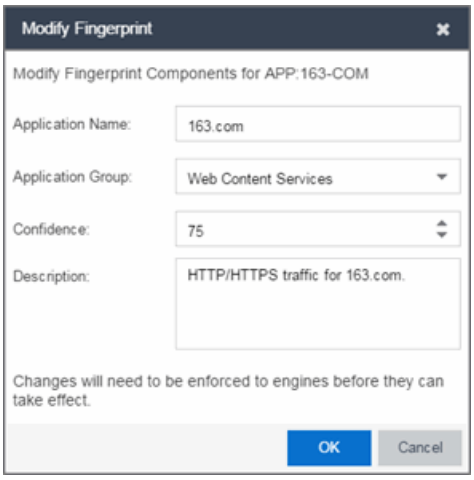
Modifying a Fingerprint

Modify a fingerprint's application name, application group, confidence level, and description from the Fingerprints tab.

1. Select the **Analytics** > **Fingerprints** tab.



2. Right-click on the desired fingerprint and select **Modify Fingerprint** from the menu. The Modify Fingerprint window opens.



3. Make the desired changes:
    - Application Name — The name of the application that the fingerprint detects. If you change the application name, you are prompted to select whether to change the application name for only the currently selected fingerprint or for all fingerprints that have that same application name.

      NOTE: If you change both the Application Name and Application Group:
      If the new Application Name matches an existing name, the application group changes to the new group for all fingerprints with that new name, regardless of whether you choose to change the name for only the selected fingerprint or for all fingerprints with that name.
    - Application Group — Organizes fingerprints into different types of applications such as Web applications or Business applications. You can sort the Application Flows view by application group, making it easier to view the data. If you change the application group for a fingerprint, it changes the group for all fingerprints with that same application name. If none of the existing groups are appropriate, you can create a new group by entering a new group name.
    - Confidence — Defines the reliability of this fingerprint. Higher confidence fingerprints override lower confidence fingerprints, if multiple fingerprints match a flow. Values are 1-100, with 100 being absolutely reliable. The confidence level only applies to the currently selected fingerprint.
    - Description — A description of the fingerprint. The description only applies to the currently selected fingerprint.
4. Click OK.

5. Enforce to push the change to your engines.

Related Information

- ExtremeAnalytics tab

Update Fingerprints

ExtremeAnalytics uses fingerprints to identify to which application a network traffic flow belongs. A fingerprint is a description of a pattern of network traffic which can be used to identify an application. Extreme Management Center provides thousands of system fingerprints with the ExtremeAnalytics feature. In addition, you can modify these fingerprints and create new custom fingerprints.

In order to add and modify fingerprints, you must be a member of an authorization group assigned the Extreme Management Center ExtremeAnalytics Read/Write Access capability.

Updating Fingerprints

New and updated fingerprints are provided via a fingerprint update website. Perform a one-time manual update of the fingerprint database or configure a scheduled update to be performed automatically from the Configuration tab. Custom fingerprints are not overwritten when an update is performed.

When a fingerprint update is performed, the fingerprint update server is checked for newer fingerprints than what is available on the Extreme Management Center server. If there are newer fingerprints, they are downloaded, and the fingerprint definitions are updated with any new fingerprint definition files. You need to enforce your engines following an update to push the updated fingerprints to the engines.

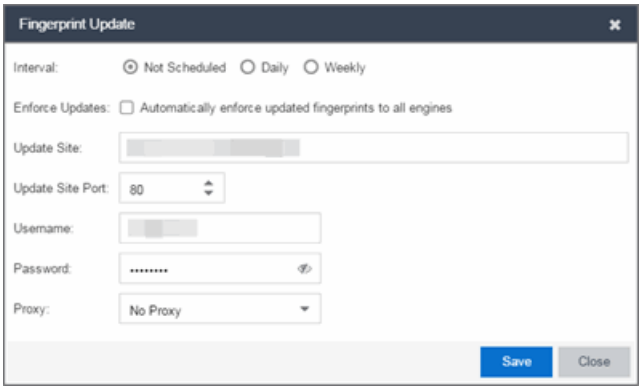
Perform a Fingerprint Update

Perform a manual one-time update of the fingerprint database. To access the update website, you need to create an Extranet account at ExtremeNetworks.com and define a username and password for the account. You need the username and password in order to perform updates.

1. Select the **Analytics** tab in Extreme Management Center and then select the **Configurations** view.
2. In the left-panel tree, expand the System folder and select **Fingerprints**.

3. Click the **Menu** icon (≡) and select **Update Fingerprints**. If you have already configured your Fingerprint Update settings, the update is performed immediately.

   If you have not configured your settings, the Fingerprint Update window opens.



   a. Leave the **Interval** selection as **Not Scheduled**.
   b. Select the **Enforce Updates** checkbox to automatically update fingerprints on all engines. Not selecting this checkbox requires you to update each engine manually.
   c. The **Update Site** field displays the default path to the official fingerprint update site. Typically, this field does change unless for security reasons the system does not have access to the internet and an internal update site must be used.
   d. The **Update Site Port** is the port on the update site to which the update connects. The port cannot be changed unless you are using a custom update site.
   e. Enter the credentials used to access the fingerprint update website. These are the username and password credentials you defined when you created an Extranet account at ExtremeNetworks.com.
   f. If your network is protected by a firewall, you need to configure proxy server settings to use when accessing the website. In the **Proxy** field, select **Use Proxy** or **Use Proxy with Credentials** and enter your proxy server address and port ID. (Consult your network administrator for this information.) If your proxy server requires authentication, enter the proxy username and password credentials. The credentials you add here must match the credentials configured on the proxy server.
   g. Click **Save**. The Fingerprint Update is performed immediately.

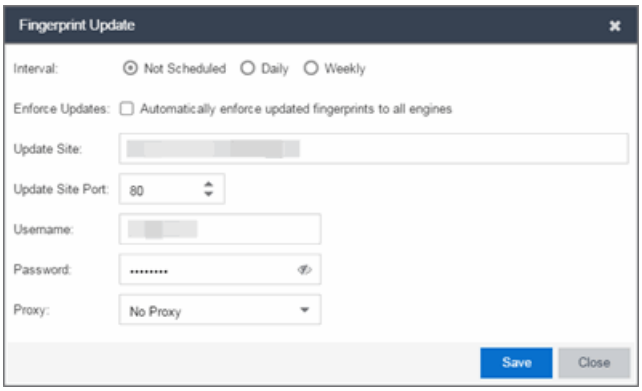
4. If you did not select the **Enforce Updates** checkbox, enforce to push the changes to your engines when the update is complete.

Schedule Fingerprint Updates

You can schedule fingerprint updates performed automatically on a daily or weekly basis.

To access the update website, you need to create an Extranet account at ExtremeNetworks.com and define a username and password for the account. You need the username and password in order to schedule updates.

1. Select the **Analytics** tab in Extreme Management Center and then select the Configuration view.
2. In the left-panel tree, expand the System folder and select **Fingerprints**.
3. Click on the **Menu** icon (≡) and select Fingerprint Update Settings. The Fingerprint Update window opens.



4. Select the update interval which defines how frequently the update is performed: **Daily** or **Weekly**.
5. If you have selected **Weekly**, select the day of the week you would like the update performed.
6. Enter the scheduled time you would like the update performed.
7. Select the **Enforce Updates** checkbox to automatically update fingerprints on all engines. Not selecting this checkbox requires you to update each engine manually.
8. The **Update Site** field displays the default path to the official fingerprint update site. Typically, this field does not change unless for security reasons the system does not have access to the internet and an internal update site must be used.

9. The **Update Site Port** is the port on the update site to which the update connects. The port cannot be changed unless you are using a custom update site.
10. Enter the credentials used to access the fingerprint update website. These are the username and password credentials you defined when you created an Extranet account at ExtremeNetworks.com.
11. If your network is protected by a firewall, configure proxy server settings to use when accessing the website. In the **Proxy** field, select **Use Proxy** or **Use Proxy with Credentials** and enter your proxy server address and port ID. (Consult your network administrator for this information.) If your proxy server requires authentication, enter the proxy username and password credentials. The credentials you add here must match the credentials configured on the proxy server.
12. Click **Save**.
13. If you did not select the **Enforce Updates** checkbox, enforce to push the changes to your engines when the update is complete.

Related Information

- ExtremeAnalytics tab

Custom Fingerprint Examples

The Application Analytics feature uses fingerprints to identify to which application a network traffic flow belongs. A fingerprint is a description of a pattern of network traffic which can be used to identify an application. Extreme Management Center provides thousands of system fingerprints with the Application Analytics feature. In addition, you can create new custom fingerprints.

For additional information, see Getting Started with Application Analytics.

This Help topic provides examples of three different types of custom fingerprints you can create:

- Fingerprints Based on a Flow
- Fingerprints Based on an Application or Application Group
- Fingerprints Based on a Destination Address

For additional information, see Add and Modify Fingerprints.

Fingerprints Based on a Flow

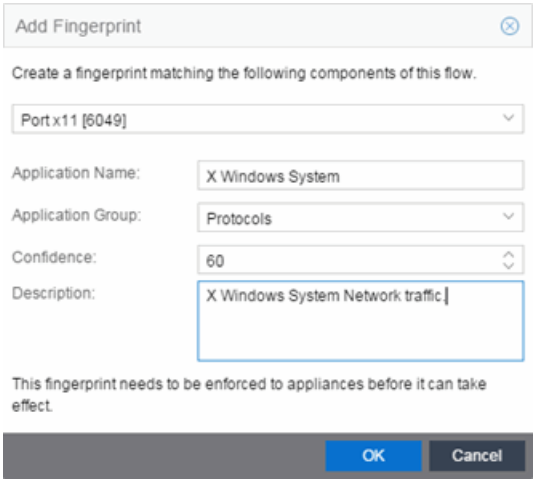
This example demonstrates how to create a custom fingerprint based on X Window System network traffic.

In the Extreme Management Center Flows table (with the Show Unclassified View selected) you notice several flows that had an X Window System source port 6049. Since these flows are not currently identified with a fingerprint, you can create a fingerprint for those flows based on the port that x11 traffic normally runs over.

Use the following steps to create the fingerprint.

1. Select the **Analytics** tab.
2. Select the **Application Flows** tab.
3. In the table, select the **Show Unclassified View**.
4. Right-click on a flow with the **x11 Source Port** and select **Fingerprints** > **Add Fingerprint**.

5. The Add Fingerprint window opens.



6. Use the drop-down list to select matching Portx11 [6049].
7. Set the Application Name to X Window System.
8. Set the Application Group to Protocols.
9. Set the Confidence level to 60 (the default). A fingerprint with a confidence higher than 60 can supersede this fingerprint, if it also matches the flow.
10. Click OK to create the fingerprint.
11. Enforce to push the new fingerprint to your engines.

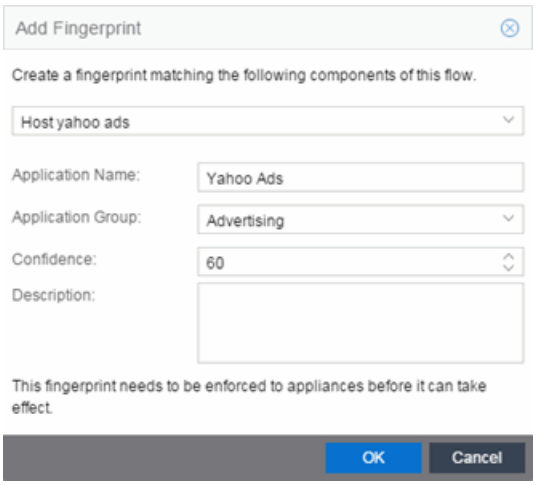
Fingerprints Based on an Application or Application Group

This example demonstrates how to create a fingerprint for some unclassified web traffic.

In the Extreme Management Center Application Flows table (with the Show Unclassified Web Traffic View selected) you noticed several flows for the "yahoo ads" application that are part of the Web Applications group. You want to create a fingerprint that provides an application and application group specifically for this traffic, instead of letting it default to the Web Applications group. The new fingerprint categorizes "yahoo ads" flows into the Yahoo Ads ld application and the Advertising application group.

Use the following steps to create the fingerprint.

1. Select the Analytics tab in Extreme Management Center.
2. Select the Application Flows tab.
3. In the table, select the **Show Unclassified Web Traffic View**.
4. Right-click on a flow with the yahoo ads application and select **Fingerprints** > **Add Fingerprint**.
5. The Add Fingerprint window opens.



6. Use the drop-down menu to select matching the "yahoo ads" host.
7. Set the **Application Name** to **Yahoo Ads**.
8. Set the **Application Group** to **Advertising**.
9. Set the **Confidence** level to **60** (the default). A fingerprint with a confidence higher than 60 can supersede this fingerprint, if it also matches the flow.
10. Click **OK** to create the fingerprint.
11. Enforce to push the new fingerprint to your engines.

Fingerprints Based on a Destination Address

In both of the previous examples, you created a new custom fingerprint to cover a case where no appropriate fingerprint existed. You may also want to create a new fingerprint for traffic flows already identified as one application, but should be categorized as something else.

For example, let's say you have a Git repository on your network. Git repositories (a source code management system used in software development) are

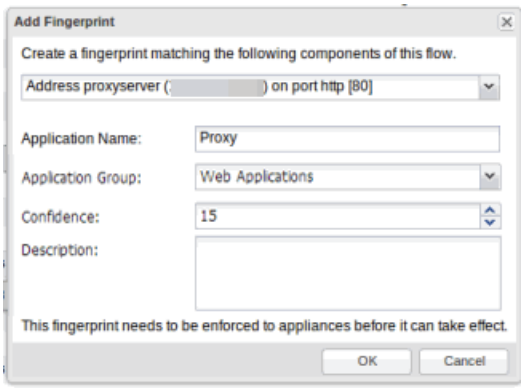
frequently accessed via SSH on port 22 (the standard TCP port assigned for SSH traffic). In this case, the SSH traffic flows is identified using the system SSH port-based fingerprint.

But what if you would like to more closely monitor who is accessing the Git repository? If you know you are running the Git server on a certain system (10.20.117.102 port 22, for our example), you can create a custom fingerprint to identify the Git traffic flows.

The fingerprint is based on one of the SSH flows using the IP address/port of the Git server and have a higher confidence than the system port-based fingerprint. The higher confidence fingerprint will override the lower confidence fingerprint when determining a match for the traffic flow.

Use the following steps to create the fingerprint.

1. Select the Analytics tab in Extreme Management Center.
2. Select the Application Flows tab.
3. In the table, right-click on an SSH port-based flow with the Git server destination address and select **Fingerprints** > **Add Fingerprint**.
4. The Add Fingerprint window opens.



5. Use the drop-down menu to select matching the Git server IP address and port.
6. Set the **Application Name** to **Git**.
7. Select an **Application Group** that makes the most sense for your network. It might be **Web Collaboration**, **Databases**, **Business Applications**, or **Storage**. You can also create a new **Application Group** using the **Create Custom Application Group** option available from the gear menu in the Fingerprint Details tab. (You would need to do this before you create the custom fingerprint.)

8. Set the Confidence level to 60, which is a higher confidence than the current fingerprint which is set at 10.
9. Click OK to create the fingerprint.
10. Enforce to push the new fingerprint to your engines.

Related Information

For information on related Application Analytics topics:

- Analytics Tab
- Add and Modify Fingerprints

How to Deploy ExtremeAnalytics in an MSP or MSSP Environment

This Help topic presents instructions for deploying ExtremeAnalytics within an MSP (Managed Service Provider) or MSSP (Managed Security Service Provider) environment. It includes the following information:

Configuring Extreme Management Center Behind a NAT Router

If the Extreme Management Center server is located behind a NAT (Network Address Translation) router, use the following steps to add an entry to the nat_config.txt file that defines the real IP address for the Extreme Management Center server. This allows the Extreme Management Center server to convert the NAT IP address received in the Application Analytics engine response to the real IP address used by the Extreme Management Center server. Not adding the real IP address for the Extreme Management Center server to the nat_config.txt file results in the Application Analytics engine incorrectly displaying a state of IMPARED (orange) rather than UP (green).

NOTE: The text in the nat_config.text file refers to a remote IP address and a local IP address. For this configuration, the NAT IP address is the remote IP address and the real IP address is the local IP address.

1. On the Extreme Management Center server, add the following entry to the `<install directory>/appdata/nat_config.txt` file.
   `<NAT IP address>=<real IP address>`
2. Save the file.
3. If the Extreme Management Center Management server IP address is not configured to use the NAT IP address of the Extreme Management Center server, perform the following steps:
   a. Enter the following command at the engine CLI:
      `/opt/appid/configMgmtIP <IP address>`

Where *<IP address>* is the NAT IP address of the Extreme Management Center server.
Press Enter.

b. Restart the appidserver once the new IP address is configured by typing:
`appidctl restart`
Press Enter.

4. On the Extreme Management Center server, add the following text to the *<install directory>*`/appdata/NSJBoss.properties` file. In the second to last line, specify the hostname of the Extreme Management Center server.

NOTE: The Application Analytics engine functions as a client computer independent of the server. Both engines and clients must be able to resolve the hostname you specify.

```
# In order to connect to a NetSight server behind a NAT fi
rewall or a
# NetSight server with multiple interfaces you must define
 these two
# variables on the Extreme Management Center
server. The java.rmi.server.hostname
# should be the hostname
(not the IP) if multiple IPs are being used
# so that each client can resolve the hostname to the corr
ect IP that
# they want to use as the IP to connect to.
java.rmi.server.hostname=<hostname of NetSight server>
java.rmi.server.useLocalHostname=true
```

5. Save the file.
6. Add the Extreme Management Center server hostname to your DNS server, if necessary.

NOTE: Application Analytics engines, remote Extreme Management Center clients, and any Extreme Access Control engines must be able to connect to Extreme Management Center using this hostname.

Related Information

For information on related windows:

- Application Analytics Engine Advanced Configuration Panel

Network Locations

In order to take full advantage of the reporting features in ExtremeAnalytics, you must first configure network locations. Defining network locations identify IP ranges for certain end-systems in your network, provides client flow data in your ExtremeAnalytics reports, and provides additional options for working with report search criteria. Locations can be imported or exported as a CSV formatted file. Additionally, configuring the location of your Application Analytics engine provides ExtremeAnalytics with improved flow data.

Configuring network locations is useful if you have already reserved certain IP address ranges for certain physical locations on your network. Create network locations that correspond to these reserved IP ranges. The network locations are then used to identify the portion of the network where the application flow source resides by matching the client's IP address to the ranges included in each network location. Create multiple locations to identify different buildings, sites, or geographical areas of your network. Even if you have no such policies, you can create a single network location that identifies which IP address ranges belong to resources in your network.

A location is defined with a name, description, and one or more IP address ranges specified by an IP address/mask. When a client's IP address matches any IP address/mask in a location, the client is determined to have that location. If the client matches the address/mask of several locations, the location with the most specific mask (the highest CIDR value) is used.

The name of the network location that matches the client's IP address is listed in the Location column of the Application Flows table in the Analytics tab. This allows you to search, sort, and filter flow data according to location. ExtremeAnalytics uses this data to provide a summary of the data for locations, which can be viewed as either an hourly or high-rate report in the Analytics Browser.

You must be a member of an authorization group that has been assigned the Extreme Management Center ExtremeAnalytics Read/Write Access capability in order to manage network locations. For additional information, see Getting Started with Application Analytics.

This Help topic provides the following information about managing Extreme Management Center network locations:

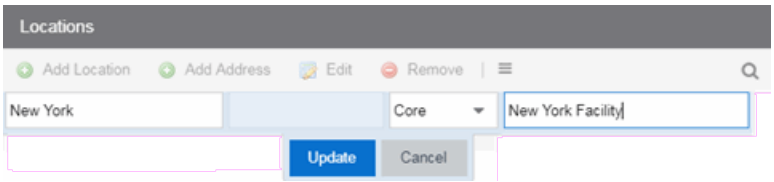
Managing Locations

Locations are created and managed in the Configuration view of the Analytics tab.

Adding Locations

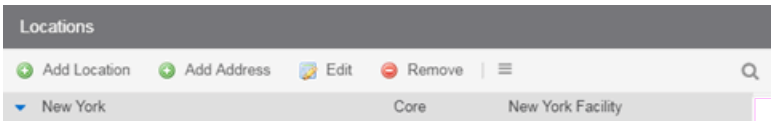
To add a location:

1. Access the Analytics tab and select the Configuration tab.
2. In the left-panel tree, select Locations.
3. In the right-panel Locations tab, click the Add Location button and enter a name for the new location in the first text box. If desired, enter a role for the location in the drop-down menu and a description in the text box.

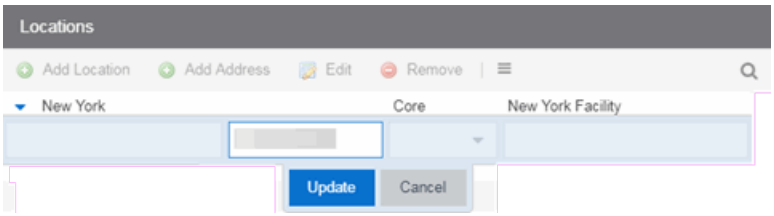


4. Click Update.

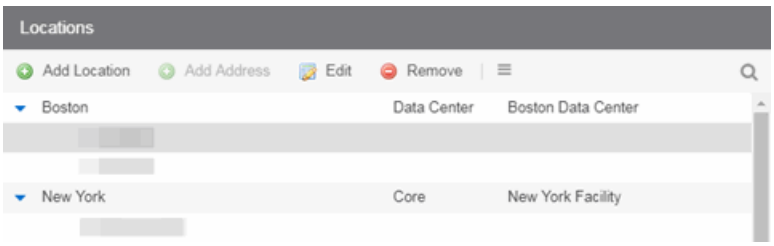
   The new location is added.



5. Select the location in the list, click the Add Address button, and enter an IP address/mask in the field in CIDR notation.



6. Click **Update**. The IP address/mask is added to the list under the location. Repeat steps 5 and 6 to add as many IP addresses/masks as necessary. The following image shows the Locations panel with multiple locations defined.



Editing Locations

To edit a location name, description, or address/mask:

1. Access the Extreme Management Center **Analytics** tab and select the Configuration view.
2. In the left-panel tree, expand System and select **Locations**.
3. In the right-panel Locations view, select the location name, role, description, or address/mask that you want to edit.
4. Click the **Edit** button and make the desired changes to the location name, description, or address/mask. You can also double-click on a name, description, or address/mask to make the desired changes, instead of using the **Edit** button.
5. Click **Update**.

Removing Locations

To remove a location or address/mask:

1. Access the **Analytics** tab and select the Configuration view.
2. In the left-panel tree, expand System and select **Locations**.

3. In the right-panel Locations view, select the location name or address/mask that you want to remove.
4. Click the **Remove** button.

Importing Locations

To import locations from a CSV file:

1. Access the Extreme Management Center **Analytics** tab and select the Configuration view.
2. In the left-panel tree, expand System and select **Locations**.
3. In the right-panel Locations view, click the **Gear** button (≡) and select **Import from CSV**.
   The Import Locations window appears.
4. Click the **Select File** button and navigate to the folder in which the CSV file is located.
5. Select the CSV file and click **Open**.
6. Click one of the following options in the Import Options section of the window to determine how Extreme Management Center handles existing locations:
   a. Select **Discard all locations and import new ones** to replace all locations currently listed in the Locations view with the locations imported from the CSV file.
   b. Select **Import locations, overwriting existing locations** to replace existing locations currently listed in the Locations view with locations imported from the CSV file, but leave all other locations in the Locations view unchanged.
   c. Select **Import locations, but do not change existing locations** to add new locations to the Locations view, but prevent existing locations currently listed in the Locations view from being overwritten by locations imported in the CSV file.
7. Click **Import**.
   The locations are imported to the Extreme Management Center.

Exporting Locations

To export locations and save them as a CSV file:

1. Access the Extreme Management Center **Analytics** tab and select the Configuration view.
2. In the left-panel tree, expand System and select **Locations**.
3. In the right-panel Locations view, click the **Menu** button (≡) and select() **Export to CSV**.
   The CSV file is saved to the web browsers default download location.

Searching Locations

To search for a specific location or address/mask in the Locations view, enter the location name or address/mask in the **Search** field and press **Enter**. The search results are displayed in the view.

Related Information

For information on related ExtremeAnalytics topics:

- Getting Started with ExtremeAnalytics
- Analytics Tab

Wireless

The **Wireless** tab in Extreme Management Center 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. Click on 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 Extreme Management Center.

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 on 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. Extreme Management Center 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 Extreme Management Center tabs and reports. For more information on authorization capabilities, see the Help topic How to Configure User Access to Extreme Management Center Applications located in Suite-Wide Tools > Authorization Device Access.

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. Click the **Gear** button ( ) to open additional fields from which you can configure the information presented in the reports.

Click on 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. Clicking on any node in the tree provides contextual information for that node.

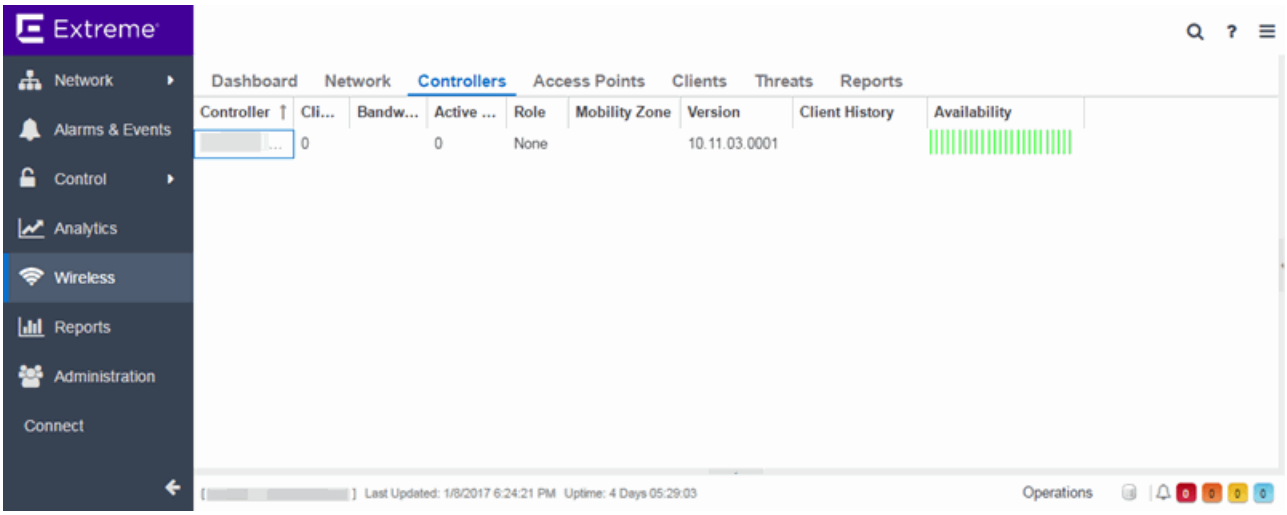
Select **Discover All Controllers** in the **Tools** menu at the bottom of the tree panel to perform a discover operation that looks for any configuration changes on

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, click the down arrow next to the **Discover** button and select **Discover Controller**.

Click **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. Click on 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 click on the gray arrow to open the AP Details window that provides controller, bandwidth, and client information. Click on a single AP name link to open an in-depth AP Summary view for the selected AP.

Click on 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 Extreme Management Center map or to maps based on AP location
- Removing selected APs from associated maps
- Searching maps for the selected APs

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, click 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 clicking on a client's MAC address in the table.) From the Client History window, you can click 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 Extreme Management Center 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 click 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 clicking on 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.

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. Click on the link to open the AP Details window that provides controller, bandwidth, and client information.

  From the AP History sub-tab, click 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 menu 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

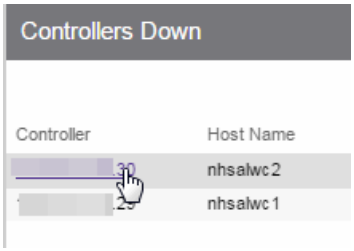
The **Reports** tab allows you to view information about the APs, controllers, and wireless traffic on your network. Available reports are accessible via the **Reports** drop-down menu at the top of the tab.

Click 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.

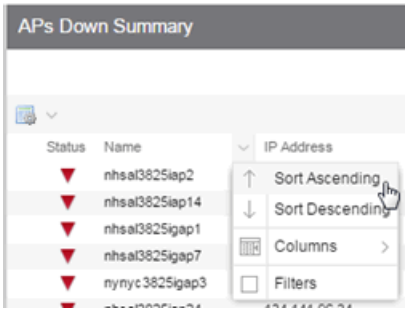
Report Features

Extreme Management Center reports include the following features (depending on the report selected):

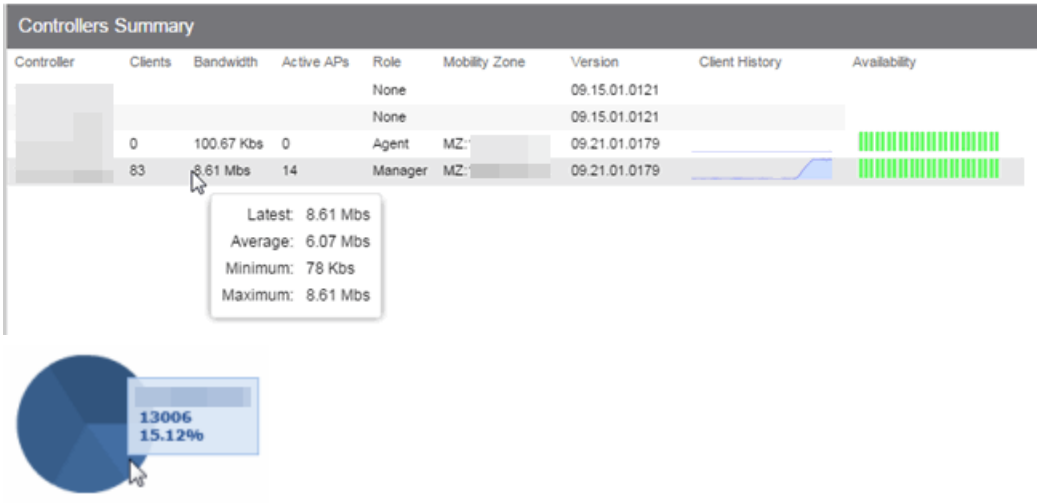
- Drill-down for Details — Link to summary reports containing more detailed information. For example, in the Controller Summary report, clicking on a controller shows a detailed report for that controller over time.



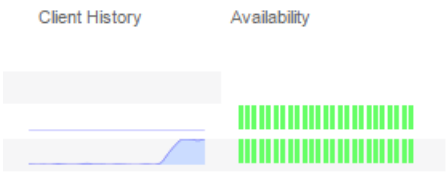
- Interactive Tables — Manipulate table data in several ways to customize the view for your own needs:
  - Click on the column headings to perform an ascending or descending sort on the column data.
  - Hide or display different columns by clicking on a column heading drop-down arrow and selecting the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

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

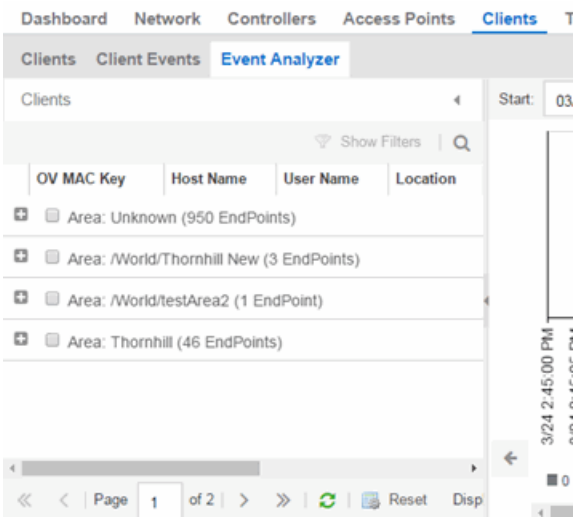
Event Analyzer

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.
- Clicking a Location on the Wireless > Clients tab opens the Event Analyzer for the end-points that occurred for all APs in that Location.
- Clicking a MAC address on the Wireless > Clients tab opens the Event Analyzer for only that end-point.

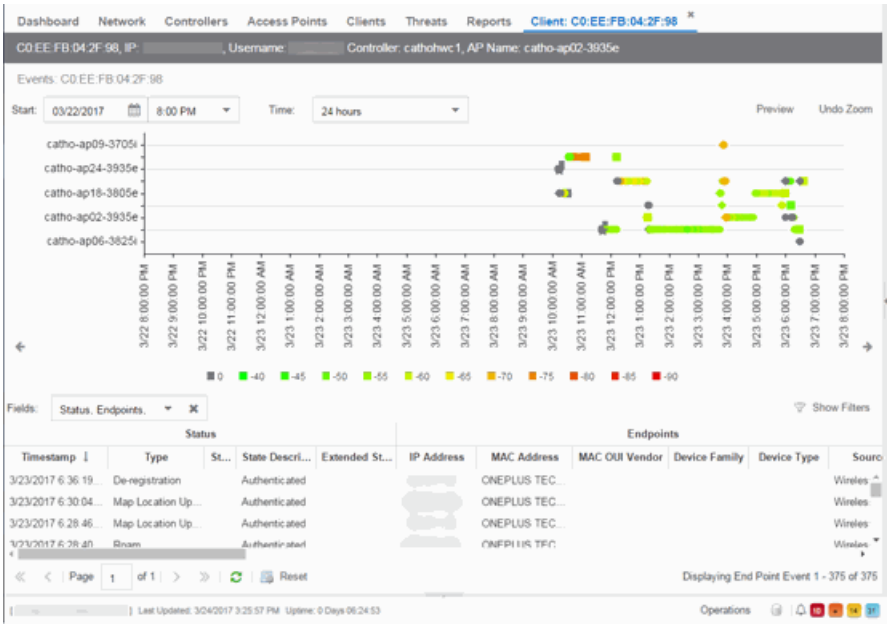
When accessing the tab using the top two methods, a Clients section is available in the left-panel. This section provides you with the ability to display end-point events for specific AP locations.



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

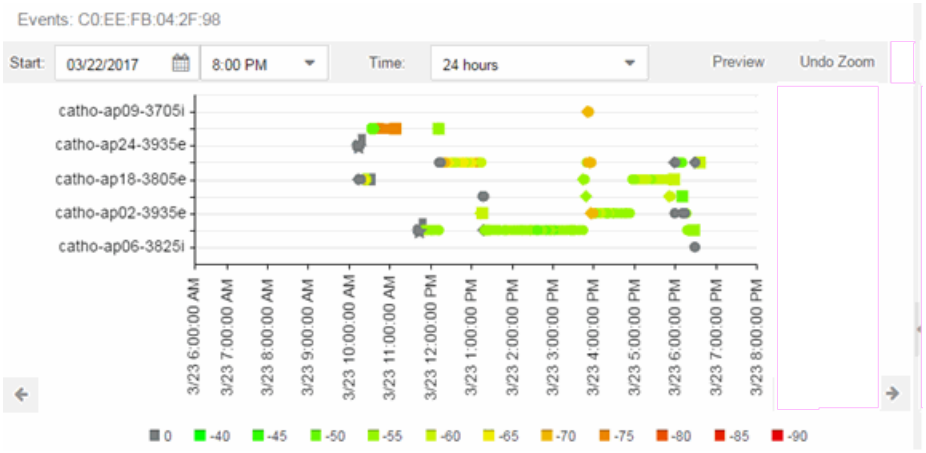
The top of the tab contains a graph displaying the RSS (Received Signal Strength) for the end-point events.

The bottom contains a table showing information about each event.



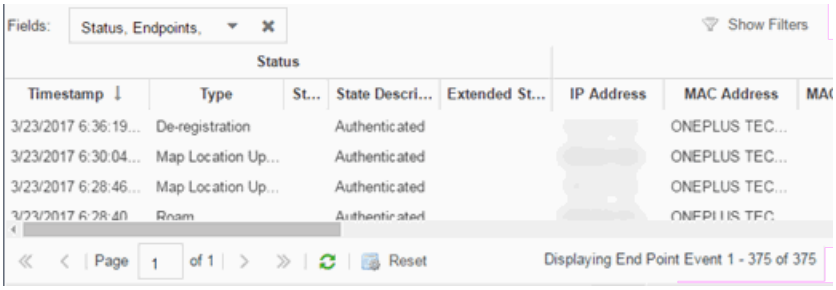
RSS Graph

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 menu to select groups of columns to display in the table:

- Select **Status** to display the following columns in the table:
  - Timestamp
  - 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
    - Extreme Access Control Engine/Source IP
- Select Metrics to display the following columns in the table:
    - RSS
    - SNR
- Select Threat/Risk to display the following columns in the table:
    - Categories
    - Start Time
- Select Network Service to display the following columns in the table:
    - Switch IP
    - Controller IP

Related Information

For information on related Extreme Management Center topics:

- Wireless

Governance Overview

The Extreme Management Center **Governance** tab provides oversight into the configuration of your devices and wireless threat alerts to ensure you are compliant with industry best practices.

IMPORTANT: The **Governance** tab is available and supported by Extreme on an Extreme Management Center engine running the Linux operating system supplied by Extreme. Other Linux operating systems can support Governance functionality, but python version 2.7 or higher must be installed. Additionally Governance 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 a governance audit against devices on the **Governance** tab or against device archives on the Archives tab.

NOTE: **Governance** tab functionality requires you to acquire an additional license.

Extreme Management Center provides a set of audit tests that allow you to test the configuration of your devices. Groups of audit tests comprise a regime, which tests for a specific regulation or standard. Extreme Management Center uses the results to determine a score that indicates compliance with a regulation or standard.

The regimes included in the **Governance** tab are automatically included in your Extreme Management Center version 8.1 installation on an Extreme Management Center engine, but you must import them on a non-Extreme Management Center 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. Once the regime meets your needs, use it to run a governance audit against a device or set of devices. You cannot run individual audit tests against a device.

The **Governance** 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.

Related Information

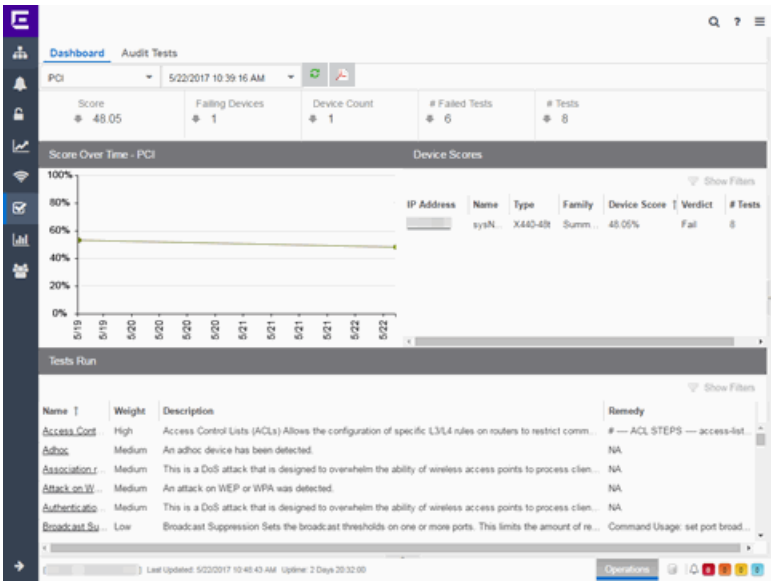
For information on related tabs:

- Governance Dashboard
- Audit Tests
- Archives

Governance Dashboard

The **Governance** > **Dashboard** tab provides an overview of your 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 governance audit to view the results in the tab. Click 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 governance audit you select using the regime and date in the drop-down menu.

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. Clicking 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 governance audit. Clicking 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 governance audit. Clicking 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 governance audit. Clicking 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 governance audit. Clicking 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 menu 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 governance audit on each device.

IP Address

The IP address of the device tested.

Clicking an address in the IP Address column opens that device in the Device Details tab, which provides governance 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 Extreme Management Center.

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 governance 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 governance 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.

Clicking 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 governance audit.

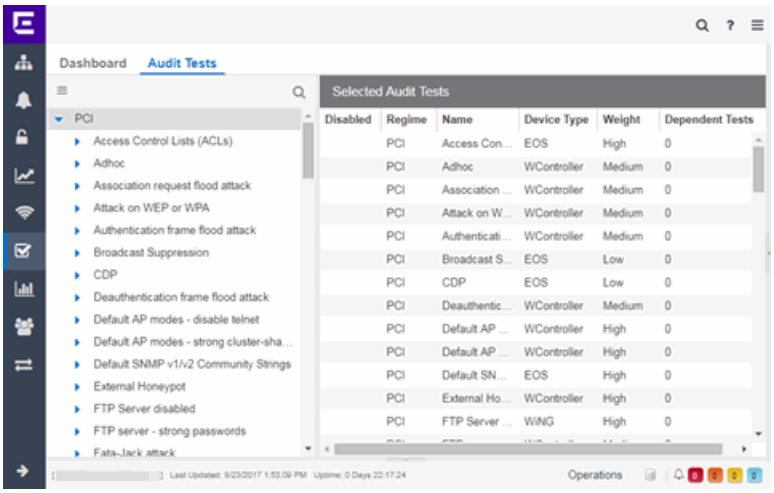
Related Information

For information on related topics:

- Governance
- Audit Tests
- Configure Device

Audit Tests

The **Audit Tests** tab displays a set of audit tests that check for vulnerabilities in your devices. The tab also allows you to create your own audit tests you can add to regimes.

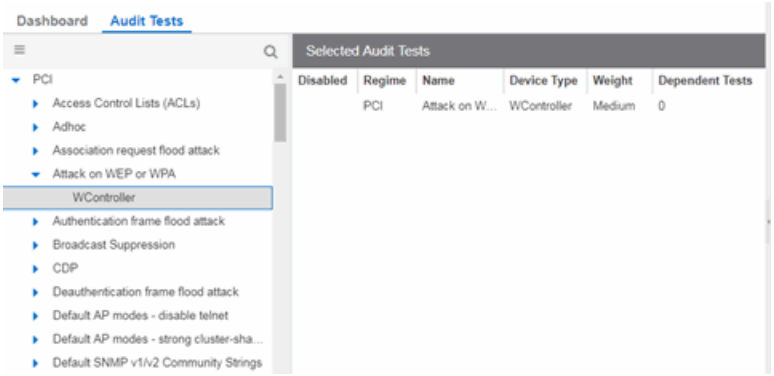


The Audit Test list contains a list of all of the audit tests available in Extreme Management Center, contained within the regulatory and standards regime of which it is a part. Each individual audit test contains the device types on which the test can be run.

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. Click the **Magnifying Glass** icon (🔍) and begin typing to search within the regimes for a specific audit test.

Disable an audit test by right-clicking it in the left-panel and selecting **Disable Audit Test**. Delete an audit test by right-clicking it in the left-panel and selecting **Delete Audit Test**.

NOTE: Only user-created audit tests or audit tests in user-created regimes can be deleted. Additionally, only user-created regimes can be deleted.



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 a governance 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.

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.

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.

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.

Weight

The value in the Weight column of the Selected Audit Tests table indicates the priority of the audit test:

- High
- Medium
- Low

Dependent Tests

This shows the number of audit tests that must run successfully before the selected test runs.

For example, when running an audit test to ensure a device is running the latest version of an anti-virus software, you might first check whether the device has anti-virus software installed. The audit test verifying the version does not run if the audit test checking whether an anti-virus software is installed fails.

Use the **Menu** icon (≡) in the left-panel to add a new regime or audit test, edit existing regimes or audit tests, or run the regime against a device or group of devices. These options are also available via the right-click menu in the left-panel.

Select a regime from the left-panel, click the **Menu** icon and select **Run Regime** to open the **Run Regime** window, where you select the device against which to run the audit.

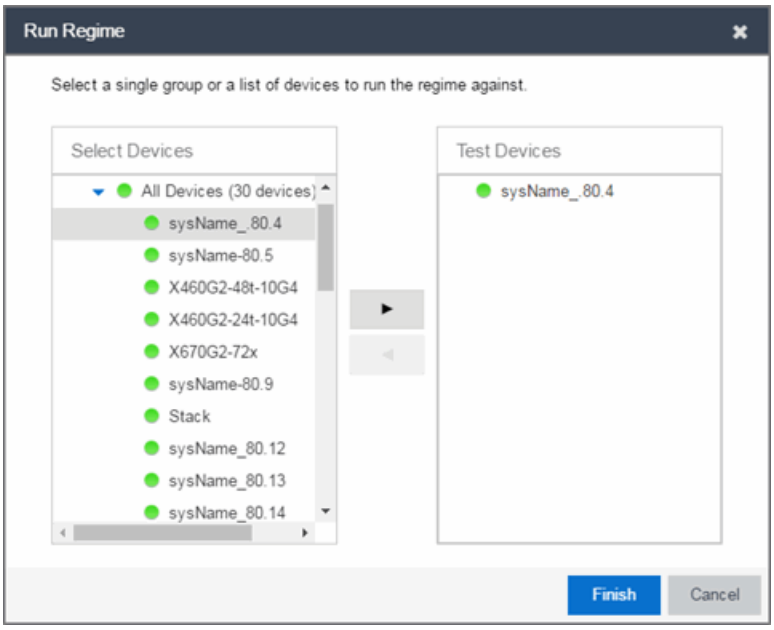
Related Information

For information on related tabs:

- Governance
- Scheduler

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 Extreme Management Center.



Select Devices

Expand the folders and select a single device, multiple devices, or a single device group. Click 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 click the left arrow button **<**.

Right Arrow Button

Click **>** to add the device(s) or device group to the Test Devices list.

Left Arrow Button

Click **<** to remove the device(s) or device group from the Test Devices list.

Finish Button

Click the **Finish Test** button to run the selected audit test(s) on the devices selected in the Test Devices list. The progress of the governance audit is displayed in the Operations table.

Related Information

For information on related tabs:

- Governance
- Scheduler

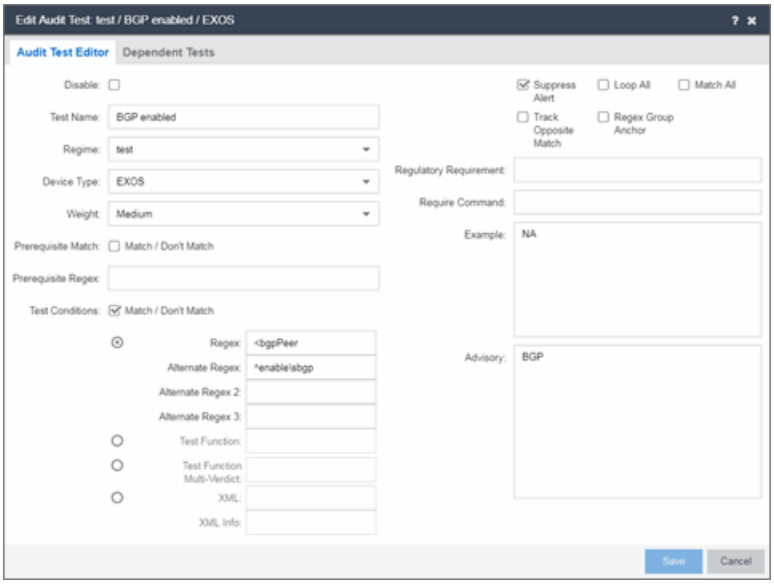
Create/Edit Audit Test

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 **Governance** > Audit Tests tab by selecting a regime in the left-panel, clicking the **Menu** icon (≡), and selecting **Add** > **Audit Test**.

Access the Edit Audit Test window by selecting an audit test in the left-panel, clicking 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 a governance 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. Extreme Management Center 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 clicking the Menu icon and selecting Add or Edit > Regime.

Device Type

The type of device being tested. In version 8.1, Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center is comparing a device's configuration file.

Alternate Regex

A second regular expression against which Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center 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).

Test Function

A python function you can configure if the audit test requires more complex logic to test a configuration.

Test Function Multi-Verdict

A python function you can configure to return multiple verdicts. Use this to configure audit tests for wireless controllers with complex configurations.

XML

Select the button and enter the XML element in the wireless threat data for which the audit test is checking.

XML Info

Enter the set of `Info` elements from the wireless threat XML data for which the audit test is checking.

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 a governance 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 governance 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 governance 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 Extreme Management Center 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

Reports

Extreme Management CenterReports provide historical and real-time reporting, offering high-level network summary information as well as detailed reports and drill-downs.

From the **Reports** tab, you have three options:

- Reports — 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 Extreme Management Center page to access detailed information about many of the reports.
- Custom Report — 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. Display options let you display 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. Click the **Info** button at the top-right of the Extreme Management Center page to access detailed information about custom report options.
- Report Designer — Create a custom dashboard report accessible from the **Reports** tab.

Additionally, the Menu icon (☰) at the top of the screen provides links to additional information about your version of Extreme Management Center.

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 Extreme Management Center tabs and reports. For more information on authorization capabilities, see the Help topic, "How to Configure User Access to Extreme Management Center Applications," located in Extreme Management Center Suite-Wide Tools > Authorization Device Access.

To collect data in your Extreme Management Center reports, you must enable statistics and flow collection for your network devices, interfaces, and wireless clients. For instructions, see How to Enable Data Collection.

Reports

The Reports catalog lets you select a report from the following report types:

- Extreme Access Control — Provides an overview of end-system connection information. You can also see these reports and others on the Control tab.
- Extreme Access Control Health — Provides reports on end-system assessment and state information. In the Risk Level pie chart, click on a pie section to open a filtered end-system grid for more detailed information about end-systems at that risk level.
- Extreme Access Control System — Provides a report of the top ten end-systems by engine.
- Application Analytics — These reports provide visibility into the applications on your network and who's using those applications.
- Console — The NMS Dashboard report provides summary NMS data including top 5 switch, interface, and host statistics as well as important Wireless data. Host data is collected from network devices that support the Host Resource MIB, such as Extreme Management Center engines, Linux systems, and Windows PCs. For more information, click the Info button (i) at the top-right of the Reports tab.
- Data Center Manager — The DCM reports provide an overview of all virtual machines on the network broken down into VM distribution per Identity and Access 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, down devices, inventory summary (including archive distribution, devices backed up, database properties, scheduled events, asset tracking information, and the ability to track the changes made to a specific device), top devices by IPv6 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).
- Interface — These reports present information on your top interfaces by active flows, bandwidth, bandwidth summary, least availability, POE usage, and utilization.
- OpenScape — The OpenScape LIA (Location and Identity Assurance) report provides an overview of all OpenScape phones on the network categorized by phone count, phone type, phone software version, and phone distribution by access switch, as well as a list of phone information by MAC address.

- Policy — Provides a policy rule hit summary report showing top services and roles by rule hits.
- Server — These reports provide data on the Extreme Management Center 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.
- 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. 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.

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, click the Info button i 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 Application Analytics, IAM, Console, and Wireless dashboards, and customizing report components to meet your specific needs.

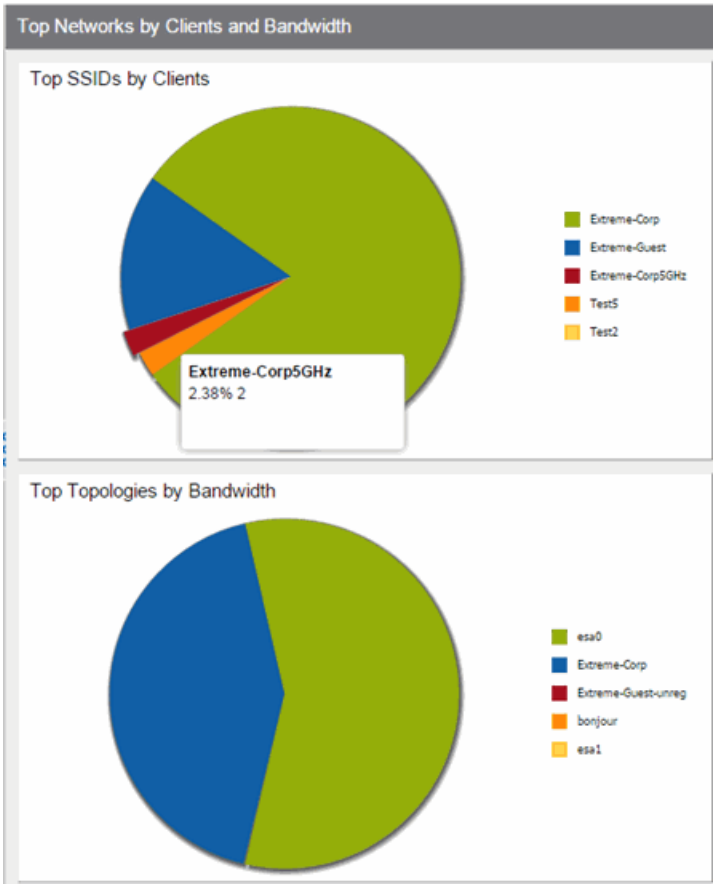
Once a report is created, it is available from the Reports tab.

For instructions on creating a custom report, see How to Use the Report Designer.

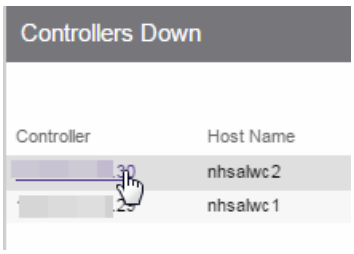
Report Features

Extreme Management Center reports include the following features (depending on the report selected):

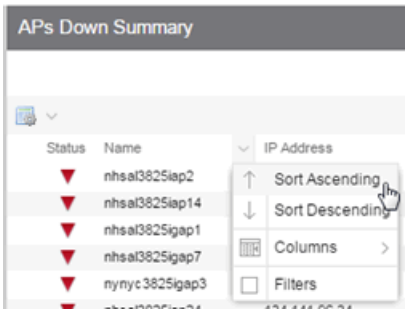
- Hover Over for Info — Hover over a pie section to display the name of the segment, the percentage represented by the segment and the number of elements. for some reports, clicking on a pie section opens a filtered end-systems grid for more detailed information.



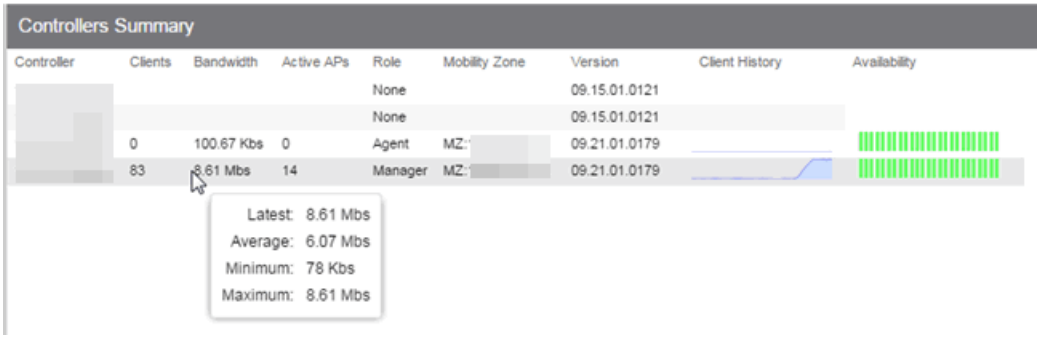
- Drill-down for Details — Link to summary reports containing more detailed information. For example, in the Controller Summary report, clicking on a controller shows a detailed report for that controller over time.



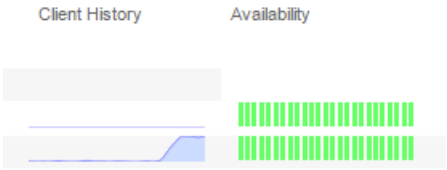
- Interactive Tables — Manipulate table data in several ways to customize the view for your own needs:
  - Click on the column headings to perform an ascending or descending sort on the column data.
  - Hide or display different columns by clicking on a column heading drop-down arrow and selecting the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

For information on related Extreme Management Center tabs:

- Administration
- Alarms and Events
- Network
- Search
- Wireless

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. Once 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 Extreme Management Center 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

Once you change a system report, the new, customized report replaces the original report in the **Reports** tab and all other places in Extreme Management Center 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.

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 menu to change a component in a panel, or click the **Delete** button to delete a panel.
4. Click 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.

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 menu in the Applications Browser section when you customize a system report or create a new report.

Related Information

- ExtremeAnalytics

Custom Components in

Custom Components

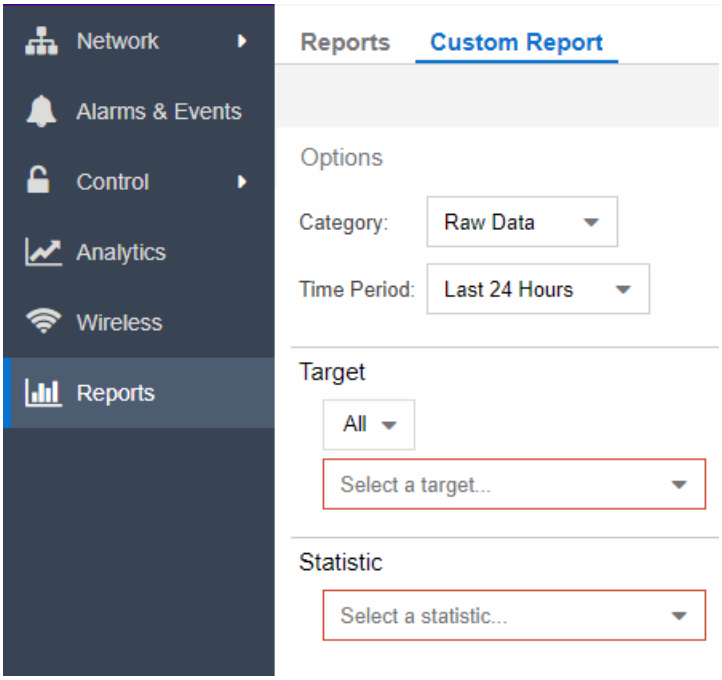
When you create an Advanced Browser report in the ExtremeAnalytics Browser, you can save it to the **Report Designer** to use as a custom component. The custom component uses the target, statistic, start time, and search criteria you defined in the Advanced Browser report.

Custom components are listed in the My Components section in the left-panel of the Report Designer. They are available for selection from the **Component** drop-down menu in the Applications Browser section when you customize a system report or create a new report.

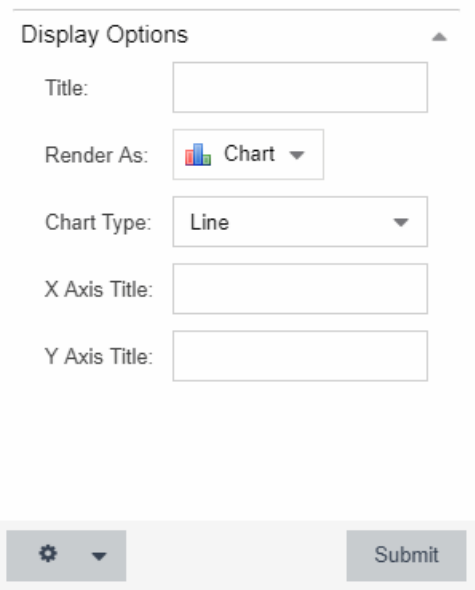
Create a New Component

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 menu. 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 menu. Then select the specific target from the **Select a target** drop-down menu.
4. Select the **Statistic** you want to display from the drop-down menu.
5. Enter your **Display Options** to design your chart. You can choose to render the data as a chart or grid.



6. Click **Submit.**
7. Click the **Gear** button (⚙) in the bottom left corner and choose from the drop-down menu:
    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

Extreme Management Center'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 Extreme Management Center.

To view the diagnostic reports and schedules in the **Administration** tab, you must be a member of an authorization group assigned the OneView > Access OneView and OneView > Access OneView Administration capabilities. For additional information about configuring user capabilities, see Users.

This Help topic provides information on the following sub-tabs:

- Profiles
- Users
- Server Information
- Certificates
- Options
- Backup/Restore
- Diagnostics
- Vendor Profiles

Profiles

The **Profiles** tab allows you to establish access to the devices on your network by creating identities used for authentication when performing SNMP queries and sets. Extreme Management Center 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, Extreme Management Center'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 allows 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 Extreme Management Center. There are three authentication methods available: OS Authentication (the default), LDAP Authentication, and RADIUS Authentication.

Server Information

The Server Information tab allows you to view and manage current client connections and Extreme Management Center locks.

Certificates

The Certificates tab provides a central location for managing the Extreme Management Center server certificate.

From this tab you can:

- Update the Extreme Management Center server certificate by replacing the server private key and certificate.
- View and change the client trust mode that specifies how Extreme Management Center clients handles a server certificate.
- View and change the server trust mode that specifies how servers handles certificates from other servers.

Options

Extreme Management Center options allow you to configure the behavior of Extreme Management Center. These options apply across all Extreme Management Center 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:

- Site Options
- Status Polling Options
- Syslog Options
- TopN Collector Options
- Trap Options
- Web Server Options
- Wireless Manager Options

Backup/Restore

The Backup/Restore tab allows 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. Use the Level menu at the top-left of the page to select the desired report level.

- 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 allows you to add a license and allows 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. Beta features can also be enabled from the Advanced level. For additional information on beta features, please contact Extreme Networks Support.
- Diagnostic Level — This level includes all Basic and Advanced reports as well as access to the North Bound Interface. 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 Extreme Management Center 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 Extreme Management Center 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 may 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 Extreme Management Center reporting database. This allows 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 allows you to edit configurations for device types. You can enter additional information about the device type to help identify it in Extreme Management Center.

Vendor Profiles are a beta feature and are only available by selecting **Enable Beta Features** on the **Administration** > Diagnostics tab.

Related Information

For information on the other Extreme Management Center tabs:

- Alarms and Events
- Devices
- Reports
- Wireless

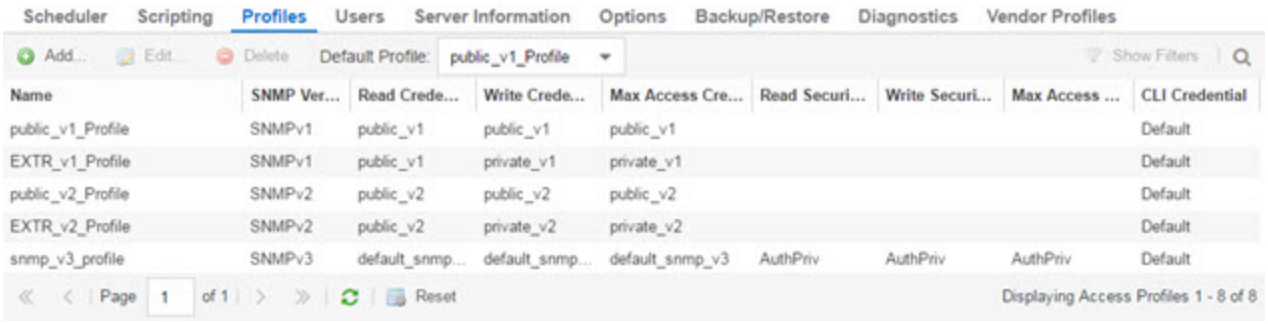
Profiles

Extreme Management Center applications access devices in order to control certain device functions and retrieve information for device properties views, FlexViews and periodic polling. This tab lets you 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 Extreme Management Center 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 menu 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 Extreme Management Center installation and cannot be deleted.

SNMP Version
This is the SNMP protocol version for the profile. Profiles can be configured for SNMPv1, SNMPv2c, or as SNMPv3.

Read, Write, Max Access Credential
When the Version is SNMPv1 or SNMPv2c, the Read, Write, and Max Access columns in the table contain the Community Name for each access level. When the Version is SNMPv3, the Read, Write, and Max Access columns in the table contain the credential specified for each access level.

Read, Write, Max Access Security Level
When the Version is SNMPv3, these columns contain the security level specified for each access credential. When the Version is SNMPv1 or SNMPv2c, these columns do not apply.

CLI Credential
The CLI credential specified for the profile.

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

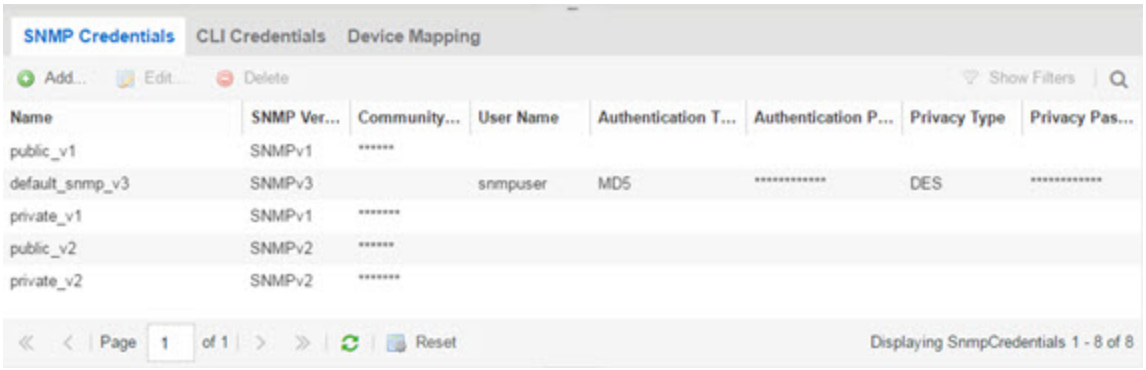
Edit Button
Opens the Add/Edit Profile window where you can modify the SNMP version and passwords/community names used by a selected profile.

Delete Button
Removes the selected Profile from the Device Access Profiles table. You cannot delete the profile currently selected to be the Default Profile.

SNMP Credentials Subtab

This tab lists all of the SNMP credentials created in the Extreme Management Center 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 Extreme Management Center database.

SNMP Version

This is the SNMP protocol version for the credential. Credentials can be configured for SNMPv1, SNMPv2c, or as SNMPv3.

Community Name

For SNMPv1 or SNMPv2c credentials, this is the Community Name used for device access.

User Name

For SNMPv3 credentials, this is the User Name used for device access.

Authentication Password/Authentication Type, Privacy Password/Privacy Type

For SNMPv3 credentials, these columns show the authentication protocol (None, MD5, or SHA) and privacy protocol (None or DES) and passwords used by the credential.

Add Button

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

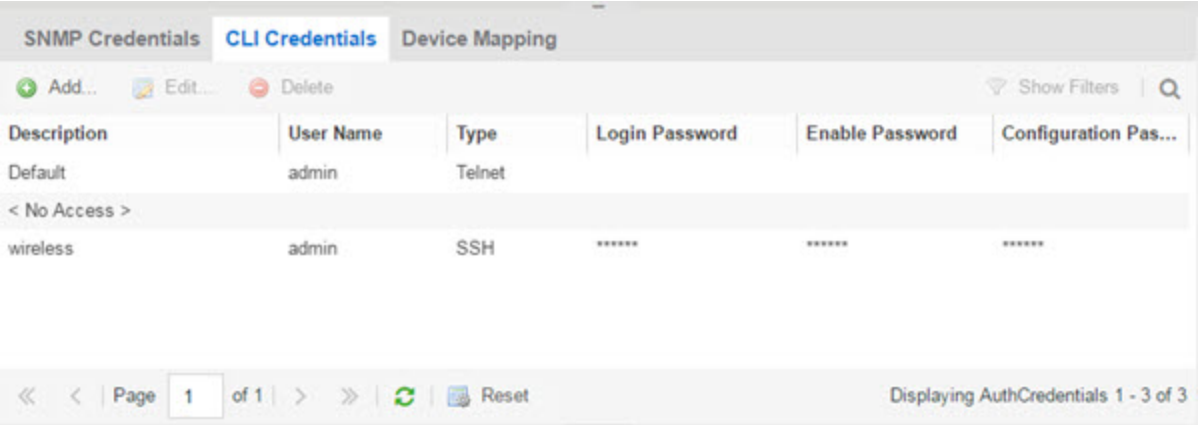
Edit Button

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 Extreme Management Center 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

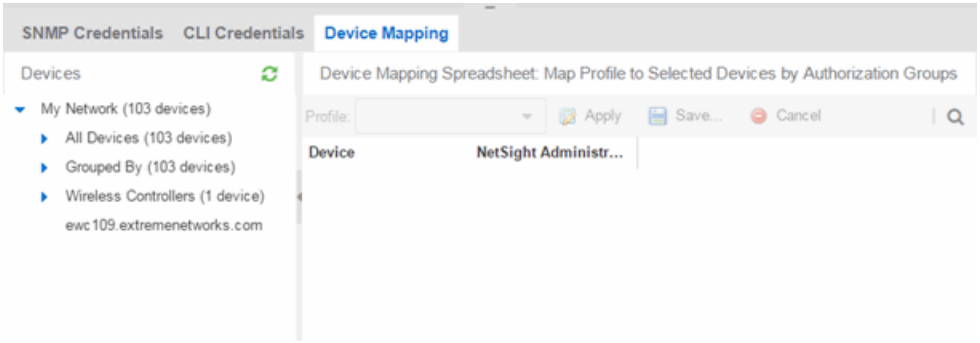
Opens the Add/Edit CLI Credential window where you can modify a CLI credential selected from the CLI Credentials table.

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 (Extreme Management Center) Administrator Group and each *Authorization Group* you defined. The *NetSight Administrator* column shows the profile used by the Extreme Management Center 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.

Select a Profile from the drop-down menu, click the authorization groups to which you want to apply the profile, and click Apply.

Apply Button Apply

Sets the profile selected in the **Profile** drop-down menu as the profile for the Authorization Groups selected in the table.

Save Button Save...

Saves your changes on the device or devices selected.

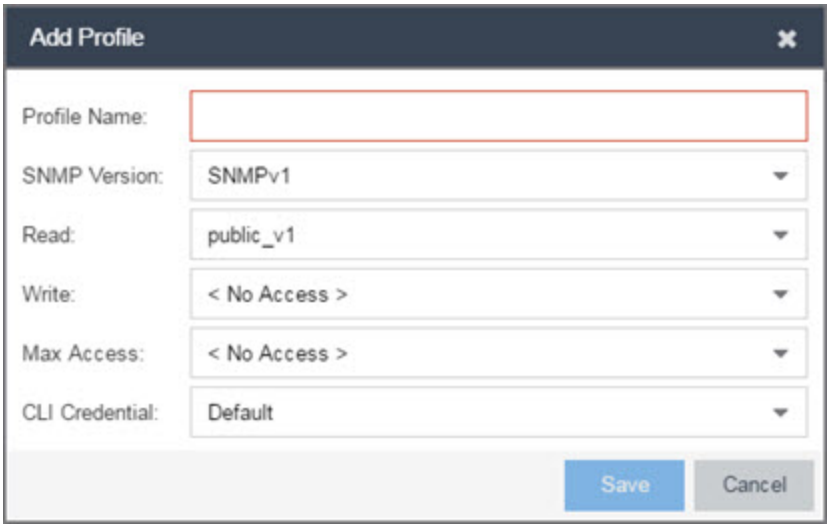
Cancel Button Cancel

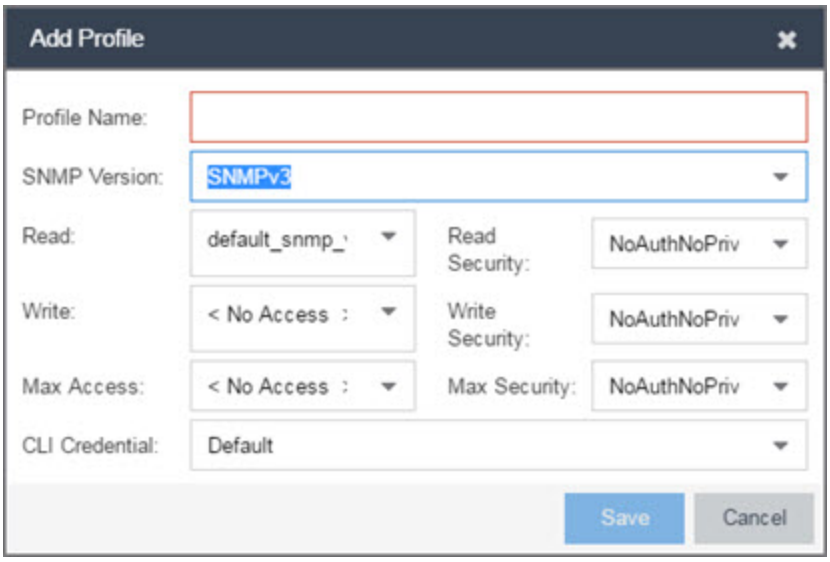
Discards your unsaved changes.

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 SNMPv1 or SNMPv2c is selected, the editor provides fields where you can configure access levels using Community Names. With SNMPv3 selected, you can configure access levels using Credentials and Security Levels.

Read, Write, Max Access

SNMPv1, SNMPv2c

Select the SNMP Credential used for the Read, Write, Max Access. These fields define the community names used for these levels of access. You can also select New to open the Add/Edit SNMP Credential window.

- Read — This Community Name is used for *get* operations.
- Write — This Community Name is used for *set* operations.
- Max Access — This Community Name is used for *set* operations that require administrative access, such as changing community names.

SNMPv3

Select the SNMP Credential used for the Read, Write, Max Access levels, defined by Credentials and Security Level:

Credentials

Credential Names are assigned to each of the three SNMPv3 access levels used for the Read, Write and Max Access operations. You can also select New to open the Add/Edit SNMP Credential window.

- Read — used for read operations (*gets*).
- Write — used for write operations (*sets*).
- Max Access — used for write operations (*set*) that require administrative access.

Security Level

Each access level can be assigned a security level:

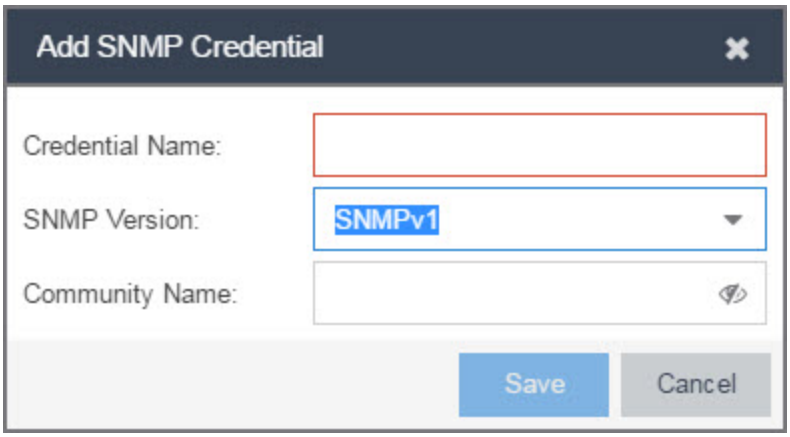
- AuthPriv — Highest security level requiring authentication and privacy (encrypted information).
- AuthNoPriv — Requires authentication, but unencrypted information.
- NoAuthNoPriv — Neither authentication nor privacy required.

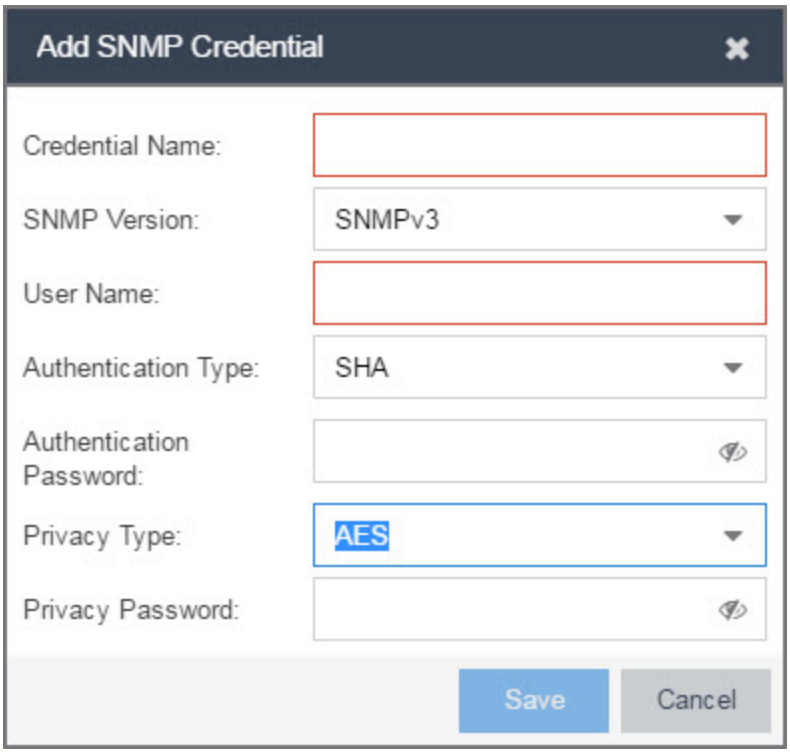
CLI Credential

Use the drop-down menu to select the CLI Credential for this profile. CLI credentials provide support for device management using the command line interface (CLI). You can also select New to open the Add/Edit CLI Credential window.

Add/Edit SNMP Credential Window

This window lets you define or edit the names and community names/passwords for SNMP credentials.





Credential Name

A unique name (up to 32 characters) assigned to this access credential. You can define a new credential or select a name from the table to modify settings for an existing credential. You cannot edit the name of an existing credential.

SNMP Version

This is the SNMP protocol version for the credential. Credentials can be configured for SNMPv1, SNMPv2, or as SNMPv3. When either SNMPv1 or SNMPv2 is selected, the window provides fields where you can configure access levels using Community

Names. With SNMPv3 selected, you can configure access levels using Authentication and Privacy Types.

Community Name

For SNMPv1 or SNMPv2 credentials, this is the Community Name used for device access.

User Name

For SNMPv3 credentials, this is the User Name used for device access.

Authentication Type

For SNMPv3 credentials, select MD5, SHA1, or None, from this drop-down menu.

Authentication Password

This is the password (between 1 and 64 characters in length) used to determine Authentication. If an existing password is changed and the credential is currently used with a profile applied to one or more devices, a confirmation dialog is opened to determine how the changes are handled. You are asked if you want to change the password on the device(s). You can then select the devices where the password is changed and, if this user is a valid user on the device(s), then the new password is set on the device. Select the Eye icon to display your password.

Privacy Type

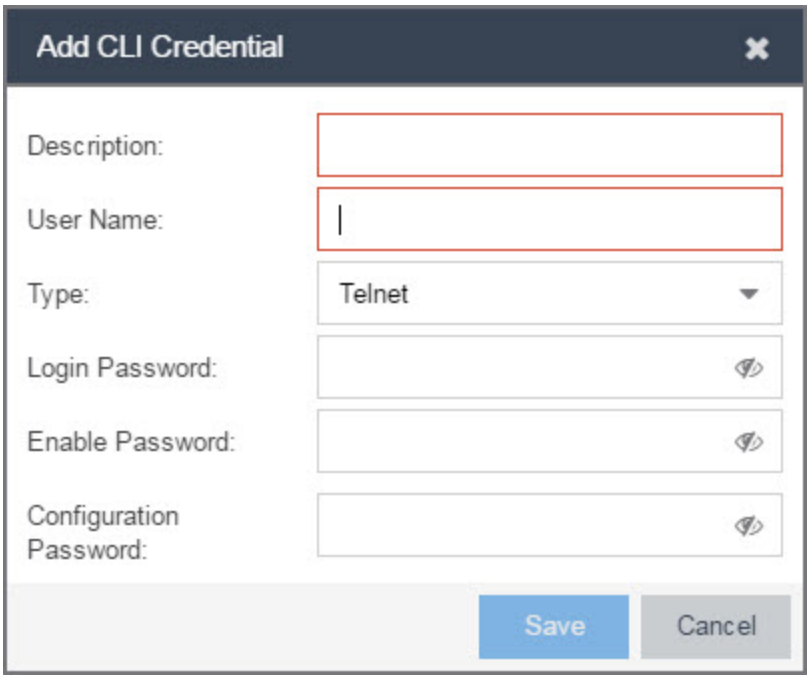
For SNMPv3 credentials, select DES or None from this drop-down menu.

Privacy Password

This is the password (between 1 and 64 characters in length) used to determine Privacy. If an existing password is changed and the credential is currently used with a profile applied to one or more devices, a confirmation dialog is opened to determine how the changes are handled. You are asked if you want to change the password on the device(s). You can then select the devices where the password is changed and, if this user is a valid user on the device(s), then the new password is set on the device. Select the Eye icon to display your password.

Add/Edit CLI Credential Window

This window lets you define or edit the user name and passwords for a CLI credential.



Description

A description of the credential.

User Name

The User name used for device access.

Type

The communication protocol used for the connection (SSH or Telnet).

Passwords

The passwords used to determine different levels of access to the device:

- Login — The password required to start a CLI session. Select the **Eye** icon to display your password.
- Enable — The password for entering Enable mode. Select the **Eye** icon to display your password.
- Configuration — The password for entering Configure mode. Select the **Eye** icon to display your password.

NOTE: When configuring CLI Credentials for ExtremeWireless Controllers, you must add the username and password Login credentials for the controller to this Add/Edit Credential window in order for Wireless Manager to properly connect (SSH) to the controller and read device configuration data. However, the 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

The **Vendor Profiles** tab allows you to add new device families to Extreme Management Center, which includes any element of the device family: Company, Vendor, Subfamily, and DeviceTypes. With the addition of properties for the new device family, the elements determine the reports available for the device in its DeviceView, the FlexView filters available for the device, and the scripts that apply to the device.

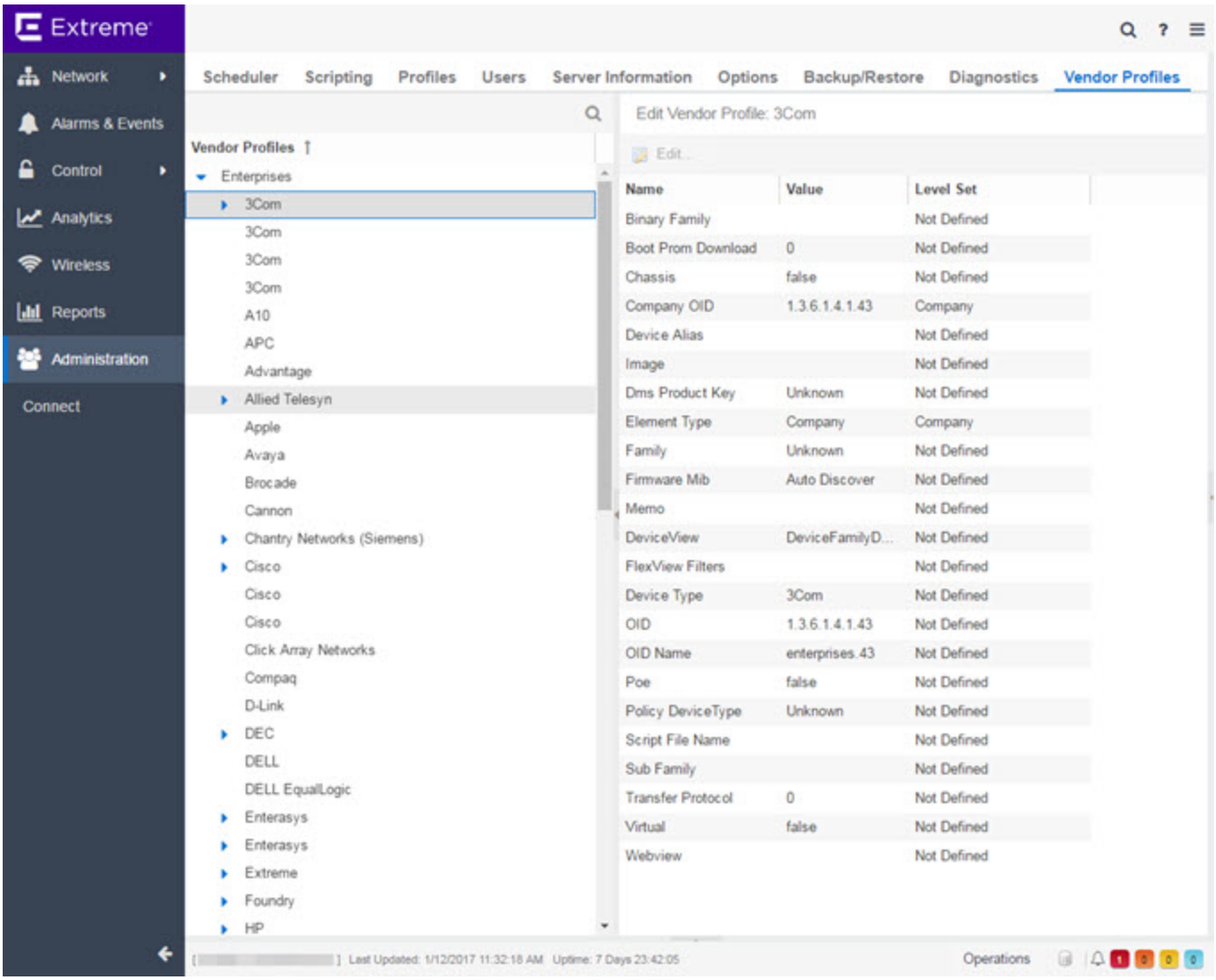
Vendor Profiles are a beta feature and are only available by selecting **Enable Vendor Profiles** on the **Administration** > Diagnostics tab.

IMPORTANT: Only make changes to this tab if you are an expert user. Incorrectly configuring this tab causes significant adverse effects in Extreme Management Center and may require you to reinstall.

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 Extreme Management Center 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.

NOTE: To remove all user-defined Vendor Profile configurations and restore the default system configurations, click the **Restore to Defaults** button on the **Administration** > **Diagnostics** > **System** > **Vendor Profile Cache** tab.



Vendor Profiles List

The left-panel of the Vendor Profiles tab contains a list of device vendors, displayed in alphabetical order. For those vendors with multiple products listed in Extreme Management Center, click 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.

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 DeviceType are either not applicable, or are used from another device.

The configuration of these fields determines how Extreme Management Center displays the element selected in the left-panel. Additionally, Extreme Management Center uses this information to determine the reports, filters, and scripts that apply to a device. It may be necessary to add a Property to a certain DeviceType to configure it in Extreme Management Center.

Related Information

For information on related windows:

- Users/Groups Tab
- Site Tab

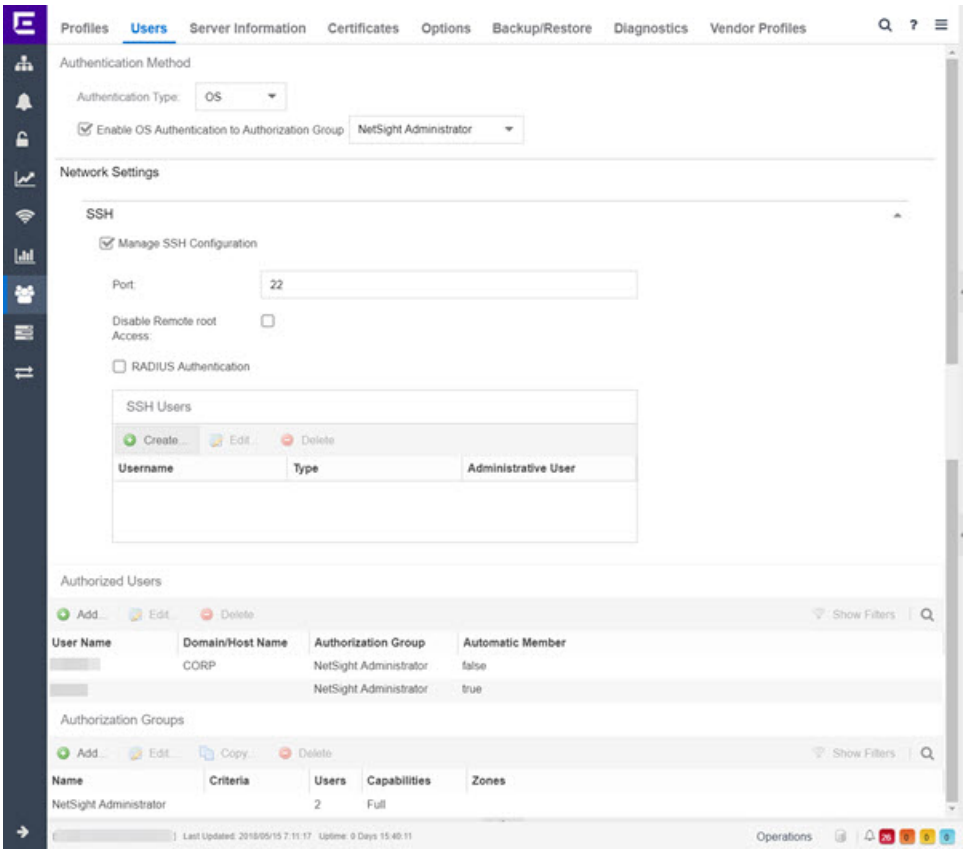
Users

Use the Users tab to create the authorization groups that define the access privileges (called *Capabilities*) to specific Extreme Management Center 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 Extreme Management Center. There are three authentication methods available: OS Authentication (the default), LDAP Authentication, and RADIUS 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 Extreme Management Center, see How to Add Users in Extreme Management Center.



Users/Groups Access

Click 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 clicking this button restricts access to other users.

Once you are finished making changes, click 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 Extreme Management Center client or access the Extreme Management Center database using the Extreme Management Center Server Administration web page.

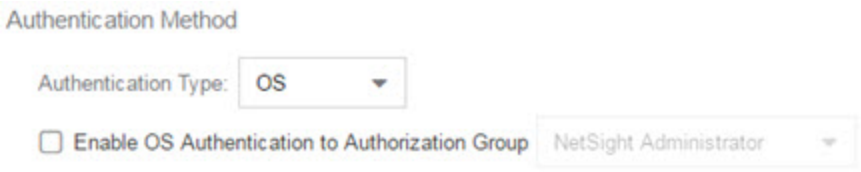
The following authentication methods are available:

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

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

OS Authentication (Default)

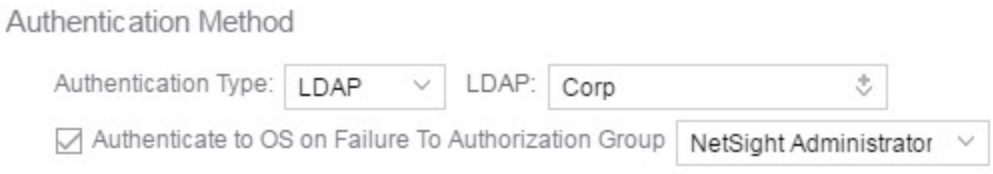
With this authentication method, the Extreme Management Center Server uses the underlying host operating system to authenticate users. Use the Authorized Users table to create a list of users allowed access and define their access capabilities.



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 Extreme Management Center Server uses the specified LDAP configuration to authenticate users.



Use the drop-down menu 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.

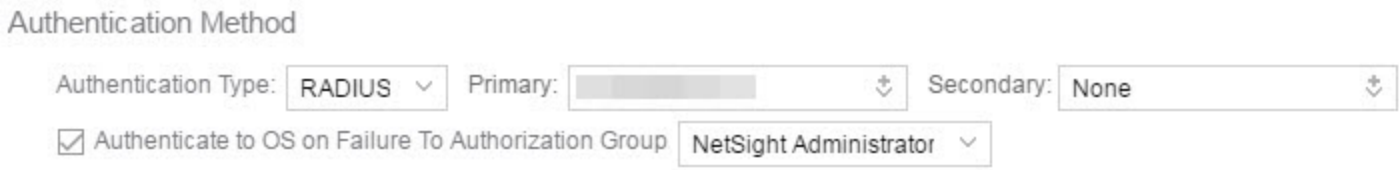
With LDAP Authentication, configure dynamic assignment of users to authorization groups based on the attributes associated with a user in Active Directory. For example, create an authorization group that matches everyone in a particular organization, department, or location. When a user authenticates, 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 Extreme Management Center Server uses the specified RADIUS servers to authenticate users.

NOTE: The RADIUS Authentication mode supports the PAP authentication type.



Use the drop-down menu 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

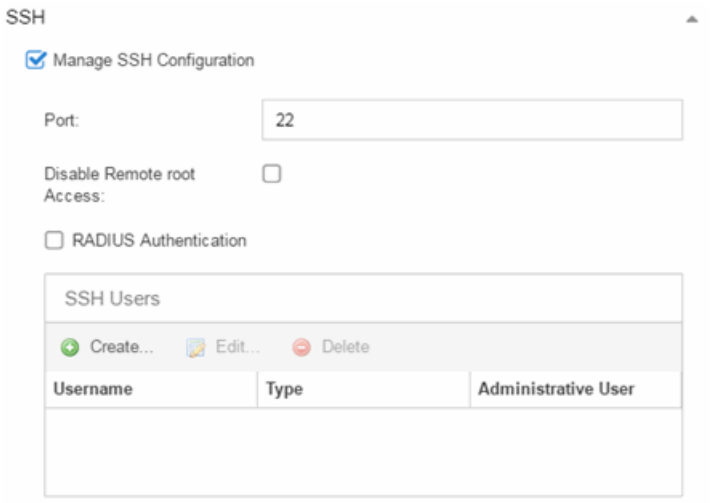
matched against a list of criteria specified as part of each authorization group. The first group with a criteria met by the user's attributes becomes the authorization group for that user. The user is then added to the Authorized Users table as an automatic member, with that authorization group.

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.

Network Settings

SSH configuration provides additional security features for the Extreme Management Center engine.

Select the Manage SSH Configuration checkbox and provide the following SSH information.



Port
: The port field allows you to configure a custom port to be used when launching SSH to the engine. The standard default port number is 22.

Disable Remote root Access
: Select this option to disable remote root access via SSH to the engine and force a user to first log in with a real user account and then su to root (or use

sudo) to perform an action. When remote root access is allowed, there is no way to determine who is accessing the engine. With remote root access disabled, the /var/log/message file displays users who log in and su to root. The log messages looks like these two examples:

```
sshd[19735]: Accepted password for <username> from
10.20.30.40 port 36777 ssh2
su[19762]: + pts/2 <username>-root
```

Enabling this option does not disable root access via the console. Do not disable root access unless you have configured RADIUS authentication or this disables remote access to the Extreme Management Center 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

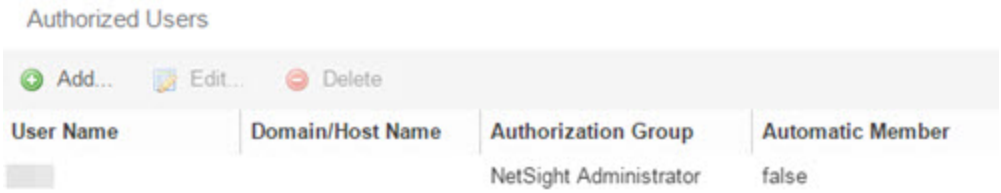
Use the toolbar buttons to create a list of users allowed to log in to the Extreme Management Center engine using SSH. You can add Local and RADIUS users and grant the user Administrative privileges, if appropriate. A user that is granted administrative rights can run sudo commands and commands that 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 Extreme Management Center 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 **false**. These users are granted permission to log in, no matter what the authentication setting is set to: OS Authentication, LDAP Authentication, or RADIUS authentication. All authentication methods allow the non-automatic users to log in.

User Name

The users added as authorized users.

Domain/Host Name

The user's domain/hostname used to authenticate to the Extreme Management Center database.

Authorization Group

The authorization group to which the user belongs.

Automatic Member

A value of **true** indicates that the user is automatically added to the authorization group via LDAP or RADIUS authentication, or the OS Authentication Automatic Membership feature. A value of **false** 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

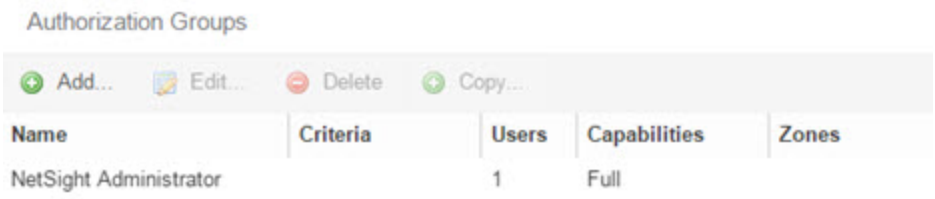
Opens the Add/Edit User window, which allows you to modify the authorization group membership for the selected user.

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 Extreme Management Center 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 or RADIUS authentication, users are dynamically assigned to authorization groups based on the attributes associated with that user in Active Directory. 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 Extreme Management Center 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 or RADIUS. 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.

Criteria
This column displays the membership criteria defined for the associated group.

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.

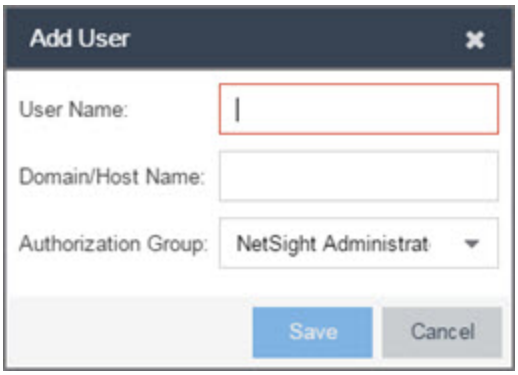
Delete
Removes the selected group from the Groups table.

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 Extreme Management Center database.



User Name

The name used for this authorized user.

Domain/Host Name

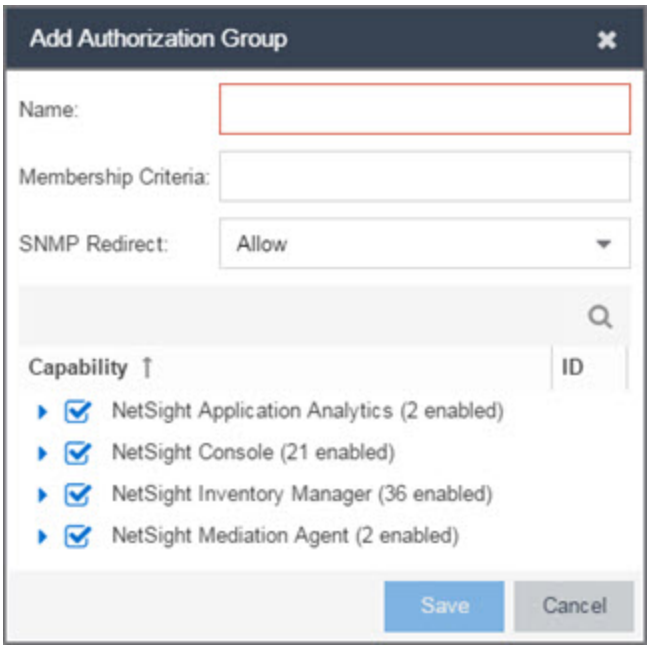
The user's domain/hostname used to authenticate to the Extreme Management Center database.

Authorization Group

Use the drop-down menu 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.

NOTE: Extreme Management Center 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 Extreme Management Center Server, regardless of the setting for Client/Server SNMP Redirect.

- NEVER — Never redirects SNMP requests to the Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center database. For additional information on discovering and adding devices, see How to Discover Devices in Extreme Management Center.

For a list of instructions outlining the initial setup of your network in Extreme Management Center, see Extreme Management Center Initial Configuration Checklist.

When you first log into Extreme Management Center 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 Extreme Management Center, which is accomplished by performing the following steps:

1. Create Authorization Groups
2. Add Users to Authorization Groups
3. Select the Authentication Method

IMPORTANT: Extreme Management Center 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 Extreme Management Center users.

1. Access the **Administration** > Users tab.
2. Click 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 allows you to make changes to the authorization groups and authorized users.

3. Click the **Add** button in the Authorization Groups section at the bottom of the tab.
4. Enter the appropriate information for each authorization group using Extreme Management Center.
   The Capability section of the window allows 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. Click 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 Extreme Management Center and add them to an authorization group depending on the level of access they require.

1. Click 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. Click the **Save** button to save the new user.
4. Repeat the process to add all Extreme Management Center users for each authorization group.

Select the Authentication Method

Finally, use **Administration** > **Users** tab to select the method by which users authenticate when accessing Extreme Management Center.

Extreme Management Center 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 menu 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. Click the **Release Lock** button to allow other users to make changes.

The users you added now have access to the functionality you configured for their respective authorization group.

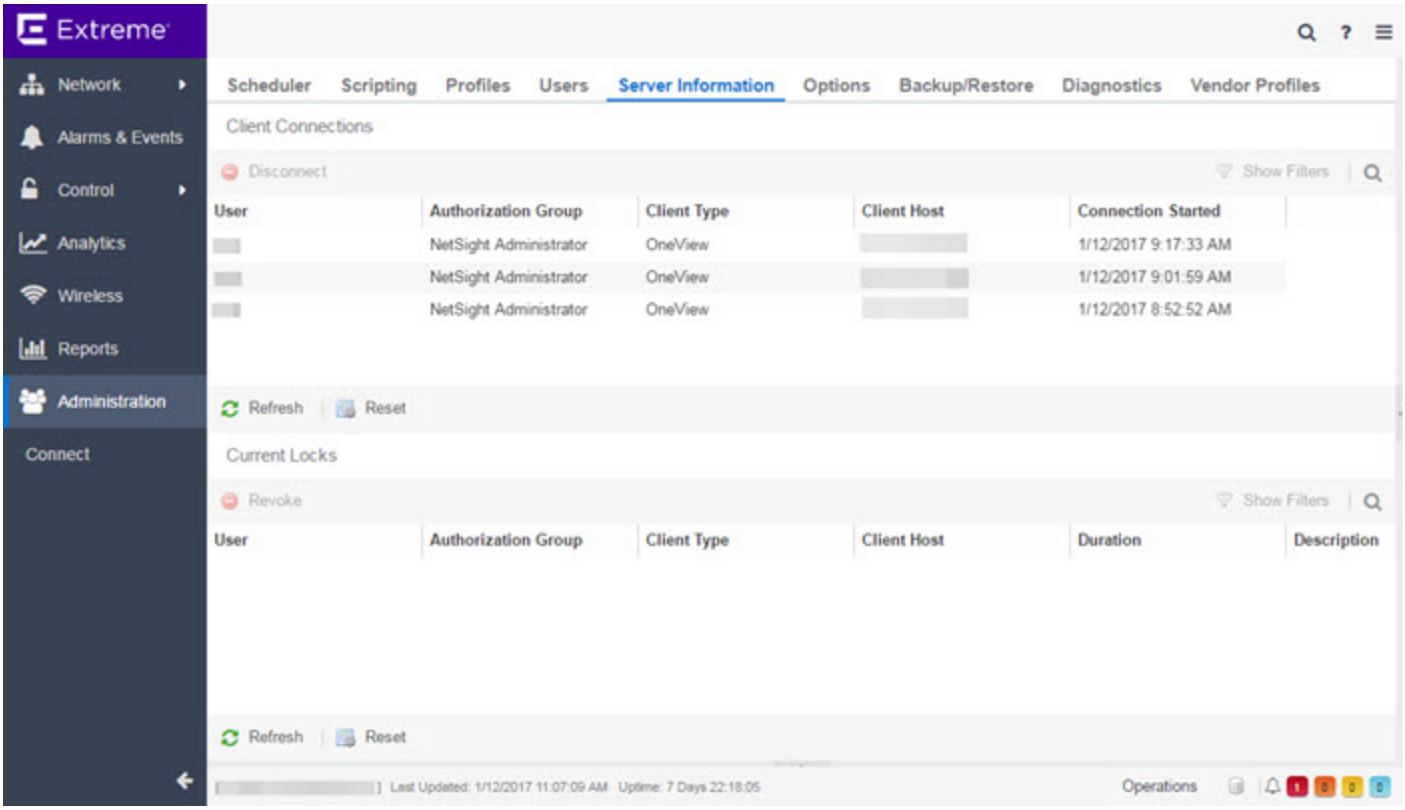
Related Information

For information on related topics:

- Users
- Authorization Group Capabilities

Server Information

The Server Information tab lets you view and manage Extreme Management Center 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 Extreme Management Center 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 clicking 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 Extreme Management Center 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:

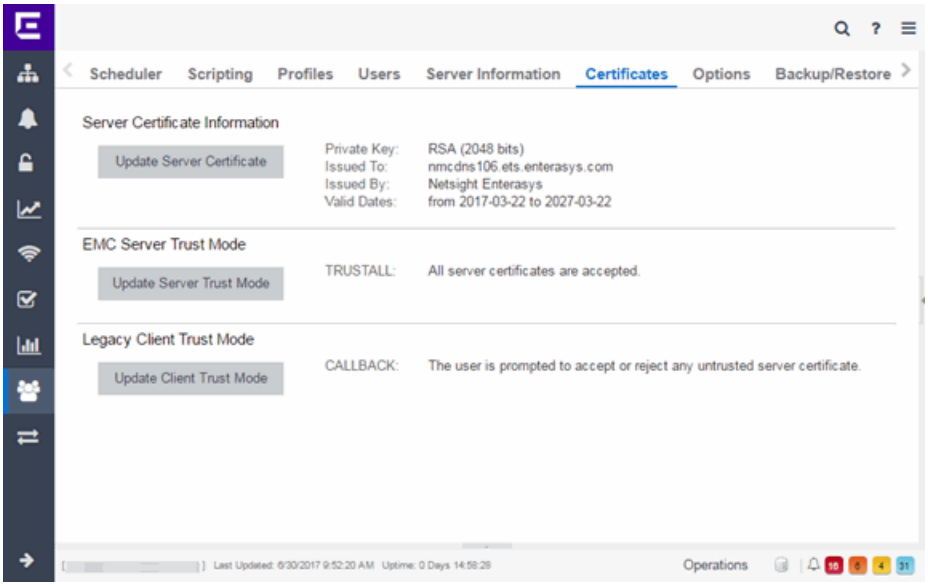
- Users

Extreme Management Center Certificates

The **Certificates** tab provides a central location for managing certificates in Extreme Management Center.

Use this tab to perform the following:

- Update the Extreme Management Center server certificate by replacing the server private key and certificate.
- View and change the server trust mode that specifies how servers in the Extreme Management Center 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

Click the **Update Server Certificate** button to open the Update Server Certificate window, where you can replace the Extreme Management Center server private key and certificate. For information and steps on how to update the certificate, see How to Update the Server Certificate.

XMC Server Trust Mode

This section displays the current server trust mode that specifies how servers in the Extreme Management Center deployment handle certificates from other servers. Click the Update Server Trust Mode button to open the Update Server Certificate 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. Click the Update Client Trust Mode button to open the Update Client Certificate Trust Mode window, where you can change the client trust mode.

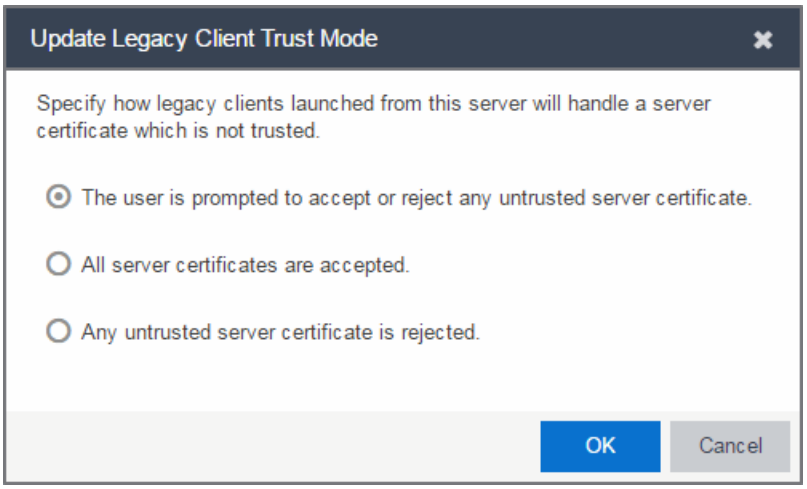
Related Information

For information on related windows:

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

Extreme Management Center Update Legacy Client Trust Mode Window

This window lets you update the client certificate trust mode that specifies how Extreme Management Center 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.



Extreme Management Center use server certificates to provide secure communication between the Extreme Management Center server and legacy java application clients. When a server certificate is replaced, Extreme Management Center 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.

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.

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.

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

Extreme Management Center Update Server Certificate Window

The Extreme Management Center server uses a private key and server certificate to provide secure communication for administrative web pages, Extreme Management Center and Extreme Access Control Dashboard tools, and for internal communication between servers. The Update Server Certificate window lets you replace the Extreme Management Center server certificate. You can access this window from the Administration > Certificates tab.

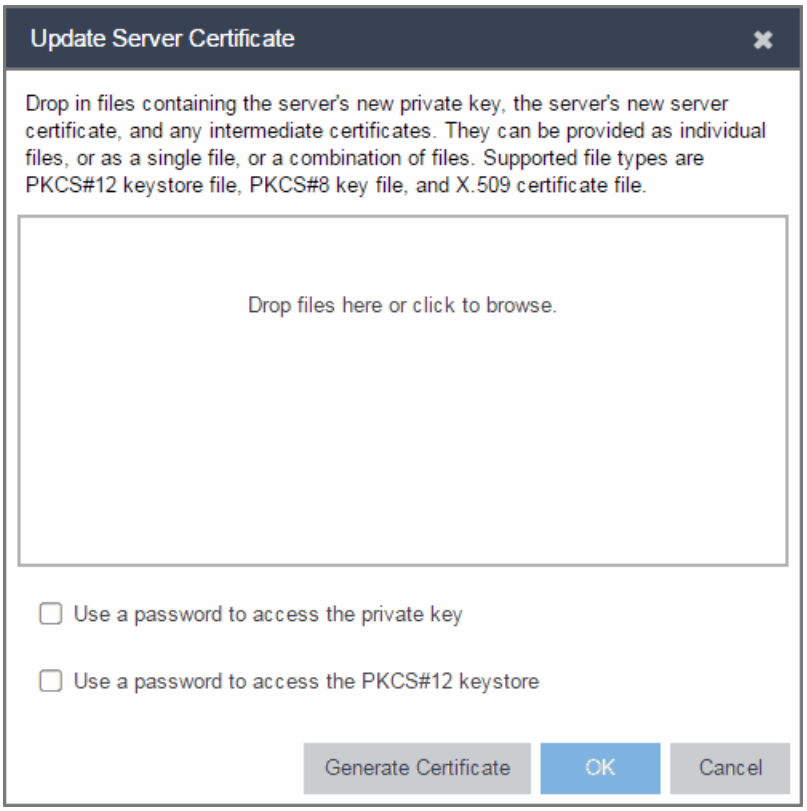
During installation, Extreme Management Center generates a unique private server key and server certificate. While these provide secure communication, there may be cases where you want to update the Extreme Management Center server certificate to a custom certificate provided from an external certificate authority, or add certificates in order to meet the requirements of external components with which Extreme Management Center must communicate. Additionally, you may want to 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 Extreme Management Center server to deploy the new private key and server certificate.

NOTE: Whenever the Extreme Management Center server certificate is changed, other Extreme Management Center components may be affected by the change and stop trusting the server. You can specify how Extreme Management Center clients and other servers handle updated certificates by configuring the client trust mode and server trust mode settings. Before updating the Extreme Management Center 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 Extreme Management Center 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

Click Generate Certificate to automatically generate a new private key and certificate using the same method that occurs when Extreme Management Center is installed. Using this method does not require you to provide any files or passwords.

OK

Click OK to save your changes.

Cancel

Click Cancel to close the window and discard your changes.

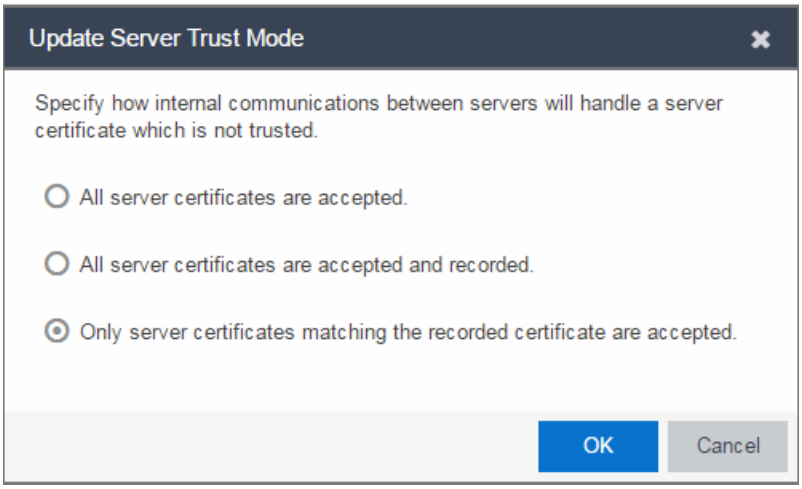
Related Information

For information on related topics:

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

Extreme Management Center Update Server Trust Mode Window

This window lets you set the server certificate trust mode that specifies how all the servers in your Extreme Management Center deployment handles certificates received from other servers. Access this window from the Administration > Certificates tab.



Depending on your deployment, there can potentially many servers in Extreme Management Center and Extreme Access Control. For example, there is the Extreme Management Center server, the Extreme Access Control engine servers, and Extreme Access Control assessment servers. In addition, there may be external servers such as LDAP servers with which both Extreme Management Center and Extreme Access Control may 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 Extreme Management Center/Extreme Access Control deployment, and is also suitable when the network is sufficiently protected from spoofing attacks.

Use this mode when troubleshooting trust problems on the network. It allows the Extreme Management Center server to communicate with all Extreme Access Control engines, and configure those engines to accept all certificates. This restores any communication broken due to a trust issue and allows you to resolve the problem from Extreme Access Control.

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.

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.

When the trust mode is changed, the Extreme Management Center server is immediately changed to use the new mode. Extreme Access Control engines begin using the new trust mode when enforced.

For more information on how to use trust modes, see Advanced Security Options in the Secure Communication Help topic.

Related Information

For information on related topics:

- Certificates Tab
- Update Client Certificate Trust Mode Window

How to Update the Server Certificate

Extreme Management Center allows you to change the server key and certificate generated during installation. While these provide secure communication, you may want to update to a certificate provided from an external certificate authority, or add certificates in order to meet the requirements of external components with which Extreme Management Center 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 Extreme Management Center 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 How to 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

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 Extreme Management Center 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. Extreme Management Center 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 Extreme Management Center and Extreme Access Control 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 Extreme Management Center server certificate is changed, other Extreme Management Center components may be affected by the change and stop trusting the server. Extreme Management Center 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 Extreme Management Center 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. Click the **Update Server Certificate** button. The Update Server Certificate window opens.
3. Drag and drop a private key, certificate file, or a keystore file. Click 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. Click **OK**.

   A confirmation window listing your file information displays.
7. Confirm that the information you provided is correct.
8. Click **Yes** to proceed with the certificate replacement.

   The private key and server certificate updates on the Extreme Management Center server.
9. Restart the Extreme Management Center server to deploy the new private key and server certificate.

Verifying the Certificate

Once 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 Extreme Access Control Dashboard web page at `https://<NetSight Server FQDN>:8443/Monitor/jsp/nac/dashboard.jsp`. or the Extreme Management Center 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.

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 -topk8
      -out <output file>
      ```

      For example:
      ```
      openssl genrsa 2048 | openssl pkcs8 -topk8 -out
      ```

```
server.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.

2. Create a Certificate Signing Request:

   a. Enter the following command to generate a CSR file. Use the output file name you used in step 1 above as the input file, and specify the output file name you prefer:

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

   For example:

   ```
   openssl req -new -key server.key -out server.csr
   ```

   b. You are prompted for information that appears in the certificate. When you are prompted for a Common Name, specify the fully qualified host name of the Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center 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 clicking 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.

The capabilities are divided into suite-wide and application-specific capabilities. Checking a capability grants access to that capability.

The following sections provide a description of each capability:

- Extreme Management Center Application Analytics
- Extreme Management Center Console
  - Wireless Manager
  - VLAN Models
- Extreme Management Center Mediation Agent
- Extreme Management Center NAC Manager
- Extreme Management Center OneView
- Extreme Management CenterPolicy Manager
- Extreme Management Center Suite
  - Authorization/Device Access
  - Common Web Services
  - Credentials Web Service
  - Device Local Management WebView
  - Devices

Extreme Management Center Application Analytics

Application Analytics Read Access

Allows the ability to access the Analytics tab and view the Application Analytics reports. The Application Analytics feature is available with the Extreme Management Center (NetSight) Advanced (NMS-ADV) license.

Application Analytics Read/Write Access

Adds the ability to view the Analytics > Configuration tab and configure Application Analytics engines and NetFlow and Application Telemetry Collecting devices. Also adds the ability to create and modify fingerprints.

Extreme Management Center Console

Launch a NetSight (Extreme Management Center) Console Client

Allows the ability to launch the Console application. An error message appears for users who do not have this capability when they attempt to launch Console.

MIB Tools

Allows the ability to launch MIB Tools from the Console menus.

Allow SNMP sets to Devices

Allows the ability to write SNMP sets to network devices.

Modify Compass SNMP MIBs

Allows the ability to select Compass SNMP MIBs in the Compass options panel.

Modify Device Access

Allows the ability to modify device access information in the Access Properties tab.

Show Passwords in Clear Text
Allows the ability to view passwords in clear text in various Console windows.

Device Manager
Allows the ability to launch Device Manager from a device.

TFTP Download
Allows the ability to perform a configuration upload/download or firmware image download on a device.

Trap Configuration
Allows the ability to launch and use the Trap Receiver Configuration window.

Configure FlexViews
Allows the ability to create and modify FlexViews.

Syslog Configuration
Allows the ability to launch and use the Syslog Receiver Configuration window.

Wireless Manager

Launch
Allows the ability to launch Wireless Manager from the Console Tools menu.

Configure
Allows the ability to configure Wireless Manager.

VLAN Models

View
Allows the ability to view VLAN Models using the VLAN Elements Editor, accessed from the VLAN tab in Console.

Configure
Allows the ability to configure VLAN Models using the VLAN Elements Editor, accessed from the VLAN tab in Console.

Extreme Management Center Mediation Agent

Read access to the Mediation Agent Web Services API
Provides the Application Analytics engine with read access to Extreme Management Center (Extreme Management Center) via web services API.

Read/Write access to the Mediation Agent Web Services API

Provides the Application Analytics engine with read/write access to Extreme Management Center via web services API.

Extreme Management CenterNAC Manager

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.

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.

Read access to the NAC Web Services API

Provides read access to the NAC web service, which is a third-party integration point. The NAC web service exposes methods for manipulating NAC infrastructure components.

Read/write access to the NAC Web Services API

Provides read/write access to the NAC web service, which is a third-party integration point. The NAC web service exposes methods for manipulating NAC 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/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.

Extreme Management Center OneView

Access OneView

Allows the ability to launch the Extreme Management Center web-application formerly known as OneView, but does not provide any Extreme Management Center report access. Selecting only this capability without any other capabilities would be the same as not allowing access to Extreme Management Center.

Access OneView Reports

Adds the ability to view all reports accessed from the Reports tab.

Access OneView Search

Adds the ability to use the Search tab.

Access OneView Administration

Adds the ability to access administration tools and enable data collection.

NetFlow Read Access

Adds the ability to view the Flows tab.

Maps

Allows the ability to perform the following map functions:

- Maps Read Access - Adds the ability to access the Map tab and view the maps.
- Maps Read/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).

Events and Alarms

Allows the ability to perform the following event and alarm functions:

- OneView Event Log Access - Allows the ability to view device information and event log details.
- OneView Alarms Read Access - Allows the ability to view current alarms in the Alarms and Events tab.
- OneView Alarms Read/Write Access - Allows the ability to view and clear alarms in the Alarms and Events tab.

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.

Identity and Access

Allows the ability to perform the following Extreme Access Control functions:

- Access OneView 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.
- 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.

NetSight (Extreme Management Center) Manager Access

Adds the ability to access the NetSight (Extreme Management Center) Manager.

Extreme Management Center Policy Manager

Launch NetSight (Extreme Management Center) Policy Manager

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.

Read/Write capabilities for Policy Enforcement and Management

Allows the ability to manage and enforce policy to network devices using Policy Manager.

Read/Write access to the Policy Web Service APIs

Provides read/write access to the Policy web service, which is a third-party integration point. The Policy web service allows programmatic access to policy management.

Extreme Management Center Suite

The following capabilities apply to all Extreme Management Center applications.

Authorization/Device Access

View Authorization/Device Access

Allows the ability to view, but not to configure the Authorization/Device Access tool, accessed from the Tools menu in any Extreme Management Center application. Users who attempt to access the tool without this capability see an error message.

Configure Users, User Groups, and Capabilities

Allows access to the Users/Groups tab in the Authorization/Device Access tool and the ability to create and edit users and authorization groups.

Configure Profiles/Credentials

Allows access to the Profiles/Credentials tab in the Authorization/Device Access tool and the ability to define the SNMP credentials used to access network devices and the profiles that use those credentials.

Configure Profile/Device Mapping

Allows access to the Profile/Device Mapping tab in the Authorization/Device Access tool and the ability to specify the SNMP profiles each authorization group uses when communicating with each device.

Configure LDAP and RADIUS 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.

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.

Common Web Services

Read access to the Web Services APIs2

Provides read access to the Extreme Management Center Common web service, which is a third-party integration point. The Common web service exposes methods for manipulating Extreme Management Center infrastructure components.

Read/write access to the Web Services APIs

Provides read/write access to the Extreme Management Center Common web service, which is a third-party integration point. The Common web service exposes methods for manipulating Extreme Management Center infrastructure components.

Credentials Web Service

Read operations

Provides read access to the Extreme Management Center Credentials web service, allowing programmatic access to authentication profiles and credentials used for device access.

Read/write operations

Provides read/write access to the Extreme Management Center Credentials web service, allowing programmatic access to authentication profiles and credentials used for device access.

Device Local Management WebView

Auto Login to Web Local Management for NAC Appliances

Allows the ability to launch local management for Extreme Access Controlengines 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 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.

Devices

Add, Discover, and Import

Allows the ability to add devices using the Add Device window, discover devices using the Discover tool, and import devices using the File > Device List > Import Devices option.

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 Extreme Management Center database.

Export

Allows the ability to export a device list using the File > Device List > Export option.

Configure Status Polling Options

Allows the ability to set suite-wide Status Polling options available from the Tools > Options window.

Execute Command Scripts

Allows the ability to execute command scripts (using the Command Script tool) on a device in Console or Inventory Manager.

Events and Alarms

Events

Allows the following Event configuration capabilities:

- View Event Logs - View event logs in all Extreme Management Center 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.
- Configure Event Options - Set suite-wide Event Logs options available from the Tools > Options window.
- Acknowledge Events - Acknowledge events in the event log.

- Configure Server Log Managers - Add, edit, and remove Log Managers using the Event View Manager window.
- Clear and Roll Server Log Managers - Clear and roll event logs on the Extreme Management Center Server using the button in the lower-right corner of the event log.

Alarms

Allows the following Alarm configuration capabilities:

- View - View alarms in the Event Log.
- Configure - Configure alarms using the Alarms Manager window.

Extreme Management Center (formerly NetSight) All User Options

These capabilities provide the ability to set suite-wide options that apply to all users, using the Tools > Options window.

Configure Services for NetSight (Extreme Management Center) Server Options

Allows the ability to specify TFTP settings.

Configure SMTP E-mail Options

Allows the ability to specify the SMTP E-Mail server used by the Extreme Management Center E-Mail notification feature.

Request and Configure ExtremeNetworks.com Support

Allows the ability to request information about the latest Extreme Management Center 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 Extreme Management Center products and firmware are available and allow you to download newer versions to keep your software and firmware current.

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.

Server Information

View Server Information

Allows the ability to view, but not to configure the Server Information tool, accessed from the Tools menu in any Extreme Management Center application. Users who do not have this capability see an error message when they attempt to access the tool.

Configure Server View

Allows the ability to view and configure Extreme Management Center Console client connection options:

- View - Access and view the Client Connections Options window.
- Configure - Configure the type and number of clients that can connect to your server.

Extreme Management Center Database

Allows the following Extreme Management Center database management capabilities:

- View or Change Database Password - View and change the password the Extreme Management Center Server uses to access the database.
- Change Database URL - Change the URL the Extreme Management Center Server uses when connecting to the database.
- Backup Database - Save the currently active database to a file.
- Restore or Initialize Database - Restore the initial database or restore a saved database.
- Initialize Plugin Data - Initialize a specific Extreme Management Center application's components in the Extreme Management Center database by using the File > Database > Initialize Components menu option.

Disconnect Clients

Allows the ability to disconnect clients in the Client Connections tab and to configure the User Inactivity option in the Client Connections Suite-Wide options panel.

Revoke Locks

Allows the ability to revoke operation locks in the Locks tab.

Server Information

The Server Information tab lets you view and manage Extreme Management Center client connections and locks. You must be assigned the appropriate user capabilities to access and use this tab.

ZTP+ Registration

Allows the ability to configure a ZTP+ enabled device and add it to Extreme Management Center.

Northbound API

Extreme Management Center Northbound API Read Access

Allows the ability to access Extreme Management Center information from third-party integrations via an API.

Vendor Profiles

Extreme Management Center Vendor Profile Read Access

Allows the ability to view vendor profiles on the Administration tab in Extreme Management Center.

Extreme Management Center Vendor Profile Read/Write Access

Allows the ability to view and configure vendor profiles on the Administration tab in Extreme Management Center.

Workflows

Extreme Management Center Workflows Read Access

Allows the ability to view workflows on the Tasks tab in Extreme Management Center.

Extreme Management Center Workflows Read/Write Access

Allows the ability to view and edit workflows on the Tasks tab in Extreme Management Center.

NOTE: Access to some Extreme Management Center components is determined by capabilities in other capabilities groups:

NetSight (Extreme Management Center) Console > Wireless Manager > Launch
Adds the ability to view the **Wireless** tab.

NetSight (Extreme Management Center) Suite > Devices > Add, Discover and Import
Adds the ability to add devices in the **Network** tab.

NetSight (Extreme Management Center) 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.

Extreme Access Control Options

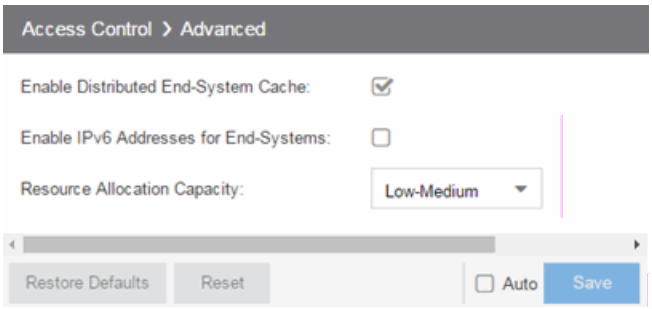
Selecting Extreme Access Control in the left panel of the **Options** tab provides the following view, where you can edit settings associated with the **Control** > Extreme Access Control tab. The right-panel view changes depending on what you select in the left-panel tree. Expand the Extreme Access 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. Clicking this button changes the field back to the system default value.

Click the link for information on the following Extreme Access Control options:

Advanced

This view lets you configure advanced settings for the **Extreme 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 Extreme Access Control 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 Extreme Management Center Server (using this option) and on the Extreme Access Control engines using the cache.

When this feature is enabled, the Extreme Management Center Server and the Extreme Access Control 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 Extreme Management Center Server and the Extreme Access Control engine, and end-systems are adding or moving frequently.

Enable IPv6 Addresses for End-Systems

The Enable IPv6 Addresses for End-Systems option allows Extreme Access Control to collect, report, and display IPv6 addresses for end-systems in the end-systems table. When this option is changed, you must enforce your engines before the new settings take effect. In addition, end-systems need to rediscover their IP addresses in order to reflect the change in the end-systems table. This can be done by either deleting the end-system or performing a Force Reauth on the end-system.

Only end-systems with a valid IPv4 address as well as one or more IPv6 addresses are supported. End-systems with only IPv6 addresses are not supported. End-system functionality support varies for IPv6 end-systems. For complete information, see IPv6 Support in the Extreme Management Center Configuration Considerations Help topic.

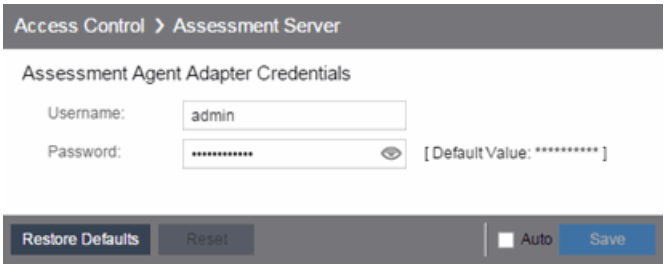
Resource Allocation Capacity

The Resource Allocation Capacity option lets you configure the Extreme Management Center resources allocated to end-system and configuration processing services. The greater the number of end-systems and engines in your Extreme Access Control deployment, the more resources it requires.

- Low - For low performance shared systems.
- Low-Medium - For medium performance shared systems, or low performance dedicated systems
- Medium - For medium performance shared systems, or medium performance dedicated systems.
- Medium-High - For high performance shared systems, or medium performance dedicated systems.
- High - For high performance dedicated systems.
- Maximum - For extremely high performance dedicated systems.

Assessment Server

These options let you provide assessment agent adapter credentials.

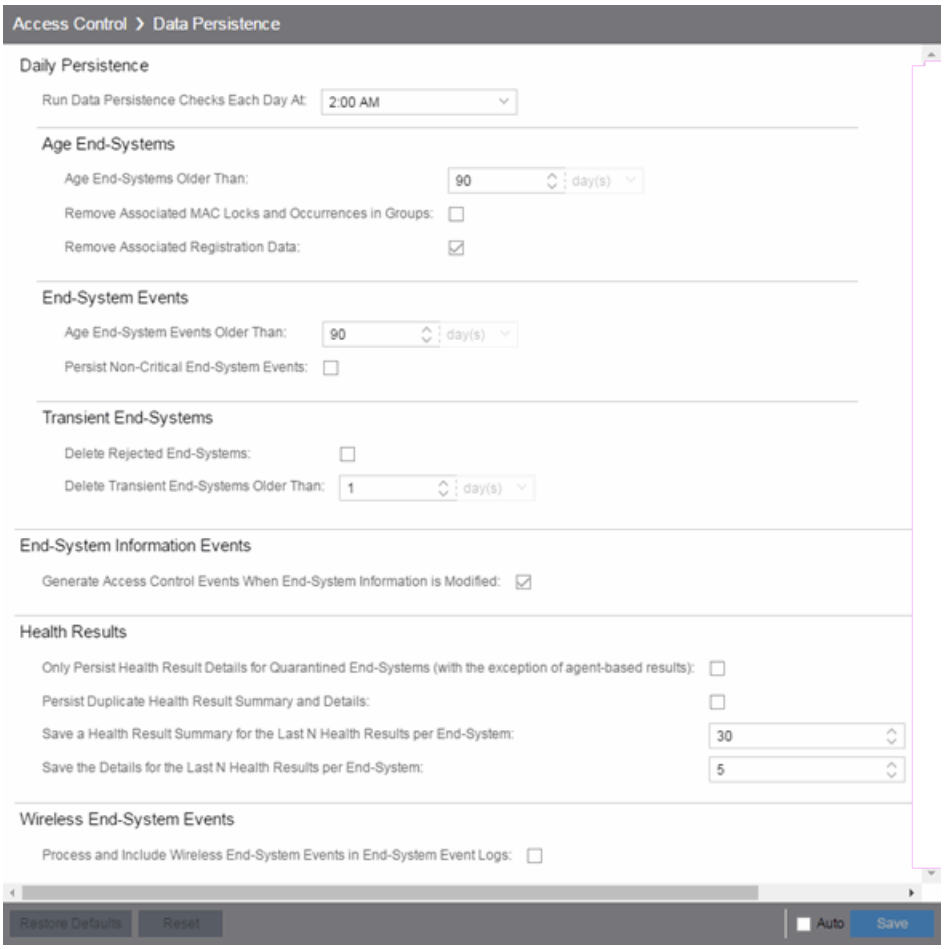


Assessment Agent Adapter Credentials

Specify the username and password the Extreme Access Control engine uses when attempting to connect to network assessment servers, including Extreme Networks Agent-less, Nessus, or a third-party assessment server (an assessment server not supplied or supported by Extreme Management Center). The password is used by the assessment agent adapter (installed on the assessment server) to authenticate assessment server requests. Extreme Management Center 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

This panel lets you customize how Extreme Access Control ages-out or deletes end-systems, end-system events, and end-system health (assessment) results from the tables and charts in the End-Systems view.



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 Extreme Management Center keeps end-system information in the database. Each day, when the Data Persistence check runs, it searches the database for end-systems for which Extreme Access Control did not receive an event in the number of days specified (90 days by default). It removes those end-systems from the End-System table in the End-Systems tab.

If you select the Remove Associated MAC Locks and Occurrences in Groups checkbox, the aging check also removes any MAC locks or group memberships associated with the end-systems being removed.

The Remove Associated Registration Data checkbox is selected by default, so that the aging check also removes any registration data associated with the end-systems being removed.

End-System Events

Age End-System Events Older Than

End-system events are stored in the database. Each day, when the Data Persistence check runs, it removes all end-system events which are older than the number of days specified (90 days by default).

Persist Non-Critical End-System Events

Select this checkbox to save non-critical end-system events (e.g. duplicate end-system events, re-authentication events where the end-system's state did not change) to the database.

Transient End-Systems

Delete Rejected End-Systems

Select this checkbox to delete end-systems in the Rejected state as part of the cleanup.

Delete Transient End-Systems Older Than

Specify the amount of time to keep transient end-systems in the database before they are deleted as part of the nightly database cleanup task. The default value is 1 day. A value of 0 disables the deletion of transient end-systems. Transient end-systems are unregistered end-systems not seen for the specified number of days.

End-systems are not deleted if they are part of an End-System group or there are MAC locks associated with them.

End-System Information Events

Generate Extreme Access Control Events When End-System Information is Modified

Select the checkbox if you want Extreme Access Control to generate an event when end-system information is modified.

Health Results

Only Persist Health Result Details for Quarantined End-Systems (with the exception of agent-based results)

Select this checkbox to only save the health result details for quarantined end-systems (with the exception of agent-based health result details, which are always saved for all end-systems).

Persist Duplicate Health Result Summary and Details

Select this checkbox to save duplicate health result summaries and details. By default, duplicate health results obtained during a single scan interval are not saved. For example, if the assessment interval is one week, and an end-system is scanned five times during the week with identical assessment results each time, the duplicate health results are not saved (with the exception of administrative scan requests such as Force Reauth and Scan, which are always saved). This reduces the number of health results saved to the database.

Save a Health Result Summary for the Last N Health Results per End-System

Specify how many health (assessment) result summaries are saved and displayed in the End-Systems tab for each end-system. By default, the Data Persistence check saves the last 30 health result summaries for each end-system.

Save the Details for the Last N Health Results per End-System

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

Wireless End-System Events

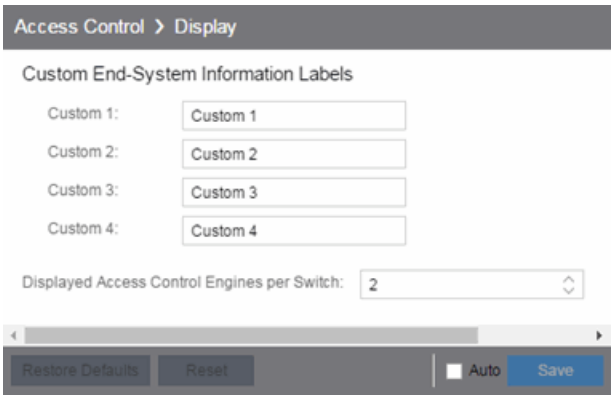
Process and Include Wireless End-System Events in End-System Event Logs

Select the checkbox if you want Extreme Management Center to generate an event when wireless end-system information is modified. This option is disabled by

default.

Display

This Options view lets you 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 Extreme Access Control Gateways you can select when adding or editing a switch in an Extreme Access Control Engine group.



Custom End-System Information Labels

This option lets you specify new text for the **Custom** column headings in the End-System table on the **End-Systems** tab.

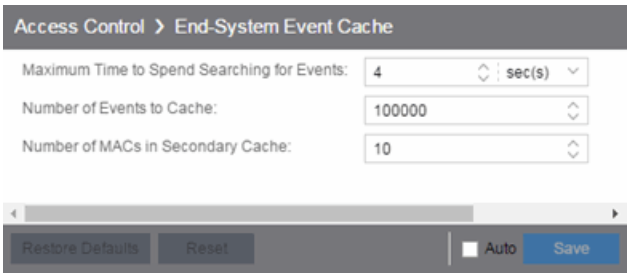
Displayed Extreme Access Control Engines per Switch

Select the number of Extreme Access Control engines displayed in the Add Switches to Group or Edit Switches in Group windows. By default, these windows allow you to configure two Extreme Access Control engines per switch for redundancy, but this option allows 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 allows Extreme Access Control to quickly retrieve and display end-system events without having to search through the database.

These options let you configure the amount of resources used by the end-system event cache.



Maximum Time to Spend Searching for Events

Specify the time Extreme Management Center 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 may 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 click Save.

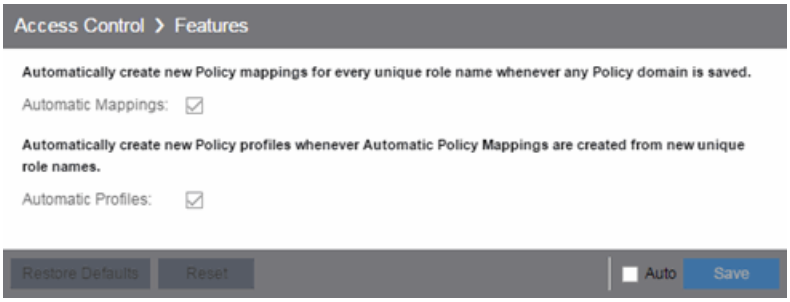
When an engine configuration audit is performed during an Enforce operation, warning messages may be displayed in the audit results listed in the Enforce window. If there is a warning associated with an engine, you are given the option to acknowledge the warning and proceed with the enforce anyway.

These settings allow you to select specific warning messages you do not want displayed in the audit results. This allows 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 Extreme Access Control configuration. By selecting that warning here, it is ignored in future audit results and you no longer need to acknowledge it before proceeding with the Enforce.

Features

This panel lets you 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 Extreme Access Control windows.



Notification Engine

This panel lets you define the default content contained in Extreme Access Control notification action messages. For example, with an email notification action, define the information contained in the email subject line and body. With a syslog or trap notification action, define the information included in the syslog or trap message.

There are certain "keywords" available to use in your email, syslog, and trap messages to provide specific information. Following is a list of the most common keywords used. For additional information, see Keywords.

- $type - the notification type.
- $trigger - the notification trigger.
- $conditions - a list of the conditions specified in the notification action.
- $ipaddress - the IP address of the end-system that is the source of the event.
- $macaddress - the MAC address of the end-system that is the source of the event.
- $switchIP - the IP address of the switch where the end-system connected.
- $switchPort - the port number on the switch where the end-system connected.
- $username - the username provided by the end user upon connection to the network.

Custom Arguments

If the notification action specifies a custom program or script to be run on the Extreme Management Center Server, then use this field to enter the "all" option. Using the "all" option returns values for all the Extreme Access Control Notification keywords applicable to the notification type. For additional information, see Keywords.

Email Subject
Defines the text and keyword values included in the email subject line.

Email Body
Defines the text and keyword values included in the email body.

Syslog Message
Defines the text and keyword values included in the syslog message.

Syslog Tag
Defines the string used to identify the message issued by the syslog program.

Trap Message
The varbind sent in the trap.

Trap Message OID
The OID of the varbind being sent that represents the message.

Trap OID
The OID that defines the trap.

Event Queue Service Period
Defines how often the queue is checked for events to process. The dispatcher runs once 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.

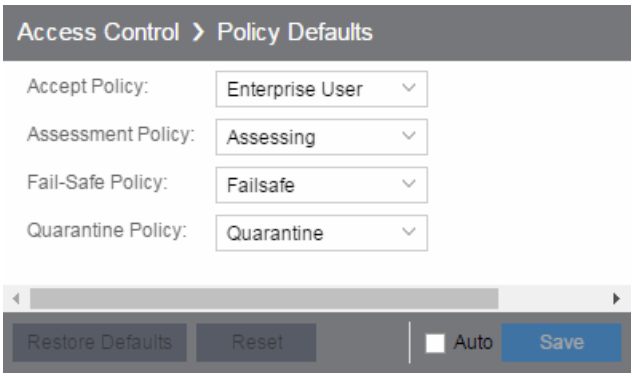
Maximum Events Serviced Each Period
The maximum number of events pulled from the queue for processing each service period. By default, the dispatcher processes 100 events every service period.

Policy Defaults

This Options view lets you 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 Extreme Access Control profile. For example, if you specify an Assessment policy called "New Assessment" as the Policy Default, then "New Assessment" is automatically displayed as the first selection in the Assessment Policy drop-down menu in the New Extreme Access Control Profile window.

Extreme Management Center 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. Once 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 Extreme Access Control engine and passed an assessment (if an assessment was required), or the "Replace RADIUS Attributes with Accept Policy" option is used when authenticating the end-system.

Assessment Policy

Select the default Assessment policy. The Assessment policy is applied to an end-system while it is being assessed (scanned).

Fail-Safe Policy

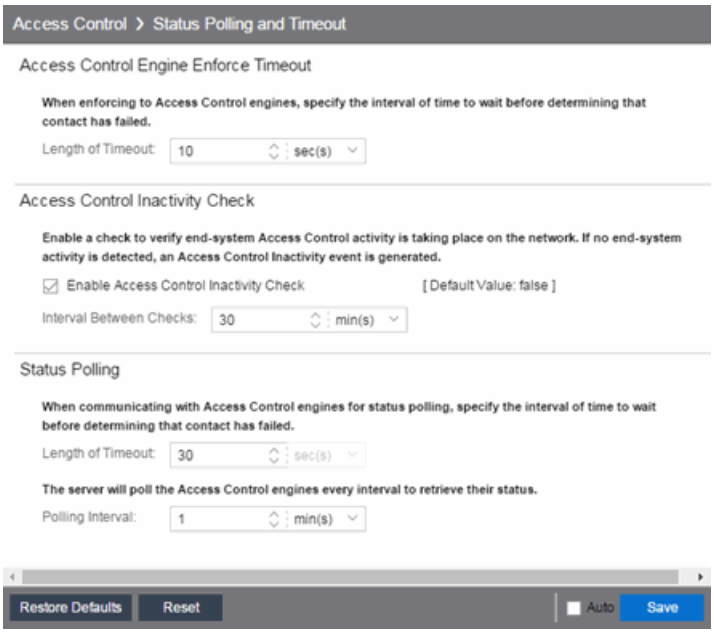
Select the default fail-safe policy. The fail-safe policy is applied to an end-system if the end-system's IP address cannot be determined from its MAC address, or if there is a scanning error and an assessment of the end-system could not take place.

Quarantine Policy

Select the default Quarantine policy. The Quarantine policy is applied to an end-system if the end-system fails an assessment.

Status Polling and Timeout

This Options panel lets you specify the enforce timeout and status polling options for Extreme Access Control engines.



Extreme Access Control Engine Enforce Timeout

When enforcing to Extreme Access Control engines, this value specifies the amount of time Extreme Management Center waits for an enforce response from the engine before determining the engine is not responding. During an enforce, an Extreme Access Control 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.

Extreme Access Control Inactivity Check

Enable a check to verify end-system Extreme Access Control activity is taking place on the network. If no end-system activity is detected, an Extreme Access Control Inactivity event is sent to the Events view. Use the Alarms and Events tab to configure custom alarm criteria based on the Extreme Access Control Inactivity event to create an alarm, if desired.

Status Polling

Length of Timeout — When communicating with Extreme Access Control engines for status polling, this value specifies the amount of time Extreme Management Center waits before determining contact failed. If Extreme Management Center does

not receive a response from an engine in the defined amount of time, Extreme Management Center considers the engine to be "down". The engine status refers to Messaging connectivity, not SNMP connectivity. This means that if the engine is "down," Extreme Management Center is not able to enforce a new configuration to it.

Polling Interval — Specifies the frequency Extreme Management Center polls the Extreme Access Control engines to determine engine status.

Related Information

For information on related topics:

- Extreme Access Control

Alarm Options

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

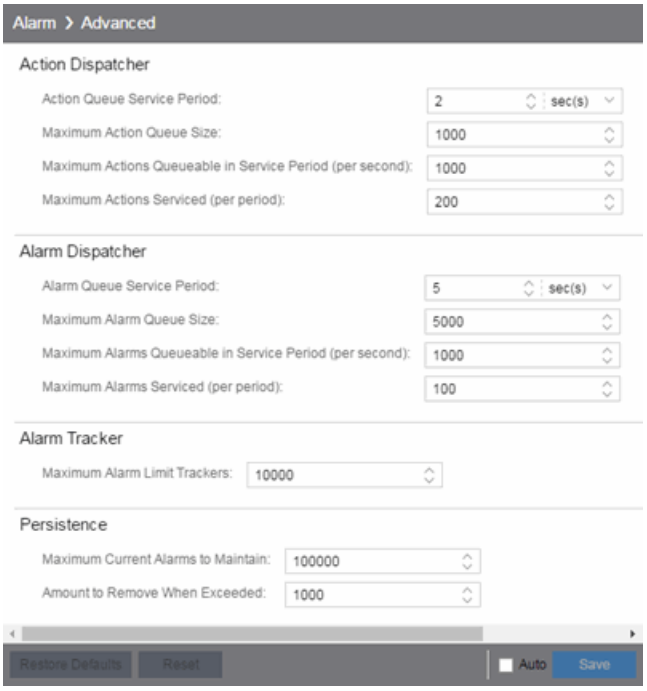
Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.

Click the link for information on the following Alarm options:

- Advanced
- Alarm Action Defaults
- Alarm History
- Consolidate Email
- Override Email

Advanced

This view lets you configure advanced settings for the alarms functionality in Extreme Management Center. These settings apply to all users.



Action Dispatcher Options

Use these options to limit resources used by Extreme Management Center 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 once 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 once 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 Extreme Management Center 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 once 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 once 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

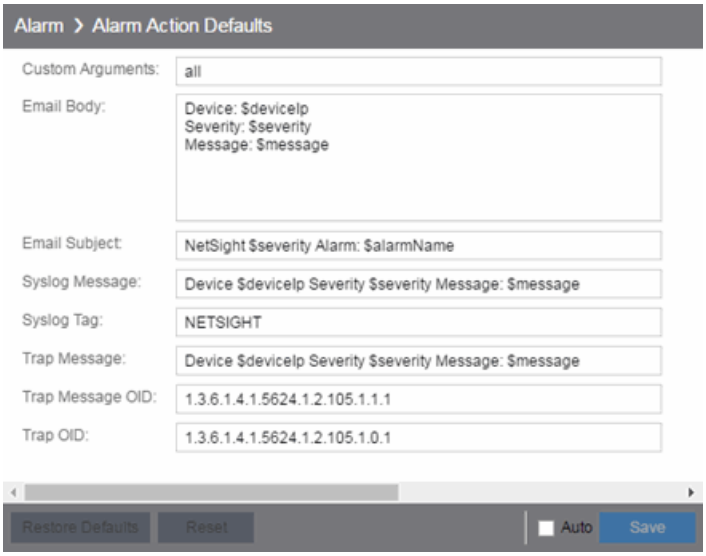
When you define an alarm with a limit, Extreme Management Center tracks whether the limit is exceeded and when to reset the count. This option sets the maximum number of alarms that Extreme Management Center tracks. (An alarm limit specifies the number of times the alarm action performed for an alarm.)

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 Extreme Management Center 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. These values are used 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 Extreme Management Center 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.

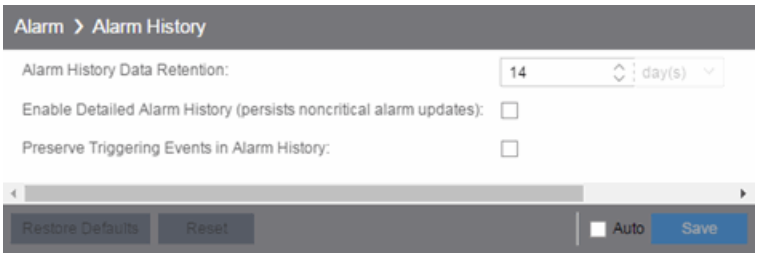
Trap Message
The varbind sent in the trap.

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.

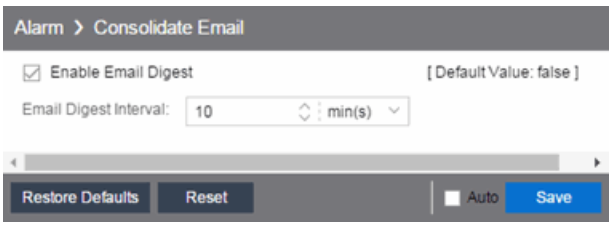
Enable Detailed Alarm History (persists noncritical alarm updates)

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 clicking the View Trigger button in the Alarm History window.

Consolidate Email



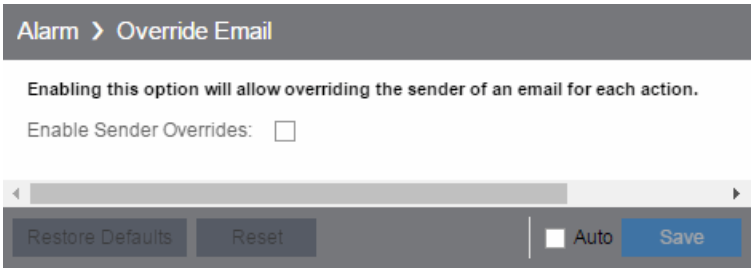
Enable Email Digest

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 Extreme Management Center waits before sending an email of alarm actions when Select Enable Email Digest is selected.

Override Email



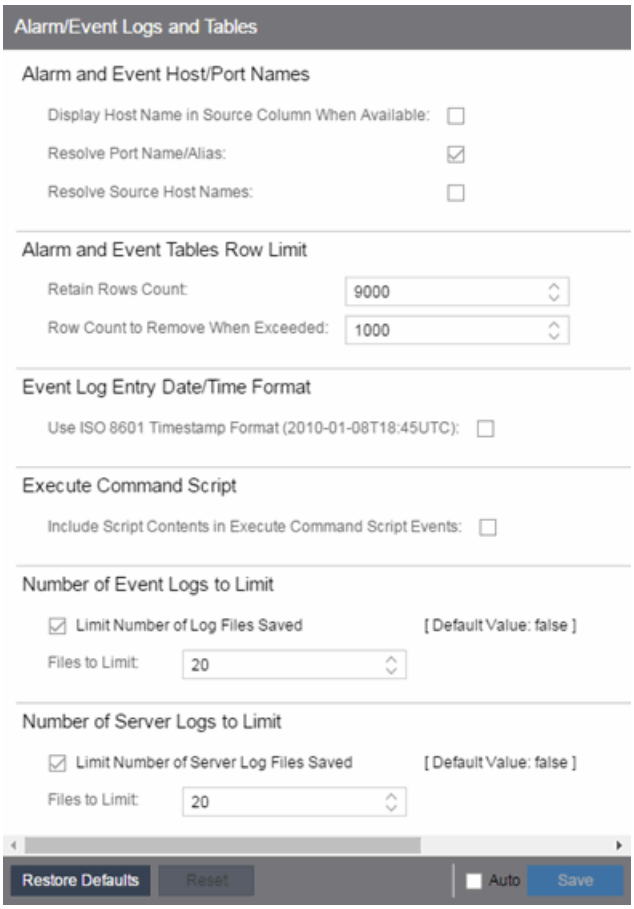
Selecting this option allows you to override the sender of an email for an alarm email action, including the ability to set the sender's password, if needed. Since

alarms are typically sent out as email/text messages, this option allows IT staff to set different ring-tones based on the alarm definition. Doing this on a smartphone typically involves changing the ring-tone for calls from a specific person.

Alarm/Event Logs and Tables Options

Selecting Alarm/Event Logs and Tables in the left panel of the **Options** tab provides the following view, where you can specify options for limiting disk usage by alarm and event logs, and Extreme Management Center server logs. These settings apply to all users. You must be assigned the appropriate user capability to configure these options. For additional information, see Extreme Management Center Log Files.

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



Alarm and Event Host/Port Names

These options let you 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 Extreme Management Center.
- 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.)

Alarm and Event Tables Row Limit

These settings determine the number of table rows displayed in all of the logs on both the Alarms and Events tabs 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.

Event Log Entry Date/Time Format

This option lets you 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 Extreme Management Center 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.

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 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 Server Logs to Limit

A new server log is created every day. This option limits the number of server log files that are 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.

Compass Options

Selecting Compass in the left panel of the **Options** tab provides the following view, where you can specify Compass SNMP and Search options.

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

Search Limits

These options are for the Compass search in Extreme Management Center. In addition to search options, they include search limit settings, which are used to help limit the Extreme Management Center 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 Extreme Management Center Compass searches that can be performed at one time.
- Time Limit for a Search — The maximum search time.

Search Extreme Access Control Database

Select this checkbox to include Extreme Access Control data in Compass searches. The Compass search begins by resolving IP address to MAC address in order to start searching for MAC-IP pairs from the network. When a match is found in the Extreme Access Control Database, the SNMP MIBs are **not** searched unless the **Search SNMP MIBs with Database Match** checkbox is also selected. If the **Extreme Access Control** checkbox is deselected, then the Extreme Access Control Database is not used to resolve IP address to MAC address.

Search SNMP MIBs with Database Match

Select this checkbox to include various SNMP MIB objects when performing searches. When the checkbox is selected, the SNMP MIBs section displays, from which you can select the individual SNMP MIB objects to include in Compass searches. For additional information, see Compass SNMP MIBs Descriptions.

Related Information

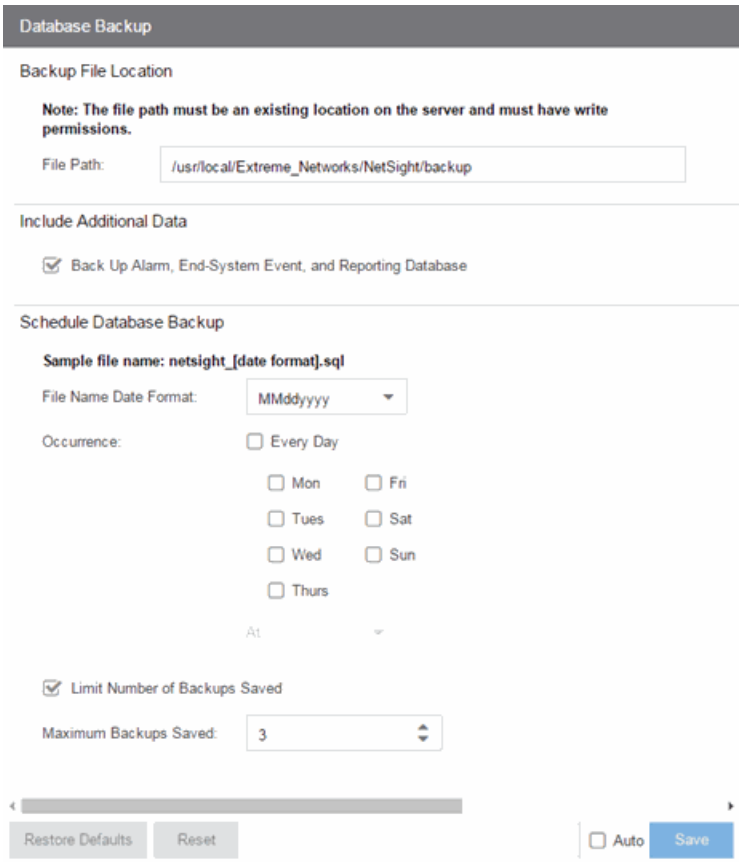
For information on related tasks:

- How to Set Extreme Access Control Options

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 Extreme Management Center database. An up-to-date database backup is an important component to ensuring that critical information pertaining to all Extreme Management Center applications is saved and readily available, if needed.

Changing a value from the system default causes a **Default Value** button to appear. Clicking 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

This checkbox lets you enable and disable the automatic backup of alarm data, end-system event data, and Extreme Management Center 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 menu.

Occurrence

Select one or more days of the week and specify a time for the backup to be performed. The backup takes place at the same time for each selected day.

Limit Number of Backups Saved

Select the checkbox to limit the number of scheduled backup files saved.

Maximum Backups Saved

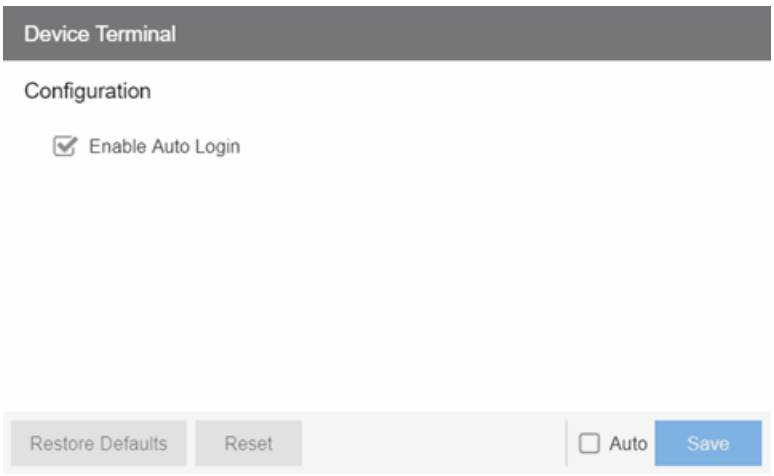
If Limit Number of Backups Saved is selected, enter the maximum number of scheduled backup files to save. When the limit is reached, older backups are removed when a new scheduled backup completes.

For additional information, see Tuning Database Backup Storage.

Device Terminal Options

Selecting Device Terminal in the left panel of the **Options** tab provides the following view, where you can configure options related to the **Open Device Terminal** option on the **Devices** tab.

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



Configuration

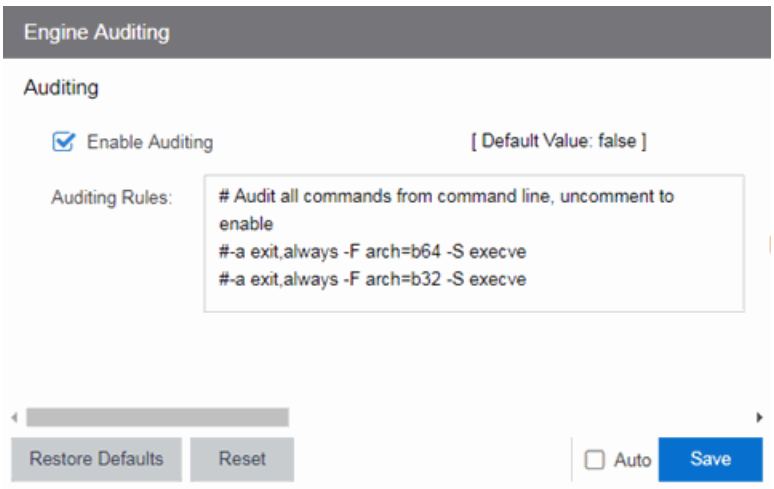
Enable Auto Login

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.

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 Extreme Management Center server CLI via SSH.

Changing a value from the system default causes a **Default Value** button to appear. Clicking 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 Extreme Management Center to store all commands entered by users connected to the Extreme Management Center CLI via SSH in the syslog file.

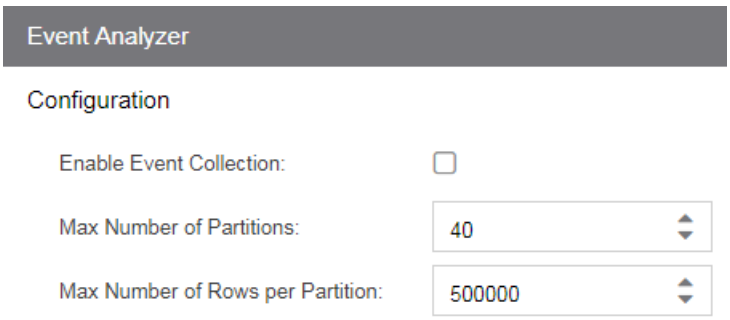
Auditing Rules

Remove the # symbol from the beginning of a command line to enable the command and store user commands entered using the Extreme Management Center CLI.

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 Extreme Management Center.

Changing a value from the system default causes a **Default Value** button to appear. Clicking 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

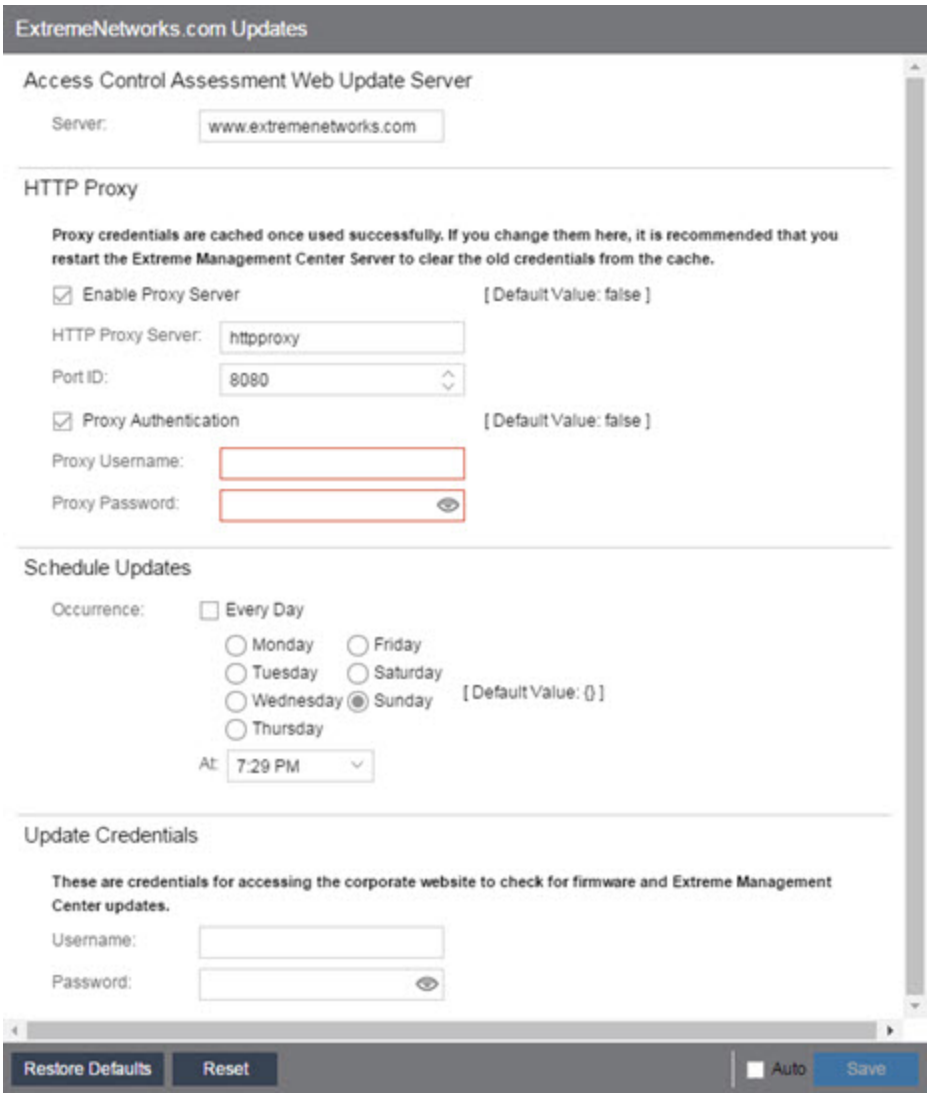
Enter the maximum number of rows for each partition used for the Event Analyzer.

NOTE: Only change this value if you are an expert user.

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 Extreme Management Center 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. Clicking this button changes the field back to the system default value.



Extreme Access Control Assessment Web Update Server

Displays the web update server used by Extreme Access Control to update Extreme Access Control assessment server software. This update operation pertains only to Extreme Access Control 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 once used

successfully. If you change them here, restart the Extreme Management Center 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

This section lets you schedule when Extreme Management Center 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 menu.
- To check for updates once a week — 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 menu.
- To disable scheduled updates — Do not select the Every Day checkbox or any of the radio buttons or click the Default Value button to clear your selection.

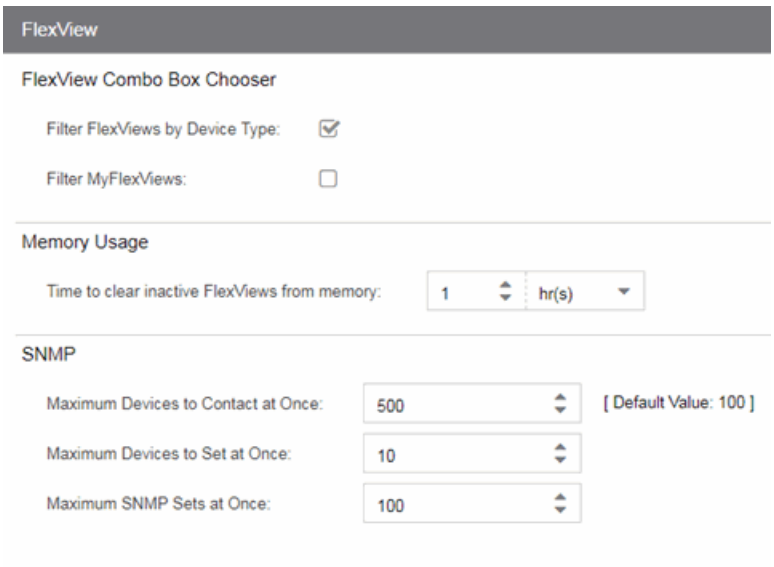
Update Credentials

Enter the credentials used to access the ExtremeNetworks.com website to obtain firmware and Extreme Management Center 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.

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 Extreme Management Center.

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



FlexView Combo Box Chooser

This section allows you to determine how FlexViews are displayed.

Filter FlexViews by Device Type

Select this box to filter FlexViews based on the device type.

Filter MyFlexViews

Select this checkbox to allow Extreme Management Center to filter FlexViews you create.

Memory Usage

Filter FlexViews by Device Type

The amount of time before Extreme Management Center removes inactive FlexViews from memory.

SNMP

These status polling options pertain to devices whose poll type is set to SNMP.

Maximum Devices to Contact at Once

The maximum number of IP addresses Extreme Management Center attempts to contact (read) simultaneously.

Maximum Devices to Set at Once

The maximum number of IP addresses Extreme Management Center attempts to perform PDU (protocol data unit) sets against simultaneously.

Maximum SNMP Sets at Once

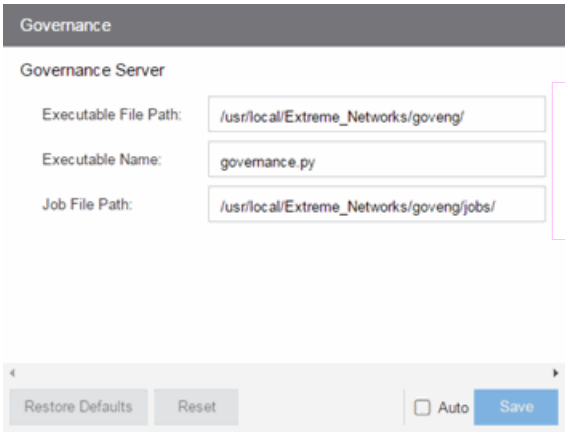
The maximum number of SNMP PDU sets Extreme Management Center attempts to contact simultaneously.

Governance Options

The options on this tab are designed for functionality included in a future release.

Selecting Governance in the left panel of the Options tab provides the following view, where you can specify the Governance engine file name used by Extreme Management Center, 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. Clicking this button changes the field back to the system default value.



Executable File Path

The directory in which the Governance engine executable file is located.

Executable Name

The name of the executable file used by the Governance engine.

Job File Path

The path to the directory in which the job files are located. The Governance engine uses job files to test device configurations in order to provide you with vulnerability information.

Impact Analysis Options

Selecting **Impact Analysis** in the left panel of the **Options** tab provides the following view, where you can edit settings associated with the Impact Analysis dashboard. The right-panel view changes depending on what you select in the left-panel tree. Expand the Impact Analysis tree to view all the different available options. These settings apply to all users.

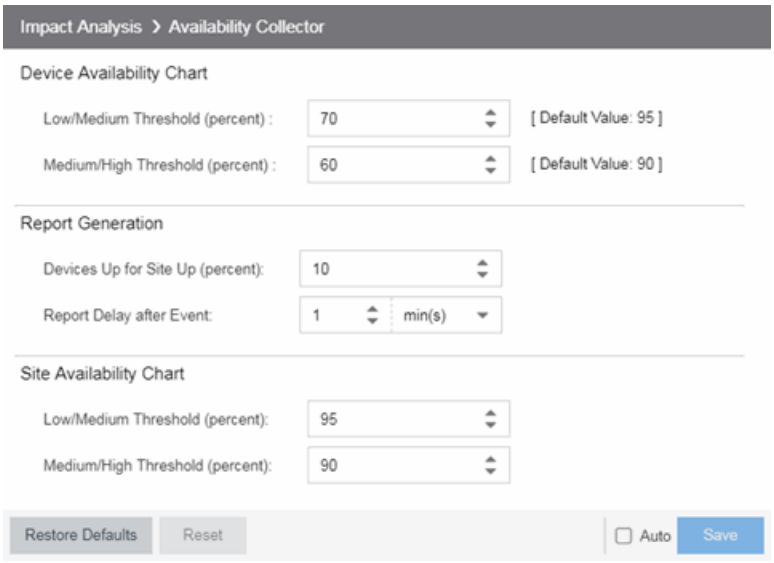
Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.

Click the link for information on the following Impact Analysis options:

- Availability Collector
- Capacity/Health Collector
- Configuration Collector
- Performance Collector

Availability Collector

These options allow you 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 Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center can reach. If the value falls below the percentage entered here, the Extreme Management Center considered the site down.

Report Delay after Event

Indicates the amount of time Extreme Management Center waits before reporting a device is down.

Site Availability Chart

Low/Medium Threshold (percent)

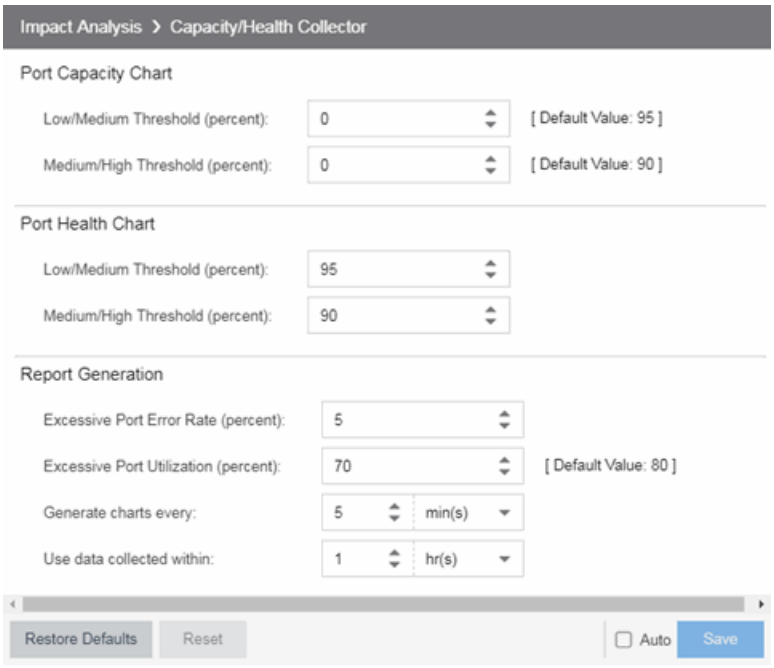
Indicates the percentage of devices included in a site that Extreme Management Center can reach. If the value falls below the percentage entered here, the Impact Status of the Site Availability chart moves from Low to Medium. For devices to be included, data collection must be enabled.

Medium/High Threshold (percent)

Indicates the percentage of devices included in a site that Extreme Management Center 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

These options let you 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 Extreme Management Center 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 Extreme Management Center considers the port utilization excessive. A port utilization below the percentage entered here is considered acceptable.

Generate charts every

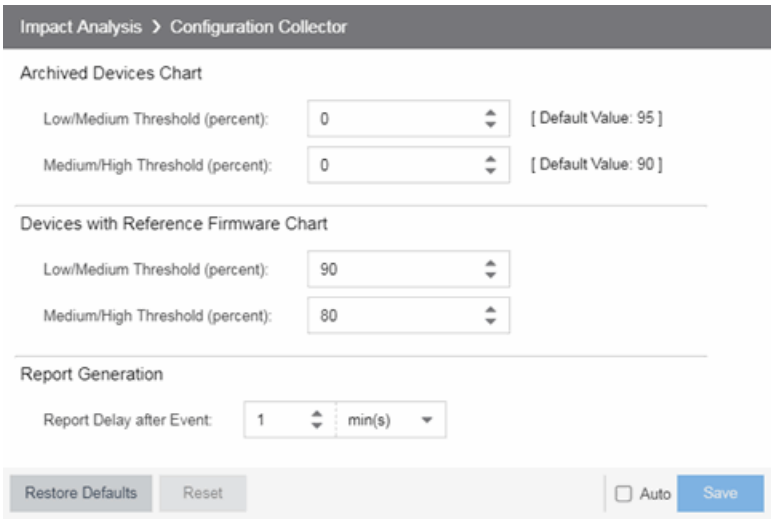
Indicates the interval between which Extreme Management Center polls ports to generate the Port Capacity and Port Health charts.

Use data collected within

Select the

Configuration Collector

These options allow you 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 in the last 30 days. 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 in the last 30 days. 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.

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

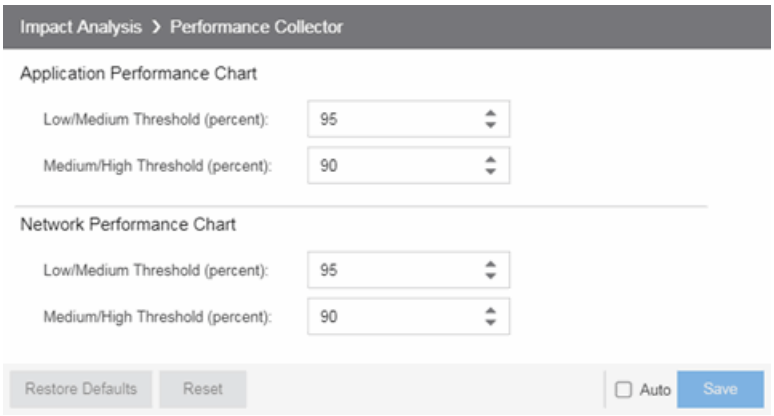
Report Delay after Event

Indicates the amount of time Extreme Management Center 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

These options allow you to configure the thresholds of the Application and Network Performance charts in the Impact Analysis dashboard.

These options let you configure the amount of resources used by the end-system event cache.



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

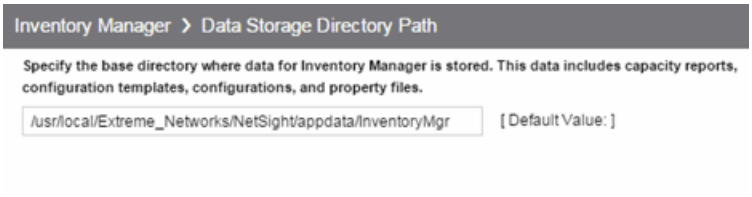
Inventory Manager Options

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. Clicking this button changes the field back to the system default value.

Data Storage Directory Path Setting

This option allows you 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 Extreme Management Center can find them.



File Transfer Settings

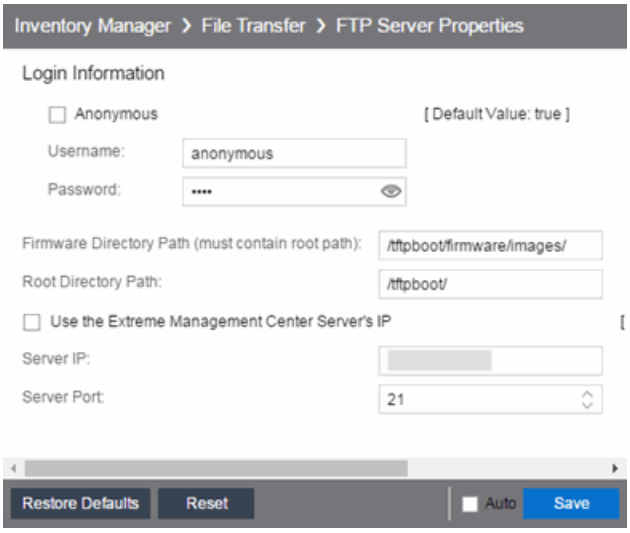
These options specify the FTP, SCP, or TFTP file transfer settings used when upgrading firmware.

Click the link for information on the following File Transfer Settings options:

- FTP Server Properties Settings
- SCP Server Properties Settings
- TFTP Server Properties Settings

FTP Server Properties Settings

These options allow you to set FTP server properties and login information. Use this view to specify the FTP server IP address, set paths to the root and firmware directories, and set 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 Extreme Management Center 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 (e.g. C:\ for Windows and /root/ for Linux).
- 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 // (Linux systems) or backslashes \\ (Windows systems) to indicate the name of the system, and one slash or backslash to indicate the path within the computer. For example, on a Windows system, instead of using

  `h:\` (where h:\ is mapped to the tftpboot directory on the remote drive)

  use

  `\\yourservername\tftpboot\`

Use the Extreme Management Center Server's IP

Select this checkbox if your FTP server is on the same machine as the Extreme Management Center Server. Selecting this checkbox disables the Server IP field.

Server IP

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

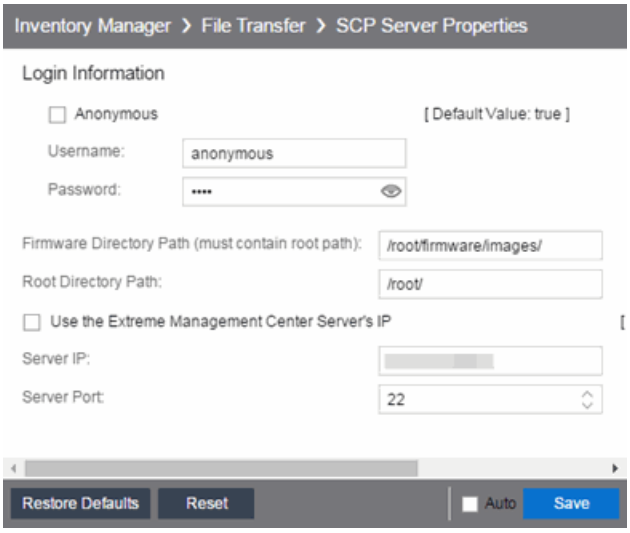
Server Port

Specify the port number on which your FTP server is configured to run.

SCP Server Properties Settings

These options allow you to set SCP server properties and login information. Use this view to specify the SCP server IP address, set paths to the root and firmware directories, and set 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 Linux system, the default firmware directory is `/root/firmware/images/`. On a Windows system, an SCP server is not installed by default, so the default **Firmware Directory Path** is `C:\tftpboot\firmware\images\`. This path needs to be updated once the SCP server is installed and a valid directory is created. For additional information, see How to Upgrade Firmware. If you are using an SCP server on a remote system, use the UNC standard described in the following Note when specifying the path.

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 Linux system, the default root directory is `/root/`. On a Windows system, an

SCP server is not installed by default, so the default Root Directory Path is `C:\tftpboot\`. This path needs to be updated once the SCP 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 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 (e.g. C:\ for Windows and /root/ for Linux).
- 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 // (Linux systems) or backslashes \\ (Windows systems) to indicate the name of the system, and one slash or backslash to indicate the path within the computer. For example, on a Windows system, instead of using
  `h:\` (where h:\ is mapped to the firmware\images directory on the remote drive)
  use
  `\\yourservername\firmware\images`

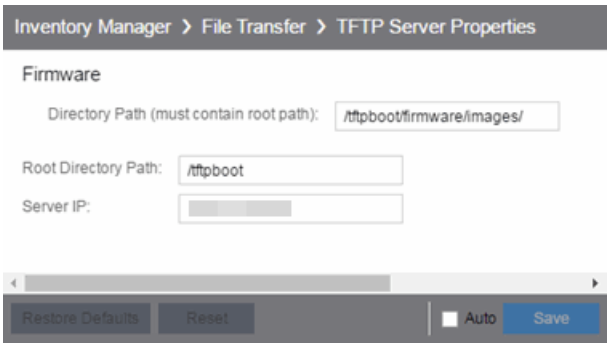
Use the Extreme Management Center Server's IP
Select this checkbox if your SCP server is on the same machine as the Extreme Management Center Server. Selecting this checkbox disables the Server IP field.

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.

TFTP Server Properties Settings

These options allow you to set TFTP server properties. This view lets you set the firmware directory path, the TFTP root directory path, and 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 Extreme Management Center 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 (e.g. C:\ for Windows and /root/ for Linux).
- 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 // (Linux systems) or backslashes \\ (Windows systems) to indicate the name of the system, and one slash or backslash to indicate the path within the computer. For example, on a Windows system, instead of using

  `h:\` (where h:\ is mapped to the firmware\images directory on the remote drive)

  use

  `\\yourservername\firmware\images`

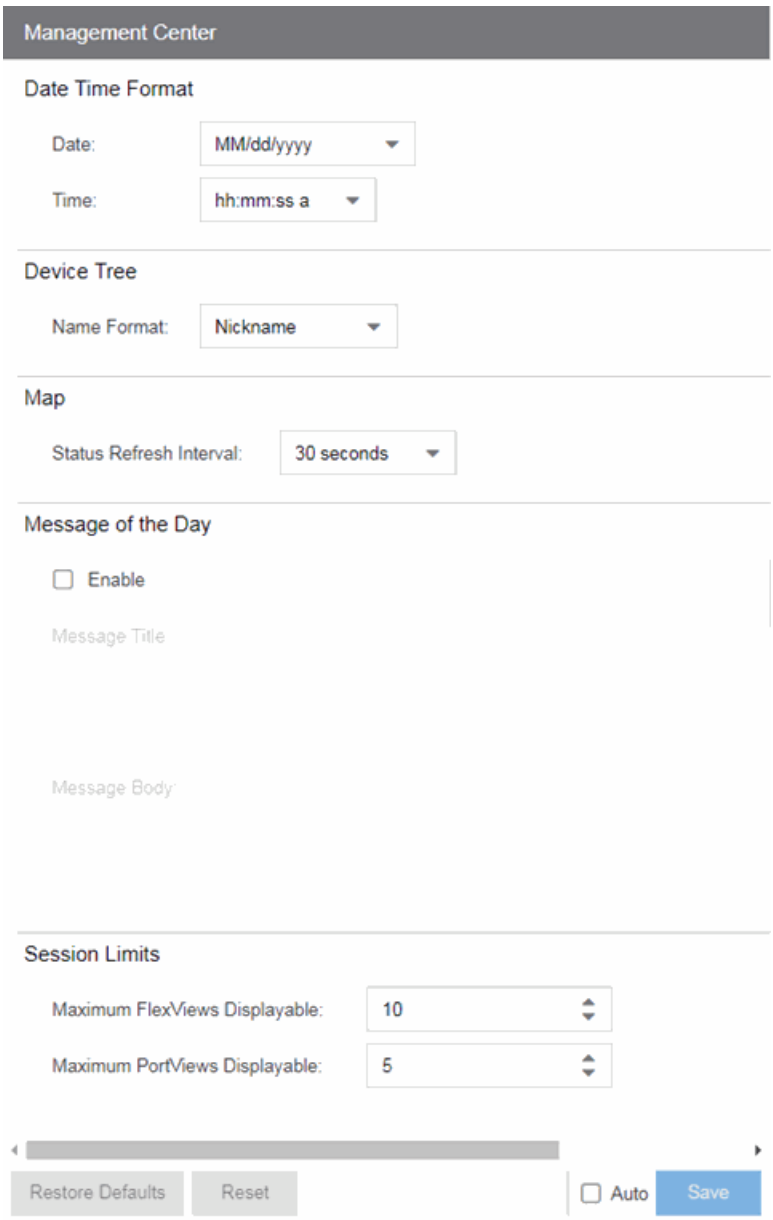
Server IP

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

Options

Selecting Extreme Management Center in the left panel of the **Options** tab provides the following view, where you can customize Extreme Management Center preferences. These settings apply to the user currently logged-in.

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



Date Time Format

Date

Select how the date is formatted in Extreme Management Center.

The letters in this field signify the following:

- MM — Month
- dd — Day
- yyyy — Year

Time

Select whether time is formatted as a 12-hour (hh:mm:ss a) or 24-hour (HH:mm:ss) clock.

The letters in this field signify the following:

- hh — Hour
- mm — Minute
- ss — Second

Device Tree

Name Format

Select one of the following options:

- 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 Edit Devices window.

Map

Status Refresh Interval

Select the interval that determines how often maps are automatically refreshed by Extreme Management Center. 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 Extreme Management Center.

Message Title

Enter a title for the message displayed to all Extreme Management Center users when the Enable checkbox is selected.

Message Body

Enter a body for the message displayed to all Extreme Management Center 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

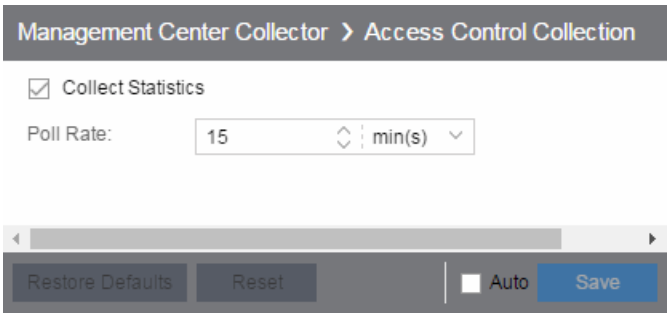
Allows you to determine the maximum number of PortViews displayed per session.

Collector Options

Selecting Extreme Management Center Collector in the left panel of the **Options** tab provides the following view, where you can configure Extreme Management Center Collector tree settings. These settings let you access advanced device and interface collection settings for the Extreme Management Center Collector.

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

Access Control Collection



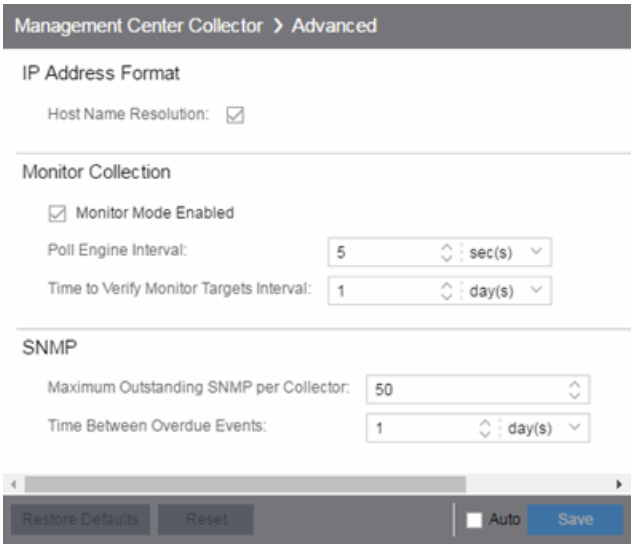
Collect Statistics

Select this checkbox to enable Extreme Access Control data collection.

Poll Rate

The amount of time the data collector waits between polling Extreme Access Control engines.

Advanced



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 this feature only. (Host name resolution is enabled globally using the Enable Name Resolution option.)

Monitor Mode Enabled

Use this option to enable or disable monitor mode statistic collection. If monitor mode is disabled, the Monitor Mode option is not available when configuring device or interface statistics collection. All monitor mode statistic collection is stopped and the monitor cache is cleared. For additional information, see Enable 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 Monitor Targets Interval

The interval between a check of all targets (devices and interfaces) set to Monitor 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

Monitor mode for those targets or configure appropriate threshold alarms in order to reduce unnecessary statistic collection.

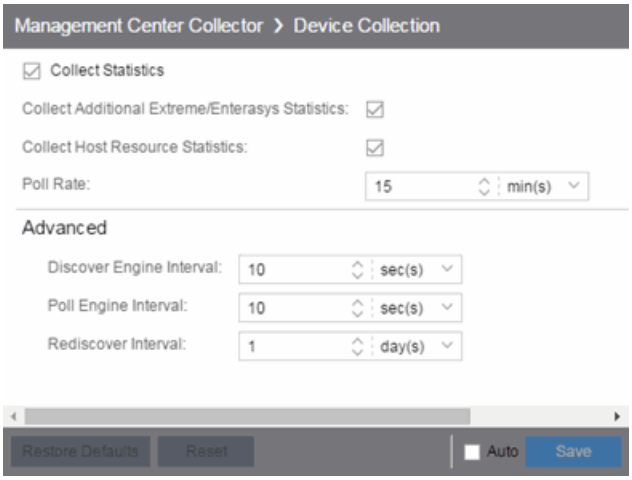
Maximum Outstanding SNMP per Collector

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.

Device Collection



Collect Statistics

Enables or disables additional statistics collection.

Collect Additional Extreme/Enterasys Statistics

Enables or disables Extreme and Enterasys switch resource statistics collection.

Collect Host Resource Statistics

Enables or disables host resource statistics collection.

Poll Rate

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

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.

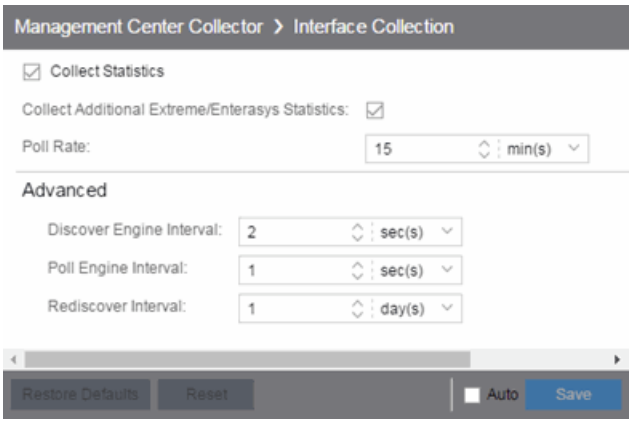
Poll Engine Interval

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.

Interface Collection



Collect Statistics

Enables or disables additional statistics collection.

Collect Additional Extreme/Enterasys Statistics

Enables or disables Extreme and Enterasys switch resource statistics collection.

Poll Rate

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

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.

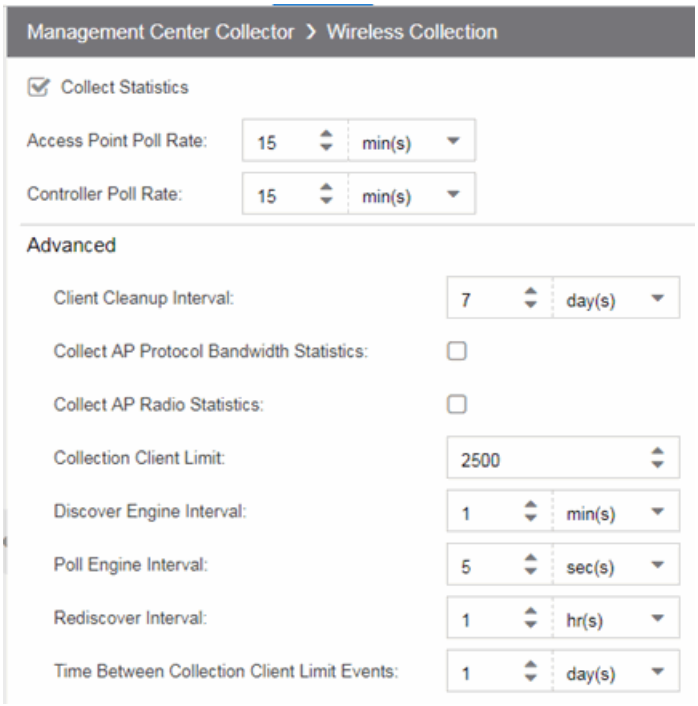
Poll Engine Interval

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



Collect Statistics

Use this checkbox to enable or disable wireless data collection.

Access Point Poll Rate

The amount of time the data collector waits between polling wireless access points. Valid values are 1-60 minutes.

Controller Poll Rate

The amount of time the data collector waits between polling wireless controllers. Valid values are 1-60 minutes.

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.

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 Protocol 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.

Collection Client Limit

The maximum number of wireless clients for which statistics are stored per collection interval. Valid values are 1 to 30,000.

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.

Time Between Collection Client Limit Events

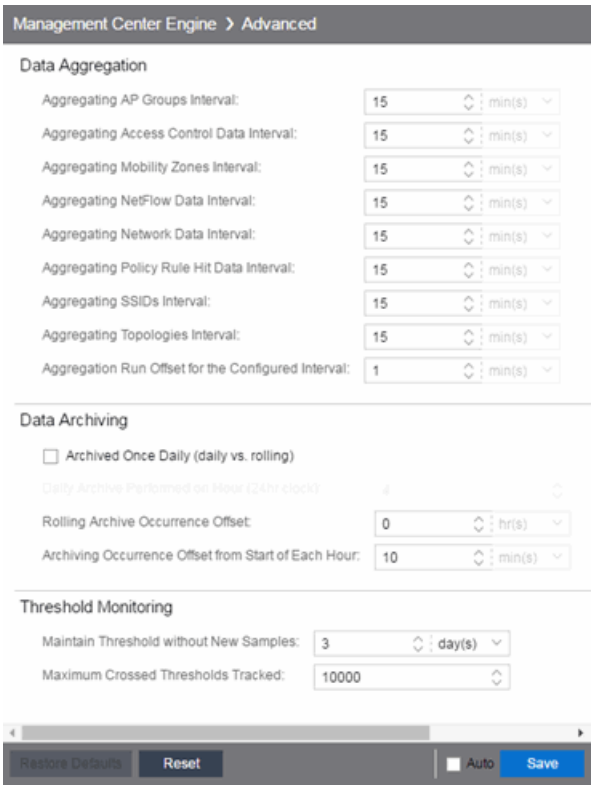
During a client cleanup, if a client is inactive for the amount of time specified here, then the client is aged out. Historical statistics already persisted are not removed.

Engine Options

Selecting Extreme Management Center 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. Clicking this button changes the field back to the system default value.

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, Extreme Access Control, 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 may 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).

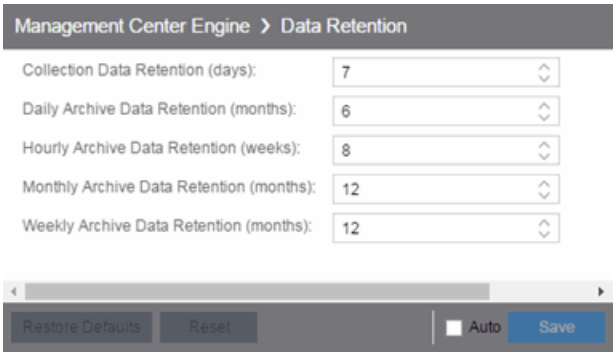
- Daily Archive — Select this checkbox to archive all the collection data (including the raw data, and the hourly, daily, weekly, and monthly data) once a day at a certain time. The Daily Archive Performed on Hour (24) field displays, where you can specify the hour of day to perform the daily archive. 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 may be performed before all the data is reported to the database. In cases with a long latency in reporting data to the database, you may need to increase the offset in order to make sure all the data is included in the archive.

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.

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.

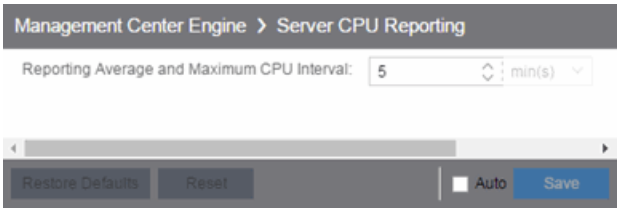
Monthly Archive Data Retention (months)

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



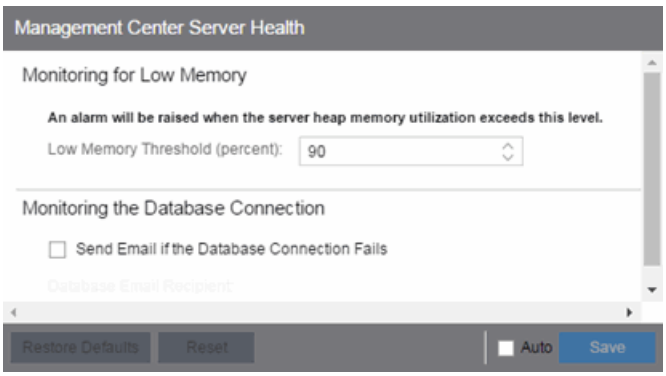
Reporting Average and Maximum CPU Interval

Extreme Management Center collects CPU usage statistics monitoring for the Extreme Management Center server. At 5 minute intervals (the default interval) the collected usage data is averaged, and the average and maximum statistics are reported to the Extreme Management Center database to provide data for the Extreme Management Center 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.

Server Health Options

Selecting Extreme Management Center Server Health in the left panel of the Options tab provides the following view, where you can configure warnings to help monitor the Extreme Management Center server health.

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



Monitoring for Low Memory

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.

Monitoring the Database Connection

Send Email if the Database Connection Fails

Select the checkbox to send an email notification if the Extreme Management Center database goes down, and when the database comes back up again.

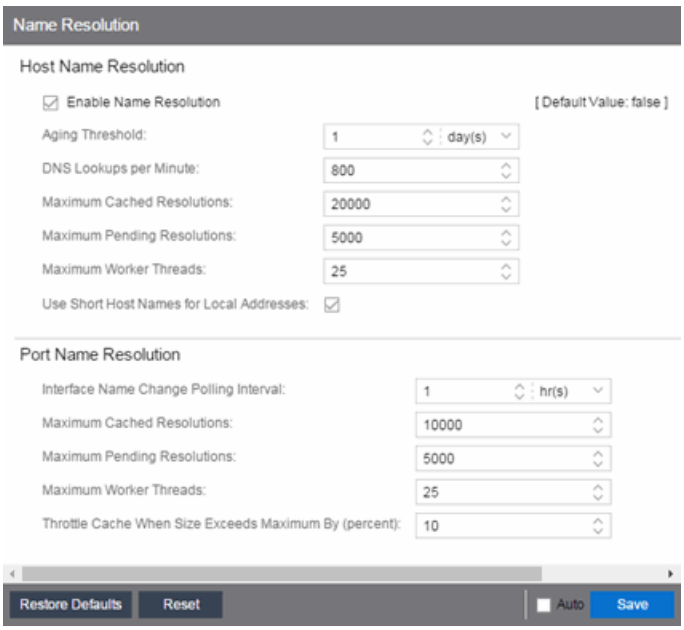
Database Email Recipient

If Send Email if the Database Connection Fails is selected, enter the email address of the person to whom the email notification is sent.

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. Clicking 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

This option allows host names to be displayed in place of IP addresses throughout Extreme Management Center. This feature is primarily used by NetFlow. With name resolution enabled, flow data would show "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

This option determines how long IP/host name pairs are cached in memory. After the aging threshold time has passed, the IP/host name pair is removed from the cache in order to prevent stale IP/host name associations. This option addresses the fact that DHCP assigns a new IP address to users frequently, especially on reboots. Without an aging threshold, host names continue to be associated to the IP they had at the first lookup. The default value is 24 hours; the minimum value is 1 hour.

DNS Lookups per Minute

The maximum number of host name lookups that the DNS server can perform each minute. This prevents host name resolution from using so many resources on a switch, which may 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" would display as "jsmith-ws" if mycompany.com is listed as a local address domain. This option can be disabled when troubleshooting problems with host name resolution, or if IP addresses are preferred.

Port Name Resolution

Use this section to set options for resolving device port indices to port names and port aliases, and device port names and port aliases to port indices.

Interface Name Change Polling Interval

This option specifies how often the port name resolution service checks devices to see if port information has changed.

Maximum Cached Resolutions

The maximum amount of port data that can be cached in memory. This number can be adjusted to control the amount of memory used by this service.

Maximum Pending Resolutions

The maximum number of port name resolution requests that can be queued up. This number can be adjusted to control the maximum amount of time spent waiting for a resolution.

Maximum Worker Threads

The maximum number of port name lookups that can be done at the same time. This number can be adjusted to control the amount of system resources used by port name resolution.

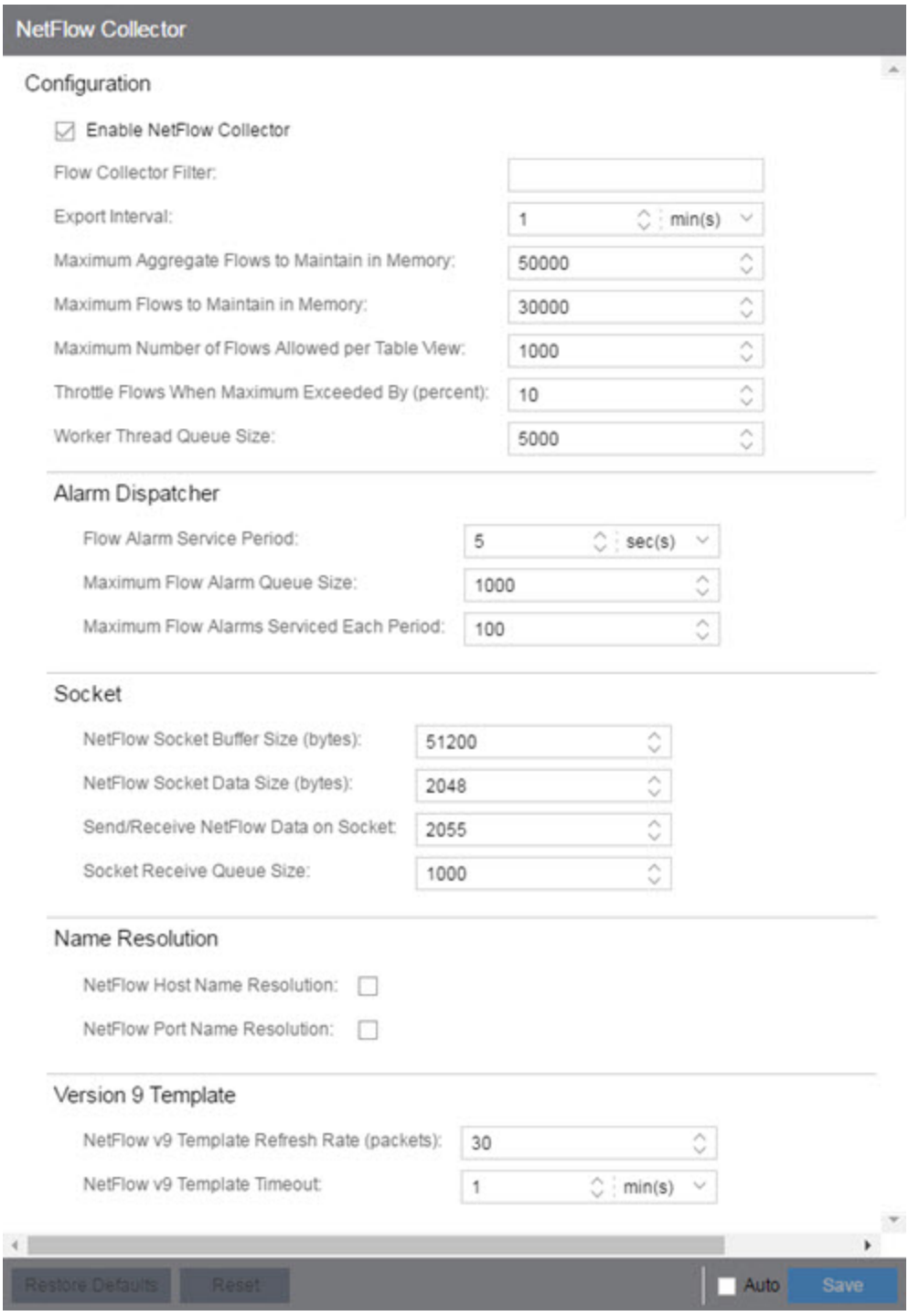
Throttle Cache When Size Exceeds Maximum By (percent)

This option controls how much port data is discarded from the cache when its size is exceeded. Adjust this to control how an overfull cache is reduced.

NetFlow Collector Options

Selecting NetFlow Collector in the left panel of the Options tab provides the following view, where you can configure NetFlow Collector settings in Extreme Management Center.

Changing a value from the system default causes a Default Value button to appear. Clicking 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 Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center 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 may 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 once 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 Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center is enabled globally using the Extreme Management Center Name Resolution option. The Name Resolution option must also be enabled for this NetFlow option to take effect.

NetFlow Port Name Resolution

Select this option to resolve device port indices to port names and port aliases, and device port names and port aliases to port indices, if possible. This option allows you to disable port name resolution for NetFlow only. (Port name resolution is enabled globally using the Name Resolution option.)

Version 9 Template

NetFlow v9 Template Refresh Rate (packets)

The number of export packets the flow sensor sends before retransmitting a template to the collector when using NetFlow Version 9.

NetFlow v9 Template Timeout

The amount of time the flow sensor waits before retransmitting a template to the collector when using NetFlow Version 9.

Network Monitor Cache Options

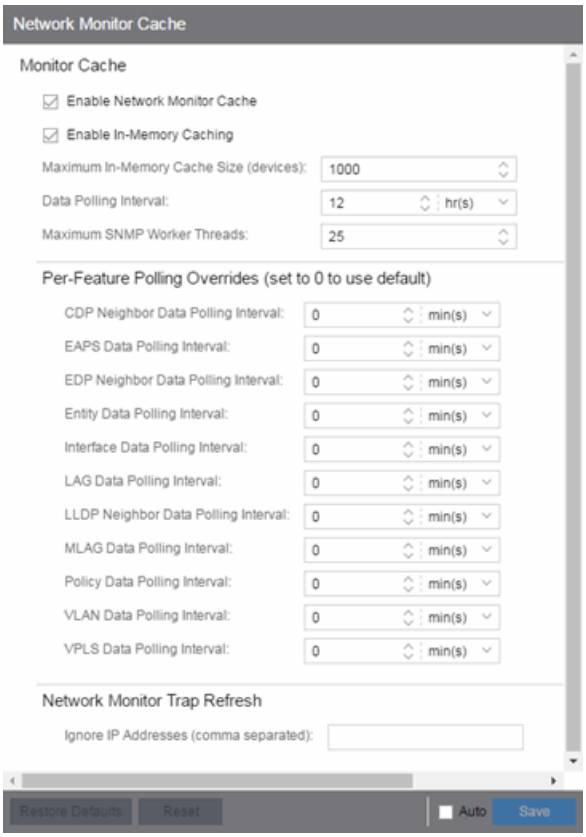
Selecting Network Monitor Cache in the left panel of the Options tab provides the following view, where you can edit network monitor cache settings. The network monitor cache stores information about the physical topology of a device, with additional emphasis on port information. Data is pulled from multiple places including slot and port details (Entity, ifTable), default role (Policy), neighbor link details (CDP, EDP, LLDP), Ethernet Automatic Protection Switching (EAPS), and Multi System Link Aggregation (MLAG).

Changing a value from the system default causes a Default Value button to appear. Clicking 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 may 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 Extreme Management Center 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 Extreme Management Center 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.

Per-Feature Polling Overrides

Use the fields in this section to set unique polling intervals for individual cache features polled more frequently. Set to 0 to use the default interval set for the Data Polling Interval.

Network Monitor Trap Refresh

Ignore IP Addresses (comma separated)

Enter a comma-separated list of the IP addresses for which you do not want Extreme Management Center to be the trap destination.

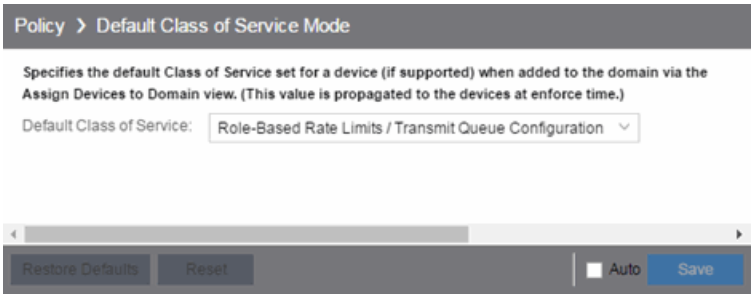
Policy Options

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

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

Default Class of Service Mode

The **Default Class of Service** option allows you to specify the default Class of Service (CoS) mode to set on a device (if supported) when it is created in Extreme Management Center or added to the domain via the **Policy** tab. The default setting is **Role-Based Rate Limits/ Transmit Queue Configuration**. The CoS mode is written to the devices when an Enforce operation is performed. This setting applies to all users.



Select the CoS mode or select the option to disable rate limits on devices. Only certain devices such as the N-Series Gold and Platinum devices support both modes, but you cannot enable both at the same time. For additional information, see Getting Started with Class of Service.

Rate Limits Disabled

Select this mode to disable rate limits. This means that any priority-based rate limits are not written to devices on enforce, and any role-based rate limits are not included in roles written to devices on enforce.

Role-Based Rate Limits/Transmit Queue Configuration

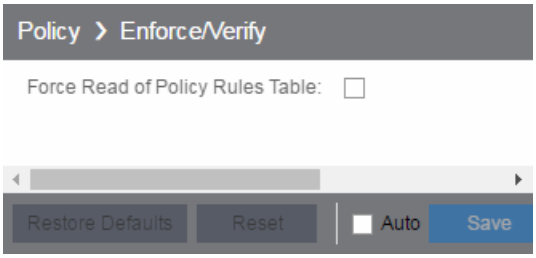
Select this mode to configure role-based rate limits and transmit queues on devices. These rate limits are defined within a CoS and are associated with a specific role via

a rule action or as a role default. They are implemented based on the role assigned to a port. This mode also allows transmit queue behavior to be configured for the CoS. For additional information, see How to Define Rate Limits and How to Configure Transmit Queues.

Priority-Based Rate Limits

Priority-based rate limits are supported in Extreme Management Center for use with legacy devices such as the E7 and E1 devices. For additional information, see Priority-Based Rate Limits.

Enforce/Verify



Force Read of Policy Rules Table

To improve performance during the verify operation, Extreme Management Center uses the "Last Changed" attribute on the device to determine if any rules changed. Selecting the Force Read of Policy Rules Table option causes Extreme Management Center to perform the verify operation using the rules table instead of the attribute. This may cause the verify operation to take longer to perform. Do not select this option unless instructed by Extreme Networks Support.

Related Information

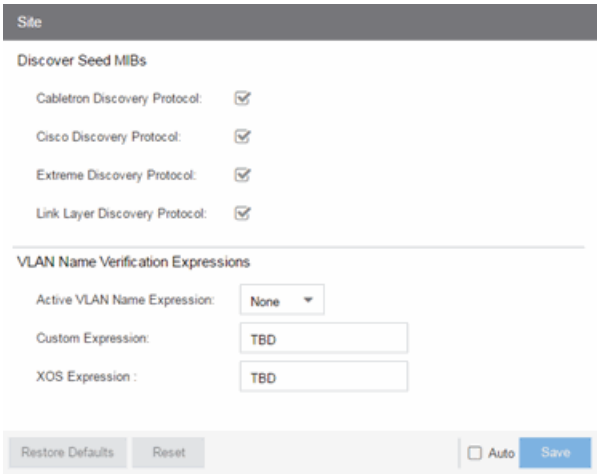
For information on related topics:

- Policy

Site Options

Selecting Site in the left panel of the Options tab provides the following view, where you can allow or deny specific protocols when discovering devices for a site.

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



Discovery Seed MIBs

Cabletron Discovery Protocol

Select this option to allow each Site Seed IP Address to use the Cabletron Discovery Protocol (ctCDP) to detect devices to add to Extreme Management Center.

Cisco Discovery Protocol

Select this option to allow each Site Seed IP Address to use the Cisco Discovery Protocol (CDP) to detect devices to add to Extreme Management Center.

Extreme Discovery Protocol

Select this option to allow each Site Seed IP Address to use the Extreme Discovery Protocol (EDP) to detect devices to add to Extreme Management Center.

Link Layer Discovery Protocol

Select this option to allow each Site Seed IP Address to use the Link Layer Discovery Protocol (LLDP) to detect devices to add to Extreme Management Center.

VLAN Name Verification Expressions

Active VLAN Name Expression

Select the set of rules Extreme Management Center uses to verify your operating system supports a VLAN Name.

Custom Expression

Enter a VLAN Name to verify your custom device's operating system supports a VLAN Name. The VLAN Name entered is verified against the rules selected in the Active VLAN Name Expression field.

XOS Expression

Enter a VLAN Name to verify your ExtremeXOS device's operating system supports a VLAN Name. The VLAN Name entered is verified against the rules selected in the Active VLAN Name Expression field.

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 Extreme Management Center when sending emails to users. Extreme Management Center 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. Clicking 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

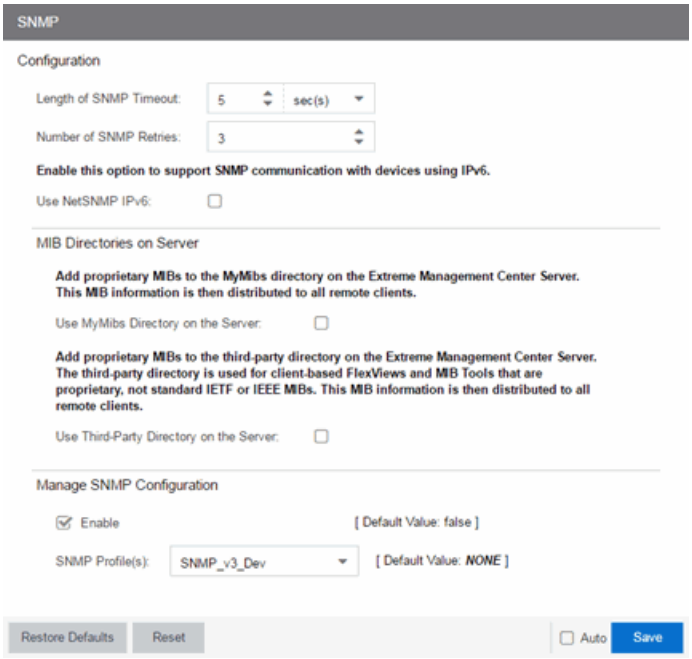
The password for the user account entered in the Sender's Email Address field. Select the Eye icon to display your password.

SNMP Options

Selecting SNMP in the left panel of the **Options** tab provides the following view, which allows you to configure SNMP options.

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

These options apply to all users. For these settings to take effect, the Extreme Management Center Server must be restarted.



Configuration

Length of SNMP Timeout

The amount of time Extreme Management Center waits before trying to contact a device again. The default value for this setting is 5 seconds. The value for this setting must be between 1 and 60 seconds.

Override this value on a per-device basis in the **SNMP Timeout** field in the Configure Device window.

NOTE: When SNMP requests are redirected through the server, all SNMP timeouts are extended by a factor of four (timeout X 4) to allow 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 3 retries, which means that Extreme Management Center retries a timed-out request three times after the initial attempt at contact is made, making a total of four attempts to contact a device. The value for this setting must be between 1 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 allows 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 allow the Extreme Management Center 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 Extreme Management Center remote clients.

Use Third-Party Directory on the Server

Select this checkbox to allow the Extreme Management Center 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 Extreme Management Center remote clients.

CAUTION: Do not use the MyMibs or third-party directories unless it is required on your network, as selecting these options may cause Extreme Management Center Server instability and undesirable consequences.

Manage SNMP Configuration

Enable

Select this checkbox to allow access to the Extreme Management Center and Extreme Access Control engines for the profiles you select in the SNMP Profile(s) drop-down menu.

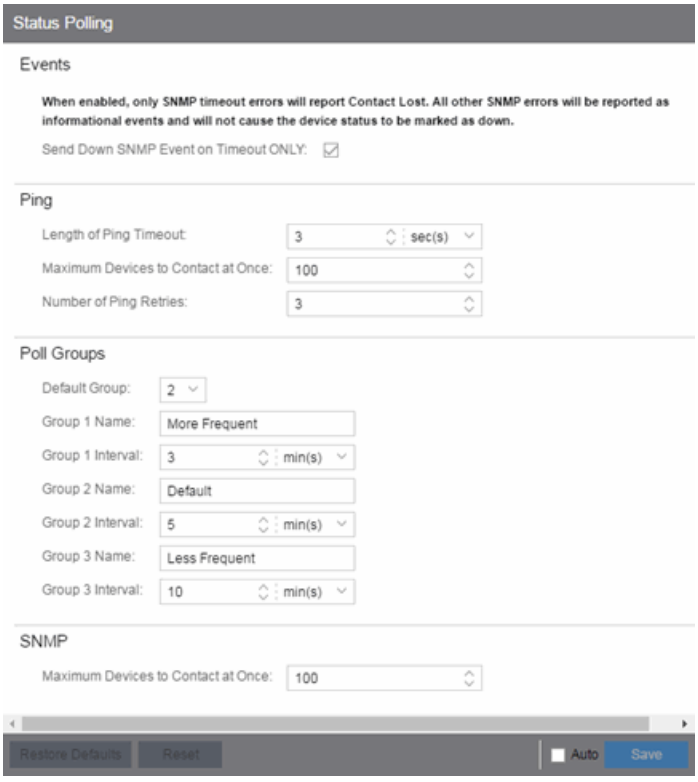
SNMP Profile(s)

Select the profiles with access to the Extreme Management Center and Extreme Access Control engines. The type of 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.

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 Extreme Management Center polls devices. Extreme Management Center uses the polling options and poll groups defined here to contact the devices and update tree information. When a device is added to the Extreme Management Center 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. Clicking 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

These status polling options pertain to devices whose poll type is set to **Ping**.

Length of Ping Timeout

The amount of time Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center 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

There are three distinct poll groups, and each device belongs to one of the three groups. This lets you 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 menu. When a device is added to the Extreme Management Center 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. Extreme Management Center 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. Once all the devices are polled, Extreme Management Center 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

This status polling option pertains to devices whose poll type is set to SNMP.

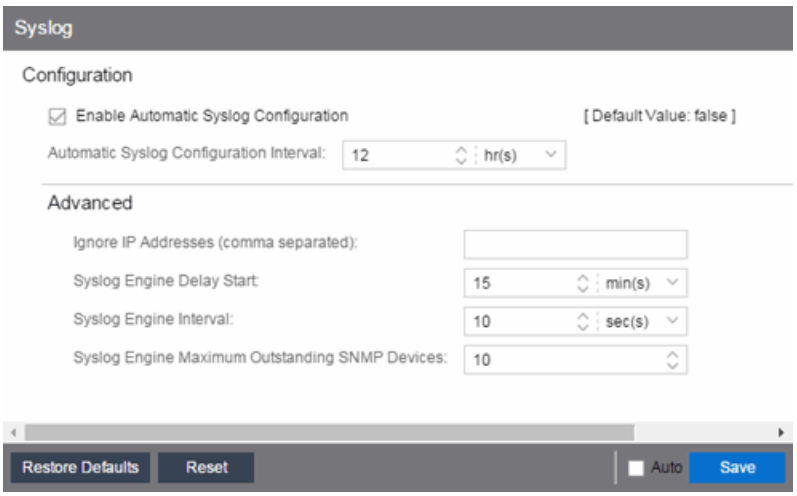
Maximum Devices to Contact at Once

The maximum number of IP addresses that Extreme Management Center attempts to contact simultaneously. The maximum value for this field is 1,000.

Syslog Options

Selecting Syslog in the left panel of the Options tab provides the following view, where you can set Extreme Management Center to automatically configure devices to send syslog information.

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



Enable Automatic Syslog Configuration

Select the checkbox to configure Extreme Management Center 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 Extreme Management Center automatically gathers information and posts it to the syslog.

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 Extreme Management Center waits before information in the syslog is aggregated and archived.

Syslog Engine Interval

The amount of time Extreme Management Center 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, Extreme Management Center automatically configures the device.

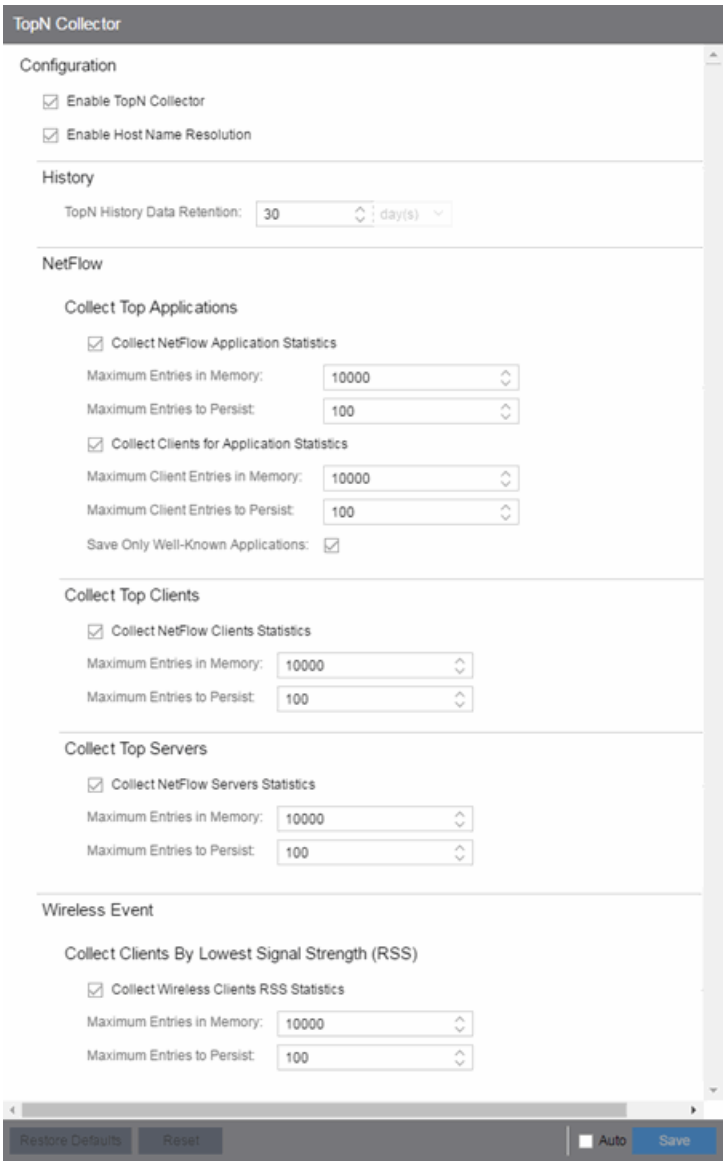
Syslog Engine Maximum Outstanding SNMP Devices

The maximum number of outstanding SNMP devices archived by the syslog.

TopN Collector Options

Selecting TopN Collector in the left panel of the Options tab provides the following view, where you can enable the TopN collector and host name resolution, and configure the number of days Extreme Management Center 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. Clicking 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

This setting determines the number of days TopN information remains available for viewing in reports. The default number of days is 30, with a minimum value of 1 day and a maximum value of 180 days. Changes to this option take effect with the next nightly TopN history cleanup task performed by the Extreme Management Center server.

NetFlow

The TopN Collector collects the data used in TopN reports for applications, client applications, clients, and servers. The collector collects data over a one hour time period. At the end of the hour, the collector evaluates the data and stores only the most significant details collected for that hour. When changing the value for Maximum Entries in Memory or Maximum Entries to Persist, the new value takes effect during the next hour of data collection. For example, if you change the value at 3:05 or 3:55, the new value takes effect during the hour that starts at 4:00.

If more entries are needed during the hour than the maximum, additional entries are stored on disk, which is slower. This results in a direct trade-off in memory usage versus CPU usage. Increasing these values might use more memory and decreasing these values might use more CPU.

Collect Top Applications

Collect NetFlow Application Statistics

Select this checkbox to enable the collection of application TopN data.

Maximum Entries in Memory

Specify the number of application entries to save during each hourly interval to use in TopN reporting. The default maximum number of entries in memory is 10,000 with a minimum value of 1,000 and a maximum value of 1,000,000.

Maximum Entries to Persist

Specify the number of application entries to save at the end of each hourly interval. The default number of entries to persist is 100, with a minimum value of 5 and a maximum value of 1,000.

Collect Clients for Application Statistics
Select this checkbox to enable the collection of data about the clients using the applications in TopN data.

Maximum Client Entries in Memory
Specify the number of client entries to save during each hourly interval to use in TopN reporting. The default maximum number of entries in memory is 10,000 with a minimum value of 1,000 and a maximum value of 1,000,000.

Maximum Client Entries to Persist
Specify the number of client entries to save at the end of each hourly interval. The default number of entries to persist is 100, with a minimum value of 5 and a maximum value of 1,000.

Save Only Well-Known Applications
Select this checkbox to save only data from well-known applications in the TopN data.

Collect Top Clients

Collect NetFlow Clients Statistics
Select this checkbox to enable the collection of client TopN data.

Maximum Entries in Memory
Specify the number of client entries to save during each hourly interval to use in TopN reporting. The default maximum number of entries in memory is 10,000 with a minimum value of 1,000 and a maximum value of 1,000,000.

Maximum Entries to Persist
Specify the number of client entries to save at the end of each hourly interval. The default number of entries to persist is 100, with a minimum value of 5 and a maximum value of 1,000.

Collect Top Servers

Collect NetFlow Servers Statistics
Select this checkbox to enable the collection of server TopN data.

Maximum Entries in Memory
Specify the number of server entries to save during each hourly interval to use in TopN reporting. The default maximum number of entries in memory is 10,000 with a minimum value of 1,000 and a maximum value of 1,000,000.

Maximum Entries to Persist

Specify the number of server entries to save at the end of each hourly interval. The default number of entries to persist is 100, with a minimum value of 5 and a maximum value of 1,000.

Wireless Event

Collect Wireless Clients RSS Statistics

Select this checkbox to enable Wireless Controllers to collect signal strength data for TopN reporting.

Maximum Entries in Memory

Specify the number of signal strength entries to save during each hourly interval to use in TopN reporting. The default maximum number of entries in memory is 10,000 with a minimum value of 1,000 and a maximum value of 1,000,000.

Maximum Entries to Persist

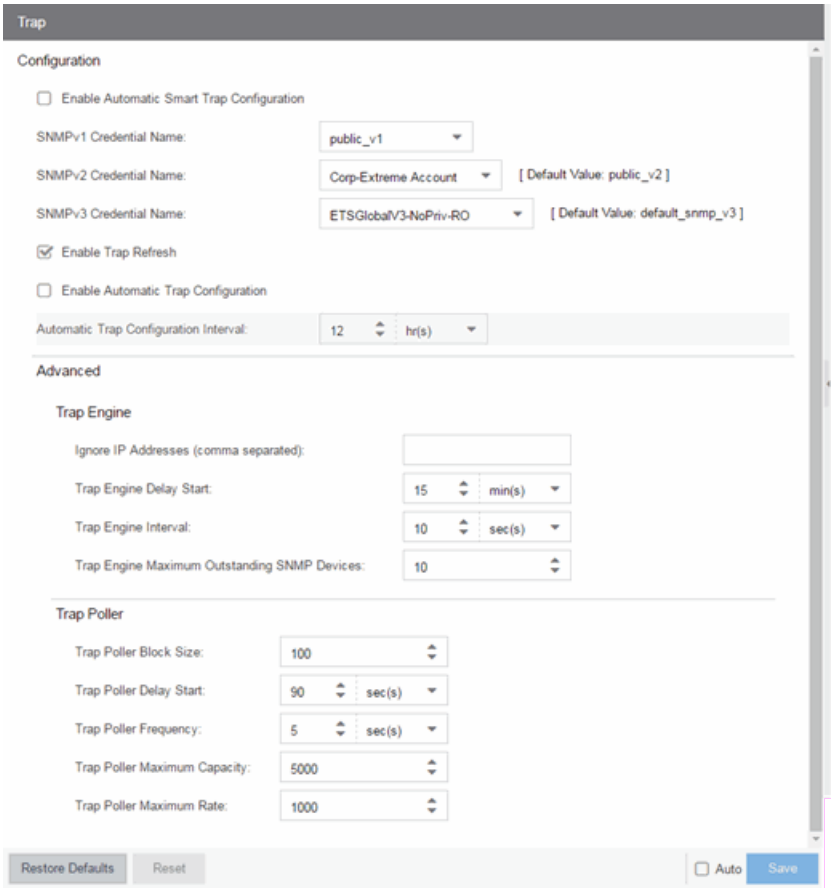
Specify the number of signal strength entries to save at the end of each hourly interval. The default number of entries to persist is 100, with a minimum value of 5 and a maximum value of 1,000.

Trap Options

Selecting Trap in the left panel of the Options tab provides the following view, where you can set trap options for Extreme Management Center.

SNMP traps are messages a device sends to Extreme Management Center 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. Clicking 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 allow your ExtremeXOS devices to send Extreme Management Center a trap when a change occurs on the device.

SNMPv1 Credential Name
Select the SNMPv1 credentials used to access the device. 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 used to access the device. 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 used to access the device. You can modify the credentials found in this list in the SNMP Credentials section on the Administration > Profiles tab.

Enable Trap Refresh
Select this option to allow Extreme Management Center to refresh information on the devices when the trap is received.

Enable Automatic Trap Configuration
Select this option to configure the ExtremeXOS switches on your network to send Extreme Management Center 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 Extreme Management Center.

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 Extreme Management Center.

Trap Poller Frequency
Select the frequency with which the trap engine polls devices.

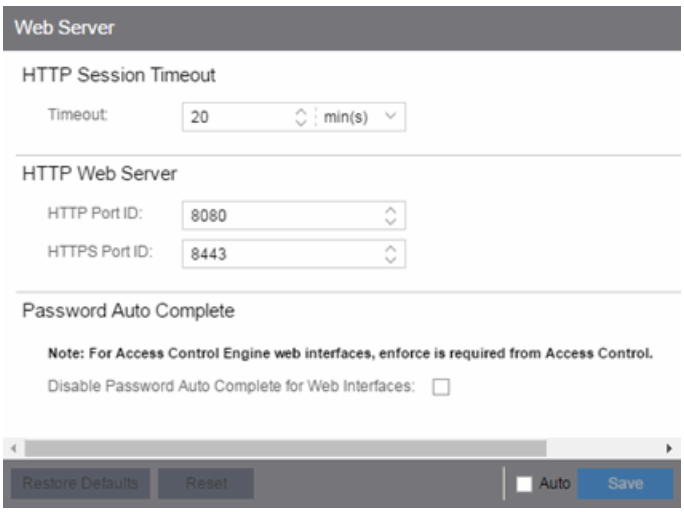
Trap Poller Maximum Capacity
Select the maximum number of devices the trap engine polls for traps.

Trap Poller Maximum Rate
Select the maximum number of devices the trap engine polls at one time.

Web Server Options

Selecting Web Server in the left panel of the **Options** tab provides the following view, where you can specify web browser options when using Extreme Management Center.

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



HTTP Session Timeout

The **Timeout** option lets you specify a session timeout value for all Extreme Management Center web-based views.

HTTP Port ID

The **HTTP Port ID** field lets you specify the HTTP port IDs for HTTP web server traffic. This port must be accessible through firewalls for users to install and launch Extreme Management Center client applications. By default, Extreme Management Center uses port ID 8080. If you change the port ID, you must restart the Extreme Management Center Server for the change to take effect.

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

When adding a new Extreme Access Control engine, the **HTTP Port ID** must be **8080**.

HTTPS Port ID

The HTTPS Port ID field lets you specify the HTTPS port IDs for HTTP web server traffic. This port must be accessible through firewalls for users to install and launch Extreme Management Center client applications. By default, Extreme Management Center uses port ID 8443. If you change the port ID, you must restart the Extreme Management Center 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 Extreme Management Center polls the Extreme Access Control engine.

When adding a new Extreme Access Control engine, the HTTPS Port ID must be 8443.

Password Auto Complete

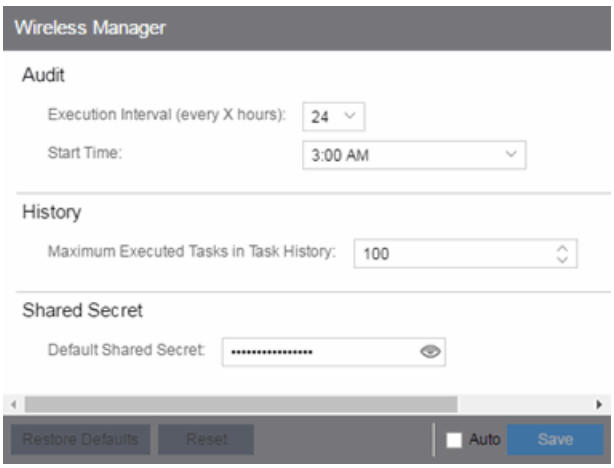
The Disable Password Auto Complete for Web Interfaces option lets you disable automatic password completion for users logging into Extreme Management Center web interfaces. Note that for Extreme Access Control web interfaces, you must enforce from the Control > Extreme Access Control tab for the option to take effect.

These settings apply to all users. You must be assigned the appropriate user capability to change this setting.

Wireless Manager Options

Selecting Wireless Manager in the left panel of the Options tab provides the following view, where you can specify options for the Wireless Manager application.

Changing a value from the system default causes a Default Value button to appear. Clicking 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 menu to select the interval in hours between the start of successive audits. Auditing once every 24 hours is sufficient for most sites, but more frequent auditing can be enabled through this option.

Start Time

Use the drop-down menu 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 Extreme Management Center to authenticate with the controller.

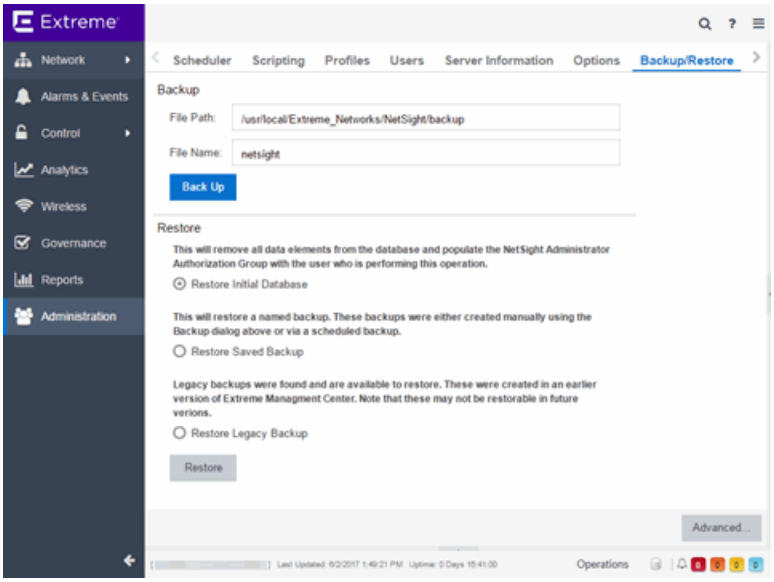
When Extreme Management Center discovers a new controller, Wireless Manager attempts to authenticate with the controller using this shared secret. For proper functioning, Extreme Management Center and the controller must be configured with the same shared secret. Each controller can be configured with 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. For additional information, see Shared Secrets Page.

Backup/Restore

This tab allows you 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 8.1 of Extreme Management Center 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 Extreme Management Center.

Additionally, there are specific database backup migration requirements for this release.



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 Path
Enter the path to the directory to which you want to save the file.

File Name
Enter a name for the database backup file.

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 Extreme Management Center server, enforce all Extreme Access Control engines.

Restore Initial Database
Select this option to remove all data elements from the database and populate the Extreme Management Center 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 menu 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 menu to select the file from which you want to populate the database.

NOTE: If there are no legacy database backups saved (backups saved in version 7.1), this field does not display.

When restoring a saved legacy database to a new Extreme Management Center server installation, any memory or database configuration changes on the original server requires a manual change on the new server in order to replicate the configuration of the original Extreme Management Center server.

- Changes to the default -Xmx memory settings in the `<install directory>\services\nsserver.cfg` file needs to be duplicated on the new server when the database is restored. To change the memory setting to match the previous server, stop the Extreme Management Center server and edit the nsserver.cfg file.
- The mySQL my.ini file also needs to be manually updated to match any changes made on the original server.

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 Extreme Management Center server uses when it connects to the database.

IMPORTANT: When Extreme Management Center is installed, it automatically secures the MySQL database server by removing all the root and anonymous users from the MySQL user database. Extreme Management Center then adds one generic user name (user = netsight) and password (password = enterasys). Change this password, as all customers who install Extreme Management Center know this generic password.

Connection URL

Displays the URL the Extreme Management Center server uses when connecting to the database. For troubleshooting purposes, (for example, if you can't connect to the database) you may wish to enter a new connection URL. Enter a new URL in the following format, and click Apply:
`jdbc:mysql://[hostname]/<database>` where [*hostname*] is optional.

NOTE: You must restart both the Extreme Management Center server and client after you change the Connection URL.

Password
Enter the password the Extreme Management Center uses when connecting to the database. Select the Eye icon to display your password.

NOTE: You must restart both the Extreme Management Center 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

Use the Options window (Tools > Options) to set Suite options that apply across all Extreme Management Center applications. In the Options window, the right-panel view changes depending on what you have selected in the left-panel tree. Expand the Suite folder in the tree to view the suite-wide options you can set.

Instructions on setting the following Suite options:

- Advanced SNMP Settings
- Advanced Suite Settings
- Alarm Configuration
- Alarm/Event Logs and Tables
- Client Connections
- Database Backup

- Data Display Format
- Date/Time Format
- Diagnostic Configuration
- ExtremeNetworks.com Update
- MAC OUI Vendor List
- Name Resolution
- NetSight Feedback Program
- NetSight Server Health
- Network Monitor Cache
- Port Monitor
- Services for NetSight Server
- SMTP E-Mail Server
- Status Polling
- System Browser
- Tree
- Web Server

Advanced SNMP Settings

The Advanced SNMP Settings view provides the option to have the NetSight Server use the MyMibs directory or thirdparty directory.

The MyMibs directory is where you add proprietary MIBs to the MIB database on the NetSight Server. This MIB information is then distributed to the NetSight remote clients. If you select this option, the NetSight Server will also use the MyMibs directory (e.g. the MIBs will be included in the SNMP Server Stack).

The third party directory is used for client-based FlexViews and MIB Tools that are proprietary (Enterprise MIBs owned by other companies), not standard IETF or IEEE MIBs. If you select this option, the NetSight Server will also use the third party directory.

CAUTION: In most situations, it is recommended that the NetSight Server should **not** use the MyMibs or thirdparty directories. However, the option is provided for situations where that behavior is warranted. Be aware that selecting this option could result in NetSight Server instability and undesirable consequences.

The Use NetSNMP IPv6 option allows you to SNMP-manage network devices that have IPv6 addresses assigned to them. You must have this option selected in order to be able to add a device with an IPv6 address.

These options apply to all users. For these setting to take effect, the NetSight Server must be restarted.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Advanced SNMP Settings.
3. Select the desired advanced SNMP options.
4. Click **OK** to set the option and close the window. Click **Apply** to set the option and leave the window open.
5. Restart the NetSight Server for these settings to take effect.

Advanced Suite Settings

The Advanced Suite Settings view provides the option to enable or disable NetSight Suite Beta Features. A list of the beta features can be found in the NetSight Suite Release Notes. When you enable the Beta features, you will be asked for a Beta Activation Key. Contact Extreme Networks Support to obtain a Beta Key. Once you enable the beta features, the button will change to "Disable Beta Features."

This option applies to all users. For this setting to take effect, the NetSight Server must be restarted. To enable beta features:

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Advanced Suite Settings.
3. In the right-panel, select the **Enable All Beta Features** checkbox and enter the NetSight Beta Activation Key. Contact Extreme Networks Support to obtain a Beta Key.
4. Click **OK** to set options and close the window. Click **Apply** to set options and leave

the window open.

5. For this setting to take effect, the NetSight Server must be restarted.

Alarm Configuration

Use the Alarm Configuration view to configure options for how alarms are handled on your network. These settings apply to all users.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Alarm Configuration. The Alarm Configuration view opens.
3. In the **Consolidated Email Option** section, the **Enable Email digest** option lets you combine alarm action emails into a single email. Select the option and specify an interval. Email notifications will be collected over the specified interval and then delivered as a single consolidated email.
4. In the **Alarm History** section, select the desired options:
   Enable Detailed Alarm History – 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. If you enable Detailed Alarm History, repeat occurrences of an alarm being raised will also be recorded.
   Preserve Triggering Events in Alarm History – This option preserves alarm triggering events, so that any triggering events are stored with the alarm history record. This allows you to view the triggering event by clicking the View Trigger button in the Alarm History window.
   Number of Days to Maintain Alarm History – Specify (in days) how long the Alarm History will be retained.
5. Select the **Enable Sender Overrides** option to add an E-Mail Sender and E-Mail Sender Password field to the Console Alarms Manager Edit Action Overrides window. This allow you 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.
6. Use the **Alarm Action Defaults** section to define the default content contained in alarm action messages. For example, with an email action, you can define the information contained in the email subject line and body. With a syslog or trap action, you can specify certain information that you want contained in the syslog or

trap message. These values will be used unless they are overridden in an individual alarm.
The message content is configured as a template, with the content passed directly 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.
For an explanation of each field, see the Alarm Configuration view.
For a complete list of available Alarms Manager keywords, see the Edit Action Overrides window in the Console online Help.

7. Click the **Advanced Settings** button to open the Alarm Advanced Settings window where you can set advanced alarm options.
8. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

Setting Alarm/Event Logs and Tables Options

Use the Alarm/Event Logs and Tables view to specify options for limiting disk usage by alarm and event logs and NetSight server logs. These settings apply to all users. You must be assigned the appropriate user capability to configure these options. For more information on configuring log files, see the NetSight Log Files Help topic in the Console online Help.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Event Logs. The Event Logs view opens.
3. In the **Number of Event Logs to limit** section, you can select an option to limit the number of application log files that are saved to the `<install directory>\NetSight\appdata\logs` directory. (The option does not limit the number of Traps or Syslog logs that are saved.) Select one of the following options:
   - **Do not limit the number of log files saved** -- Allows you to keep any number of application log files.
   - **Limit the number of log files saved to** -- Sets a limit to the number of application log files saved. Older files are deleted when the maximum number is reached. Enter the desired number.

4. In the Number of Server Logs to limit section, you can select an option to limit the number of server log files that are saved to the `<install directory>\NetSight\appdata\logs` directory. Select one of the following options:
    - Do not limit the number of log files saved -- Allows you to keep all server log files.
    - Limit the number of log files saved -- Sets a limit to the number of server log files saved. Older files (determined by the date of the file in the filename) are deleted when the maximum number is reached. Enter the desired number.
5. In the Number of Rows to keep in Event and Alarm tables section, specify settings that determine the number of rows that will be maintained in all of the tables in the Alarm and Event Log view. The table size reaches an absolute limit when the number of rows is equal to the value of the two parameters added together minus one. With the next entry, the table is clipped back to the number of rows set by the Clip to nnnn rows value. Subsequent entries will allow it to grow again until the Clip when above is exceeded by nnnn rows limit is reached and the table is again clipped.
6. In the Event Log entry timestamp format section, specify the timestamp format used for event log entries in the actual application log files. (This option does not affect the log entries displayed in NetSight client Event Log views.) Select one of the following options:
    - Use raw timestamp format -- Displays timestamps in a raw non-readable format.
    - 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.
7. In the Event and Alarm Table Host/Port Names section, you can configure host name and port name resolution, and display the device hostname in the Source column in alarm and event tables:
    - 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 Suite Name Resolution option.)
    - Display host name in source column if available
    - 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 Suite Name Resolution option.)

8. The Execute Command Script feature includes script contents in logged events, which is not secure if the script includes passwords. If the **Execute Command Script** option is deselected (default), the script is removed from the logged event. Select this option to include script contents in Execute Command Script events.
9. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

Setting Client Connection Options

Use the Client Connections view to configure client connection options.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Client Connections.
3. In the right panel, select the **Enable disconnect from user inactivity** checkbox if desired, and specify the amount of time (in minutes) before the disconnect will take place. This option specifies a duration of end user inactivity (no keyboard or mouse activity) before the user will be disconnected from the NetSight Server. If this option is enabled, after the specified amount of time, the end user will be disconnected from the NetSight Server and the application will close. This option will apply to the current logged-in user. You must be a member of an authorization group that has been assigned the Server Information > Disconnect Clients capability to configure this option.
4. Select the **Redirect Client/Server SNMP Communications** checkbox, if desired. When a client and server are running on different workstations, SNMP requests are made from the client workstation and device status polling requests are made from the server. Checking this option redirects all SNMP requests through the server. In this configuration, the server uses the same Status Polling settings that would have been used by the client. Redirecting all SNMP requests to the server workstation could adversely affect performance of NetSight applications. This option applies to the current logged-in user and has no effect when the client and server are running on the same workstation. You must be a member of an authorization group that allows users to configure SNMP Redirection in order to configure this option.
5. Configure the **Messaging Credentials** option. Messaging credentials are used for establishing connections between the NetSight server and Extreme Access Control

engines and the Extreme Management Center server. If your network includes Extreme Access Control engines running version 4.0.1 or earlier, you must enable the "Allow legacy credentials for messaging connections" checkbox. If your engines are version 4.1 or later, you should disable the checkbox. This option applies to all users.

6. Select the Show Credentials checkbox to view the current messaging credentials. This option applies to all users.
7. Click OK to set options and close the window. Click Apply to set options and leave the window open.

Scheduling a Database Backup

Use the Database Backup view to schedule backups of the NetSight database. An up-to-date database backup is an important component to ensuring that critical information pertaining to all NetSight applications is saved and readily available, if needed. These option applies to all users.

Select one or more days of the week and specify a time for the backup to be performed. The backup will take place at the same time for each selected day.

The database is backed up to the specified directory. 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 will not be accepted.

Both the start and stop of the database backup are logged to the Console Event View log for verification and tracking purposes.

For more information, see Tuning Database Backup Storage in Performance Tuning section of the NetSight Technical Reference.

1. Select Tools > Options in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Database Backup.
3. In the right panel, select the days of the week and a time for the backup to be performed.
4. Specify whether to save all backup files or limit the number of files saved. If you specify a number of files to save, then older backups are removed after a scheduled backup is completed and the limit has been reached.
5. Specify the directory where the backup will be stored.

6. The Backup Alarm and Reporting Database checkbox lets you enable and disable the automatic backup of alarm data and OneView reporting data. Because the alarm and reporting databases can be quite large, this allows you to control the amount of disk space used by the database backup operation.
7. You can customize the date and time formats of backup files by selecting the option that formats the date – day (DD), month (MM), and year (YYYY) – according to your personal preference.
8. Click OK to set options and close the window. Click Apply to set options and leave the window open.

Setting Data Display Format Options

Use the Data Display Format view to specify your network mask, MAC address separator, how to display end-system MAC addresses in right-panel tables, and auto group delimiter display options. You can also specify how to display devices in the device tree. These settings will apply to the current logged-in user.

1. Select Tools > Options in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Data Display. The right-panel Data Display view is displayed.
3. Specify one of the following network mask options:
   - CIDR (where translation is possible) – Network masks are entered and displayed using CIDR (Classless Inter-Domain Routing) format. 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* for a 16-bit mask.

     NOTE: Dot delimited masks without contiguous left-most "one" bits cannot be translated to CIDR. For example, the dot-delimited mask *255.0.255.0* is a valid mask, but cannot be displayed in CIDR format.

   - Dot Delimited – Network masks are entered and displayed using dotted decimal format. Dotted decimal notation represents IP addresses and network masks as four octets separated by periods. For example, a 16-bit mask in dotted decimal notation is *255.255.0.0*.

4. Specify whether you want MAC addresses displayed with a period (.), colon (:), or dash (-) separator (e.g. 00.00.1D.76.66.66, 00:00:1D:76:66:66, or 00-00-1D-76-66-66).
5. Specify how you want to display end-system MAC addresses in right-panel tables. You can display them as a full MAC address or with a MAC OUI (Organizational Unique Identifier) prefix. This allows you to display the associated vendor the MAC address belongs to, if an OUI mapping exists. You can also limit the vendor name to a certain number of characters, if desired. When the Display Unknown MACs as Unknown checkbox is selected, the MAC address for unknown users is displayed as "Unknown" in the End-Systems view. If the checkbox is not selected, the pseudo MAC address assigned to each device is displayed instead of "Unknown" for end-systems learned on an L3 controller.
6. Specify the Auto Group Delimiter you want to use. This character is used 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). This option defines 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.
7. Specify how device names should be displayed in the left-panel tree:
   - Use IP Address – use the device's IP address.
   - Use System Name – use the administratively-assigned name of the device taken from the *sysName* MIB object.
   - Use User Defined Nickname – use the user-defined nickname as defined in the Console Properties Tab (Device).
8. Click OK to set options and close the window. Click Apply to set options and leave the window open.

Setting Date/Time Format Options

Use the Date/Time Format view to customize the date and time formats to your own personal preference. These settings will apply to the current logged-in user.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. Select Date/Time Format in the left-panel tree. The right-panel Date/Time Format view is displayed.
3. Select the **Date** option that formats the date – day (DD), month (MM), and year (YYYY) – according to your personal preference.
4. Select the **Time** option that formats the time – 12-hour or 24-hour clock – according to your personal preference.
5. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

Setting Diagnostic Configuration Options

Use the Diagnostic Configuration view to configure the level of information collected in client-side diagnostic logs. The information collected in these logs can be used for troubleshooting purposes. Each NetSight application has its own log. The diagnostic information is recorded in the log for the application you are currently working in. The logs are located in the following directory:

Windows: \Documents and Settings\<user home directory>\Application Data\NetSight\logs

Linux: ~/NetSight/logs

The table in this Options view lists the NetSight applications and various NetSight components, and lets you configure the level of information to be collected for each one.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. Select Diagnostic Configuration in the left-panel tree. The right-panel Diagnostic Configuration view is displayed.
3. In the table, select the row(s) you would like to edit, and toggle the Show/Hide Table Editor button  to display the Table Editor row at the bottom of the table. In the Table Editor row, click on the last column and use the drop-down list to select the desired level:
    - Restore Defaults – restores the level to its factory default setting.
    - log4j File Override – sets the level to the level specified in the log4j.properties file.
    - Off – turns off all diagnostic logging.

- 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.

CAUTION: The Informational and Verbose settings will create large log files and may impact system performance.

4. Once you have selected a new level, a green exclamation mark (!) marks the cells that have been changed (but not Applied) and the Apply button becomes active. Click Apply to apply the changes to the table.
5. Click OK to close the window.

Setting ExtremeNetworks.com Update Options

Use the ExtremeNetworks.com Update view to configure options for accessing the ExtremeNetworks.com website to obtain information about the latest NetSight 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.

1. Select Tools > Options in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select ExtremeNetworks.com Update. The ExtremeNetworks.com Update view opens.
3. To schedule a routine time to check for updates, use the drop-down list to select the desired frequency (Daily, Weekly, Disabled) for checking for updates. If you specify a Weekly check, use the drop-down list to select the day of the week you wish the check to be performed, and set the desired time. If you specify a Daily update, set the desired time.
4. If necessary, you can change the NAC assessment web update server. This is the web update server used by NAC Manager to update NAC assessment server software. This update operation pertains only to Extreme Access Control on-board agent-less assessment servers.

5. If your network is protected by a firewall, you will need to configure proxy server settings to use when accessing the ExtremeNetworks.com website. In the HTTP Proxy Server section, click **Edit** to open the Edit Proxy Settings window. Select the **Specify 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 once used successfully. If you change them here, it is recommended that you restart the NetSight Server to clear the old credentials from the cache. Click **OK**.

   NOTE: The update procedure will use these proxy settings only when necessary, otherwise the settings will be ignored.

6. Enter the credentials that will be used to access the ExtremeNetworks.com website to obtain firmware and NetSight update information. You will need to create an account at ExtremeNetworks.com and define a user name and password for the account, then enter the same credentials here.
7. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

MAC OUI Vendor List

Use the MAC OUI Vendor List view to display the IEEE OUI and Company_id Assignments public mapping list, and update and modify the list, if desired. For example, you can update the list to the latest version from the IEEE website, and if you have devices that do not have an OUI (Organizational Unique Identifier), you can add your own vendor entries.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder and select MAC OUI Vendor List. The MAC OUI Vendor List view opens.
3. Use the toolbar buttons at the top of the table to add, edit, or delete MAC OUI vendors, or update the MAC OUI Vendor list from either the IEEE website or a file.
4. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

Setting Name Resolution Options

Use the Name Resolution view to set options related to host name and port name resolution.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Name Resolution. The Name Resolution view opens.
3. Use the Host Name Resolution section to set options for resolving host names to IP addresses and IP addresses to host names.
    a. The **Enable Name Resolution** option allows host names to be displayed in place of IP addresses throughout NetSight. When enabled, the feature is primarily used by NetFlow. With name resolution enabled, flow data would show "Client=rsmith-ws Server=proxy-usa", rather than "client=134.141.1.2 server = 134.141.1.1". The option is off by default because name resolution can add additional load on the network's DNS server.
    b. The **Use short hostnames for local addresses** option is enabled by default when hostname resolution is enabled, and applies to OneView only. When enabled, the hostname cache will remove the fully qualified hostname's domain if it matches one of the specified local address domains. For example, "jsmith-ws.mycompany.com" would display as "jsmith-ws" if mycompany.com is listed as a local address domain. This option can be disabled when troubleshooting problems with hostname resolution, or if IP addresses are preferred.
    c. The **Local Address domains** is a list of *home domains* that will be deleted from a local hostname when it is added to the hostname cache. Use the Add Domain field to add or remove a domain. You can add multiple home domains when subdomains are defined for your network. This option applies to OneView only.
    The first time the hostname cache service is started, if the Local address domains list has not been defined, NetSight will attempt to auto-populate it by resolving the IP address of the NetSight server. If it resolves to a subdomain, NetSight will create multiple entries for all subdomains but the root domain (.com). If it cannot do this successfully, the list will not be populated.

d. Enter the **Maximum number of cached resolutions**, which is the maximum number of IP/hostname pairs that can be cached in memory. This number can be adjusted to control the amount of memory used by this service.

e. Enter the **Maximum number of pending resolutions**, which is the maximum number of hostname resolution requests that can be queued up. This number can be adjusted to control the maximum amount of time spent waiting for a resolution.

f. The **Aging Threshold** option determines how long IP/hostname pairs will be cached in memory. After the aging threshold time has passed, the IP/hostname pair is removed from the cache in order to prevent stale IP-hostname associations. This option addresses the fact that DHCP assigns a new IP address to users frequently, especially on reboots. Without an aging threshold, hostnames will continue to be associated to the IP they had at the first lookup. The default value is 24 hours; the minimum value is 1 hour.

g. The **DNS Lookups Per Minute** option set the maximum number of hostname lookups that the DNS server can perform each minute. This prevents hostname resolution from using so many resources on a switch that switching of real traffic is affected.

4. Use the Port Name Resolution 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.

   a. Enter the **Maximum number of cached resolutions**, which is 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.

   b. Enter the **Maximum number of pending resolutions**, which is 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.

   c. Enter the **Interface name change polling interval**, which specifies how often the port name resolution service checks devices to see if port information has changed.

5. Use the **Advanced Settings** button to open the Name Resolution Advanced Settings Options window, where you can set advanced name resolution options.

6. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

NetSight Feedback Program

This option allows you to enable or disable participation in the NetSight Customer Feedback Program. If you participate, NetSight gathers anonymous usage information that will be used to better understand how NetSight software is used and to make decisions on enhancing the product. This bi-directional communication with ExtremeNetworks.com also enables features for you such as the ability to get best practices firmware configurations, find the latest firmware updates based on your own network, create Support cases directly from NetSight that automatically upload troubleshooting information, and more.

The information gathered will not be used for marketing purposes or to contact you.

Setting NetSight Server Health Options

Use the NetSight Server Health view to select an option to send an email if the NetSight database goes down, and when the database comes back up.

1. Select Tools > Options in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select NetSight Server Health. The NetSight Server Health view opens.
3. Select the Send email option.
4. Enter the email address of the person who should receive the notification.
5. Click OK to set options and close the window. Click Apply to set options and leave the window open.

Setting Network Monitor Cache Options

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).

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 will increase background SNMP performed by the server.

Storing this information greatly improves performance for views in NetSight that request it. The cache should generally be left enabled for the best experience.

Use the Network Monitor Cache view to configure options for the cache.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. Select Network Monitor Cache in the left-panel tree. The right-panel Network Monitor Cache view is displayed.
3. Use the **Enable Device Cache** checkbox to enable or disable the Network Monitor Cache. Enabling the cache improves performance for NetSight views that request this information.
4. Use the **Enable In-Memory Caching** checkbox to enable or disable the in-memory cache. To limit memory usage, you can disable the In-Memory Cache and have the network monitor cache rely directly on the database.
5. Use the **Maximum In-Memory Cache Size** option to set the maximum number of devices whose data will be stored in the In-Memory Cache. This option lets you adjust the amount of memory the cache will use.
6. Use the **Data Polling Interval** option to set the frequency (in minutes) that the device data is checked for changes. If the device data is stale, the data is refreshed in the cache. Reducing the interval will increase background SNMP performed by the server.
7. Use the **Advanced Settings** button to open a window where you can set network monitor cache advanced options.
    - **Maximum number of SNMP worker threads** option. The cache is populated with results from SNMP queries to devices. If multiple devices are added to the cache at the same time, this number determines the maximum number of threads that can send SNMP queries in parallel.
    - **Per-Feature polling overrides.** Allows you to set unique polling intervals for individual cache features that should be polled more frequently. Set to 0 to use the interval set for the Data Polling Interval.

Setting Port Monitor Options

Use the Port Monitor view to specify Port Monitor display options. These settings will apply to the current logged-in user.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder and select Port Monitor. The Port Monitor view opens.
3. In the **Interval between Polls** field, enter the amount of time (in seconds) that should elapse between polls of the device.
4. In the **Table Colors** section, use the buttons to select the primary and secondary row colors you want to display in tables. A sample of your selection will be displayed in the Sample table scheme to the right of your selections.
5. In the **Enable Display of Port Monitor Data** section, use the checkboxes to specify what data will be displayed for a Port Monitor session. If the Show Empty Panels Collapsed checkbox is selected, panels without information will be collapsed so those panels with information are easier to view.
6. In the **Maximum Open Port Monitor Count** field, specify the maximum number of Port Monitor windows that can be open at one time. If too many windows are open at one time, system operation may be impacted. The default setting is 5.
7. Click **OK** to set the option and close the window.

Setting Services for NetSight Server Options

Use the Services for NetSight Server view to specify your TFTP settings. These settings apply to all users. You must be assigned the appropriate user capability to configure these options.

1. Select **Tools > Options** in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Services for NetSight Server.
3. Specify a TFTP root directory, whether you are using the NetSight TFTP server or another TFTP server. The root directory is the base directory to which the TFTP server is allowed access. The TFTP server will be allowed to create files to or read files from this directory and any of its subdirectories. Use the default root directory,

or if you would like to use an alternate root directory, enter a path to that directory in this field or use the Browse button to navigate to the directory. Changing the TFTP root directory may require restarting the TFTP server.

NOTE: If you are using a TFTP server other than the NetSight TFTP service, 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 (e.g. C:\ or D:\).
- 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 // (UNIX or Linux systems) or backslashes \\ (Windows systems) to indicate the name of the system, and one slash or backslash to indicate the path within the computer. For example, on a Windows system, instead of using
  `h:\` (where h:\ is mapped to the tftpboot directory on the remote drive)
  use
  `\\yourservername\tftpboot\`

4. If the TFTP server resides on a remote system, or if the local system is configured with multiple IP addresses, enter the IP address for the TFTP service in the TFTP Server IP Address field. This field accepts both IPv4 and IPv6 addresses.
5. Click OK to set options and close the window. Click Apply to set options and leave the window open.

Setting SMTP E-Mail Server Options

Use the SMTP E-Mail Server view to specify the SMTP E-Mail server that will be used by the NetSight E-Mail notification feature. The E-Mail notification feature is used in Console's alarm action configuration, as well as in Inventory Manager's Capacity Planning report scheduling and in Automated Security Manager actions. These settings apply to all users. You must be assigned the appropriate user capability to configure these options.

1. Select Tools > Options in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select SMTP E-Mail Server.
3. In the right panel, specify the SMTP (E-Mail) server that should be used for outgoing messages generated by the E-Mail notification feature.
4. Enter the sender's address that will be inserted in outgoing e-mail notification messages. The address should be in a fully qualified format such as "sender's name@sender's domain."
5. Enter the password that will be provided by the user before the email can be processed.
6. Click OK to set options and close the window. Click Apply to set options and leave the window open.

Setting Status Polling Options

Use the Status Polling view to specify options for polling devices in the left-panel device tree. Console uses the polling options and poll groups defined here to contact the devices and update tree information. When a device is added to the NetSight database using the Add Device menu option or a Console CDP Seed IP Discover, it is added to the default poll group selected here. (A Console IP Range Discover lets you assign devices to any of the three poll groups.) You can then reassign individual devices or device groups to a different poll group using the Access view in the Console Properties tab. These settings apply to all users. You must be assigned the appropriate user capability to configure these options.

Optimal Poll Intervals

There are three distinct poll groups, and each device belongs to one of the three groups. This lets you poll critical devices at a more frequent interval, while polling non-essential devices less frequently.

The overall density of polling is controlled by the Maximum number of devices to contact at once setting. This determines the maximum number of devices from each group that can be polled at any given time. Console always attempts to poll up to the maximum number of devices until all of the devices in the three groups have been polled. As responses are received and devices are removed from the poll queue, other devices are added to the queue. Once all the devices have been polled, Console stops polling and batches information to update clients.

If the Maximum number of devices to contact at once is too high, such that the poll density is too high, system performance will degrade 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, the poll density (Maximum number of devices to contact at once) should be reduced to increase performance.

The default Maximum number of 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.

1. Select Tools > Options in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Status Polling. The Status Polling view opens.
3. In the SNMP section, set the status polling options for devices whose poll type is set to "SNMP."
    a. Set the Maximum number of devices to contact at once. This is the maximum number of IP addresses that Console will attempt to contact simultaneously.
4. In the Ping section, set the status polling options for devices whose poll type is set to "Ping."
    a. Set the Number of Ping Retries. This is the number of attempts that will be made to ping a device. The default setting is 3 retries, which means that Console retries a timed-out request three times, making a total of four attempts to contact a device.
    b. In the Length of Ping Timeout field, enter the amount of time (in seconds) that Console waits before re-trying to contact a device. The default setting is 3 seconds. The maximum setting is 20 seconds.

        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.

    c. Set the Maximum number of devices to contact at once. This is the maximum number of IP addresses that Console will attempt to contact simultaneously.
5. In the Poll Group section, there are three poll groups that each define a unique poll frequency. A poll frequency specifies the actual length of the poll cycle. You can rename the poll groups according to your network's needs and specify different poll frequencies. For example, if you are monitoring devices on the other side of a WAN

link, you can rename a poll group to "WAN Devices" and then assign that poll group to those devices. Poll group names must be unique. For more information on setting poll group intervals, see the guidelines outlined in Optimal Poll Intervals.

6. Select one group as the default poll group. When a device is added to the NetSight 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 Access view in Console's Properties tab.
7. Click OK to set options and close the window. Click Apply to set options and leave the window open.

Setting System Browser

Use the System Browser view to specify the web browser for NetSight to use when launching web pages from NetSight applications. This setting applies to the current logged-in user.

1. Select Tools > Options in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select System Browser.
3. In the right panel, select your preferred web browser. The browser selections displayed depend on the web browsers installed on your system. Select Default to specify the system default browser.
4. Click OK to set options and close the window. Click Apply to set options and leave the window open.

Tree

Use the Tree view to specify whether a warning message will be displayed when performing drag and drop operations on devices and device groups in the network elements tree. For example, if you drag a device in the tree to a user-defined folder, the warning appears asking if you are sure you want to drop the selected device into this folder. This warning allows you to verify that you do indeed want to perform a drag and drop operation to that folder, and prevents you from inadvertently moving devices. However, if you find it annoying to have the warning appear each time you do a drag and drop operation, you can deselect the option. This setting applies to the current logged-in user.

1. Select Tools > Options in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Tree.
3. In the right panel, deselect the checkbox if you do not want the warning to appear.
4. Click OK to set options and close the window. Click Apply to set options and leave the window open.

Web Server

Use the Web Server view to specify the HTTP and HTTPS port ID for HTTP web server traffic. This port must be accessible through firewalls for users to install and launch NetSight client applications. By default, NetSight uses port ID 8080 (HTTP) and 8443 (HTTPS). If you change the port ID, you must restart the NetSight Server for the change to take effect.

This setting applies to all users. You must be assigned the appropriate user capability to change this setting.

1. Select Tools > Options in the menu bar. The Options window opens.
2. In the left-panel tree, expand the Suite folder, and select Web Server.
3. In the right panel, enter the desired port IDs.
4. Specify a session timeout value for all NetSight web-based views, such as NetSight OneView web pages and Console FlexViews.
5. The Password AutoComplete option lets you disable automatic password completion for users logging into NetSight web interfaces such as OneView. Note that for Extreme Access Control web interfaces, you must enforce from the Extreme Access Control tab for the option to take effect.
6. Click OK to set options and close the window. Click Apply to set options and leave the window open.
7. You must restart the Extreme Management Center Server for any Port ID changes to take effect.

Related Information

For information on related windows:

- Suite Options Window

Tasks Overview

The **Tasks** tab in Extreme Management Center 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:

- Scheduled Tasks
- Saved Tasks
- Scripts
- Workflows
- Workflow History

The Menu icon (☰) at the top of the screen provides links to additional information about your version of Extreme Management Center.

Scheduled Tasks

The Scheduled Tasks tab allows you to configure Extreme Management Center to automatically perform the following tasks:

- Generate a subset of available reports in PDF format
- Run a workflow
- Run a script
- Email information to Extreme Networks Support
- Discover newly added devices

NOTE: For the email notification to work, configure your SMTP Email Server options. Click the **SMTP** button to open the SMTP Email Server window, where you can define your outgoing email server and the sender's address for your email notifications.

The Scheduled Tasks table lets you view currently scheduled tasks and use toolbar buttons to add, edit, copy, and delete a scheduled task. Click 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. Click the red icon for error details.

Click 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 Extreme Management Center. Select **Scheduled Task** from the drop-down menu at the top of the table to view task execution events and errors.

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

Extreme Management Center provides you with predefined scripts and allows you to create your own.

Extreme Management Center scripts are files containing CLI commands, control structures, and data manipulation functions. Scripts can be executed on one or more devices or ports, simultaneously on multiple devices or ports, or on one device or port at a time.

You can create tasks, which run a script on specified devices or ports at specified times, either on a one-time or recurring basis. Tasks execute the script according to a schedule you configure.

Workflows

Workflows you create are modeled as diagrams, with each action linked in a chain. Once you create a workflow, Extreme Management Center performs a complex series of steps with a single click. 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. Once you create a workflow, you can schedule it to run on a periodic basis you configure on the **Scheduled Tasks** tab.

IMPORTANT: Workflows require special access. To access workflow functionality, contact Global Technical Assistance Center (GTAC).

Workflow History

The Workflow History tab provides 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.

Related Information

For information on related tabs:

- Scheduled Tasks
- Saved Tasks
- Scripts
- Workflows
- Workflow History

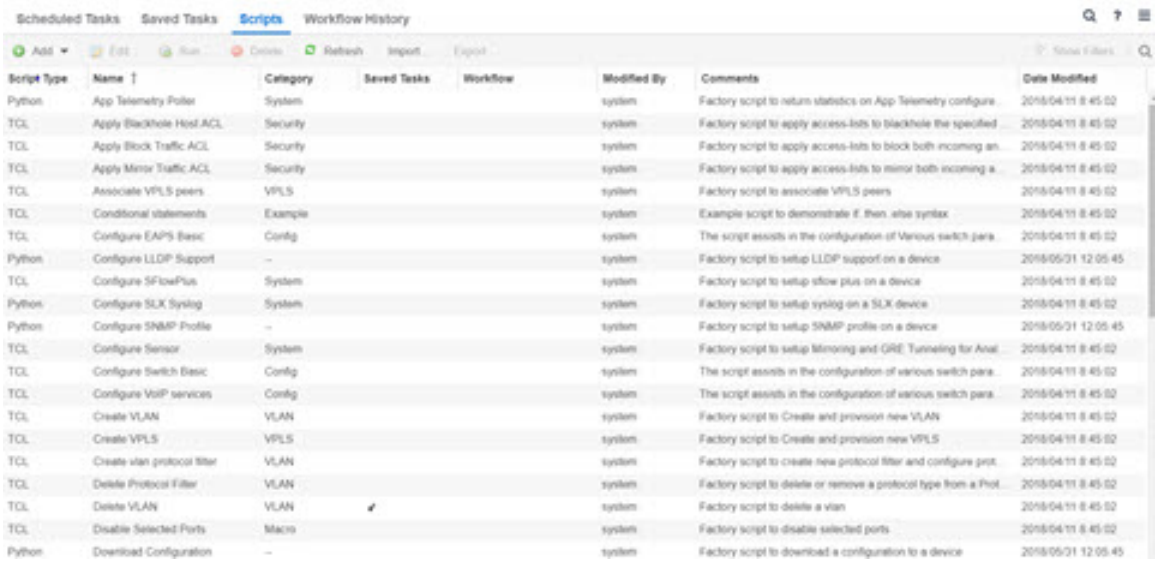
Scripts Overview

Scripting functionality is built into Extreme Management Center, which provides you with predefined scripts and allows you to create your own.

Extreme Management Center 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 Extreme Management Center, 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.

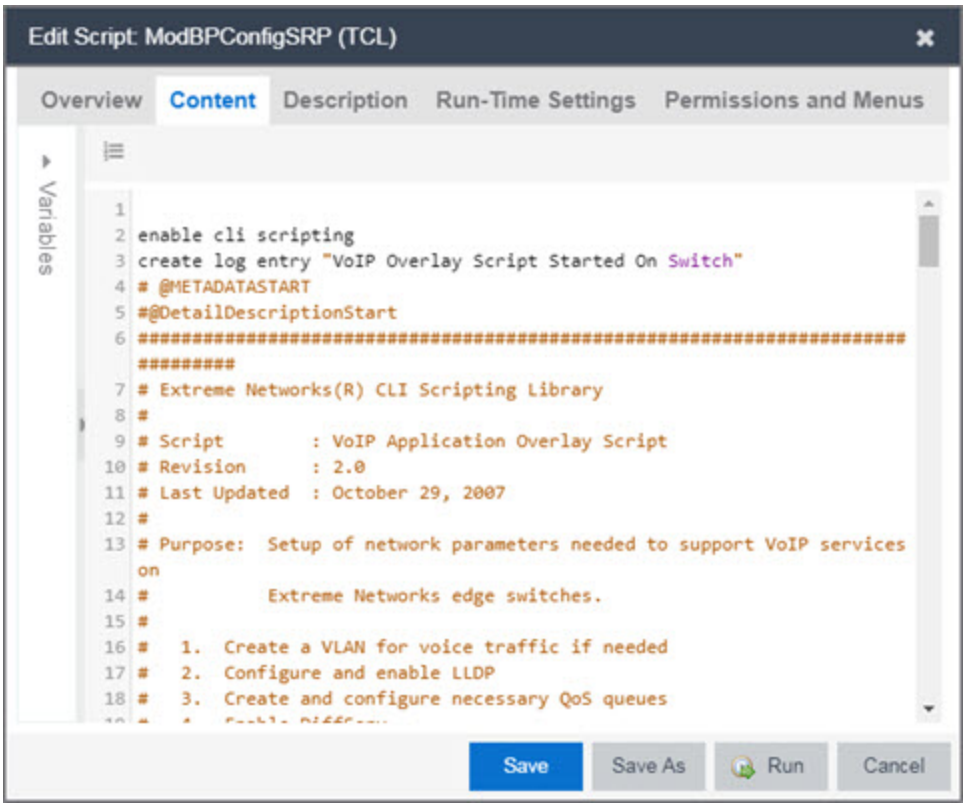
Comments

Comments or a description of the script.

Date Modified

The date the script was last modified.

Double-click a script to open the script editor dialog.



Related Information

For information on related tabs:

- How to Create Scripts in Extreme Management Center
- Workflows
- Saved Tasks
- Scheduled Tasks

How to Create Scripts

This chapter describes the scripting functionality built into Extreme Management Center and describes how to use Extreme Management Center to create scripts.

Extreme Management Center Scripts Overview

Extreme Management Center scripts are files containing CLI commands, control structures, and data manipulation functions. Extreme Management Center 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.

Extreme Management Center allows you to create Extreme Management Center 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.

Extreme Management Center scripts are similar to ExtremeXOS scripts in that they are collections of ExtremeXOS CLI commands and control structures. Extreme Management Center scripts add some additional commands specific to Extreme Management Center.

In general, Extreme Management Center scripts support syntax and constructs from the following sources:

- ExtremeXOS CLI commands — ExtremeXOS CLI commands in an Extreme Management Center script are sent to the device or port and the response can be used by the script. Abbreviated ExtremeXOS commands do not work unless you prefix the shortened command with CLI.

  For example, to abbreviate `show vlan`, type `CLI sh vlan`.
- ExtremeXOS CLI scripts — Control structures such as IF..ELSE and DO..WHILE can be used in Extreme Management Center scripts. See "CLI Scripting" in the *ExtremeXOS User Guide* for more information on ExtremeXOS script functionality and syntax.
- Python scripting language — Create scripts using the python programming language.
- TCL scripting language version 8.1 — For general information about the TCL scripting language, see www.tcl.tk.

  Syntax and constructs from these sources work seamlessly within Extreme Management Center scripts. For example, the response from a switch to an ExtremeXOS CLI command issued from a script can be processed using TCL functions.

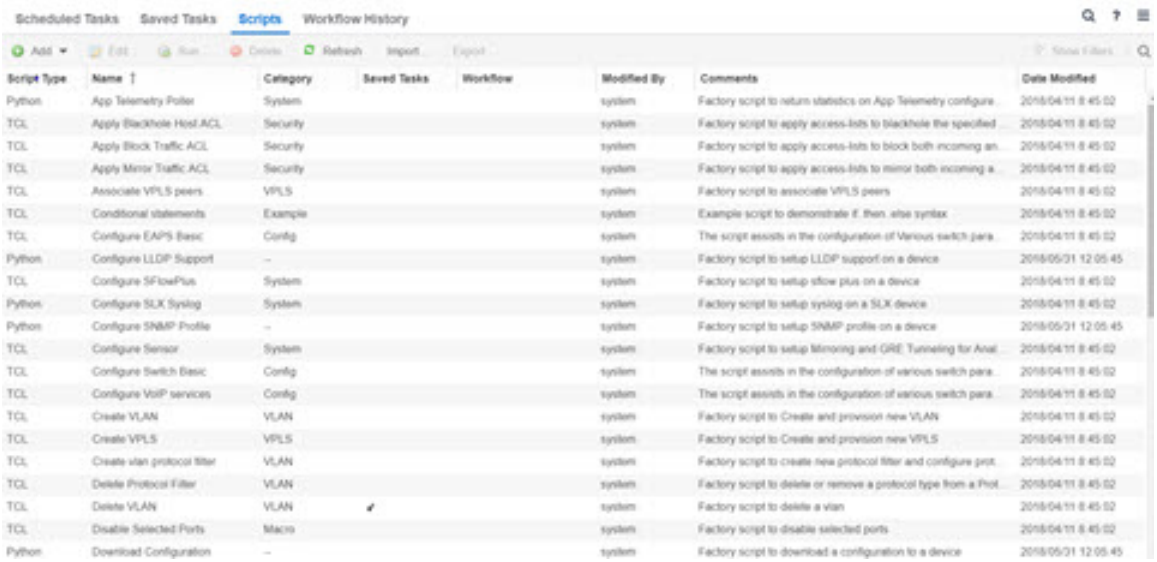
Bundled Extreme Management Center Scripts

Extreme Management Center includes a number of sample scripts you can use as templates for your own Extreme Management Center scripts. These scripts perform such tasks as enable/disable ports, apply ACLs, restart engines, and configure VLANs.

The sample scripts included with Extreme Management Center 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 Extreme Management Center Script Interface

To display the scripts configured in Extreme Management Center, select the **Tasks** tab, then click the **Scripts** tab.

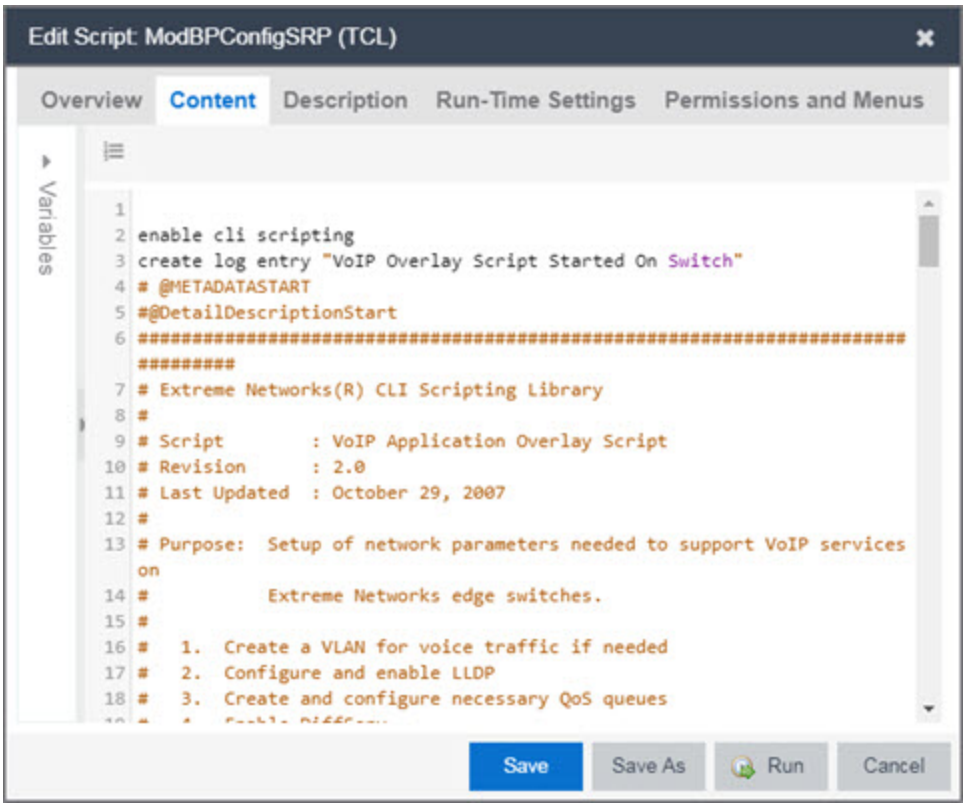


The Scripts tab contains the following information:

- **Script Type** — The language in which the script is written.
- **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.
- **Name** — The name of the script. The script **Name** is defined when adding the script and can not be edited.
- **Workflow** — Indicates if the script is included in a workflow.

- Comments — Comments or a description of the script.
- Modified By — The name of the last user to modify the script.
- Date Modified — The date the script was last modified.

Double-click a script or select a script and click the Edit button to open the Edit Script window.



The Extreme Management Center Edit Script window allows you to add content to a script, set values for parameters, specify run-time settings, and specify the Extreme Management Center users with permission to run the script.

Depending on the type of script you are editing, the following tabs may appear in the Extreme Management Center 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.

- Run-Time Settings — Specifies script settings applied when the script is run.
- Permissions and Menus — Specifies Extreme Management Center user roles with the ability to run the script, and whether or not, and where, the option to run the script appears in the Extreme Management Center interface, such as on a menu or in a shortcut menu.

Managing Extreme Management Center Scripts

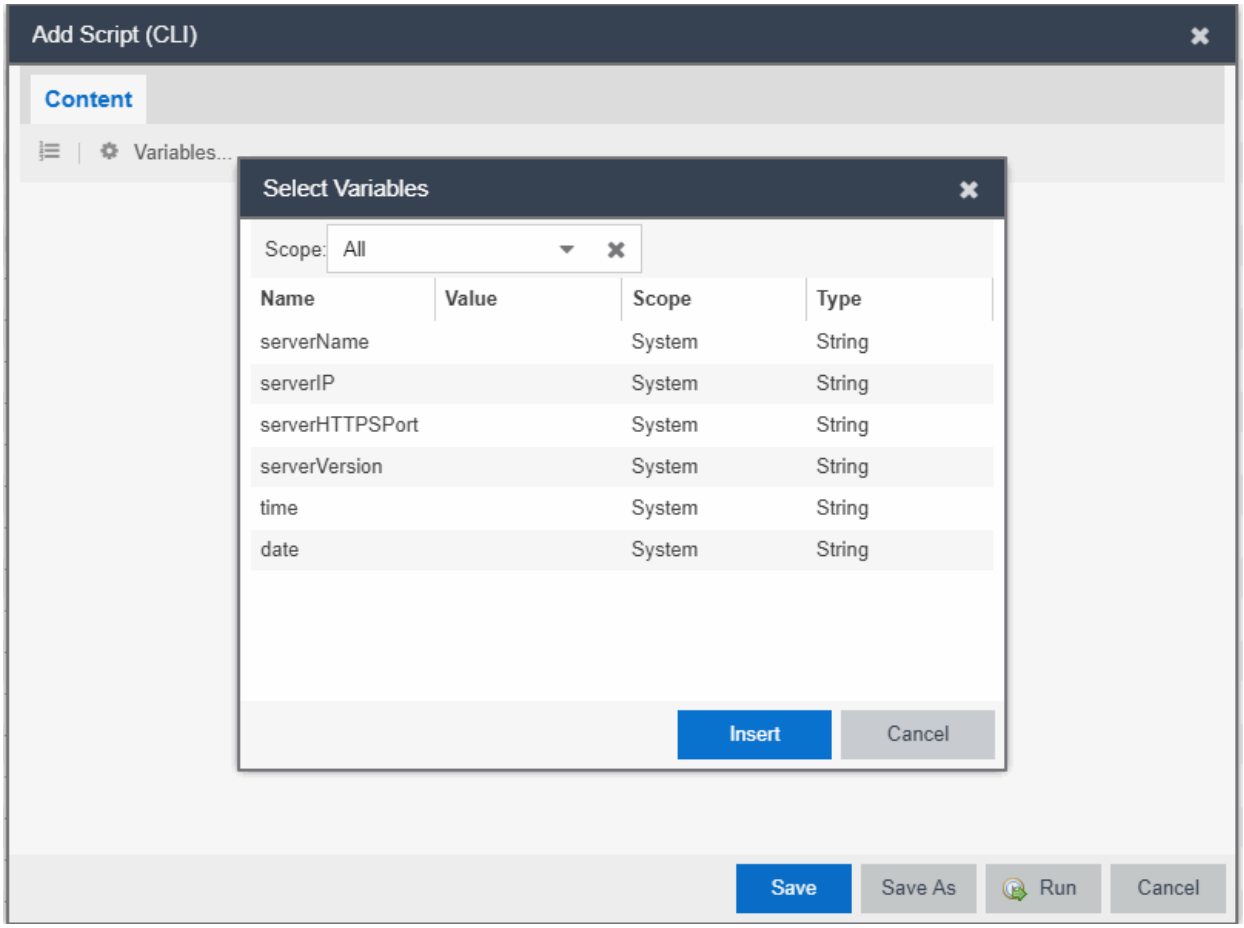
With scripting, you can:

- Create an Extreme Management Center Script
- Specify Run-Time 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 Extreme Management Center
- Export a Script
- Save Script as a Task

Create an Extreme Management Center Script

1. Click Scripts on the Tasks tab.
2. Click the Add button.
3. Select the type of script you are creating:
    - TCL — A Tool Command Language script. 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. Proceed to step 4.

4. When selecting **CLI** from the **Add** drop-down menu, the **Add Script** window opens, where you can enter the CLI commands for the script. Click **Variables** to open the **Select Variables** window, from which you can select variables you define on the Custom Variables tab.



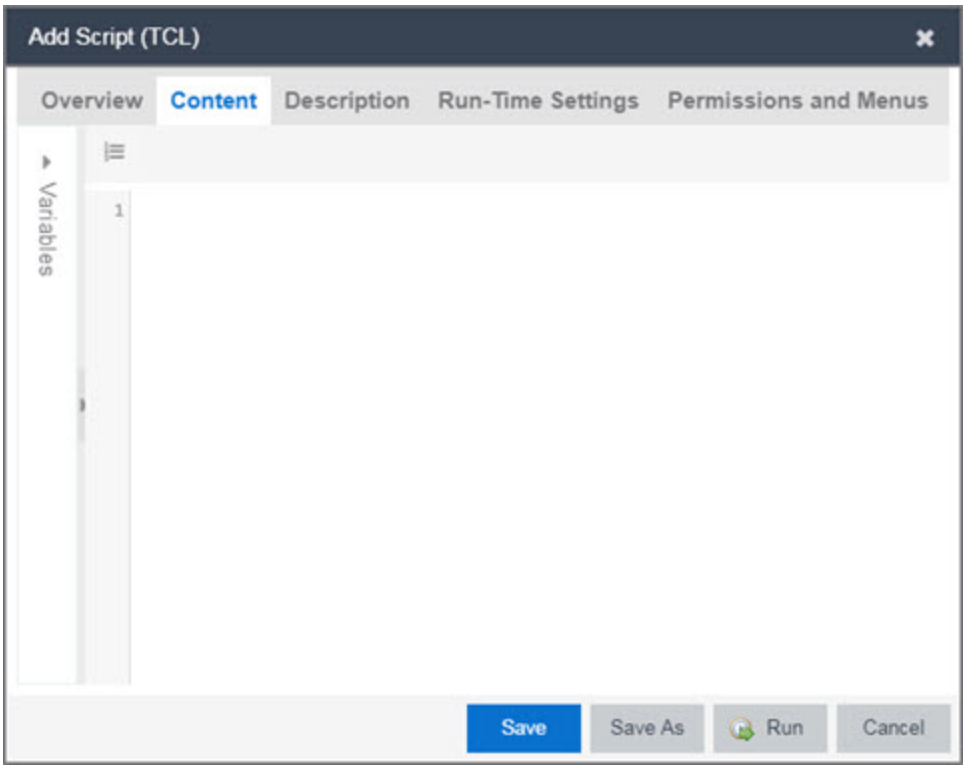
Use the **Scope** drop-down menu to select either **All**, **Global**, or **System** from the drop-down menu, depending on how you configured the variable you are inserting. Click **Insert** to add the variable to your script.

Click **Save** to save the CLI script on the **Scripts** tab or click **Save As** to save the script to the Extreme Management Center server.

Click **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.
- Run-Time Settings — Specify script settings applied when the script is run.
- Permissions and Menus — Specify Extreme Management Center user roles with the ability to run the script, and whether or not, and where, the option to run the script appears in the Extreme Management Center interface, such as on a menu or in a shortcut menu.



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

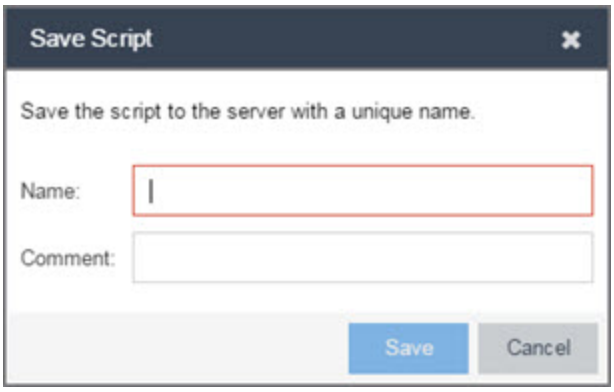
list of system variables appears under Variables. To add a variable to the script, double-click the variable.

8. Enter script commands after the metadata section of the script.

   The following are examples of types of script commands supported in Extreme Management Center:

   - ExtremeXOS 12.1 and later CLI scripting commands
   - TCL commands
   - Constructs

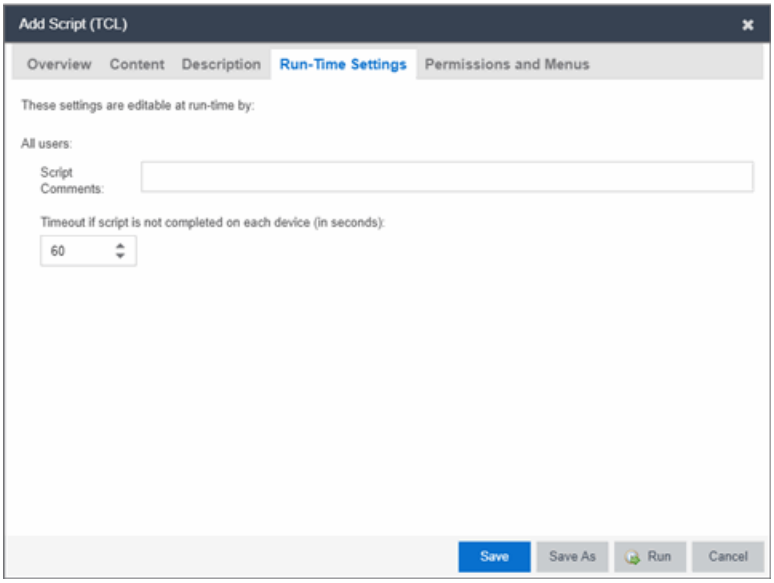
9. Click the **Run-Time Settings** tab to specify run-time settings.
10. Click the **Permissions And Menus** tab to specify which Extreme Management Center user roles have permission to run the script, and whether or not, and where, the script appears in the menu or in a shortcut menu.
11. Click **Save**. The **Save Script** window appears.



12. Type a name for the script file in the **Name** field and a comment about the script in the **Comment** field, if necessary.
13. Click **Save**.
14. Click **Run** to run the script now or **Cancel** to run the script at a later time.

Specify Run-Time Settings for a Script

To specify the run-time settings for a script, click the **Run-Time Settings** tab.



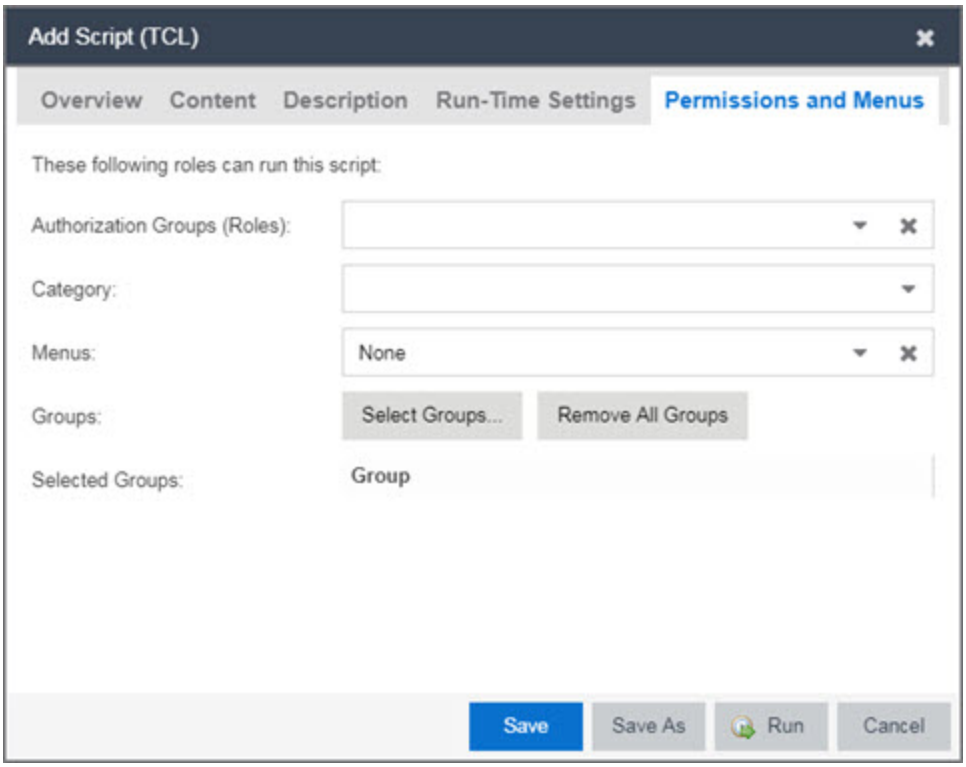
Use this tab to specify the following settings:

- 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 Extreme Management Center 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.

Click 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 menu.

Category

Select the **Category** group from the drop-down menu, which defines the Tasks submenu in which the script is grouped throughout Extreme Management Center.

Menus

Select the Tasks submenus in Extreme Management Center in which you want the script to display from the drop-down menu. Select **Multi-Device** for User Device Group scripts.

Groups

Click the **Select Groups** to select the device groups on which the script displays.

Selected Groups

Displays the Groups in which the script is included.

Run a Script

From the Network 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. Click **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, click the **Description** tab to view the description defined for the script.
6. Click **Next**.

   The **Verify Run Script** tab opens.
7. Verify your script selections, and then click **Run**.
8. On the **Results** tab, you see the results of the script including any errors.
9. Click **Close**.

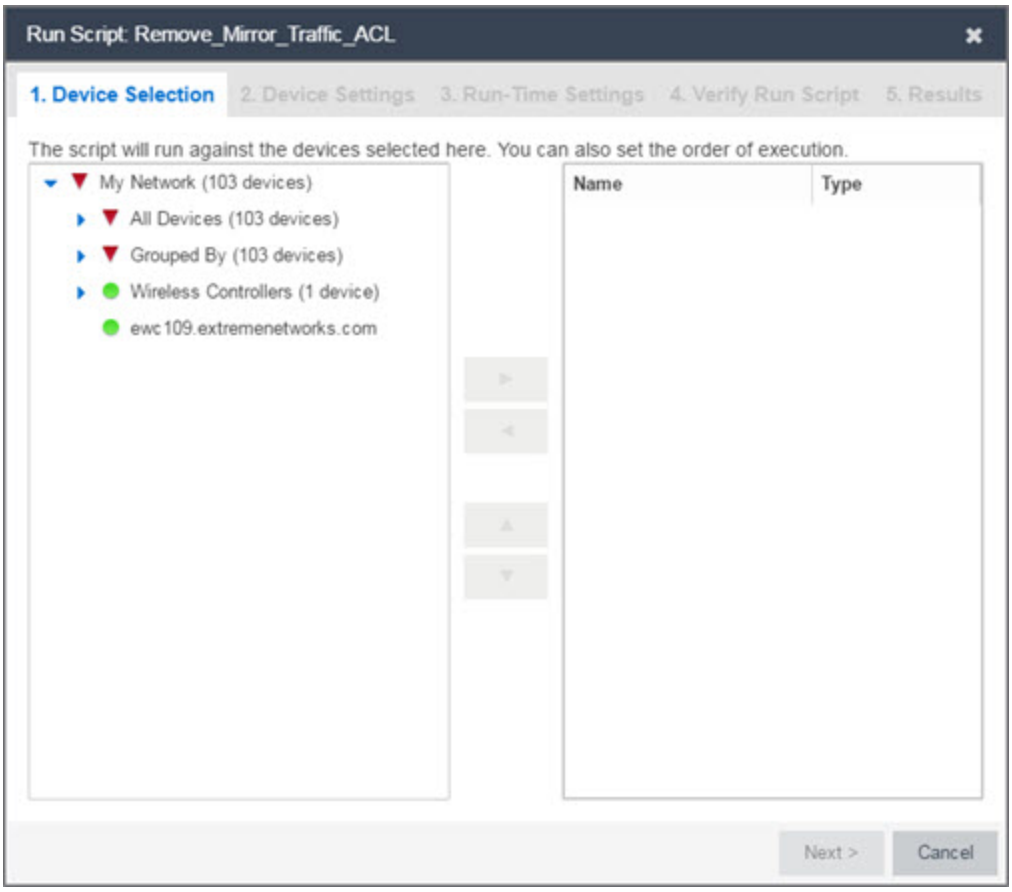
From the Tasks tab

1. Click **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 clicking its row and then click **Run**. The Run Script window opens.

NOTE: Be sure to select only 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. Click **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, click the **Description** tab to view the description defined for the script.
7. Click **Next**.
8. On the **Run-Time Settings** tab, configure the run-time 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. Click Next. On the Verify Run Script tab, verify your script selections, and then click Run.
10. On the Results tab, you see the results of the script including any errors.
11. Click Close.

View Script Results

Once 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.

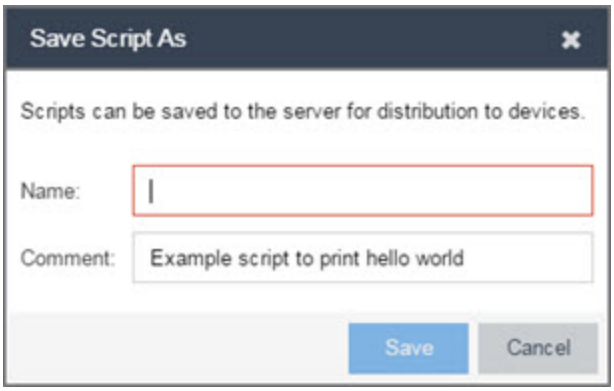
An event is stored in the console.log file in the `<install directory>/appdata/logs` folder each time a script is executed. The event in the log contains the location of the audit file. These audit logs reside in the tmp directory and remain for two weeks (per user), or until the next server restart, whichever comes first. The number of audit files written to the folder is limited to 1,000 files. Once the number of files exceeds 1,000, the oldest 100 are deleted.

Edit a Script

To edit a script:

1. In the Tasks tab, click Scripts.
2. In the scripts table, select the script you want to edit.
3. Click the Edit button. The script opens in the Edit Script window, where you can edit the script.
4. Save the script:
    a. Click the Save button to save your changes to the script.
    b. Click 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. Click **Save**.

The script is saved.

Delete a Script

To delete a script:

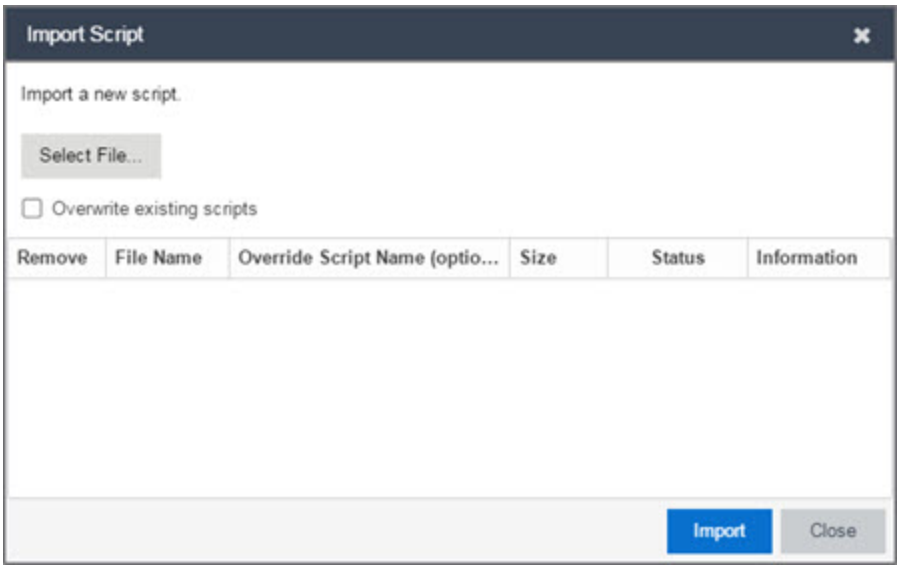
1. In the **Tasks** tab, click **Scripts**.
2. In the scripts table, select one or more scripts you want to delete.
3. Click the **Delete** button.
4. Click **Yes** to confirm the script deletion.

Import Scripts into Extreme Management Center

Import XML-formatted scripts into Extreme Management Center.

To import a script:

1. In the **Tasks** tab, click **Scripts**.
2. Click the **Import** button.



3. Click **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 edit the name of the script.
5. Click **Import**.
6. Verify the script is imported and click **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. Click 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 run-time settings, and then allows you to manually run the script task at a later time or schedule it to run in the future either once, 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 **Run-Time Settings** tab.
3. Enter a new name for the task in the **Task Name** field.

Extreme Management Center saves the script to the **Saved Tasks** tab.

Extreme Management Center Script Reference

This section contains reference information for Extreme Management Center scripts. It contains the following topics:

- Metadata Tags
- Extreme Management Center-Specific Scripting Constructs
- TCL Support in Extreme Management Center Scripts
- Entering Special Characters
- Line Continuation Character
- Case Sensitivity in Extreme Management Center Scripts
- Reserved Words in Extreme Management Center Scripts
- ExtremeXOS CLI Scripting Commands Supported in Extreme Management Center Scripts
- Extreme Management Center-Specific System Variables

An Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center 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.

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 Extreme
Management Center 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. Once 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 menu 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 ""
```

Extreme Management Center-Specific Scripting Constructs

This section describes the scripting constructs specific to Extreme Management Center:

- Specifying the Wait Time Between Commands
- Printing System Variables
- Configuring a Carriage Return Prompt Response
- Synchronizing the Device with Extreme Management Center
- 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 Extreme Management Center

The PerformSync command manually initiates a synchronization for specified Extreme Management Center 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, Extreme Management Center 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 Extreme Management Center Scripts

The following TCL commands are supported in Extreme Management Center scripts:

after	concat	for	info	lrange	puts	set	unset
append	continue	foreach	interp	lreplace	read	split	update
array	eof	format	join	lsearch	regexp	string	uplevel

binary	error	gets	lappend	lsort	regsub	subst	upvar
break	eval	global	lindex	namespace	rename	switch	variable
catch	expr	history	linsert	open	return	tell	vwait
clock	fblocked	if	list	package	scan	time	while
close	flush	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 Extreme Management Center 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 Extreme Management Center script.

Line Continuation Character

The line continuation character is not supported in Extreme Management Center scripts. Place each command statement on a single line.

Case Sensitivity in Extreme Management Center Scripts

The commands and constructs in an Extreme Management Center 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 Extreme Management Center documentation.

Example (Usage of the Extreme Management Center command ECHO)

```
echo hi (valid)

echo [echo hi] (error)

echo [ECHO hi] (valid)
```

Reserved Words in Extreme Management Center Scripts

The following words are reserved by Extreme Management Center and cannot be used as variable names in a script:

- Names of system variables (see Extreme Management Center-Specific System Variables)
- Names of Extreme Management Center command extensions (see Extreme Management Center-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 Extreme Management Center Scripts

Extreme Management Center 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 12.1 and higher support this command.
- Example — `if ($VAREXISTS(foo)) then show var foo endif`

$TCL

- Evaluates a given TCL command. The following constructs support the $TCL command:
  - `set var if`
  - while
- See TCL Support in Extreme Management Center 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 12.1 CLI scripting. Use the $TCL (string toupper <string>) command instead. Example: set var foo $TCL ("foo") .

---

show var

- Prints the current value of a specified variable.
- Switch Compatibility — Devices running ExtremeXOS 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`

Extreme Management Center-Specific System Variables

The following system variables can be set in Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center server.

$serverName
The host name of the Extreme Management Center server.

$serverPort
The port number used by the Extreme Management Center 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 Extreme Management Center server.

$vendor
Vendor name of the device; for example, Extreme.

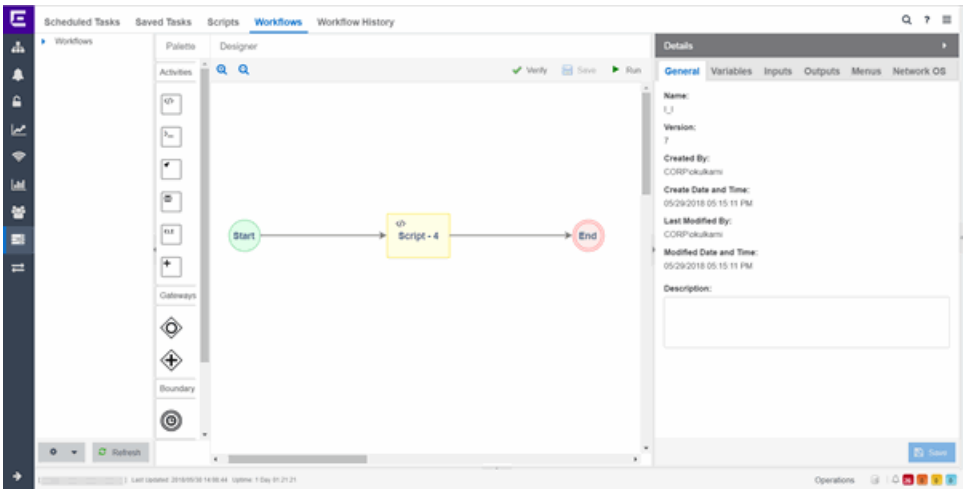
Related Information

For information on related topics:

Workflows

Workflows you create are modeled as diagrams, with each action linked in a path that a workflow execution can take. Once you create a workflow, Extreme Management Center performs a single action or a complex series of steps with a single click. You can also define a set of actions that take place if an action occurs successfully, and another set of actions that take place if that action does not occur successfully.

IMPORTANT: Workflows require special access. To access workflow functionality, contact Global Technical Assistance Center (GTAC).

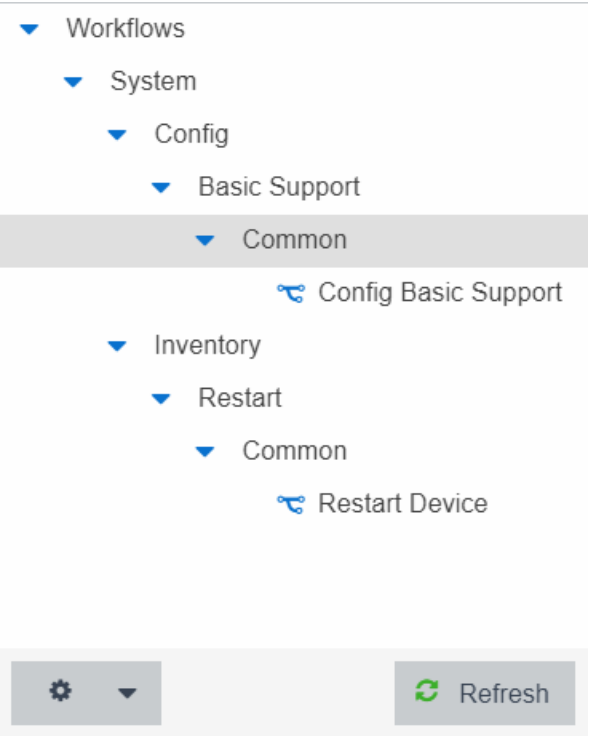


Once you create a workflow, you can configure it as a task. You can then run the workflow task on specified devices or ports, either on a one-time or recurring basis via the Saved Tasks or Scheduled Tasks tab, respectively. Additionally, you can configure a workflow to automatically begin when an alarm occurs in Extreme Management Center on the Alarm Actions tab.

The Workflows tab contains four sections:

Workflows list

The Workflows list displays the system workflows as well as workflows and workflow groups you create.



The system-defined workflows, contained in the System workflow group, provides you with sample workflows designed to perform tasks in Extreme Management Center. These workflows and workflow groups cannot be deleted or modified, but can be copied by right-clicking the workflow in the Workflows list and clicking Save As. Use the copies you create as templates to create additional workflows.

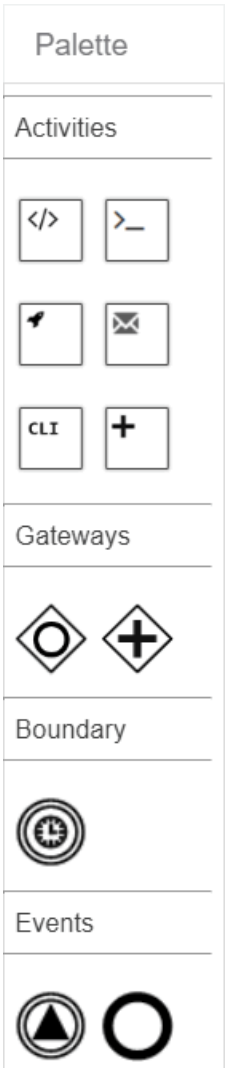
- Config Basic Support — Configures ICX and SLX devices so they are supported by Extreme Management Center.
- Restart Device — Restarts an ICX or SLX device.

Click 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.

Click 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

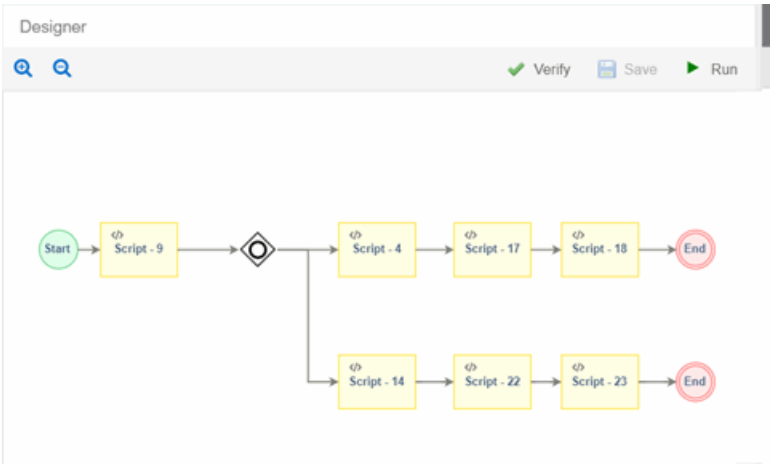
Activities	 Script Activity	Use the **Script Activity** icon to add a script to your workflow. Drag the **Script Activity** icon into the Designer at the location in the workflow where you want the script to execute. Click the script and use the **Details** section to configure the script for the workflow.
	 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. Click 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. Click 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. Click 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. Extreme Management Center 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. Click 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 variables and receive a single output from the activities in the group. Drag the icon into the Designer at the location in the workflow where you want to include the group. Drag the appropriate activites from within the Designer into the **Activity Group** box to add them to the group. Activies dragged from the Palette cannot be 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 10 seconds, then the boundary timer path is taken if the activity takes more than 10 seconds. Additionally, the workflow engine performs a check every 10 seconds, so if a timer is set to 10 seconds on an activity, then the boundary timer path may be executed between 10-20 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 clicking **Attach Boundary Timer**.

Events	 Signal	Add a **Signal** event to the workflow to either generate an event when the workflow passes that event within the workflow. Use the **Signal Type** drop-down menu 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

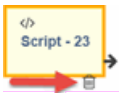
The Designer section of the tab allows you to organize the Activities, Gateways, Boundaries, and Events you select into your workflows. Drag the icons to reorder your workflow paths.



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 — Click and drag the **Arrow** icon to link the item to the next item in the workflow. If the border around the next item is green, the link is valid. If the 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.



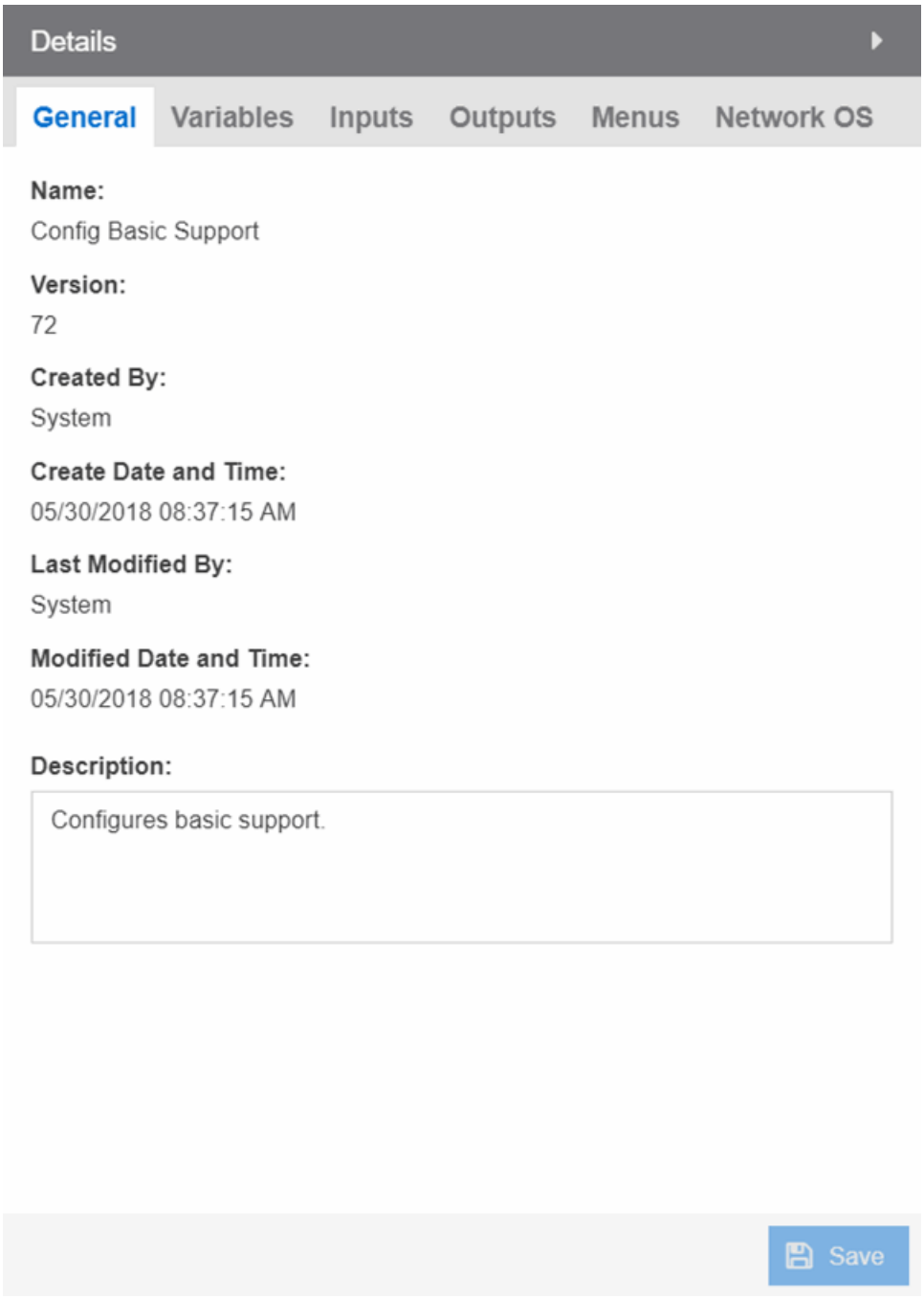
Delete — Click the **Delete** icon to remove the item from the workflow.

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.
- **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 Activities included in the workflow that are undefined or require a prompt to run. Click the **Previous** and **Next** buttons to navigate through the items you need to configure. Click the **Gear** icon ( ) to open a menu from which you can save the workflow as a task in the Saved Tasks tab. Click the **Run** button to execute the script.
  - If your workflow includes the **devices** variable, you are prompted to select the devices on which the workflow is run.
  - If your workflow includes the **ports** variable, you are prompted to select the ports on which the workflow is run.
  - If your workflow includes an Activity on which the **Prompt User** checkbox is selected on the **Inputs** tab, you are prompted to configure that Activity prior to running the workflow.

Details

Use the Details section to configure the behavior of each item in the workflow. Select the Activity, Link, Gateway, Boundary, or Event in the Designer section to display the details for that item in the Details section.



The Details section contains tabs that vary depending on what you select in the Designer section of the tab:

- General
- Condition
- Variables

- Inputs
- Outputs
- Menus
- Network OS

General

The General tab displays the basic information about what 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.

Custom Id
A user-defined alphanumeric ID for the selected item.

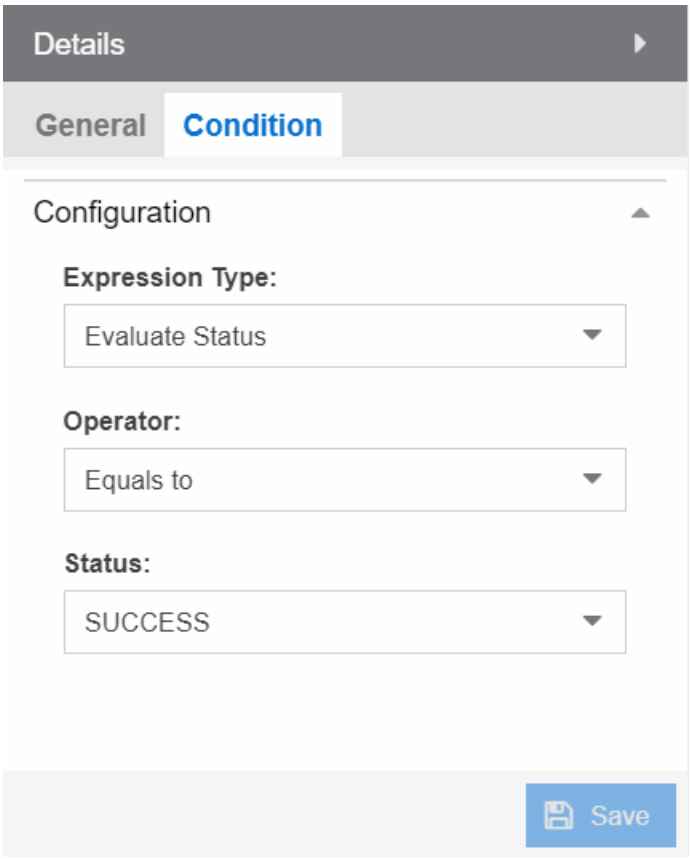
NOTE: The '-' and '_' characters are also valid.

Description
A description of the selected item.

Save
Click 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

Click 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 (e.g. SUCCESS).

Status

Status indicates the previous activity's output. Extreme Management Center compares this value using the relationship defined as the Operator against the output status of the previous activity to determine if the workflow continues after the link.

Evaluate Variables

Variable

Variable indicates the output variable Extreme Management Center 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 (e.g. Equals to).

NOTE: When Operator is In, Extreme Management Center 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", Extreme Management Center observes the variable as "abc,123" (one string), while Extreme Management Center 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 Extreme Management Center compares the Variable using the relationship defined as the Operator to determine if the workflow continues after the link.

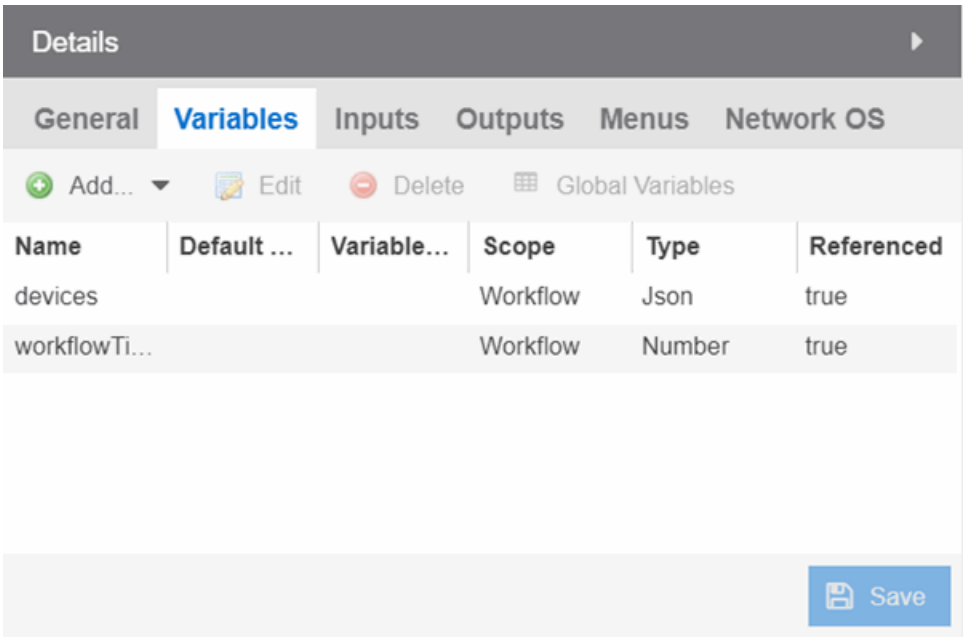
Expression

Expression

Expression indicates a custom expression Extreme Management Center 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, Extreme Management Center 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.

Extreme Management Center 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.

Name

Displays the name of the variable.

Default Value

Displays the value Extreme Management Center uses when substituting the variable. Enter a value associated with the variable type you define.

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

Click the Add icon to add a new line to the table from which you can create a new variable.

Edit

Click the Edit icon to edit an existing variable.

Delete

Click the Delete icon to remove a variable from the list.

NOTE: Variables for which Referenced is True cannot be deleted.

Global Variables

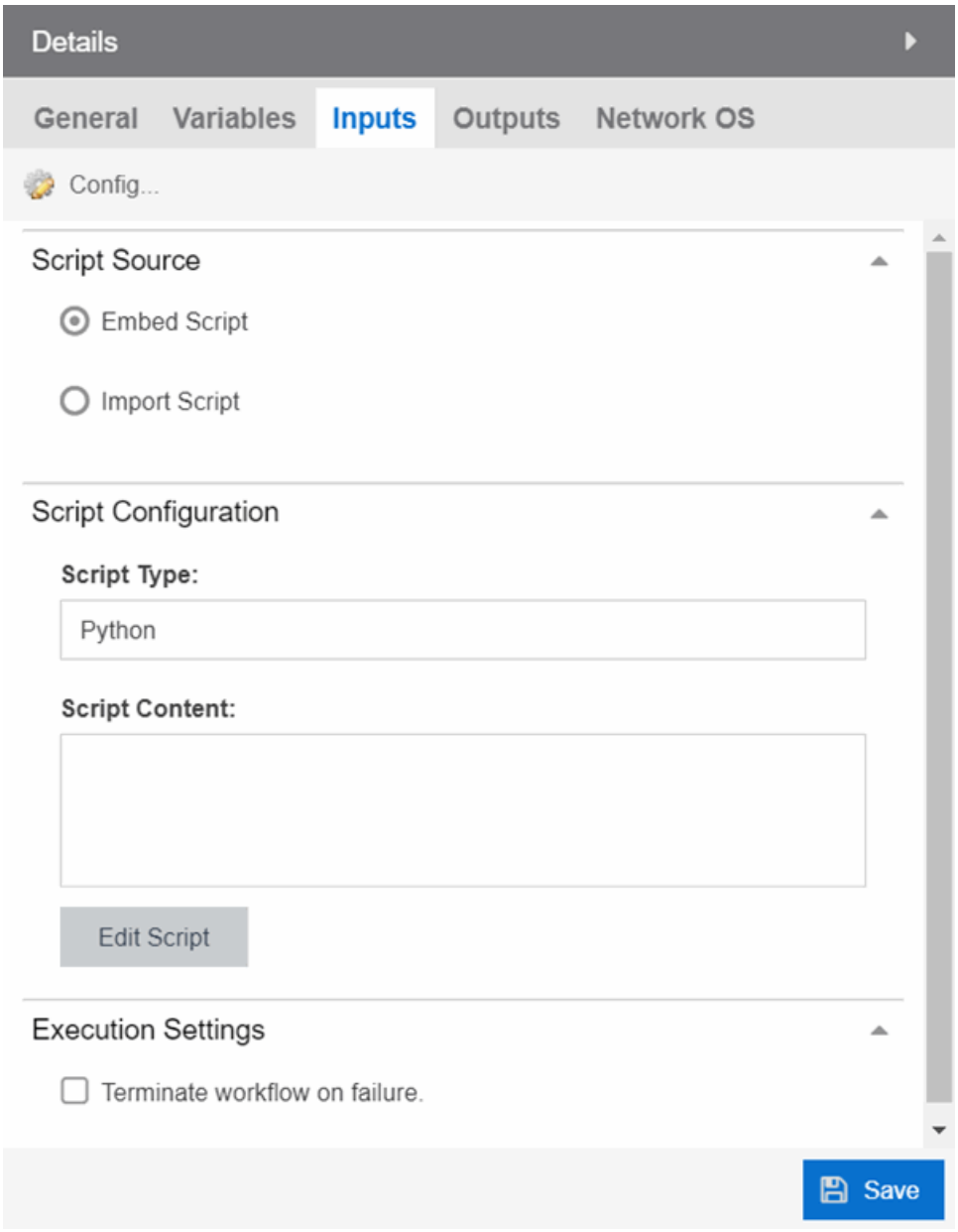
Click the button to open a new window, where you can select Global variables to include in your activity. Global variables include system-defined variables and those user-defined variables you create on the Site > Custom Variables tab.

Save

Click Save to save your changes to the workflow.

Inputs

The Inputs tab displays when you select an activity or when nothing is selected for the entire workflow.



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

Enter the appropriate input configuration for your workflow.

Timeout

Indicates the amount of time before the workflow times out.

Terminate workflow on failure

Select the checkbox to stop the workflow if the workflow does not complete the activity successfully.

Config

Click to open the Manage Inputs window to display a list of the variables the activity uses. Select a variable and click Edit to perform the following tasks:

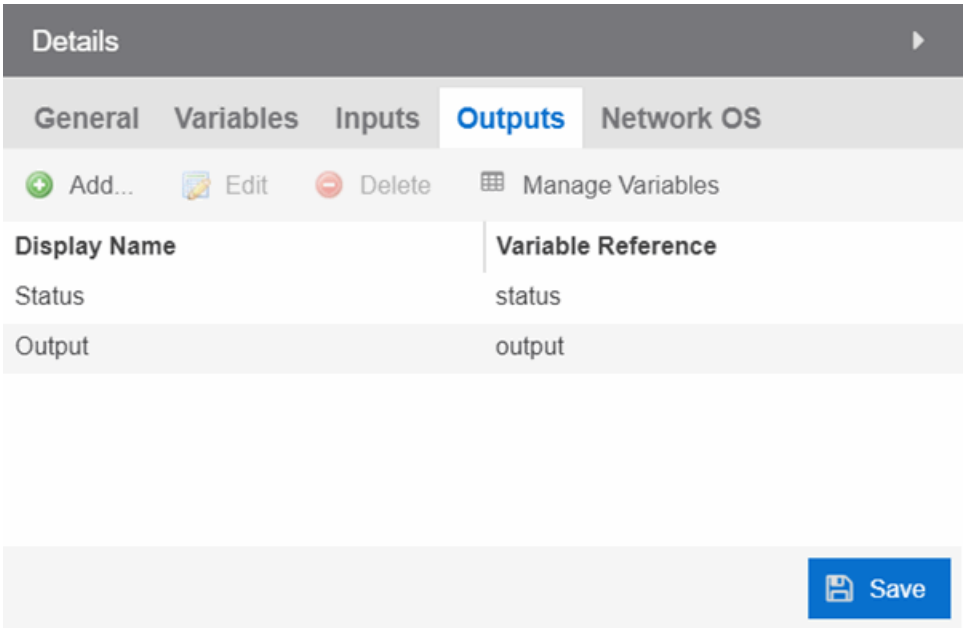
- Modify the variable on which the variable you are creating is dependent via the Variable Reference drop-down menu
- Indicate the workflow requires you to enter the variable value for the activity to complete successfully by selecting the Required checkbox
- Indicate the workflow prompts the user for a value by selecting the Prompt User checkbox

Save

Click 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.



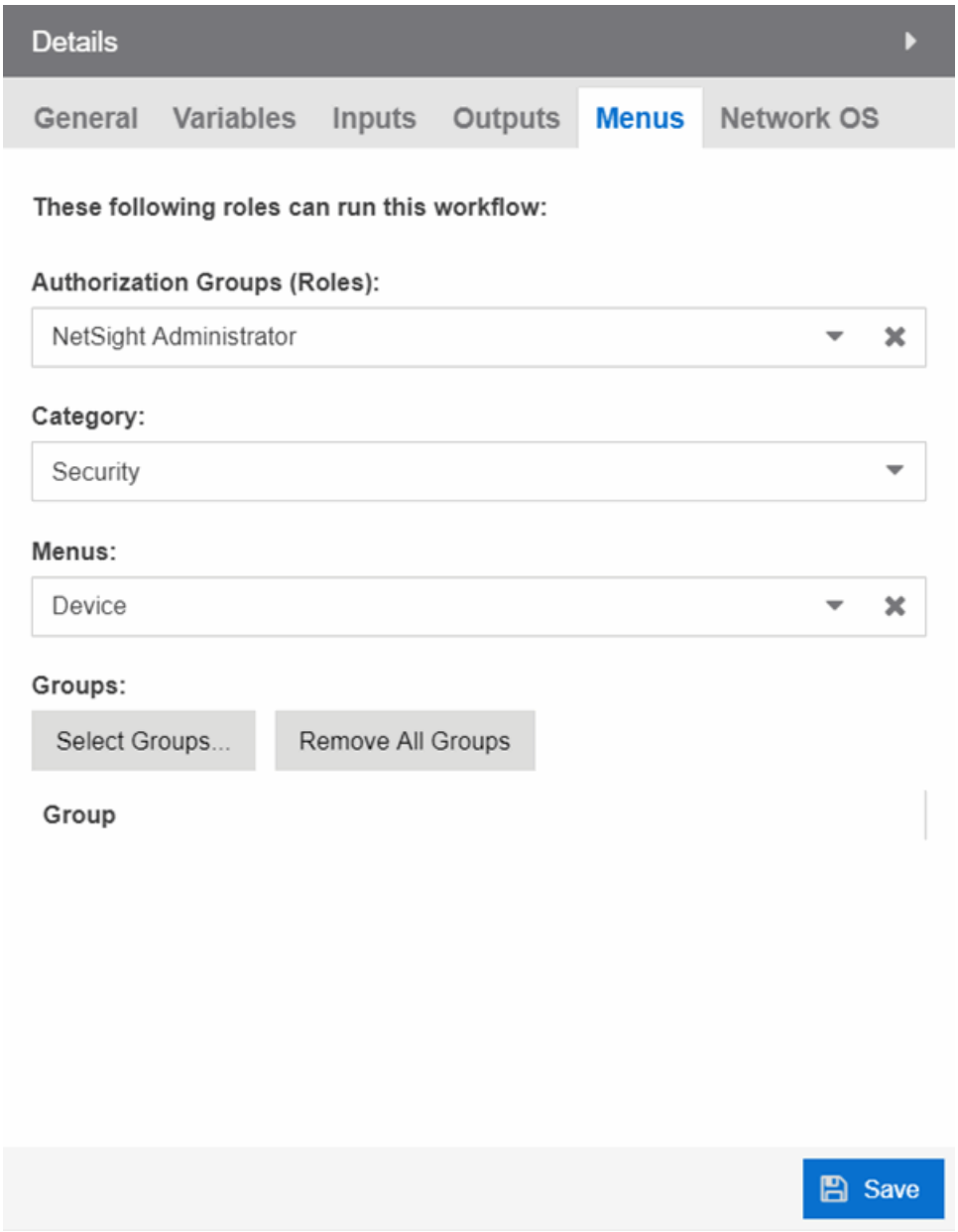
The Outputs tab allows you to specify the output variable you use to determine the result of the activity. You can then use this variable as the input variable for the next activity in the workflow, or as the final output in the workflow.

NOTE: Output variables configured via Output tab are only applicable to the Shell and HTTP activities.

Click **Save** to save your changes to the workflow.

Menus

The **Menus** tab displays for the workflow level (e.g. 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.



Authorization Group (Roles)

Select the Authorization Groups with the ability to execute the workflow from the drop-down menu.

Category

Select the **Category** group from the drop-down menu, which defines the Tasks submenu in which the workflow is grouped throughout Extreme Management Center.

Menus

Select the Tasks submenus in Extreme Management Center in which you want the workflow to display from the drop-down menu. Select **Multi-Device** for User Device Group workflows.

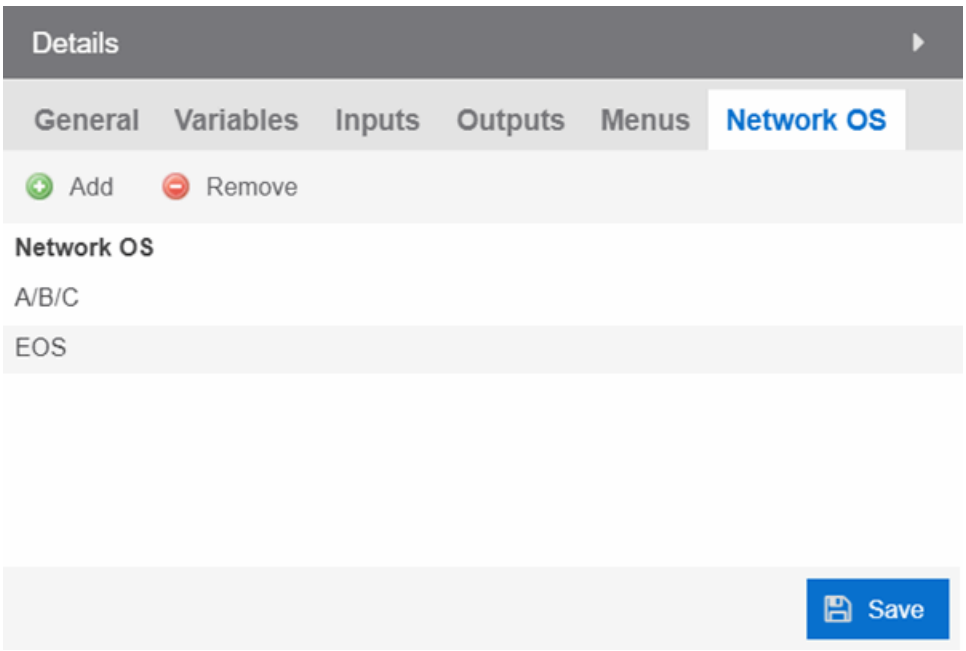
Groups

Click 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.

Click **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.



Click **Save** to save your changes to the workflow.

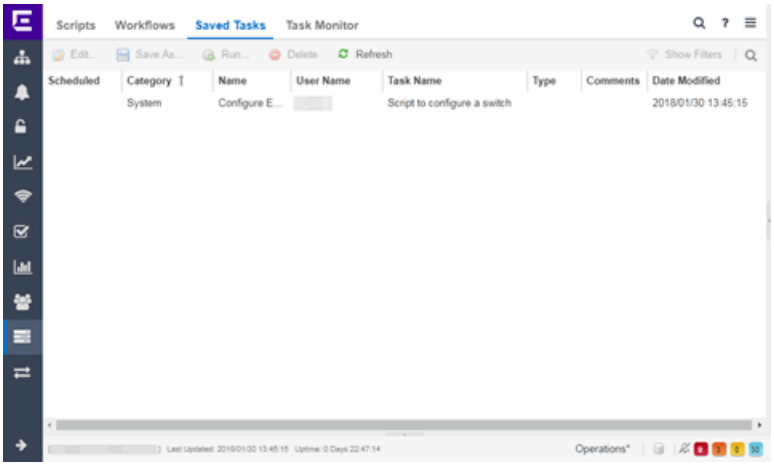
Related Information

For information on related tabs:

- How to Create Scripts in Extreme Management Center
- Saved Tasks
- Scheduled Tasks

Saved Tasks

After running a script or workflow on a device or a group of devices, you can save it as a task to run again later. The **Saved Tasks** tab displays the tasks you save for a particular set of devices.



Edit

Click **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

Click **Save As** to save the task with a new **Name**, which you can then edit.

Run

Click **Run** to run the task as configured.

Delete
Click Delete to remove the task from the Saved Tasks tab.

Refresh
Click 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 assigned to the saved task. The Name is defined when saving the script or workflow as a saved task and can not be edited.

User Name
The name of the user who saved the task.

Task Name
The name of the script or workflow running as a result of executing the task. The Task Name is defined when creating the script or workflow 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 Extreme Management Center 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 Extreme Management Center
- Workflow
- Scheduled Tasks

Extreme Connect Overview

The Extreme Management Center **Connect** tab allows you to integrate third-party software with Extreme Management Center's Extreme Access Control solution.

Additionally, the Menu icon (☰) at the top of the screen provides links to additional information about your version of Extreme Management Center.

Extreme Management Center's Extreme Access Control solution allows you to monitor end-systems and configure the appropriate experience for users accessing your network based on a variety of criteria. Network administrators may also have a variety of other tools to help monitor and control the user experience. Extreme Connect bridges the gap between these tools and allows you to control your network configurations from within Extreme Management Center.

NOTE: Extreme Connect requires an Extreme Management Center advanced license (NMS-ADV).

ExtremeXOS devices using Extreme Connect must be running version 21.1.2 or later.

Navigating the Connect Tab

The tab contains three sub-tabs:

- Configuration — Provides information about all of the end-systems and end-system groups analyzed by each of your supported network monitoring tools (called modules) and allows you to configure the end-user experience using each module.
- Domains — Allows you to search for a particular end-system in multiple versions of Extreme Management Center and returns information found using your third-party software. You can also add or remove MAC addresses from end-system groups.
- Services API — Allows you to execute a client/server application, known as a web service.

Extreme Connect Requirements

The following outlines the system requirements for Extreme Connect:

- Extreme Management Center version 7.0
- Enough switches that support multi-user authentication and policy for the number of end-user sessions on the network.

Related Information

For information on related tabs:

- Configuration
- Domains
- Services API
- Web Service Error Codes
- Dashboard
- Extreme Connect Troubleshooting

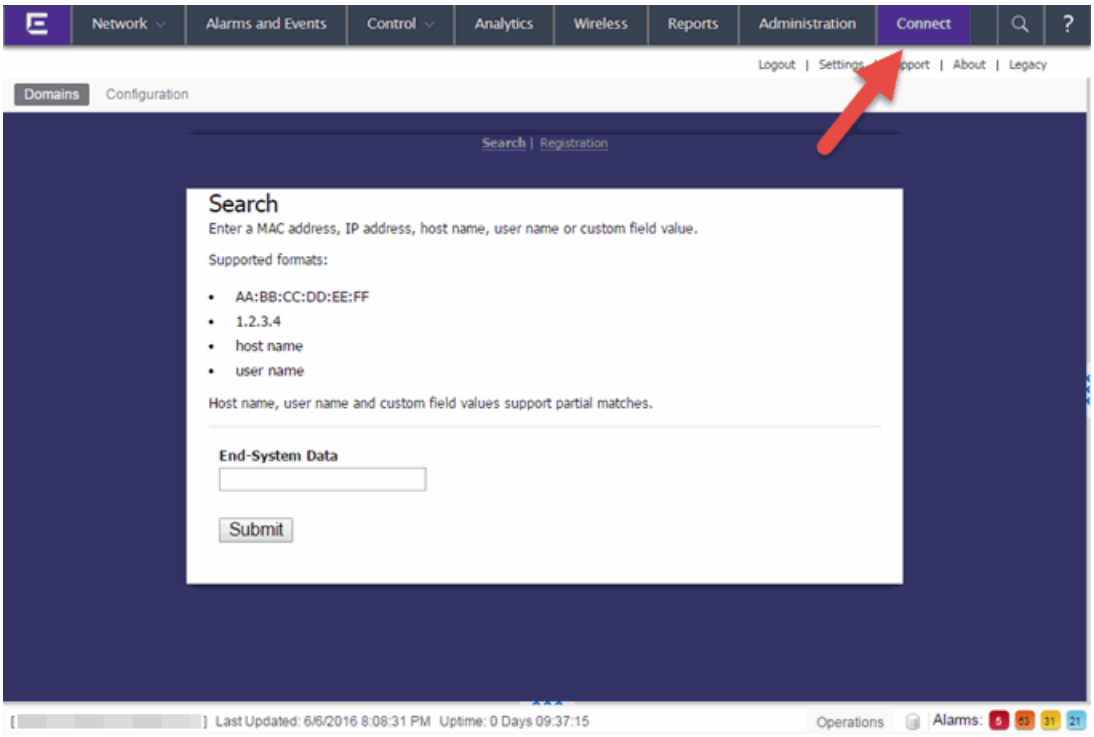
Connect Module Requirements

The Extreme Management Center Connect tab allows you to integrate third-party software with Extreme Management Center's Extreme Access Control solution.

Extreme Management Center's Extreme Access Control solution allows you to monitor end-systems and configure the appropriate experience for users accessing your network based on a variety of criteria. Network administrators may also have a variety of other tools to help monitor and control the user experience. Extreme Management Center Connect bridges the gap between these tools and allows you to control your network configurations from within Extreme Management Center.

To open the Connect tab, select Connect at the top of Extreme Management Center.

NOTE: Connect requires an Extreme Management Center advanced license (NMS-ADV).



Navigating the Connect Tab

The tab contains two tabs:

- Domains — Search for a particular end-system and return information found using your third-party software as well as add or remove MAC addresses to create end-system groups. For additional information, see Domains.
- Configuration — Provides information about all of the end-systems and end-system groups analyzed by each of your supported network monitoring tools (called modules) and allows you to configure the end user experience using each module. For additional information, see Configuration.

Additionally, the Menu at the top of the screen provides links to additional information about your version of Extreme Management Center.

Extreme Connect Requirements

The following outlines the system requirements for Extreme Connect:

- Extreme Management Center version 7.0
- Enough switches that support multi-user authentication and policy for the number of end-user sessions on the network.

For a list of the requirements for each individual module, see Module Requirements.

Related Information

For information on related tabs:

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

ExtremeConnect Configuration

The Configuration tab provides information about the end-systems and end-system groups connecting to your network.

Using third-party software (known as modules) in conjunction with the network monitoring and access control functionality found in the Extreme Management Center Extreme Access Control solution, the Configuration tab provides the most thorough information available about devices accessing your network. Additionally, the Configuration tab allows you to control end-system access to your network using each supported module's functionality.

The Configuration tab contains the following sub-tabs, each providing information about end-systems:

- Dashboard — Provides an overview of the end-systems monitored by each module and the end-systems groups accessing your network.
- End-Systems — Displays the end-systems detected for each module.
- End-System Groups — Displays the end-system groups detected for each module.

- Administration — Allows you to configure how Extreme Management Center communicates with each module and the behavior of the module within Extreme Management Center.
- Statistics — Displays various statistics about the time end-systems spent performing certain operations on the network.
- About — Provides basic information about your version of Extreme Connect, the number of modules being used by your network, and basic information detected by modules in use.

There are many different ways to configure Connect due to the different third-party softwares available.

Module Configuration

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the Extreme Management Center server.
Module log level	Verbosity of the module. Logs are stored in Extreme Management Center's server.log file.
Module enabled	Whether or not the module is enabled.
Push update to remote service	If this is set to “true”, data from other modules will be pushed to the service.
Update local data from remote service	If this is set to “true”, data from the remote service will be used to update the internal end-system table.
Pending Approval end-system group	The default end-system group name to use if an end-system is not approved yet.
Enable Data Persistence	Enabling this option will force the module to store end-system, end-system group and VLAN data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Add end-systems to end-system groups	If this is set to “true”, the MAC of the end-system will be added to an end-system group in Extreme Management Center.
Update custom fields for end-systems	If this is set to “true”, the custom field data will be update for each end-system
Update Kerberos username for end-systems	If this is set to “true”, the username will be updated for each end-system and a Kerberos reauthentication is triggered.
Update devicetype for end-systems	If this is set to “true”, the devicetype data will be update for each end-system.
Reauthorize end-system after update	If this is set to “true”, the end-system will be reauthorized after it has been added to an end-system group
Remove end-system from existing groups	If this is set to “true”, the end-system MAC will be removed from all other end-system groups, if present
Import End-system Groups	If this is set to “true”, all preconfigured MAC End-system Groups will be retrieved from Extreme Management Center. All groups with the values vlan=#NUMBER# approval=#true|false# in their description field will be automatically used by all other modules (i.e. vSphere will create portgroups for vSwitches using these values)

Verification

In order to verify whether Extreme Connect is successfully pushing data from 3rd party data sources to Extreme Management Center:

1. Open Extreme Management Center's Control > **End-Systems** tab.
2. Find an end-system updated by ExtremeConnect and navigate to the custom field – the field displays vmName=MyVirtualMachine;vmGuestFullName=Ubuntu 5…" or something similar, depending on your data sources. The information displayed here differs a bit depending on the module that reports the data to Extreme Management Center.
3. Make sure that the end-system list is actually displaying the custom field that you have chosen during installation.

NOTE: You can rename the Custom field on the Administration > Options > Access Control tab.

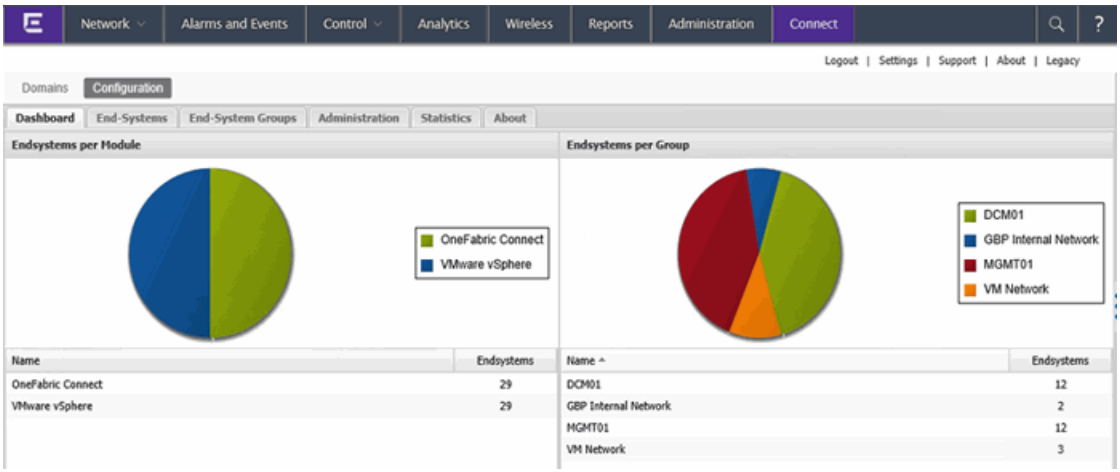
Related Information

For information on related tabs:

- Module Configuration
- Verification
- Data Center/Cloud Integration
- Extreme Management Center ExtremeConnect Security Configuration
- Extreme Management Center Connect Mobility Configuration
- Extreme Management Center ExtremeConnect Management / IT Operations Configuration
- Data Center Manager (DCM) System Configuration
- Extreme Management Center Connect Convergence Configuration
- MDM System Configuration
- Extreme Management Center Connect Assessment Configuration
- Extreme Management Center Connect Configuration Troubleshooting

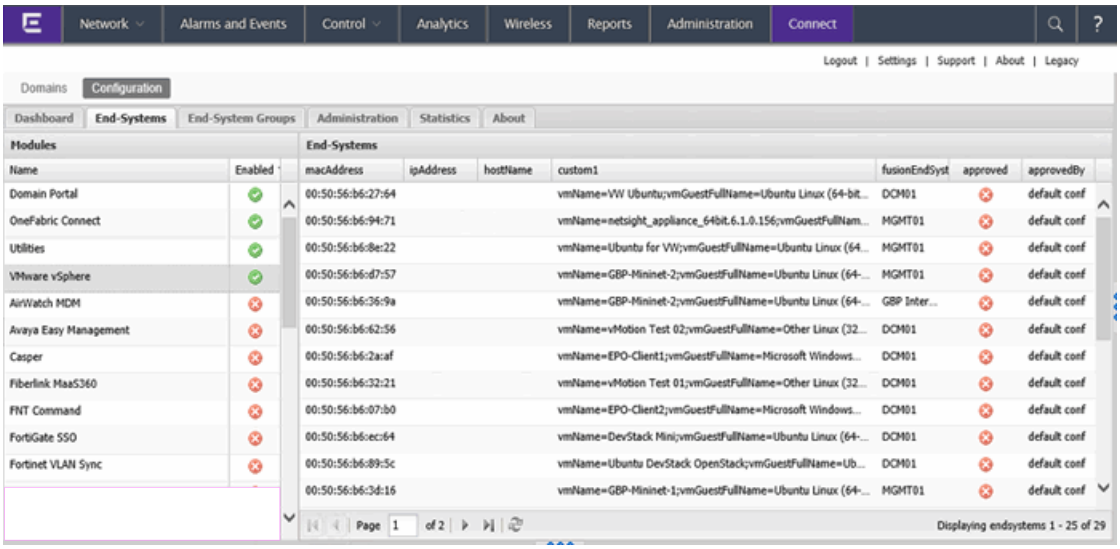
Dashboard

The **Dashboard** tab provides a top-level overview of the end-systems detected on your network. End-systems are grouped by the modules that detected them and the end-system groups to which they are assigned.



End-Systems

The **End-Systems** tab provides information about the end-systems connecting to your network.



Left Panel

The left panel of the tab shows all of the modules available in the **Connect** tab.

The **Enabled** column indicates whether the module is enabled:

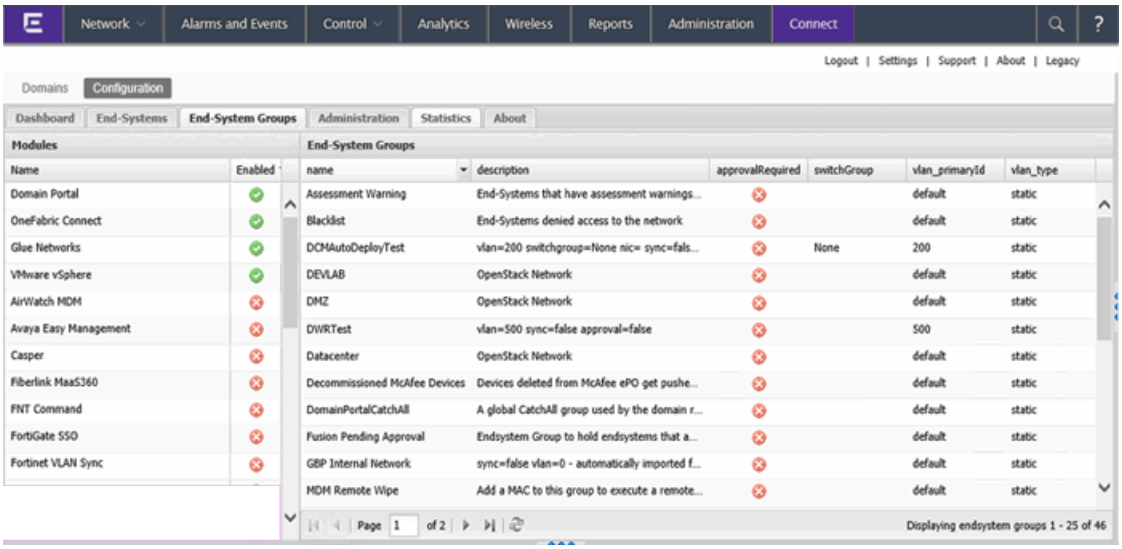
- Check icon (✓) — Module enabled on your network.
- X icon (✗) — Module not enabled on your network.

Right Panel

The right panel of the tab shows a table with information about the end-systems. Add or remove a column by clicking the down arrow at the right of a column header and selecting a checkbox associated with a column from the Columns menu.

End-System Groups

The **End-System Groups** tab provides information about the end-system groups connecting to your network.



Left Panel

The left panel of the tab shows all of the modules available in the **Connect** tab.

The **Enabled** column indicates whether the module is enabled:

- Check icon (✓) — Module enabled on your network.
- X icon (✗) — Module not enabled on your network.

Right Panel

The right panel of the tab shows a table with information about the end-system groups. Add or remove a column by clicking the down arrow at the right of a column header and selecting a checkbox associated with a column from the Columns menu.

Administration

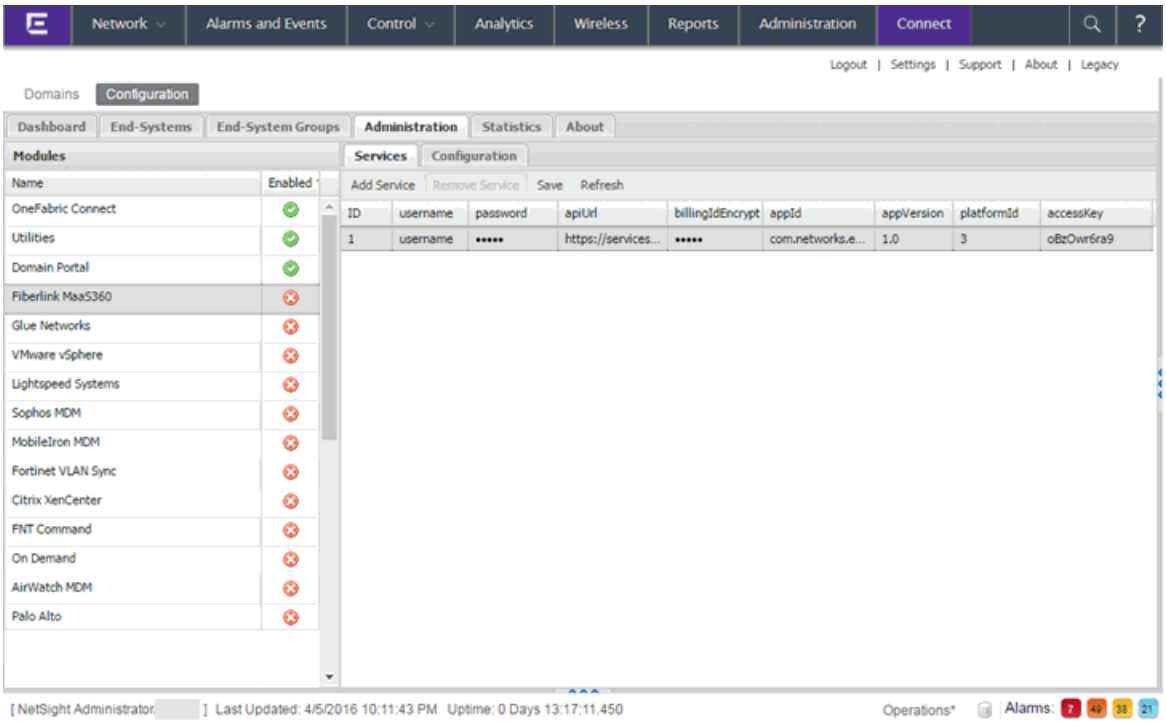
In the Administration tab, enter the information that details how Extreme Management Center connects to the module server and configure the module in Extreme Management Center.

The tab contains two sub-tabs:

- Services — A service outlines to Extreme Management Center how it connects to the server of the module you select. This includes the login credentials, IP, and port information for the module.
- Configuration — Allows you to configure how the module gathers end-system information and controls network access in Extreme Management Center and how that information is presented.

Services

Access the Services tab to specify information detailing how Extreme Management Center contacts the module's server. The Services tab allows you to specify multiple services for modules that have more than one server.



Left Panel

The left panel of the tab shows all of the modules available in the **Connect** tab.

The **Enabled** column indicates whether the module is enabled:

- Check icon (✓) — Module enabled on your network.
- X icon (✗) — Module not enabled on your network.

Right Panel

The right panel displays a table containing the services saved for the selected module. The information in this panel varies depending on the module selected in the left panel. The information below is an example using the **Fiberlink MaaS360** module.

ID
: A unique identifier for each service. This field cannot be edited.

Username
: The username used to access the module's server.

Password
: The password used to access the module's server.

apiUrl
The url that provides access to the module's server.

billingIdEncrypt
The billing account ID used for the module.

appId
The application ID used to contact the module's web service.

appVersion
The application version of the module.

platformId
The platform ID of the module.

accessKey
The key used to communicate with the module server.

Add Service
Click this button to add a new row in the Services table from which you can create a new service for the module.

Remove Service
Click this button to remove the selected row from the Services table.

Save
Click the Save button to save any changes made to services in the Services table.

Refresh
Click this button to update the table with any changes.

Configuration

The Configuration tab allows you to determine the information you want the module to gather from end-systems in Extreme Management Center as well as the module's access control behavior on the network.

Left Panel

The left panel of the tab shows all of the modules available in the Connect tab.

The Enabled column indicates whether the module is enabled:

- Check icon () — Module enabled on your network.
- X icon () — Module not enabled on your network.

Right Panel

The right panel displays two tables:

- General Configuration — Allows you to configure certain general Extreme Management Center criteria.
- Specific Configuration — Allows you to configure module-specific functionality.

Each module you select in the left panel displays different configurations, depending on the functionality available when using the module.

Name
The name of the configuration. This column cannot be edited.

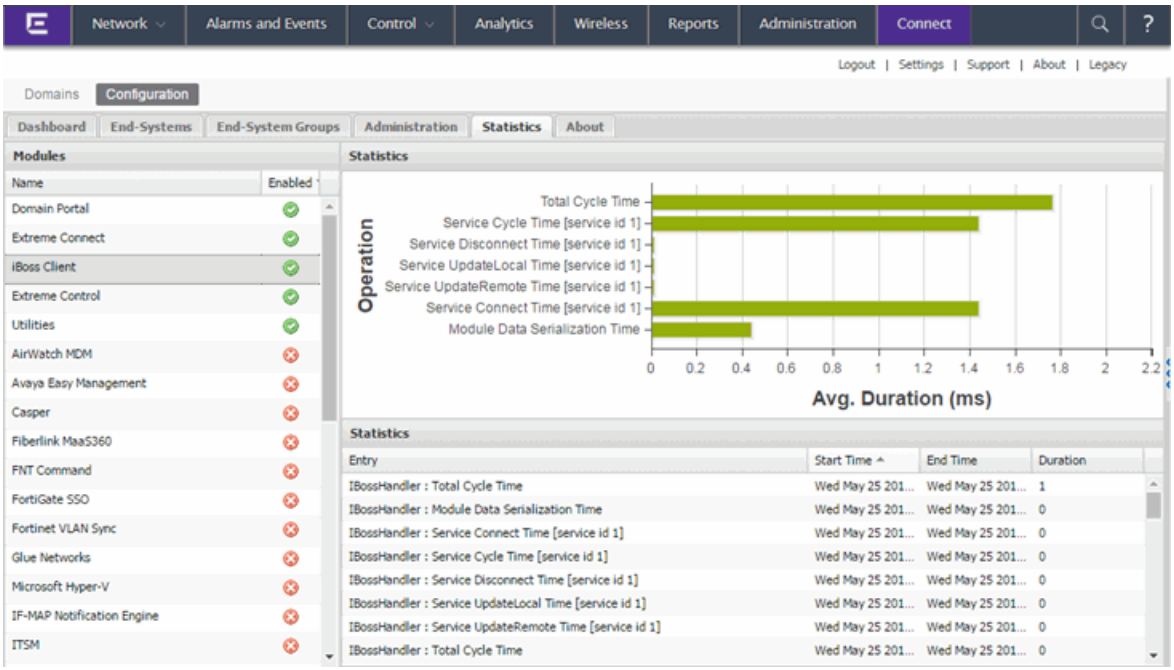
Description
A brief description of the configuration and how it affects Extreme Management Center. This column cannot be edited.

Save
Click the Save button to save your changes to any of the configurations on the tab.

Refresh
Click the Refresh button to update the Configuration tab with any changes you made.

Statistics

Select the Statistics tab to view end-system statistics for each module.



Left Panel

The left panel of the tab shows all of the modules available in the **Connect** tab.

The **Enabled** column indicates whether the module is enabled:

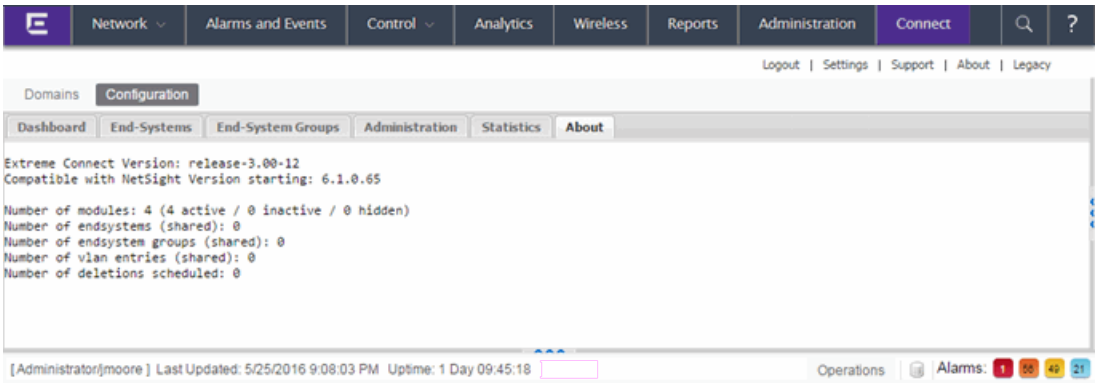
- Check icon (✓) — Module enabled on your network.
- X icon (✗) — Module not enabled on your network.

Right Panel

The right panel contains a table of the end-system statistics captured by the module and a bar graph displaying an average of the statistical entries contained in the table.

About

The **About** tab contains basic information about your version of Extreme Connect, how it is configured on your network, and information about the end-systems, end-system groups, VLANs, and scheduled deletions Extreme Connect detected on your network.



Related Information

For information on related tabs:

- Extreme Management CenterExtreme Connect Overview
- Domains

Extreme Management Center Connect Convergence Configuration

Avaya Easy Management

Polycom CMA

Microsoft Lync / Skype For Business

Analytics

Avaya Easy Management

The Avaya Easy Management integration is a one-way integration offering end-system data retrieval from Avaya on phones. This data enriches each end-system data set within Extreme Management Center and offers comprehensive reporting capabilities within OneView.

Module Configuration

Service Configuration	Description
Username	Username used to connect to the Avaya SQL Anywhere 9 DB
Password	Password used to connect to the Avaya SQL Anywhere 9 DB
Avaya DB Server IP	IP Address of the Avaya SQL Anywhere 9 DB Server
Avaya DB Server Port	TCP port of the Avaya SQL Anywhere 9 DB Server

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the Avaya DB.
Module loglevel	Verbosity of the module. Logs are stored in NetSightExtreme Control CenterExtreme Management Center's server.log file.
Module enabled	Whether or not the module is enabled.
Update local data from remote service	If this is set to true, data from the remote service will be used to update the internal end-system table.
Default end-system group	The default end-system group name to use for all phones retrieved from Avaya.
Enable Data Persistence	Enabling this option will force the module to store end-system and end-system group data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use	The custom field within NetSightExtreme Control CenterExtreme Management Center to update the information for endsystems retrieved from Avaya Easy Management (valid values: 1-4).
Format of the incoming data	Format of the data that gets stored in the custom data field. Syntax: Number: #phoneNumber#; User: #UserDefinedField1#; Hardware: #hardwareVersion#; Software: #swVersion#; Gatekeeper: #currentGatekeeperAddress#; Status: #status# Available Variables: mac, status, ipAddress, currentGatekeeperAddress, phoneNumber, swVersion, hardwareVersion, UserDefinedField1
Use global endsystem groups	This feature allows for the module to use the global endsystem groups of the OneFabric ConnectExtreme Connect.

Verification

To verify proper functioning of the Avaya Easy Management integration, validate that data on Avaya phones has been published within NAC's/OneView's custom field within the end-system list.

Polycom CMA

The Polycom CMA integration is a one-way integration offering end-system data retrieval from Polycom for managed devices. This data enriches each end-system data set within Extreme Management Center and offers comprehensive reporting capabilities within OneView.

Required configuration within the Polycom CMA Web Management: navigate to Admin → SNMP Settings and enable SNMPv3:

- Transport: UDP
- Authentication Type: SHA
- Encryption Type: AES 128 Bit

The other values can be customized to your environment. SNMP community and V3 Context Name are not evaluated.

The integration has been tested with Polycom CMA 5.5.0.ER19 but should work with older versions from 5.3.0 upwards. Both CMA 4000/5000 are supported, as well as the complete HDX and VVX 1500 line of end-points. There is no software dependency on the endpoint devices as long as they are monitored by the CMA

Module Configuration

Service Configuration	Description
Server	Polycom CMA Server IP
Password	Password used to connect to the Avaya SQL Anywhere 9 DB
SNMPv3 Security Name	SNMPv3 Security Name
SNMPv3 Auth Passphrase	SNMPv3 Auth Passphrase
SNMPv3 Privacy Passphrase	SNMPv3 Privacy Passphrase

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the Polycom CMA.
Module loglevel	Verbosity of the module. Logs are stored in NetSightExtreme Control CenterExtreme Management Center's server.log file.
Module enabled	Whether or not the module is enabled.
Update local data from remote service	If this is set to “true”, data from the remote service will be used to update the internal end-system table.
Default endsystem group	The default end-system group name to use for all managed devices retrieved from Polycom CMA.
Enable Data Persistence	Enabling this option will force the module to store end-system and end-system group data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use:	The custom field within NetSightExtreme Control CenterExtreme Management Center to update the information for endsystems retrieved from Polycom CMA (valid values: 1-4).

Service Specific Configuration	
Format of the incoming data:	Format of the data that gets stored in the custom data field. Syntax: Endpoint ID: #endPointID#, Status: #status#, Type: #type# Available Variables: endPointID, macAddress, status, type

Verification

If you configured a valid NAC end-system group to assign Polycom devices:

1. Verify that the MAC address of your Polycom end-points are now member of that end-system group in NAC.
2. Verify that for each Polycom device the end-point's device type (HDX or VVX) and the end-point's status (offline/online) has been imported.

Microsoft Lync / Skype For Business

The Microsoft Skype for Business (formerly known as Lync) integration offers dynamic call prioritizations and comprehensive reporting capabilities within OneView.

Before installing and configuring the OFConnect integration for MS Skype for Business:

1. Install the Skype for Business SDN API which can be retrieved from Microsoft: http://www.microsoft.com/en-us/download/details.aspx?id=44274
2. Make sure to point the Skype for Business SDN management service to your Extreme Management Center server (where Extreme Connect is installed).
3. Read the corresponding solution guide for further details.

Module Configuration

Service Configuration	Description
Skype for Business SDN Management Service IP	IP Address of the Skype for Business SDN management service.

General Module Configuration	
Poll interval in seconds	The time the module will wait during each run. Caution During each run (cycle) the module will perform various steps some of which are putting extra load on the Extreme Management server. It is not recommended to set this value below 600 seconds (=10 minutes). The larger the Extreme Management environment (=number of NAC end-systems, switches, access points, etc.) the higher this value should be. Setting this value too high though (for example: 7200 seconds = 2 hours) will lead to the fact that administrators won't be able to analyze call reports for up to 2 hours before those calls have ended.
Module log-level	Verbosity of the module. Logs are stored in Extreme Management's server.log file.
Module enabled	Whether or not the module is enabled.
Enable Data Persistence	Enabling this option will force the module to store end-system data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use	This field is not yet used by this integration so keep set to the default of 1.
NetSight Request Timeout	Timeout in seconds the module waits until it declares a web service call to Extreme Management as timed-out.
Time to wait for a quality update from Skype for Business	When a Skype for Business call finishes Skype for Business sometimes sends a 'QualityUpdate' shortly after the end of the call. We should be able to retrieve call quality information from this message. This timeout value defines the minimum number of seconds the module waits before it declares a call as fully ended (with or without the existence of a QualityUpdate info).
Enable audio call prioritization	Enable this to prioritize audio streams (connections/flows) for all Skype for Business calls if possible. If this is disabled, no audio streams for any Skype for Business call will be prioritized, either via XAPI or via ODL. You will still be able to access the OneView reports but no dynamic ACLs/QoS profiles will be created in the infrastructure for the audio flows. Default: true
Enable video call prioritization	Enable this to prioritize video streams (connections/flows) for all Skype for Business calls if possible. If this is disabled, no video streams for any Skype for Business call will be prioritized, either via XAPI or via ODL. You will still be able to access the OneView reports but no dynamic ACLs/QoS profiles will be created in the infrastructure for the video flows. Default: true
Enable application sharing call prioritization	Enable this to prioritize application sharing streams (connections/flows) for all Skype for Business calls if possible. If this is disabled, no application sharing streams for any Skype for Business call will be prioritized, either via XAPI or via ODL. You will still be able to access the OneView reports but no dynamic ACLs/QoS profiles will be created in the infrastructure for the application sharing flows. Default: true
QoS Profile for audio calls	The name of the QoS profile used on the XOS access switches to prioritize audio calls. This profile must be pre-configured on each access switch manually before using it.
QoS Profile for video calls	The name of the QoS profile used on the XOS access switches to prioritize video calls. This profile must be pre-configured on each access switch manually before using it.

Service Specific Configuration	
QoS Profile for application sharing calls	The name of the QoS profile used on the XOS access switches to prioritize application sharing calls. This profile must be pre-configured on each access switch manually before using it.
DSCP value for audio calls	The DSCP value to apply to audio call packets on access switches. This value can be picked up by all switches on the path between caller and callee to provide end-to-end QoS for audio calls. Default: 46
DSCP value for video calls	The DSCP value to apply to video call packets on access switches. This value can be picked up by all switches on the path between caller and callee to provide end-to-end QoS for video calls. Default: 36
DSCP value for app sharing calls	The DSCP value to apply to app sharing call packets on access switches. This value can be picked up by all switches on the path between caller and callee to provide end-to-end QoS for app sharing calls. Default: 26
Default username for web access to XOS switches	The default username to connect to XOS switches' HTTP(S) interface (xapi). This username is only used if there are no CLI credentials defined for a switch in Extreme Management. Otherwise the Extreme Management CLI username takes priority. This setting is only used if the OpenDaylight option is disabled.
Default password for web access to XOS switches	The default password to connect to XOS switches' HTTP(S) interface (xapi). This password is only used if there are no CLI credentials defined for a switch in Extreme Management. Otherwise the Extreme Management CLI password takes priority. This setting is only used if the OpenDaylight option is disabled.
Hard timeout (in minutes) for Skype for Business calls	The number of minutes after which a Skype for Business call is considered as ended even if no ended notification has been received from Skype for Business in the meantime. If the configured amount of minutes have passed between the start of a call and now this call will be considered ended ⟶ any prioritization will be removed from the infrastructure, the call data will be removed from the in-memory list and reporting data will be created for OneView reporting. This feature handles cases where for some reason the Skype for Business front-end or SDN management servers have been down or communication has been blocked and thus OneFabric Connect didn't receive the 'call ended' notifications for one or more active calls. This setting is only used if the OpenDaylight option is disabled. When using an OpenDaylight controller, the corresponding flows will timeout automatically. Default: 360 (=6 hours).
Use Skype for Business call timestamp instead of local NetSight time	The Skype for Business front-end servers typically report the call start and end timestamps in UTC time - no matter for which timezone each FE server is configured. If this option is set to 'true', these timestamps are used for OneView reporting but also to decide when to end a call (and remove its corresponding prioritizations) using the configured value for "call_hard_ timeout_in_minutes". If you enable this option you need to ensure that your Extreme Management server is also running on UTC timezone otherwise the OneView reports will be off and the hard timeout functionality for call prioritization won't work properly. It is recommended to keep this option set to 'false' -⟶ in this case, the Skype for Business timestamps will be ignored and the local Extreme Management timestamp will be used at the moment the Skype for Business notifications arrive at your Extreme Management server. Default: false.

Service Specific Configuration	
Number of days to store call reporting data	The number of days to store data on Skype for Business calls in the Derby DB. Calls that predate than the configured number of days will automatically be purged from the DB and won't appear in the OneView reports anymore. A higher value will have a negative impact on the overall performance of this module and the OneView reports. Default: 30. Purging is performed every night during the first run of the MSSkype for BusinessSDNHandler module after midnight. So if you set the interval for this module to 600 seconds purging will happen somewhere between midnight and 00:10:00 (0:10 AM).
Enable the cleanup routine for obsolete Skype for Business-related ACLs on XOS switches	Enable this to run an automated cleanup process once per night/week. It will connect to all your XOS switches via Telnet or XAPI (depending on firmware support) and try to identify obsolete Skype for Business-related dynamic ACLs. If found, it will remove those ACLs from all ports and delete the ACLs from the switch afterwards. Set the interval for this process using the next setting cleanUpObsoleteACLsOnXosSwitchesInterval. This setting is only applicable if the OpenDaylight option is disabled. When using an OpenDaylight controller, the corresponding flows will timeout automatically.
Interval for cleanup routine for obsolete Skype for Business-related ACLs on XOS switches	If the feature cleanup_obsolete_acls_from_xos_switches is enabled, use this setting here to define the interval, which will be used for the cleanup routine. Two available options: daily or weekly. The default is weekly.
Enable the clean-up routine for obsolete Skype for Business-related ACLs on EOS switches	Enable this to run an automated clean-up process once per night/week. It will connect to all your EOS switches via Telnet and try to identify obsolete Skype for Business-related policy ACLs. If found, it will delete the ACLs from the switch. Set the interval for this process using the next setting cleanUpObsoleteACLsOnEosSwitchesInterval.
Interval for clean-up routine for obsolete Skype for Business-related ACLs on EOS switches	If the feature cleanup_obsolete_acls_from_eos_switches is enabled, use this setting here to define the interval which will be used for the clean-up routine. Two available options: daily or weekly. The default is weekly.
Gateway Switches	A list of switches that are located at the edge of your network where all external Skype for Business calls pass through. If an external Skype for Business call is detected, a dynamic ACL to prioritize this call's ingressing flow will be created on all switches on this list on their ANY interface. This will enable QoS for external calls as they enter your network at those gateway switches. Ensure that these switches support the required number of dynamic ACLs for the ANY interface. If you don't want to enable this feature simply keep on empty with 127.0.0.1 in the list. If you manually modify this list make sure to keep the "id" values for all entries consistent and unique. Example entry: <gateway_switch_entry desc="Gateway Switch Entry" id="1" type="Entry"> <info>A Gateway Switch Entry</info> <value>127.0.0.1</value> </gateway_switch_entry>
Skype for Business Front-End Server IP addresses	A list of all Skype for Business front-end server IP addresses. If you want to prioritize conference calls but you cannot (or don't want to) enable any end-system tracking mechanism (RADIUS authentication, XOS IDM, OneController plugin) feature on your data center switches where your Skype for Business front-end servers are connected to, provide the list of all your FE server IPs here. When calls from or to your FE servers are seen, they will be prioritized on all gateway switches listed within the feature list "Gateway Switches". Ensure that the list of gateway switches contains all switches where your FE servers are connected. If you don't want to enable this feature simply keep a single entry with IP 127.0.0.1 and ID 1 in the list. If you manually modify this list make sure to keep the "id" values for all entries consistent and unique. This setting is only applicable if the OpenDaylight option is disabled.

Service Specific Configuration	
Use HTTPS for XAPI calls	Enable this to use HTTPS instead of HTTP for any XAPI communication with all XOS switches. If enabled, you will also need to install the SSH mod on all XOS switches and configure "enabled web https". This setting is only applicable if the OpenDaylight option is disabled. Default: false
Use OpenDaylight controller instead of XAPI for call prioritization	Enable this to use an Open Daylight controller to locate Skype for Business call end-points in the network infrastructure and prioritize audio/video calls using OpenFlow. When enabled, you will also need to configure the OpenDaylight server using various settings below. If this is disabled, it will use the Extreme Management API and XAPI on XOS switches to located end-points and prioritize calls. Default: false
IP address of the Open Daylight controller	Management IP of the Open Daylight controller. This configuration only is valid when the option use_opendaylight is set to true.
TCP/HTTP port of the Open Daylight controller	The HTTP port on which the Open Daylight REST API is provided. At the moment, only HTTP is supported. This configuration only is valid when the option use_opendaylight is set to true. Default: 8181.
Username to connect to the Open Daylight controller API	The given user should have admin rights to be able to create new flows and search for host. This configuration only is valid when the option use_ opendaylight is set to true.
Password to connect to the Open Daylight controller API	The password for the given user. This configuration only is valid when the option use_opendaylight is set to true.
Idle timeout for flows created via Open Daylight controller	The idle timeout in seconds for newly created flows. All flows created via the Open Daylight controller to prioritize Skype for Business calls will use this idle timeout setting. Set this to 0 to disable this feature. Default: 300.
Hard timeout for flows created via Open Daylight controller	The hard timeout in seconds for newly created flows. All flows created via the Open Daylight controller to prioritize Skype for Business calls will use this hard timeout setting. Set this to 0 to disable this feature. Default: 3600.
Prioritize Wifi Calls	When enabled, it is verified whether the source or destination Lync end-point are connected through an Extreme Identify wireless controller / AP. If that is the case, the corresponding call flow will be prioritized on the switchport where the corresponding Extreme Access Point is connected to. This feature is only available stating with Extreme Management 6.3 and only in Bridged@AP modes. If your wifi topology is Bridged@Controller the call flows will still be prioritized on the corresponding switch access ports but it won't have any effect as the wifi client traffic is transparently tunneled through to the controller and the ACLs/flows/policies configured on the access switch will never match any of those packets. Ensure that LLDP is enabled on both your access switches and all access points. Also ensure that you have enabled device statistics collection for OneView for all access switches where AP's are connected to. Default: true
Prioritize real-time control protocol traffic	Audio and video are typically sent using RTP, which requires two UDP ports, one for the media and one for the control protocol (RTCP). Enable this feature to also prioritize the RTCP traffic/flows. They typcially use the RTP port number reported by the Lync API plus one. So for example, if Lync reports a UDP source port of 5000 for a specific call connection the code will prioritize traffic on both ports 5000 and 5001. Default: false

Verification

In order to verify that the integration is properly assigning dynamic ACLs to prioritize Skype for Business calls in the infrastructure:

1. Start a call between two Skype for Business end-points and keep it running/active
2. Use Telnet or SSH to connect to the switches where these Skype for Business end-points are currently connected (you can use the NAC end-system list to get the switches and ports of your Skype for Business end-points easily)
3. Perform a “show config acl” to list all ACLs currently active on the switch and validate that you see at least one ACL with a name similar to the following syntax: Skype for BusinessSrcA1234567890. The first piece indicates that this ACL has been dynamically created by OFConnect to prioritize a Skype for Business call. The “Src” or “Dst” part indicates whether this ACL is used for the source or destination end-point of a call. The “A” or “V” indicates whether this ACL is used to prioritize the audio or video stream for the Skype for Business call. The rest of the name a part of the call ID retrieved from Skype for Business and thus makes this ACL name unique.
4. If you see two or even four ACL names starting with “Skype for Business…” this would indicate that both Skype for Business end-points are connected to the same switch and/or that this is an audio and video call and both streams get prioritized with unique ACLs.
5. Ensure those ACLs are bound to the correct ingress switch port.
6. In order to verify that the reporting capabilities are working as expected, login to OneView and launch the MS Skype for Business specific report found in the “Reports” tab on the left navigation pain under “VoIP →MS Skype for Business”. If this report is not visible, you might be missing the required xml reporting file.
7. Verify that you do see calls in the first tab of the report and the data seems correct.

Analytics

Reporting

Extreme Connect offers a new set of reports focused around different generalized solution sets like Data Center Management and Mobile Device Management. In addition, end-system data will be propagated in a dedicated custom field across all modules. This field will contain labels to identify

characteristics like “virtual” or “mobile” available to searches across the entire end system table in OneView.

Extreme Management Center ExtremeConnect Security Configuration

ExtremeXOS Identity Manager

The ExtremeXOS Identity Manager solution provides the network administrator with end-system visibility in Mobile IAM. This visibility will give insight on who, when, and where the user is connected to the network.

Module Configuration

Configuration Parameter	Value
Server	< IP Address(es)of Extreme NAC Appliance(s)> (semi-colon delimited)
Password	< NAC Appliance Shared Secret > (default is ETS_TAG_SHARED_SECRET)
Module Enabled	True

Extreme Management Center NAC Manager Configuration

1. Using a web browser access the Extreme Management Center launch page at the following URL: http://<Extreme Management Center Server IP>:8080
2. Click on “NAC Manager” to launch the NAV Manager application and login using an Extreme Management Center administrator credential.
3. Select the “Switches” tab and click on “Add Switch”.

4. If the ExtremeXOS switch has not previously been added as a device in the Extreme Management Center Console, click on “Add Switch”. Otherwise go to step 8.
5. In the “Add Device” window enter IP address of switch and select a SNMP profile from the drop down list, or create a new profile by selecting “New” if needed. Enter a nickname for the device (optional) then click “OK”.
6. From the device list select the switch and using the drop-down menu, select a primary NAC gateway for the switch, set “Gateway RADIUS Attributes to Send” to “Extreme Netlogin – VLAN ID” and ‘RADIUS Accounting’ to ‘Enabled”. Leave remaining configurations set to their default setting. Click “OK”.
7. Click on the “Enforce All” icon to open the “NAC Appliance Encorce” window.
8. Select the configured NAC Appliance from the list and click “Enforce”.
9. Once enforce is finished click “Close” to close the window
   Note: NAC configurations are used to manage end user connection experience and can control network access based on authentication, time and location. The following section is a basic sample configuration that will authenticate all devices and place them in the same VLAN for devices connected to the switch. Production configuration should be customized based on business needs and security requirements. Refer to Extreme Management Center NAC User’s Guide for additional information on creating custom rules.
10. Select the “Configuration” tab and click on “NAC Configuration: Default”
11. In the “NAC Configuration: Default” window click on the “Add new rule” icon
12. Enter a name for the rule, then using the pull down menu Select “MAC” for Authentication Method.
13. Using the pull down menu Select “New” to create a new location group.
14. In the “Add Location Group” window enter a Name for the location group then click on the “Add Item” icon
15. In the “Add Location Entry” window enter an entry description and select the switch using the selection button . Leave “Interface” to “Any” (all ports), then click OK.
16. Click OK to close the “Add Location Group” window, then click OK to close the “Edit Rule” window.
    Note: The newly created rule will appear in the ordered list of rules. If needed, move the rule up or down the list. Rules will be applied to an end-system based on the first rule it matches.
17. Click OK to close the “NAC Configuration” window.
18. Click on the “Enforce All” icon to open the “NAC Appliance Encorce” window.
19. Select the configured NAC Appliance from the list and click “Enforce”.

ExtremeXOS Configuration

Specific Network Login, IDM related and XML Notification Client configurations are required on the ExtremeXOS switch. Identity Management with ExtremeXOS and Extreme Management Center/NAC use only a subset of ExtremeXOS IDM features. These features including Kerberos and LLDP identity detection. ExtremeXOS FDB, IPARP, IPSecurity DHCP Snooping and Netlogin detection methods are not used.

Note: SSH module must be installed on the ExtremeXOS switch to use the XML notification feature on HTTPS. If the SSH module is not currently installed you must first download and install the separate Extreme Networks SSH software. Once the SSH module is installed, a server certificate should be created that can be used by the HTTPS server.

Refer to Secure Socket Layer section of the ExtremeXOS Concepts Guide for configuration guidelines of the HTTP server and to generate the secure certificate on the ExtremeXOS switch.

RADIUS Netlogin Configuration

1. Set the NAC appliance server as the primary RADIUS server and configure the shared-secret. Shared-secret must match shared-secret configured on the NAC appliance for this device.
    a. configure radius netlogin primary server <NAC IP> client-ip <switch IP address> vr <vr>
    b. configure radius netlogin primary shared-secret <shared secret>
2. Configure Extreme Management Center server as the primary RADIUS server and shared-secret for netlogin. Shared-secret must match shared-secret configured on Extreme Management Center for this device.
    a. configure radius-accounting netlogin primary server <NAC IP> client-ip <switch IP address> vr <vr>
    b. configure radius-accounting netlogin primary shared-secret <shared secret>
3. Enable RADIUS and RADIUS accounting on switch
    a. enable radius netlogin
    b. enable radius-accounting netlogin

Network Login (Netlogin) Configuration

1. Create authentication vlan required for netlogin and configure it the netlogin authentication vlan.
    a. create vlan nvlan
    b. configure netlogin vlan nvlan
2. Enable MAC-based netlogin on the switch and on the edge ports where users and devices will connect.
    a. enable netlogin mac
    b. enable netlogin ports <ports> mac
3. Configure the netlogin port mode for MAC-based vlan. This allows support for devices on the netlogin same port to be assigned to different vlans using MAC-based vlans.
    a. configure netlogin ports <ports> mode mac-based-vlans
4. Configure netlogin to accept and authenticate all client MAC addresses. Only MAC addresses that have a match are sent for authentication and the “default” authenticates all MAC addresses.
    a. configure netlogin add mac-list default

Identity Management Configuration

1. Enable Identity Management on switch and add edge ports where users and end system devices will connect.
    a. enable identity-management
    b. configure identiy-management add ports <ports>
2. Disable the identity-management detection methods that are not used on the edge ports where users and end system devices will connect.
    a. configure identity-management detection off fdb ports <ports>
    b. configure identity-management detection off iparp ports <ports>
    c. configure identity-management detection off ipsecurity ports <ports>
    d. configure identity-management detection off netlogin ports <ports>

LLDP Configuration

Enable LLDP on the edge ports where users and end system devices will connect.

a. enable lldp ports <ports>

XML Notification Configuration

The ExtremeXOS XML Notification feature is used to send IDM events to the Extreme Management Center server.

1. Create and configure a XML notification target.
    a. Create xml-notification target
    b. create xml-notification target Extreme Management Center url https://<Extreme Management Center IP>:8443/fusion_jboss/XosIDM vr <VR>
2. Configure credentials that XML notification will use to access the web services on Extreme Management Center. (After entering the command you will be prompted for password)
    a. configure xml-notification target Extreme Management Center user <Extreme Management Center admin username>
3. Add ExtremeXOS IDM module (idMgr) to the XML notification target in order to receive events from IDM and send them to the configured url (Extreme Management Center server web service)
    a. configure xml-notification target Extreme Management Center add idMgr
4. Enable the XML notification target.

Verification

Verify that the configuration is complete by connecting a domain client or LLDP-enabled device to the switch. The device should be identified by Extreme Management Center MAC manager and displayed End-System view in NAC managers and in Oneview.

Fortinet FortiGate

The Fortinet FortiGate integration provides a single sign-on solution and network access to end-systems by updating the FortiGate local user table and the use of RADIUS accounting.

Module Configuration

Note: FortiGate SSH username and Password must be configured if you want to create users in the FortiGate box.

For the sso-Attribute key, profile is the default value. This field must match with the value set in the FortiGate CLI

FortiGate RADIUS server name: add the value configured for RADIUS server

Configuration Option	Description
Server	FortiGate IP address
Password	FortiGate RADIUS shared secret
SSH Username	FortiGate SSH username
SSH Password	FortiGate SSH password
FortiGate RADIUS Server	FortiGate RADIUS server name, used for username local table
SSO Attribute Key	RADIUS attribute key
Add Class RADIUS Attribute	Option to add SSO attribute key to RADIUS packet
Add User to Local Table	Option to SSH to FortiGate and add username to local table

Extreme Control Configuration

1. Using a web browser access the Extreme Management Center launch page at the following URL:
   http://<Extreme Management Center Server IP>:8080
2. Using the Tools menu, select Management and Configuration → Advanced Configuration→ pull down the NAC Profiles pane.
3. Create a profile you want to match to the firewall to group users.
4. The RADIUS attribute Value references the RADIUS User Group. The group is defined by the NAC Profile.
5. Connect to the FortiGate interface.
6. Select System / Network / interfaces.
7. Select enable Listen for radius accounting messages.
8. In System / config / Features, select Enable End Point Control.
9. Go to User & Device / Authentication / RADIUS Server.
10. Create a new server and add Extreme Control server as RADIUS Server.
11. Enter the IP address and Shared Secret.
12. Check the Include in every user group box.

13. Select Single Sign-on. Add an RSSO_AGENT type RADIUS SSO.
14. Go to Authentication / Single Sign-on and create a new agent.
15. Check on the web interface that the RADIUS Server is configured correctly.
16. Configure RSSO_AGENT through the CLI.
17. For RADIUS attributes expected by the FortiGate box, default values are: (These values should be modified to accord the attribute used by FortiGate Handler)
18. In User & Device / User / User Group, create a User Group.

RADIUS Attribute Value = NAC Profile

To create a policy, go to Policy → Policy → Policy and select your parameters. Create a Policy of subtype User Identity, and add your personal filters.

iBoss Web Security

The iBoss integration provides a single sign-on solution and web content filtering capabilities based on the end system's active directory membership and network location.

Module Configuration

Configuration Options	Description
Server	IP address of the iBoss appliance
Port	iBoss web service port, default is 8015
Password	iBoss authentication key
Delimiter	Delimiter used to specify a location in the Mobile IAM rule name
Max calls	Maximum calls to iBoss appliance per second, default is 5
Max threads	Maximum active processes/calls to the iBoss appliance, default is 8
Strip username	Remove Windows or email domain from the username
Module enabled	True

This section details the steps necessary to install, configure, and test integration between Active Directory, iBoss, and Mobile IAM in a hypothetical K-12 educational environment.

The installer must have technical understanding of the Extreme Networks Mobile IAM solution and the skills required to implement a typical LDAP-integrated deployment of Mobile IAM.

Integration of iBoss and Mobile IAM is accomplished by:

1. Defining needed user groups in Active Directory
2. Defining the various locations requiring differentiated access
3. Configuration of the iBoss appliance
4. Installation and configuration of the Extreme Connect Integration services
5. Configuration of NAC

Defining Groups in Active Directory

When considering an integration project, first determine the various user populations for which you want to define access, and then place those populations into separate AD groups.

Defining Locations

Once you have determined the various end user populations and created/populated the AD groups, next determine what locations require differentiated access for each group.

Listing this location information by user group in a table is most helpful for visualization. Example of listing location by user group in the table below:

AD Group	Location
All Students	Instructional Areas
All Students	Cafeteria
All Students	Gym
All Staff	Instructional Areas
All Staff	Everywhere Else

Configuring the iBoss Appliance

There are three areas to configure on the iBoss appliance to integrate with Active Directory and Mobile IAM beyond the standard configuration needed for standard iBoss operation.

Part A – Configure LDAP Settings

1. Open a web browser and go to https://<IP address of appliance> to present the appliance logon screen. Provide the necessary credentials and click the 'Login' button.

2. Select ‘LDAP Settings’ under Network Settings to configure the Active Directory settings. The LDAP settings page is divided into three sections. The top section contains global settings for the appliance. The default settings should work fine and do not need to be edited.
3. The middle section of this page is where you define the AD domain controller iBoss will use by specifying the LDAP parameters required for communication to that domain controller. Complete this section and then click the ‘Add’ button to save the server definition.
4. Select 'Done' to save the changes and complete the LDAP configuration.

Part B – Configure AD Plugin

1. Select the ‘AD Plugin’ screen from the home page.
2. Navigate to the bottom half of the screen where it says ‘Registered AD Servers/NAC Agents’. In this screen, add a description of the Extreme Management Center server and its IP address so the iBoss server will listen to updates sent by the NAC servers.
3. The default settings can be used for Filtering Group and subnets unless told differently by support. Once these settings are saved, this section is complete.

Part C – Configure Filters

A filter group is a set of network controls that define what website content categories, programs, QoS settings, and more are allowed or not allowed to pass through the appliance for a given connection. Filter groups are applied to end system traffic on an individual basis.

1. Access the Filter Group definition pageby selecting ‘Users’ in the navigation menu on the left hand side of the page, then select the ‘Groups’ submenu link. There are five pages of definitions available for defining filter groups and each page section contains five filter group definitions, for a total of 25 available filter groups.
   Note: Filter group #1 is the default filter group and should remain unchanged.
2. Define a filter group for each AD Group/Location combination by specifying a name for each filter group using the format ADGroupName@Location. The @ symbol acts as a delimiter, so iBoss can separate the AD group name from the location name. The specified group name must be identical to the name of AD group as specified in Active Directory, and the location must be identical to the location name as defined in NAC. Spaces are allowed in both the AD group name and the name of the location.

3. Define the three AD group/location combinations for students. As there are only five filter group definitions on each page, each page of definitions must be saved separately before moving on to the next page.
4. Once you have defined the first five filters, click the 'Save' button at the bottom of the page to save changes. Navigate to the next page of filter group definitions by clicking the arrow to the left of the drop down box at the top of the page.
5. Add the remaining student group/location definition.
6. Once this definition is added be certain to click the 'Save' button at the bottom of the page to save your changes.

Configuration of NAC

The final step in configuring the integration of iBoss and Mobile IAM is to create the location definitions, set up NAC for Active Directory access via LDAP, and configure access rules for each AD group/location combination.

Recall our example table of groups and locations from Defining Locations:

AD Group	Location
All Students	Instructional Areas
All Students	Cafeteria
All Students	Gym
All Staff	Instructional Areas
All Staff	Everywhere Else

The first step is to create an LDAP user group in NAC to represent each AD group used for assigning access. Next create locations in NAC to represent the locations listed.

For this exercise we will create three NAC locations: Cafeteria, Gym, and Instructional Areas. We will not need a specific NAC location for everywhere else but instead will create a general rule to assign access for those end systems.

The name of the rule is significant and must be specified using this particular syntax. Name the rule by putting the AD group name this rule refers to on the left side of the "@" symbol, and the location this rule applies to on the right side. Since this rule applies to All Students in the Instructional Areas location, the rule name becomes "All Students@Instructional Areas".

Note: Failure to name your rules in this manner will prevent the integration from working properly.

Next, create the rule for All Students in the Cafeteria and All Students in the Gym using the same syntax.

Note: In all three cases we are assigning the same NAC profile to members of All Students.

Finally, create the two Staff access rules. The rule for All Staff in Instructional Areas follows the same format as the student rules. The final rule is different in how it is named; because there is no specific location information provided, we name the rule using just the name of the AD group itself.

Recall when we configured the filter groups in iBoss that we created a filter group with just the AD group name of All Staff. Because there is no location specified iBoss applies that filter group to any end system registered to AD accounts that are members of All Staff that are not otherwise in a defined location. Naming the rule without the @ symbol or location name tells Extreme Connect to omit the location when making the call to iBoss. Using this naming syntax allows filter groups to be assigned to end systems based solely on AD group membership.

Because this rule is more general than the previous staff access rule, it must be located below the All Staff@Instructional Areas rule in the NAC configuration in order to work correctly.

Verification

1. Using two wireless clients, connect to a test SSID and authenticate using two different accounts.
2. Ensure each account is a member of different active directory groups.
3. Configure two iBoss filtering groups that match the AD groups that each test account are part of.
4. iBoss can display information about the filter groups it assigns to end systems from its web interface. Use both NAC Manager and the iBoss management interface to confirm our integration configuration.
5. Locate both end systems so they connect from the Instructional Areas location. From the Identity and Access tab of OneView we can see that the correct rules have been applied to each end system.
6. To see the corresponding information in iBoss, open the management interface and click on ‘Users’ from the navigation menu on the left hand side of the page, then click the ‘Computers’ submenu item. Our information is listed in the ‘Detected Computers’ section of this page.

Note that both NAC and iBoss list the same end system IP address, filter set name, and AD user name for each end system. This indicates that integration is working and our configuration is correct.

Lightspeed Rocket Web Filter

The Lightspeed integration provides a single sign-on solution and web content filtering capabilities based on the end system's active directory membership.

Module Configuration

Configuration Option	Description
Server	IP address of the Rocket Web Filter appliance
Password	RADIUS Shared Secret
Module Enabled	Enables and Disables Module
RADIUS interim message interval	Send a RADIUS interim message to keep the session active, in minutes
Include Calling-Station-ID	Include the Calling-Station-ID RADIUS attribute, calling station is set to the end system's MAC adding
Include Called-Station-ID	Include the Called-Station-ID RADIUS attribute, called station is set to the switch IP address
Ignore usernames that contain	Ignore usernames that contain the entered value, multiple values can be entered with a semi-colon delimiter
Ignore NAC profiles	Ignore end system's that are assigned a NAC profile, multiple values can be entered with a semi-colon delimiter

Configuring the Rocket Appliance

In addition to the standard configuration of the Rocket Web Filter appliance, steps are required to integrate with Active Directory and Mobile IAM. Only the steps necessary for integration will be covered in this document.

Configure LDAP Settings

1. Log in to the Rocket appliance, https://<IP address of Rocket Appliance>. This presents the appliance login screen. Provide the necessary credentials and click the Login button.
2. Select the Administration menu in the top right corner of the dashboard.
3. Scroll down to the Authentication Sources to configure the Active Directory settings.
4. Select + Add Authentication Source, within this menu to add the required fields.

5. Once the Active Directory server has been saved, verify it is listed in the Authentication Sources section.
6. Select the Test button to verify the Active Directory configuration.
7. Use a known valid domain username and password, click “Test User Login.” A Success message will appear upon a successful query.

Configure RADIUS Accounting

1. The RADIUS Shared Secret is a configurable field within the Rocket appliance.
2. The Shared Secret can be found by accessing the Web Filter menu and scrolling to the bottom of the page.
3. Input the desired Shared Secret to be used between the Lightspeed Systems Rocket Web Filter appliance and the Extreme Connect Lightspeed Systems module. Note the Shared Secret value for later configuration steps.

Configure Policy Management

The next items to configure are the Rule Sets that the Rocket Web Filter appliance assigns to end-systems. Rule Sets are lists of web site categories, keywords, and actions that control how users access the Internet.

1. A pre-defined Rule Set (Block All) is assigned to an Organizational Unit (OU=Solutions Eng,DC=testing,DC=local) that is defined in the previously added Active Directory Server.
2. To access the Policy Management section of the Rocket Appliance, select Web Filter then select Policy Management from the left column.
3. Verify that the Rule Set exists in the Rule Set section of Policy Management.
4. After verifying the Rule Set exists, a new Assignment is created to assign the Rule Set to an object. Navigate to Assignments then select New Assignment.
5. In the New Assignee window, select the Type of object to be used. To browse the Authentication Source, the Search feature can be used to list all OU’s available on the server.
6. Verify the Web Filter Rule in this new assignment at the bottom of the window.

McAfee ePO

The McAfee ePO integration offers end-system assessment via ePO, automatic anti-virus signature file update via ePO and quarantining end-systems via NAC.

NOTE: The McAfee ePO module integration is not supported in Extreme Management Center 8.1.0, but will be supported in version 8.1.1.

Module Configuration

The table below describes the configuration options available for the McAfee ePO OFConnect module
(config file: McAfeeEPOHandler.xml)

Service Configuration	Description
Username	Username used to connect to the ePO API.
Password	Password used to connect to the ePO API.
Server	ePO Server IP
Port	ePO Server Port

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the adapter running on the SCVMM server.
Module loglevel	Verbosity of the module. Logs are stored in NetSightExtreme Management Control Center's server.log file.
Module enabled	Whether or not the module is enabled.
Update local data from remote service	If this is set to “true”, data from the remote service will be used to update the internal end-system table. It is recommended to set this option to “true”. You will also need to set this to “true” if you want to populate the username and device type from McAfee in NAC (see additional options below). Default: true.
Default end-system group	The default end-system group name where we assign all McAfee devices to in NAC. If you don't want end-systems from McAfee to be assigned to this default group, configure a group name which doesn't exist in NAC.
Enable Data Persistence	Enabling this option will force the module to store end-system, end-system group and VLAN data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use:	The number of the custom data field for each end-system to store the data retrieved from ePO. Available values are: 1, 2, 3 or 4. Default: 1.
Format of the incoming data:	Format of the data that gets stored in the custom data field. You can chose and combine any of the available variables: ipAddress, macAddress, osType, osServicePackVersion, nodeName, userName, datVersion, lastUpdate. But be aware that ePO might update the “lastUpdate” value for each device very regularly and OF Connect is calling Extreme Management Center’s web services to refresh that value in all end-systems custom fields. Depending on your poll interval this might put a lot of stress onto the Extreme Management Center server and it is thus recommended to _NOT_ use this variable here. It should only be used if the poll interval is very low (like once per day) and the number of end-systems isn’t too high (below 1000). Dfault: NodeName=#nodeName#; OS=#osType# (#osServicePackVersion#); User=#userName#; DAT Version=#datVersion#
End-system group for decommissioned devices:	The default end-system group for devices that existed in ePO but have been deleted. If you want to explicitly identify those devices and even authorize them differently (since they are no longer managed by ePO and that could pose a threat) you can configure the group they should automatically be moved to here and enable the corresponding feature below. Make sure you manually create this end-system group in NAC
Remove device from other groups on decommission:	Enable this to move devices which have been deleted from ePO to the NAC end-system group configured by the corresponding option above. If disabled, devices won't be automatically move to this group but rather stay with their existing group membership(s). Default: false
Delete custom data in Extreme Management Center for decommissioned devices:	If a device is deleted in ePO the end-system's custom data field in Extreme Management Center will be cleared as well. Default: false.
Overwrite the existing username with the one acquired from McAfee ePO:	If set to "true" the username for devices retrieved from ePO will overwrite the username that is already in IAM. If no username could be retrieved from ePO for a given end-system, then no change is performed in IAM. Default: false.
Overwrite the existing device type for devices with the one acquired from McAfee EPO:	If set to "true" the device type (operating system) retrieved from ePO will overwrite the device type that is already in IAM. If no operating system could be retrieved from ePO for a given end-system, then no change is performed in IAM. Default: false.
Max DAT version difference between ePO and client before triggering client update task:	Max DAT version difference between ePO and client before triggering client update task: Setting this value to 0 will disable this feature. Default: 1.
Max DAT version difference between ePO and client before generating a NetSight event	This feature can be used to create NetSight alarms based on these events. These alarms could be configured to alarm the via Email or trigger other mechanisms. Setting this value to 0 will disable this feature. Default: 4.
Max DAT version difference between ePO and client before quarantining client via NAC:	For example: If set to "7" and the difference between the DAT version on ePO's master catalog and the client's DAT version is at least 7 then the value for the corresponding assessment test result will be set to 10 and “HIGH”. You can use your IAM assessment configuration to automatically push those end-systems to a quarantine role if required. Setting this value to 0 will disable this feature. Default: 0.
Name of the ePO client task that OFConnect uses to trigger a DAT version update for individual devices:	Use the exact name as defined in ePO. Ddefine a client task in ePO that will update a client's DAT file (and maybe even more like the agent version, etc.). It will also find any client tasks where the configured name is part of. Default: Update Agent.

Service Specific Configuration	
Time before client update task is aborted by EPO	Number of minutes after which the EPO server should abort the client update task. This value is sent to the EPO server when running the "clienttask.run" web service call as an addtional parameter ("abortAfterMinutes"). Setting this value to 0 disables this feature - the parameter won't be used when making the web service call. Default: 10 minutes.
Max number of client update tasks triggered per client per day	To avoid triggering too many EPO client update tasks you can set this limit to a non-zero value. We will stop triggering EPO client update tasks after the configured maximum number of retries has been reached for the current day. As soon as the next day starts (first run after midnight), the count of retries per MAC address is automatically reset to zero and client update tasks will be triggered again as long as the device is still out of date (see dat_file_max_difference_before_trigger_update_task) or the maximum for that day has been reached again. Setting this value to 0 disables this feature →the code will trigger a client update task on each cycle as long as the device is out of date. Default: 1 update task per client per day
Max number of NetSight events generated per client per day	To avoid generating too many events you can set this limit to a non-zero value. We will stop generating NetSight events after the configured maximum number of retries has been reached for the current day. As soon as the next day starts (first run after midnight), the count of retries per MAC address is automatically reset to zero and events will be generated again as long as the device is still out of date (see dat_file_max_difference_before_generating_netsight_event) or the maximum for that day has been reached again. Setting this value to 0 disables this feature →the code will generate a event on each cycle as long as the device is out of date - no matter how may cycles/triggers per day. Default: 1 event per day
Enable Assessment:	If this is set to “true”, assessment data for all devices managed by ePO will be made available to the assessment adapter. The data will be updated on each cycle. Default: false.
Request an immediate re-assessment of an end-system if its DEVICEOUTOFDATE value changed:	If this is set to “true”, a re-assessment of each end-system where its DEVICEOUTOFDATE value changed (either from "true" to "false" or the other way round) will be requested from IAM. This will ensure that if, for example, an end-system has been pushed to Quarantine since its DAT file version was out-of-date but now it has updated the DAT version, it will immediately be re-assessed and authorized properly. If this feature is disabled, it might take hours/days for the end-system to update its NAC policy/authorization depending on the IAM assessment configuration for this end-system. This feature is only used if the assessment feature is also enabled. Default: true.
Use XAPI to trigger a reauth and thus also a re-assessment of an end-system:	If this is set to true, a re-assessment of an end-system will not be performed via a web service call but rather executed directly on the access switch of the end-system. This will be executed via XAPI so "enable web http(s)" needs to be configured on each XOS switch. This will execute the command 'clear netlogin state mac-address' with the MAC of the end-system to immediately trigger a re-auth. The re-auth then triggers a re-assessment of the end-system which should then immediately change its authorization state from ACCEPT to QUARANTINE or vise versa. This feature is only used if the reassess_endsystem feature is also enabled.
Use HTTPS for XAPI calls:	Enable this to use HTTPS instead of HTTP for any XAPI communication with all XOS switches. If enabled, you will also need to install the SSH mod on all XOS switches and configure "enabled web https". This option is only used if the reauthenticate_endsystem_using_xapi feature is also enabled.
Username to connect to any XOS switch if no CLI credentials are provided within NetSight:	If the feature reauthenticate_endsystem_using_xapi is enabled, the solution will need to authenticate on all XOS switches to perform re-authentication of end-systems. It will try to retrieve the corresponding username and password from the configured CLI credentials from Extreme Management but if there aren't any for a particular switch, then this default value will be used
Password to connect to any XOS switch if no CLI credentials are provided within NetSight:	If the feature reauthenticate_endsystem_using_xapi is enabled, the solution will need to authenticate on all XOS switches to perform re-authentication of end-systems. It will try to retrieve the corresponding username and password from the configured CLI credentials from Extreme Management but if there aren't any for a particular switch, then this default value will be used.
Name of the ePO client task that Connect uses to trigger an agent wake up:	Use the exact name as defined in ePO. Define a client task in ePO that will wake up a client's agent. This is required to Connect to wake up the agent on quarantined end-systems for which a client update task has been triggered. By default, ePO agents only report their DAT version to the ePO server once per hour. Therefore, Connect will only realize that an end-system has updated to the latest DAT Version after quite a long time and thus that end-system might be quarantined for quite a long time. Sending the latest DAT version to the ePO server through an agent wake up task will improve the behavior and get end-systems out of their quarantine state quicker

Service Specific Configuration	
Time before the agent wake up client task is triggered after a quarantine event and update task trigger:	In case an end-system was quarantined by NAC the code is triggering an ePO client update task. This task will try to update the DAT version on the end-system through the ePO agent. This process might take a few minutes. After a successful update, the ePO agent is not immediately reporting the current client DAT version back to the ePO server - it will only report this using its standard poll interval which is typically set to run once per hour. Setting this value to 0 disables this feature. Default: 0.

Verification

Any data (including assessment data) will only be updated during the configured update intervals. Any data retrieved from ePO and any action triggered in direction to Extreme Management Center are handled by the Extreme Control Handler, which has its own update interval and needs to pickup any changes/updates from ePOHandler and push it to Extreme Management Center. Depending on the number of changes/actions during one cycle and the number of end-systems managed, you will need to provide some time before you validate the data in Extreme Management Center.

Data Import to IAM

There are multiple areas to verify when data on all devices managed by ePO is imported to IAM.

The first option is to use OneView's end-system table under the "Identity and Access" tab and display the custom data field which you have configured for the McAfeeEPOHandler. If you enabled the corresponding features you should also see the username retrieved from ePO and a more detailed Device Type also retrieved from ePO.

Another option is to use the general "Search" tab and search for an end-system which is managed by ePO. It should find the end-system and display ePO data as shown below.

Assessment

If it its DAT file is running out-of-date and the corresponding assessment features are enabled, a healthy device did not update to the latest ePO DAT version and is thus running a DAT version which is older than X versions configured in the ePO handler config file. Once Extreme Connect recognizes the outdated DAT file it will populate that fact to the assessment adapter and also try to trigger the corresponding client update script on the EPO server. That update task will only be triggered for end-systems that are in ACCEPT or

QUARANTINE state to avoid trying to update end-systems that are disconnected, rejected or in error state. If IAM triggers an assessment for this end-system before the device could be updated, it will recognize that the device is out-of-date and needs to be quarantined.

At this stage, the device should have a policy (or VLAN) that doesn't allow it to harm other network devices or services but still allows the ePO server to contact and update it.

Once ePO has successfully updated the device and the next OF Connect update cycle has run, the assessment adapter will receive the updated info (from OF Connect) that the device is no longer out-of-date. OF Connect will then immediately trigger a re-assessment within IAM which will lead to re-authorizing the device into its proper policy (VLAN) since the new assessment result showed that the device is compliant and the DAT is not out-of-date anymore.

End-systems which contain the keyword "Server" in their operating system name (as retrieved from EPO) will receive a test score of 6.0 instead of 10.0 for the DEVICEOUTOFDATE test and thus won't be quarantined. This is due to the fact that most customers don't want to quarantine server systems and EPO offers a solution called MOVE which protects virtual servers without applying a DAT file to each server (→DAT version will always be 0 although these systems are protected by EPO).

Handling Deleted ePO Devices

To test this workflow remove/delete a device from ePO and wait for the next OF Connect synchronization. Then verify that:

1. The device's custom field has been emptied (if this feature has been enabled in the config file)
2. The device is now member of the IAM end-system group for decommissioned devices (if this feature has been enabled in the config file)
3. The device does not appear in the end-system list that is displayed at the bottom of the OF Connect management web site (tab: McAfee ePO). This means that the device has been deleted in the internal list as well

Palo Alto Networks

The Palo Alto integration consists of multiple solutions. The user ID solution notifies Palo Alto of IP to username mapping. The distributed IPS solutions

monitor a log file and can take action on an end-system based on the severity of the log message. It is recommended to use the Distributed IPS instead of the Palo Alto Distributed IPS moving forward.

Module Configuration

Configuration Option	Description
Username	Palo Alto username
Password	Palo Alto password
Server	Palo Alto IP address
Version	Palo Alto software version
User-ID (UID) enabled:	Enable user-ID integration
User-ID server:	User-ID agent IP address(es)
User-ID port:	User-ID agent port, default is 5006
User-ID domain:	Default username domain or NAC profile to domain mapping(s)
User-ID concurrent message:	Send concurrent User-ID messages to Palo Alto, this option should be disabled for lower end Palo Altos
User-ID vsys:	Palo Alto vsys to update, default is vsys1
User-ID multi-user message:	Send multiple User-ID mappings in 1 message. It is recommended to enable this option to lessen processing load on the Palo Alto
User-ID multi-user timer:	Time to queue User-ID mappings before sending Palo Alto User-ID message, increasing the timer will increase the number of User-ID mappings
User-ID strip email domain:	Remove email domain from the username
User-ID strip domain name:	Remove Windows domain from the username
User-ID strip domain username delimiter:	Remove all characters after the delimiter in the username
User-ID append to domain username:	Append string to username
User-ID timeout:	Palo Alto User-ID timeout
User-ID ignore usernames that contain:	Ignore usernames that contain the entered value, multiple values can be entered with a semi-colon delimiter
User-ID ignore NAC profiles:	Ignore end system's that are assigned a NAC profile, multiple values can be entered with a semi-colon delimiter
Distributed IPS (DIPS) enabled:	Enable distributed IPS integration
Distributed IPS syslog regular expression:	Regular expression match before action can be taken on an end-system
Distributed IPS syslog file	Syslog file path
Distributed IPS blacklist severity	Severity level needed to blacklist an end-system
Distributed IPS ASM server	ASM server IP address where SNMPv3 informs will be sent to
Distributed IPS ASM username	SNMPv3 username
Distributed IPS ASM password	SNMPv3 password
Distributed IPS SNMP authentication type	SNMPv3 authentication type
Distributed IPS SNMP authentication password	SNMPv3 authentication password
Distributed IPS SNMP privacy type	SNMPv3 privacy type
Distributed IPS SNMP privacy password	SNMPv3 privacy password
Module enabled:	Enable the Palo Alto solution

Distributed IPS

The distributed IPS solution monitors log files for events or opens a port on the Extreme Management server and listens for events. Once an event is received, action can be taken to add the threat to an end system group or notify Automated Security Manager (ASM) to perform a custom action.

Module Configuration

Configuration Option	Description
Name	Event name, this is the default threat name used in the end system group description
Regex	Event regular expression string
File	File, full path, to monitor for events
Port	Port number to open and listen for events on, opening a port may increase vulnerability on the ExtremeManagement server
Protocol	Port number protocol
Sender filter	Process events only from specific IP addresses to prevent spoofing, this field is used in conjunction with the port and protocol
End system group	End system group to add the threat to
End system group type	End system group type, MAC or IP
ASM Server	ASM server IP address where SNMPv3 informs will be sent to
ASM username	SNMPv3 username
ASM password	SNMPv3 password
ASM SNMP authentication type	SNMPv3 authentication type
ASM SNMP authentication password	SNMPv3 authentication password
ASM SNMP privacy type	SNMPv3 privacy type
ASM SNMP privacy password	SNMPv3 privacy password
MAC address regular expression	MAC address regular expression, it is recommended to not change this value
IP address regular expression	IP address regular expression, it is recommended to not change this value
Threat name regular expression	Threat name regular expression, the default regular expression will match a group of words surrounded by double quotes or a group of words without spaces. Example formats that will match the regular expression: “This is a threat 123” This_is_a_threat_123 This-is-a-threat-123 ThisIsAThreat123 This_is_a_Threat(123)

It is recommended to find keywords in the regular expression string and use those keywords as unique identifiers.

The event must contain either the MAC or IP address of the threat. When a MAC address based end system group is used and the threat MAC address is not in

the event, a lookup will be done to resolve the threat's IP address and vice versa for an IP based end system group.

Common wildcards that will be used are:

\w = match a character

\d = match a number

\s = match a space

. = match any character

* = match 0 or more

+ = match 1 or more

Examples of event messages and their regular expression:

Example 1. Checkpoint event message

loc=4220 filename=fw.log fileid=1402093147 time= 6Jun2014 16:01:57 action=block orig=r77 i/f_dir=outbound i/f_name=eth1 has_accounting=0 product=Anti Malware web_client_type=Chrome resource=http://sc1.checkpoint.com/za/images/threatwiki/pages/TestAntiBotBlade.html src=Winsvr2012 s_port=49600 dst=23.203.225.174 service=http proto=tcp session_id=<53924865,00000002,b17361d1,c0000001> Protection name="Check Point - Testing Bot" malware_family=Check Point Confidence Level=5 severity=2 malware_action=Communication with C&C site rule_uid={AE831485-A9C8-4681-BE8F-0E2E66904BDB} Protection Type=URL reputation malware_rule_id={27CC0EC6-7CBE-F54E-AFE0-F46162CEB057} protection_id=00233CFEE refid=0 log_id=9999 proxy_src_ip=Winsvr2012 scope=Winsvr2012 __policy_id_tag=product=VPN-1 & FireWall-1[db_tag={8119E2B3-79E5-4747-80E6-6756E42EE86D};mgmt=r77;date=1402094422;policy_name=Standard] origin_sic_name=cn=cp_mgmt,o=r77..pcfxuu Suppressed logs=1 sent_bytes=0 received_bytes=0 packet_capture_unique_id=192.168.10.189_maildir_sent_new_time1402095718.mail-4230074710-508316721.localhost packet_capture_time=1402095718 packet_capture_name=src-192.168.10.189.eml UserCheck_incident_uid=80E6C145-7AB6-D2C5-1DC5-A500F1473A70 UserCheck=1 portal_message= Your computer is trying to access a malicious server. It is probably infected by malware. For more information and remediation, please contact your help desk. Click here to report an incorrect classification. Activity: Communication with C&C site URL: http://sc1.checkpoint.com/za/images/threatwiki/pages/TestAntiBotBlade.html Reference: F1473A70 UserCheck_Confirmation_Level=Application frequency=1 days

In the above example, "Check Point - Testing Bot" is the threat name and 192.168.10.189 is the threat IP address.

Regular expression:

Protection name=$threatName malware_family.* packet_capture_name=src-$threatIpAddress

The regular expression contains unique identifiers to avoid ambiguity or incorrect matches. “Protection name=” precedes the threat name and “malware_family” follows the threat name. A wildcard (.*) is used to match against multiple characters after “malware_family.”

Simulating an event with the above message will generate the following log message in the ExtremeManagement server:

Regular expression match -> {$threatIpAddress=192.168.10.189, $threatName="Check Point - Testing Bot"}

Example 2. Watchguard event message

Jun 13 13:42:18 10.148.1.254 local1.info Jun 13 13:42:18 QA_LAB_FB 80BE052F336C0 http-proxy[1631]: msg_id="1AFF-0034" Deny 1-Trusted 0-External tcp 192.168.10.180 21.37.51.86 33444 80 msg="ProxyDrop: HTTP APT detected" proxy_act="HTTP-Client.Anti-X" host="fishherder.dyndns.org" path="/tmp/lastline-demo-sample.exe" md5="dd0af53fec2267757cd90d633acd549a" task_ uuid="235ee8f1185e4337986a0a46eb370595" threat_level="high" (HTTP-Proxy-00)

In the above example, “ProxyDrop: HTTP APT detected” is the threat name and 192.168.10.180 is the threat IP address.

Regular expression:

External tcp $threatIpAddress .* msg=$threatName proxy_act

Simulating an event with the above message will generate the following log message in the ExtremeManagement server:

Regular expression match -> {$threatIpAddress=192.168.10.180, $threatName="ProxyDrop: HTTP APT detected"}

Example 3. Palo Alto event message

Aug 25 15:51:28 PA-5060-1 -PaloAlto: -threatIpAddress 192.168.10.179 -threatName "Apache Wicket Unspecified XSS Vulnerability(36041)" –severity critical

In the above example, “Apache Wicket Unspecified XSS Vulnerability(36041)” is the threat name and 192.168.10.180 is the threat IP address.

Regular expression:

PaloAlto: -threatIpAddress $threatIpAddress -threatName $threatName

Simulating an event with the above message will generate the following log message in the ExtremeManagement server:

Regular expression match -> {$threatIpAddress=192.168.10.179, $threatName="Apache Wicket Unspecified XSS Vulnerability(36041)"}

Check Point User ID

The Check Point user ID integration updates the Check Point gateway with the username IP mapping of end systems that connect to the ExtremeControl appliance(s).

Module Configuration

Module Configuration	Description
Server	Check Point IP address
Password	Check Point shared secret
Ignore usernames that contain	Ignore usernames that contain the entered value, multiple values can be entered with a semi-colon delimiter
Ignore NAC profiles	Ignore end system's that are assigned an ExtremeControl profile, multiple values can be entered with a semi-colon delimiter
Session timeout	API user mapping timeout, in hours

Sample server log output:

```
2017-02-16 12:32:41,937 DEBUG [com.enterasys.fusion.modules.CheckPointHandler]
Sending -> https://10.224.1.252/_IA_MU_Agent/idasdk/add-identity post
{"shared-secret":"mysharedsecret","requests":[{"ip-address":"192.168.10.181","user":"doe,
john","session-timeout":3600}]}
2017-02-16 12:32:42,278 DEBUG [com.enterasys.fusion.modules.CheckPointHandler]
Response -> {
"responses" : [
{
"ipv4-address" : "192.168.10.181",
"message" : "Association sent to PDP."
}
]
}
```

Extreme Management Center Connect Mobility Configuration

AirWatch

Fiberlink MaaS360

JAMF Capser

MobileIron

Sophos Mobile Control

Citrix XenMobile

AirWatch

The AirWatch integration offers provisioning of mobile devices in the network based on device ownership and also provides assessment data within the network access control process. In addition, data within Extreme Management Center is enriched for each end-system and offers comprehensive reporting capabilities within OneView.

Module Configuration

Server Configuration	Description
Username	Username used to contact the MDM provider. Must have access rights to the respective API.
Password	Password used to contact the MDM provider.
AirWatch Server IP	IP or hostname of the MDM server.
AirWatch Webservice URL	Base URL to connect to the API of the service.
AirWatch Tenant Code	API key provided by AirWatch to access a specific customer configuration.

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the MDM provider.
Module loglevel	Verbosity of the module. Logs are stored in NetSightExtreme Management Control Center's server.log file.
Module enabled	Whether or not the server is enabled.
Push update to remote service	If this is set to true, data from other modules will be pushed to the service.
Update local data from remote service	If this is set to “true”, data from the remote service will be used to update the internal end-system table.
Default end-system group	The default end-system group name to use if an end-system is not approved yet.
Enable Data Persistence	Enabling this option will force the module to store end-system, end-systemGroup and VLAN data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use	The number of the custom data field for each end-system to store the service specific incoming data.
End-system group for Managed Business Mobile Devices	The default end-system group for corporate mobile devices.
End-system group for Managed Personal Mobile Devices	The default end-system group for personal mobile devices.
End-system group for Decommissioned Mobile Devices	The default end-system group for decommissioned mobile devices.
Enable Remote Wipe	If this option is enabled, devices will be wiped if they are moved to the MDM Remote Wipe End-system Group. • off – disabled • enterprise - always perform an enterprise wipe (only deletes corporate data) • adaptive - will perform an enterprise wipe if the device was an employee-owned device and a full wipe if it was a company device • full - always perform a full wipe regardless of ownership
Enable Quarantine Notification	If this is set to “true”, the device will be notified via the selected mode if it is quarantined
Quarantine Notification Text	Message sent in the quarantine notification to the user.
Enable Assessment	If this is set to “true”, assessment data will be made available to the assessment adapter.

Assessment Plugin Map	
Plugin Name	The Plugin ID Name.
Data Field	The AirWatch Data Field being retrieved in this test
Force Reassessment	Force Re-Assessment on content change.

Assessment Plugin Map	
Format of the incoming data	Format of the data that gets stored in the custom data field SYNTAX The end-system is currently #mdmManaged# Available Variables: • id • udid • serialnumber • imei • assetnumber • name • locationgroupid • locationgroupname • username • useremailaddress • ownership • platformid • platform • modelid • model • operatingsystem • lastseen • enrollmentstatus • compromisedstatus • compliancestatus • lastcompliancecheckon • lastcompromisedcheckon • lastenrolledon • macaddress • iscompromised • dataprotectionenabled • blocklevelencryption

Assessment Plugin Map	
	• filelevelencryption • ispasscodepresent • ispasscodecompliant
Update Kerberos username for end-systems	If this is set to "true", the username will be updated for each end-system and a Kerberos re-authentication is triggered.
Update custom fields for end-systems	If this is set to "true", the custom field data will be updated for each end-system.
Update devicetype for end-systems	If this is set to "true", the device type data will be updated for each end-system.

Variables available for custom field string are defined in the AirWatch API documentation.

Note: Look and feel of the MDM interface may change depending on customer's customizations.

Create an API User

Under AirWatch user management, all users and administrator users have access to the web services API. The process below explains how to create a generic user with Full Access:

Note: Any user with role 'API' can access the API; a new user role can be created that only grants access to the API and restricts all other access.

1. From the main Dashboard, select Menu > Accounts > Administrators.
2. From the list of users, click Add > Add User, or edit one of the existing users.
3. Select Basic next to User Type.
4. Provide the user credentials.
5. Add a role, and then click Save.
   The user and password provided in the previous screen must be provided to MDM connect in the corresponding AirWatch plugin configuration file.
6. An additional parameter to obtain for the connectivity with AirWatch´s servers is the Tenant Code. This can be obtained from AirWatch's interface in Configuration > System Settings > System > Advanced > API > REST API:
   The API key is the value that must be provided to the AirWatch module as Tenant Code

Creating a Compliance Profile

The basic variable provided by the Assessment Adaptor is the compliance status. This variable (TestID 100002) contains whether or not the mobile device with that security profile applied is compliant or not with the security requirements specified by the profile.

This variable can be taken as a global indicator of compliance with the security rules of the enterprise. Other variables can be taken into account to provide fine grained access control to the network. From NAC we may decide to use the variable PASSCODEPRESENT (TestID 100028) to verify if a device has defined a password and quarantine devices that don't have a password during the grace period allowed by the security policy.

AirWatch differentiates between Compliance Profiles and Device Profiles. Compliance Profiles define security rules that the device must comply with like:

- Installed applications
- Cellular use
- Encryption
- Version of OS
- Change of SIM

A Device Profile defines a set of configurations that the device must have in order to be considered compliant like:

- Password length
- SSID lists
- Exchange servers
- General restrictions in the device like allowing SIRI, allowing Youtube, Screen Capture, iCloud etc…
- Installed Certificates
- APNs

Some of these can be configured by the MDM itself when the profile is applied; some of them require user intervention and will probably define a grace period until they trigger a security action if the configuration hasn't been performed, e.g. the password change mentioned before.

Device and Compliance Profiles are assigned by device type, location group, ownership, etc.

Example: Define a Compliance Profile for an application.

1. Select Add > Compliance Policy.
   The wizard to create a new policy appears, select application list, the desired operation (contains) and define the name of the application (e.g., verybadapp).
2. Click Next if you have finished, or click + to add more rules to this profile.
3. The next screen will offer several remediation options, like removing or changing the device profile, notifying the user, executing a command, etc. Choose to notify the user cc'ing our systems administrator.
4. Click Next to select the device mapping.
   In the device assignment choose which devices will be checked against this profile. You can choose Platform, Manager, Ownership of the device, etc.
5. Clicking Next will take us to the summary screen.
   Now you have the chance to give a name to the compliance policy and check how many of the currently enrolled devices will pass or fail our test.
6. To enable the policy, click Finish and Activate.

Integrating AirWatch MDM in Mobile IAM's Workflow

Every time a new user is created in AirWatch MDM, the user receives an email or SMS with instructions to register his device

By following the link in the email, the user will be presented with AirWatch's login screen and the possibility to register his or her device in the MDM system.

To integrate this workflow into Extreme Networks Mobile IAM registration workflow, enable registration in Extreme Networks Mobile IAM and link to AirWatch MDM registration page from Mobile IAM captive portal.

Once registration is enabled in Mobile IAM, the administrator can manage the different messages that the user receives during the registration process.

1. Enable web registration in NAC configuration and go to the Portal Options.

2. Select Common Page Settings > change link next to Message Strings.

3. Look for the string 'RegistertoObtainAccess'.

To obtain network access, you must complete the Self Registration form.

We will change that string to contain a string similar to:

```
<h3>BYOD Self-Registration</h3>You can also register your personal device, taping here:
<form action="https://apidev-ds.awmdm.com/DeviceManagement/Enrollment"
method="GET">
<p></p>
GroupID
<select name="AC">
<option value="SE101">SE101</option>
</select>
<p></p>
<input type="submit" name="submit "value="Register your mobile device"></form>
<p></p>
```

This code will create a button that will connect to AirWatch registration page. Make sure that the url (https://apidev-ds.awmdm.com/DeviceManagement/Enrollment) is the same url being used in your deployment.

This code creates a selection for the user to select the location groups he's been assigned in case that there are several to choose.

In the example above, the option is SE101. If there is only one location group in your deployment, you can hide this content with the following code:

```
<h3>BYOD Self-Registration</h3>You can also register your personal device, taping here:
<form action="https://apidev-ds.awmdm.com/DeviceManagement/Enrollment"
method="GET">
<p></p>
<input type=”hidden” name="AC" value="SE101">
<p></p>
<input type="submit" name="submit "value="Register your mobile device"></form>
<p></p>
```

The new look of the mobile registration page is changed to reflect this new code.

In this situation, the user can provide their data in the standard Mobile IAM registration form and register as a guest to the network without control of the MDM. Or they can register the mobile device tapping in the new button and being redirected to AirWatch registration page.

4. When the device has been successfully registered with AirWatch, the Extreme Connect MDM plugin will import its data into Mobile IAM. Devices classified in MDM as Corporate owned will be place in the end-system group 'Mobile Devices Business'

and the devices classified as Personal will be added to the group 'Mobile Devices Personal' (or the group defined to that end during installation or the plugin configuration, see above in installation and post installation tasks).

5. The Mobile IAM ruleset must be adapted to reflect those groups and act accordingly depending on the newly registered devices.

Note: Devices registered by an MDM system may have an important lag until they are added to the corresponding groups. This behavior is not a malfunction of the MDM itself or the Extreme Connect MDM plugin. Due to the diversity of OSes and connectivity profiles, there is no way to know in advance when a newly registered device will provide all the data needed by the MDM software to complete the registration. It may take up to several minutes from the registration to the final landing in one of the above-mentioned groups and obtaining full access to the network.

Policy Configuration

To support the previous workflow, the device in unregistered state must be able to communicate via HTTPS with AirWatch servers and via the apple push service with Apple. Android devices require downloading an agent to be registered by AirWatch so Google Play access must be provided as well in this state.

The following policies (or more generic ones) are needed to allow Airwatch registration:

- Allow HTTPS to 12.150.127.0/24 AirWatch network
- Allow TCP 5223 to 17.0.0.0/8:TCP:5223, Apple Push service
- Allow HTTPS to 74.125.0.0/16, Google Play Downloads
- Allow TCP/UDP 5228 to 173.194.0.0/16, Google Play login

Fiberlink MaaS360

The Fiberlink MaaS360 integration requires Fiberlink authentication credentials and other account settings. This information is used in the Fiberlink MaaS360 module tab.

Module Configuration

Configuration Option	Description
Username	MaaS360 web service username
Password	MaaS360 web service password
API URL	MaaS360 web service URL, use https://services.fiberlink.com unless told otherwise by Fiberlink
Billing/Account ID	MaaS360 billing/account ID

Configuration Option	Description
Application ID	Application ID used to contact MaaS360 web service, use com.networks.extreme unless told otherwise
Application Version	Use 1.0 unless told otherwise
Platform ID	Use 3 unless told otherwise
Access Key	Do not edit this value unless told otherwise
Server	Set value to localhost

Account Billing ID: the account billing ID is used to identify the Fiberlink MaaS360 account. To find the account billing ID, log into the Fiberlink MaaS360 management page.

Service Configuration

Configuration Option	Description
Poll interval	Time period between queries to the MaaS360 web service
End system group for managed business mobile devices	Mobile IAM end-system group that corporate owned devices will be part of
End system group for managed personal mobile devices	Mobile IAM end system group that personal owned devices will be part of
Default end system group for managed mobile devices	Mobile IAM end-system group that unknown devices will be part of
Remote wipe end system group	Mobile IAM end-system group that will be used to remotely wipe a mobile device
Enable remote wipe	Enable/disable remote wipe option
Update Kerberos username	Enable/disable option to update end-system username
Update device type	Enable/disable option to update end-system device type
Notify user when quarantined	Enable/disable option to notify user when end-system is quarantined based on assessment scoring
Enable assessment	Enable/disable option to use Mobile IAM assessment agent

Verification

1. Enroll new device with MaaS360.
2. Verify device is now being managed by MaaS360.
3. Connect to test SSID, wait for re-synchronization poll to occur, and verify end system in Mobile IAM has device information from MaaS360.

Policy Configuration

To support the previous workflow, the device in unregistered state must be able to communicate via HTTPS with MaaS360 servers and via the Apple push service with Apple.

Some configurations require downloading an agent to be registered by MaaS360 so Google Play and Apple appStore access must be provided as well

in this state. If this is the case, policies must be adapted to provide connectivity to the Agent.

The following policies (or more generic ones) are needed to allow MaaS360 registration:

- •Allow HTTPS to MaaS360 network
- •Allow TCP 5223 to 17.0.0.0/8:TCP:5223, Apple Push service
- •Allow TCP/UDP 5228 to 173.194.0.0/16, Google Play login
- •Allow HTTPS to 74.125.0.0/16, Google Play Downloads

JAMF Capser

The JAMF Casper integration offers provisioning of mobile devices in the network based on Casper group membership and also provides assessment data within the network access control process. In addition, data within Extreme Management Center is enriched for each end-system and offers comprehensive reporting capabilities within OneView.

Module Configuration

Service Configuration	Description
Username	Username used to contact the MDM provider. Must have access rights to the respective API.
Password	Password used to contact the MDM provider.
Server IP	IP or hostname of the MDM server.

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the MDM provider.
Module loglevel	Verbosity of the module. Logs are stored in NetSightExtreme Management Control Center's server.log file.
Module enabled	Whether or not the server is enabled.

Service Specific Configuration	
Custom field to use	The number of the custom data field for each end-system to store the service specific incoming data.
Full Re-Sync Interval	The time after which a full data re-sync will be performed. This will also update data on devices, which are already synchronized.

Service Specific Configuration	
Format of the incoming data for iPhones	Format of the data that gets stored in the custom data field SYNTAX EXAMPLE: OS Version=#osVersion#; Last Inv. Update=#lastInventoryUpdate#; Is Managed=#isManaged#; User=#userName#; Real Name=#realName#; Email=#email# Available Variables: ipAddress, mac, osVersion, lastInventoryUpdate, isManaged, modelDisplay, userName, realName, email, isSecurityDataProtection, isSecurityBlockLevelEncryptionCapable, isSecurityFileLevelEncryptionCapable, isSecurityPasscodePresent, isSecurityPasscodeCompliant, isSecurityPasscodeCompliantWithProfile
Format of the incoming data for computers	Format of the data that gets stored in the custom data field SYNTAX EXAMPLE: OS=#osName# (#osVersion#); User=#userName#; Real Name=#realName#; Email=#email#; Phone=#phone# Available Variables: macAddress, alternateMacAddress, osName, osVersion, ipAddress, userName, realName, email, phone
Default end-system group for all iPhones	The default end-system group name to use if it is not set dynamically for all iPhones.
Default end-system group for all computers	The default end-system group name to use if it is not set dynamically for all computers.
End-system group for decommissioned devices	The default end-system group for decommissioned devices.
Overwrite the existing username for iPhones/iPads with the one acquired from CASPER	If set to "true" the username for iPhones/iPads retrieved from CASPER will overwrite the username that is already in NAC. If no username could be retrieved from CASPER for a given end-system, then no change is performed in NAC. Be aware that this might conflict with existing NAC processes if you are already retrieving and using the username through some other mechanism like 802.1X or Kerberos snooping --> this will be overwritten.
Overwrite the existing username for MACs with the one acquired from CASPER	If set to "true" the username for MACs retrieved from CASPER will overwrite the username that is already in NAC. If no username could be retrieved from CASPER for a given end-system, then no change is performed in NAC. Be aware that this might conflict with existing NAC processes if you are already retrieving and using the username through some other mechanism like 802.1X or Kerberos snooping --> this will be overwritten.
Overwrite the existing device type for iPhones/iPads with the one acquired from CASPER	If set to "true" the device type (iOS) retrieved from CASPER for iPhones/iPads will overwrite the device type which is already in NAC. If no operating system could be retrieved from CASPER for a given end-system, then no change is performed in NAC. Be aware that this might conflict with existing NAC processes if you are already retrieving and using the device type through some other mechanism like DHCP snooping --> this will be overwritten. This feature should improve your current method for end-systems managed by CASPER.
Overwrite the existing device type for MACs with the one acquired from CASPER	If set to "true" the device type (iOS) retrieved from CASPER for Macs will overwrite the device type that is already in NAC. If no operating system could be retrieved from CASPER for a given end-system, then no change is performed in NAC. Be aware that this might conflict with existing NAC processes if you are already retrieving and using the device type through some other mechanism like DHCP snooping --> this will be overwritten. This feature should improve your current method for end-systems managed by CASPER.

Service Specific Configuration	
Overwrite the existing device type for Advanced Search computers with the one acquired from CASPER	If set to "true" the device type (operating system) retrieved from CASPER for Advanced Search computers will overwrite the device type which is already in NAC. If no operating system could be retrieved from CASPER for a given end-system, then no change is performed in NAC. Be aware that this might mess up existing NAC processes if you are already retrieving and using the device type through some other mechanism like DHCP snooping --> this will be overwritten. This feature should improve your current method for end-systems managed by CASPER.
Import data on iPhones and iPads from CASPER	If set to "true" the module will retrieve data on all iPhones and iPads managed by Casper and push it into NAC. You must set this option to “true” if you want the MDM assessment adapter to work since this data is delivered to the assessment adapter via a file.
Import data on computers (MACs) from CASPER	If set to "true" the module will retrieve data on all MACs managed by Casper and push it into NAC.
Max number of days that the last inventory update for iPhones is allowed to be old	For example: If set to "5" the module will alarm (if assessment is enabled) if an iPhone's last inventory update is older than 5 days.
Write assessment relevant data to an external file or not	If this is set to “true”, assessment data for iPads/iPhones will be made available to the assessment adapter

Assessment Map Entry #	
Plugin Name	The Plugin ID Name
Data Field	The MDM Data Field being retrieved in this test.
Force Reassessment	Force Re-Assessment on content change.

Verification

To verify proper functionality validate the data within the custom field configured to use for the Casper integration in your end-system list (in NAC Manager or OneView). For each iPhone, iPad or MAC you should see information which is retrieved from Casper: If you have enabled the feature to automatically assign Casper devices (iPhones/iPads/MACs) to end-system groups in NAC based on the group name in Casper matching the end-system group name in NAC you can simply verify this functionality by opening one of the groups in OneView and validate whether the correct end-systems (=MAC addresses) are listed there.

As the Casper integration is a one-way integration there is nothing to verify on the Casper server since this integration is neither pushing data to Casper nor modifying any configuration there.

MobileIron

The MobileIron integration offers provisioning of mobile devices in the network based on device ownership and also provides assessment data within the

network access control process. In addition, data within Extreme Management Center is enriched for each end-system and offers comprehensive reporting capabilities within OneView.

Module Configuration

Service Configuration	Description
Username	Username used to contact the MDM provider. Must have access rights to the respective API.
Password	Password used to contact the MDM provider.
MobileIron Server IP	IP or hostname of the MDM server.
MobileIron Webservice URL	Base URL to connect to the API of the service.

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the MDM provider.
Module loglevel	Verbosity of the module. Logs are stored in NetSightExtreme Management Control Center's server.log file.
Module enabled	Whether or not the server is enabled.
Push update to remote service	If this is set to "true", data from other modules will be pushed to the service.
Update local data from remote service	If this is set to "true", data from the remote service will be used to update the internal end-system table.
Default end-system group	The default end-system group name to use if an end-system is not approved yet.
Enable Data Persistence	Enabling this option will force the module to store end-system, end-systemGroup and VLAN data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use	The number of the custom data field for each end-system to store the service specific incoming data.
End-system group for Managed Business Mobile Devices	The default end-system group for corporate mobile devices.
End-system group for Managed Personal Mobile Devices	The default end-system group for personal mobile devices.
End-system group for Decommissioned Mobile Devices	The default end-system group for decommissioned mobile devices.

Service Specific Configuration	
Enable Remote Wipe	If this option is enabled, devices will be wiped if they are moved to the MDM Remote Wipe End-system Group. • off – disabled • enterprise - always perform an enterprise wipe (only deletes corporate data) • adaptive - will perform an enterprise wipe if the device was a employee owned device and a full wipe if it was a company device\ • full - always perform a full wipe regardless of ownership
Enable Quarantine Notification	If this is set to "true", the device will be notified via the selected mode if it is quarantined
Quarantine Notification Text	Message sent in the quarantine notification to the user.
Enable Assessment	If this is set to "true", assessment data will be made available to the assessment adapter.

Assessment Map Entry #	
Plugin Name	The Plugin ID Name.
Data Field	The MDM Data Field being retrieved in this test.
Force Reassessment	Force Re-Assessment on content change.
Format of the incoming data	Format of the data that gets stored in the custom data field SYNTAX The end-system is currently #mdmManaged# Available Variables: Please refer to the MobileIron API Documentation for a full list of all available keywords.
Update Kerberos username for end-systems	If this is set to "true", the username will be updated for each end-system and a Kerberos re-authentication is triggered.
Update custom fields for end-systems	If this is set to "true", the custom field data will be updated for each end-system.
Update devicetype for end-systems	If this is set to true, the device type data will be updated for each end-system.

See MobileIron documentation for keywords available to use in custom field string.

Note: Look and feel of the MDM interface may change depending on customer's customizations.

Creating an API User

MobileIron provides a predefined user role for API access. Assigning the API role to a user automatically enables it to access the MDM API. A user with API access must be created to access MobileIrons API from the Extreme Management Center's interface.

1. From MobileIron's main interface select User Management and Add Local User.

Note: This step is not required if you plan to use an existing user or a user previously synchronized from a LDAP database.

2. Fill in the required fields and note the user ID and password for later use in Extreme Management Center configuration.
3. After creating a user, select it and click Assign Roles.

Once registration is enabled in Mobile IAM, the administrator can manage the different messages that the user receives during the registration process.

1. 1. To perform this configuration, enable web registration in NAC configuration and go to Portal Options.
2. 2. In Portal Options, select Common Page Settings and then click the 'change' link next to Message Strings.
3. 3. Look for the string 'RegistertoObtainAccess'.
   To obtain network access, you must complete registration using the self registration form.
   We will change that string to contain something like:

<h3>BYOD Self-Registration</h3>You can also register your personal device, taping here: <form action="https://<Mobileironserver>/<customername>/ireg" method="GET"><input type="submit" name="submit "value="Register with MobileIron"></form>

This code will create a button that will connect to MobileIron's registration page. Make sure that the url https://<Mobileironserver>/<customername>/ireg is the same being used in your deployment.

4. The new look of the mobile registration page is changed to reflect this new code. In this situation, the user can provide his or her data in the standard Mobile IAM registration form and register as a guest to the network without control of the MDM. Or they can register the mobile device tapping in the new button and being redirected to MobileIron's registration page.
5. After providing the required credentials, the user will be prompted to install a configuration profile granting the MDM software the required permissions to manage the device.
6. After completing the registration, several profiles will be installed under General > Profiles.
   When the device has been successfully registered with MobileIron, the Extreme Connect MDM plugin will import its data into Mobile IAM. Devices classified in MDM as Corporate owned will be place in the end-system group 'Mobile Devices Business'

and the devices classified as Personal will be added to the group 'Mobile Devices Personal' (or the group defined to that end during installation or the plugin configuration, see above in installation o post installation tasks).

7. The Mobile IAM ruleset must be adapted to reflect those groups and act accordingly depending on the newly registered devices.

Note: Devices registered by an MDM system may have an important lag until they are added to the corresponding groups. This behavior is not a malfunction of the MDM itself or the Extreme Connect MDM plugin. Due to the diversity of OSes and connectivity profiles, there is no way to know in advance when a newly registered device will provide all the data needed by the MDM software to complete the registration. It may take up to several minutes from the registration to the final landing in one of the above-mentioned groups and obtain full access to the network.

Policy Configuration

To support the previous workflow, the device in unregistered state must be able to communicate via HTTPS with MobileIron servers and via the apple push service with Apple.

Some configurations require downloading an agent to be registered by MobileIron so Google Play and Apple appStore access must be provided as well in this state. If this is the case, policies must be adapted to provide connectivity to the Agent.

The following policies (or more generic ones) are needed to allow MobileIron registration:

- Allow HTTPS to MobileIron network
- Allow TCP 5223 to 17.0.0.0/8:TCP:5223, Apple Push service
- Allow TCP/UDP 5228 to 173.194.0.0/16, Google Play login
- Allow HTTPS to 74.125.0.0/16, Google Play Downloads

Other Integration Options

The integration described in the previous section is one of many possible ways. The different methods will vary depending on specific requirements of the enterprise deploying the MDM-IAM integration.

Sophos Mobile Control

The Sophos Mobile Control integration requires authentication credentials and other account settings. This information is used in the Sophos MDM module tab and supports Mobile Control version 4.0.

Module Configuration

Configuration Option	Description
Customer	Customer name
Username	Web service username
Password	Web service password
Server	Server hostname or IP address. The server value is used to create the web service URL: https:<server>/mdmWebService

Service Configuration

Configuration Option	Description
Poll interval:	Time period between queries to the Sophos web service
End system group for managed business mobile devices	Mobile IAM end-system group that corporate owned devices will be part of
End system group for managed personal mobile devices	Mobile IAM end system group that personal owned devices will be part of
Default end system group for managed mobile devices	Mobile IAM end-system group that unknown devices will be part of
Remote wipe end system group	Mobile IAM end-system group that will be used to remotely wipe a mobile device
Enable remote wipe	Enable/disable remote wipe option
Update Kerberos username	Enable/disable option to update end-system username
Update device type	Enable/disable option to update end-system device type
Notify user when quarantined	Enable/disable option to notify user when end-system is quarantined based on assessment scoring
Enable assessment	Enable/disable option to use Mobile IAM assessment agent

Verification

1. Enroll new device with Sophos.
2. Connect to test SSID and wait for re-synchronization poll to occur.
3. Verify end system in ExtremeControl has device information from Sophos.

Policy Configuration

To support the previous workflow, the device in unregistered state must be able to communicate via HTTPS with Sophos server and via the Apple push service with Apple.

Some configurations require downloading an agent to be registered by Sophos so Google Play and Apple appStore access must be provided as well in this state. If this is the case, policies must be adapted to provide connectivity to the Agent.

The following policies (or more generic ones) are needed to allow Sophos registration:

- Allow HTTPS to Sophos network
- Allow TCP 5223 to 17.0.0.0/8:TCP:5223, Apple Push service
- Allow TCP/UDP 5228 to 173.194.0.0/16, Google Play login
- Allow HTTPS to 74.125.0.0/16, Google Play Downloads

Citrix XenMobile

The XenMobile integration requires authentication credentials and the XenMobile server base URL. This information is used in the XenMobile module tab.

Module Configuration

Configuration Option	Description
Username	Web service username
Password	Web service password
Server	Base URL of XenMobile server. Base URL is used to create the web service URL i.e. <base URL>/xenmobile/api/v1/device/filter

Service Configuration

Configuration Option	Description
Poll interval	Time period between queries to the XenMobile web service
End system group for managed business mobile devices	Mobile IAM end-system group that corporate owned devices will be part of
End system group for managed personal mobile devices	Mobile IAM end system group that personal owned devices will be part of
Default end system group for managed mobile devices	Mobile IAM end-system group that unknown devices will be part of
Remote wipe end system group	Mobile IAM end-system group that will be used to remotely wipe a mobile device
Enable remote wipe	Enable/disable remote wipe option
Update Kerberos username	Enable/disable option to update end-system username
Update device type	Enable/disable option to update end-system device type
Notify user when quarantined	Enable/disable option to notify user when end-system is quarantined based on assessment scoring
Enable assessment	Enable/disable option to use Mobile IAM assessment agent

Configuration Option	Description
Format of the incoming message	Format of the custom data string. Available fields are: id serialnumber imei username ownership devicename devicemodel devicetype operatingsystem lastseen enrollmentstatus compliancestatus macaddress jailbroken

Verification

1. Enroll new device with XenMobile.
2. Connect to test SSID, wait for re-synchronization poll to occur.
3. Verify end system in ExtremeControl has device information from XenMobile.

Policy Configuration

To support the previous workflow, the device in unregistered state must be able to communicate via HTTPS with the XenMobile server and via the Apple push service with Apple.

Some configurations require downloading an agent to be registered by XenMobile so Google Play and Apple appStore access must be provided as well in this state. If this is the case, policies must be adapted to provide connectivity to the Agent.

The following policies (or more generic ones) are needed to allow XenMobile registration:

- Allow HTTPS to XenMobile network
- Allow TCP 5223 to 17.0.0.0/8:TCP:5223, Apple Push service
- Allow TCP/UDP 5228 to 173.194.0.0/16, Google Play login
- Allow HTTPS to 74.125.0.0/16, Google Play Downloads

Extreme Management Center ExtremeConnect Management / IT Operations Configuration

FNT Command

The FNT Command integration offers two main functionalities:

1. Mapping of patch panel information from Command to end-systems and switch ports in Extreme Management Center/Control. Data within Extreme Management Center is enriched for each end-system and offers comprehensive reporting capabilities within OneView.
2. Exporting of Extreme Management data to FNT Command: this will export all switches, their modules, ports, GBICs and connected end-systems to Command's ADG database.

Module Configuration

Configuration Option	Description
Username	Username used to connect to the Command Oracle DB
Password	Password used to connect to the Command Oracle DB
ServerIP	IP Address of the Command Oracle DB
Server Port	TCP port of the Command Oracle DB. Default: 6201
Command Service Name	The "SERVICE_NAME" to access the Oracle DB view/table called "MEDMGR.CTFL2D_SWITCH_2_OUTLET". Refer to your Oracle DB administrator to get the service name specific to your FNT Command installation.

General Module Configuration	
Poll interval in seconds	The time (in seconds) the module will wait after each run. Since the data on patch field connections/locations is relatively static it often does not require updating every 60 seconds and it is recommended to increase the value for the poll interval. This will also decrease the processing load on the NetSightExtreme Management Control Center server. Recommendation: 3600 seconds (once per hour) but this depends on the size of your infrastructure and your requirements.
Module loglevel	Verbosity of the module. Logs are stored in NetSightExtreme Management Control Center's server.log file.

General Module Configuration	
Module enabled	Whether or not the module is enabled.
Push update to remote service	If this is set to “true”, data from other modules will be pushed to the service.
Update local data from remote service	If this is set to “true”, data from the remote service will be used to update the internal end-system table.
Default end-system group	The default end-system group name to use if it is not set dynamically.
Enable Data Persistence	Enabling this option will force the module to store end-system custom field and group membership data into a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted. It is important to enable this feature, especially in large environments, so that OF Connect doesn’t need a full re-sync of all data everytime you restart your NetSightExtreme Management Control Center server. Default: True.

Service Specific Configuration	
Custom field to use	The number of the custom data field for each end-system to store the data retrieved from Command. Available values are: 1, 2, 3 or 4. Default: 1.
Format of the incoming data	Format of the data that gets stored in the custom data field. You can chose and combine any of the available variables: outletId (ID of the patch field), outletCampus, outletBuilding, outletFloor, outletRoom. Default: #outletId# / #outletCampus# / #outletBuilding# / #outletFloor# / #outletRoom#
Update NAC End-Systems with Command outlet data	If set to True the module will retrieve outlet data (outlet id, room, building, etc.) and map it to the corresponding end-systems/ports in NAC
Command DB table name containing outlet data for NAC import	The name of the Oracle DB table that contains the Command outlet data. This is required if you enable the feature update_nac_endsystems_with_command_ outlet_data so OFC knows which table to query to retrieve data about ports and their outlet data. Default: medmgr.CTFL2D_SWITCH_2_OUTLET
Push NetSight Devices to Command Auto-Discovery Gateway	If set to 'true' the module will push NetSight switch data (IP, firmware, type, descriptor, etc.) to Command's Auto-Discovery Gateway. The module updates the corresponding database tables. The Auto-Discovery Gateway itself manages the import of the data to Command automatically
Push NAC End-Systems to Command Auto-Discovery Gateway	If set to 'true' the module will push all NAC end-systems to Command's Auto-Discovery Gateway. It will then try to "connect" these end-systems to switches and ports exported from NetSight. This option is only available if the option push_ netsight_devices_to_command_adg has also been enabled. The module updates the corresponding database tables. The Auto-Discovery Gateway itself manages the import of the data to Command automatically.
Autodiscovery Gateway DB TCP Port	The TCP port where the Autodiscovery Gateway database is running on. Default: 1521
Autodiscovery Gateway DB Username	The username to connect to the Autodiscovery Gateway database. Default: command
Password	Password used to connect to the Autodiscovery Gateway database. Default: command
The Map to use when exporting NetSight/NAC data to Command's ADG	Specify the map which should be used to export NetSight (switches) and NAC (end-systems) data to ADG. The map needs to be configured correctly in order for ADG to proerply map the incoming device types to existing, well-known device types. Default: 1

Service Specific Configuration	
Automatically process NetSight data pushed to ADG	If set to 'true' the module will automatically call the AutomatedProcessomg.sh script at the end of each synchronization cycle. This will trigger the ADG to immediately import the new data from NetSight. This is currently only supported on ADG Linux installations.
Username to connect to the ADG server via SSH and execute automated processing script	The user name to connect to the ADG server via SSH and execute the AutomatedProcessing.sh script. Make sure the user is allowed to remotely login via SSH and has the necessary privileges to execute the script located in your tomcat folder under /webapps/command/axis/WEB-INF. This is only relevant if the option adg_enable_automated_processing has been enabled.
Password to connect to the ADG server via SSH and execute automated processing script	The password to connect to the ADG server via SSH and execute the AutomatedProcessing.sh script. This is only relevant if the option adg_enable_ automated_processing has been enabled
Username for the automated processing script (Command user)	The Command user name will be provided as a parameter to the AutomatedProcessing.sh script. Make sure the user has the necessary rights within Command to perform the changes which the script triggers. This is only relevant if the option adg_enable_automated_processing has been enabled.
Password for the automated processing script (Command user)	The Command password will be provided as a parameter to the AutomatedProcessing.sh script. This is only relevant if the option adg_enable_ automated_processing has been enabled.
Tenant (=Mandant) ID for the automated processing script (Command tenant)	The Command tenant (=Mandant) to use for the user provided above. This will be used as a parameter to the AutomatedProcessing.sh script. This is only relevant if the option adg_enable_automated_processing has been enabled.
User group ID for the automated processing script (Command user group name)	The name of the Command user group to use for the user provided above. This will be used as a parameter to the AutomatedProcessing.sh script. This is only relevant if the option adg_enable_automated_processing has been enabled.
Full file path on the ADG server for the script to trigger automated processing	The full file path (path and file name) of the AutomatedProcessing.sh script. This script will be triggered on the ADG server via SSH to automatically start the data import. This is only relevant if the option adg_enable_automated_processing has been enabled. Default: /usr/share/tomcat7/webapps/command/axis/WEB-INF/AutomatedProcessing.sh
Maximum number of end-systems per web service request to NetSightExtreme Control CenterExtreme Management Center	Specify the maximum number (as integer) of end-systems that Fusion will query per request from the NetSightExtreme Control CenterExtreme Management Center server. This setting will allow you to split large end-system queries into smaller badges. Example: There are 10.000 end-systems in NetSightExtreme Control CenterExtreme Management Center/NAC. You set this max_endsystem_ per_request value to 1000. Then Fusion will perform 10 calls to the NetSightExtreme Control CenterExtreme Management Center API and retrieve 1000 end-systems per call. Default: 1000.
Timeout per web service request to NetSightExtreme Control CenterExtreme Management Center	Specify the timeout in seconds (as integer) for each web service call to NetSightExtreme Control CenterExtreme Management Center. Since these calls are handled by the TaskScheduleHandler you need to calculate a value as follows: Take the setting for poll_interval_seconds from your TaskScheduleHandler.xml config file and add a couple of seconds for the expected time it takes for the http transaction to complete. Example: 3 seconds poll interval for the TaskScheduleHandler plus a timeout of 7 seconds for the http request to be performed --> 10 seconds. Default: 10
The ID of the tenant to query Command outlet data for	Specify the Command tenant ID ("Mandant ID") which will be used to filter Command outlet data. This will help reduce the amount of data OFC has to process when importing Command outlet data and matching it to end-systems in NAC. This is only relevant if the option update_nac_endsystems_with_ command_outlet_data has been enabled.

Service Specific Configuration	
Default username for switch CLI access	The default username to connect to any switches' which don't have CLI credentials stored within NetSight. This username is only used if there are no CLI credentials defined for a switch in NetSight. Otherwise the NetSight CLI username takes priority. This is used to gather port optic info from XOS switches using a Telnet connection.
Default password for switch CLI access	The default password to connect to any switches' which don't have CLI credentials stored within NetSight. This password is only used if there are no CLI credentials defined for a switch in NetSight. Otherwise the NetSight CLI password takes priority. This is used to gather port optic info from XOS switches using a Telnet connection.

Verification

1. Login to OneView and verify the incoming data from FNT within the custom data field in the end-system table.
2. Pick a few end-systems and validate that their location data in NAC's custom field is correct according to Command data.

Glue Networks Gluware Control

The Gluware Control integration enables the option to publish Policy Domain configuration to Gluware. The policies are translated into ACL definitions that can be deployed to managed nodes of different manufacturers.

Module Configuration

The table below describes the configuration options available for the Gluware Control module (config file: GlueNetHandler.xml)

Configuration Option	Description
Username	Username used to connect
Password	Password used to connect
Webservice URL	Webservice URL of Gluware Control
Company	Tenant Company Name
Organization	Tenant Organization Name

General Module Configuration	
Poll interval in seconds	The time (in seconds) the module will wait after each run. Since the data on patch field connections/locations is relatively static it often does not require updating every 60 seconds and it is recommended to increase the value for the poll interval here. This will also decrease the processing load on the Extreme Control CenterExtreme Management Center server. Recommendation: 3600 seconds (once per hour) but this depends on the size of your infrastructure and your requirements.

General Module Configuration	
Module loglevel	Verbosity of the module. Logs are stored in Extreme Control CenterExtreme Management Center's server.log file.
Module enabled	Whether or not the module is enabled.
Push update to remote service	If this is set to “true”, data from other modules will be pushed to the service.
Update local data from remote service	If this is set to “true”, data from the remote service will be used to update the internal end-system table.
Default end-system group	The default end-system group name to use if it is not set dynamically.
Enable Data Persistence	Enabling this option will force the module to store end-system custom field and group membership data into a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted. It is important to enable this feature, especially in large environments, so that OF Connect doesn’t need a full re-sync of all data everytime you restart your Extreme Control CenterExtreme Management Center server. Default: True.

Service Specific Configuration	
Naming Convention	Only policy roles matching the naming convention format will be published (.+ for all)
Provision Switches	Automatically provision switches on enforce
Switches	Name of switch nodes to provision (seperated by ;)

The module will publish every policy domain to Gluware Control that has a matching jboACL object name. (i.e. to publish “Default Policy Domain”, create a new jboACL with the name “Default Policy Domain”).

After the data was published, the description of the ACL will be changed to “Created by Extreme Connect” and contain an Access List for every policy role present in the policy domain.

Note: Support for policy rules depends on the underlying switch hardware. Gluware Control only supports L3-L4 IP policy rules with Accept and Deny actions and only those will be published from the policy domain.

Cisco ACL Support in NAC Manager

In order to use an ACL in conjunction with a RADIUS NAC request, the RADIUS response parameters have to be adjusted for use with Cisco Switches. Certain switch models might require specific licenses to enable per-user ACL and dynamic ACL support. Please refer to the vendor documentation for additional requirements.

When adding a Cisco switch in NAC Manager:

1. Enable the “Gateway RADIUS Attributes to Send” option and select **Edit RADIUS Attribute Settings** from the drop-down menu.

2. Click the Add button to create a new profile and name it “Cisco Wired Dynamic ACL & VLAN ID”. This will send the ACL name and the VLAN ID to the switch upon authorization.
3. Open the Policy Mapping panel in OneView Control > Identity & Access > I&A Configurations > I&AProfiles > Policy Mappings > Default in order to map the policy to the desired VLAN.

Note: The Contain To VLAN action is not supported in IP ACLs and VLAN assignments have to be managed via RADIUS attributes in this case.

4. Continue with the regular NAC configuration steps to assign profiles using rules.

Verification

1. Login to Gluware Control and select Domain Objects > jboAcls.
2. Select the ACL that matches the policy domain in NetSight and verify that the Access Lists match with the policy roles.
3. ACLs are published automatically, but may need to be deployed to switches manually if automatic provisioning is not enabled.

To verify the configuration on a switch:

1. Select Nodes > lanSwitch and connect to the desired switch.
2. In addition to present default ACLs, Gluware will create one ACL matching the Policy Role in name with all rules below it. The rule precedence matches with the default precedence found in Extreme Control.

Microsoft System Center Configuration Manager (SCCM)

The Microsoft SCCM integration is a one-way integration offering end-system data retrieval from SCCM on managed devices. This data enriches each end-system data set within Extreme Management Center and offers comprehensive reporting capabilities within OneView.

Note: The SCCM server requires an adapter agent to be installed and configured prior to enabling the corresponding module within Extreme Connect. The adapter file is provided by Extreme Networks.

Module Configuration

The table below describes the configuration options available for the SCCM OFConnect module (config file: SCCMHandler.xml)

Service Configuration	Description
Adapter IP	IP Address of the SCCM adapter
Adapter Port	Port where the SCCM adapter is listening on
Pre-Shared Key	The pre-shared key used to communicate with the SCCM adapter

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the adapter running on the SCCM server.
Module loglevel	Verbosity of the module. Logs are stored in NetSightExtreme Control CenterExtreme Management Center's server.log file.
Module enabled	Whether or not the module is enabled.
Update local data from remote service	If this is set to “true”, data from the remote service will be used to update the internal end-system table.
Default endsystem group	The default end-system group name in NAC to assign all MAC addresses found in SCCM. Use a non-existing group name if you don’t want this module to assign all SCCM MAC addresses into any NAC end-system group.
Enable Data Persistence	Enabling this option will force the module to store end-system and end-system group data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use	The custom field within NetSightExtreme Control CenterExtreme Management Center to update the information for end-systems retrieved from the adapter running on the SCCM server (valid values: 1-4).
Format of the incoming data	The format of the data which is received from the adapter running on the SCCM server and written to the custom field. Syntax example: Netbios Name=#netbiosName#; User=#lastLogonUserDomain#\#lastLogonUser#; OS=#operatingSystem# (#servicePack#); Manufacturer=#computerManufacturer# Model=#computerModel# Available Variables: path, mac, netbiosName, lastLogonUserDomain, lastLogonUser, operatingSystem, servicePack, computerManufacturer, computerModel
Overwrite the existing username with the one acquired from SCCM	If set to "true" the username retrieved from SCCM will overwrite the username that is already in NAC. If no username could be retrieved from SCCM for a given end-system, then no change is performed in NAC. Be aware that this might mess up existing NAC processes if you are already retrieving and using the username through some other mechanism like 802.1X or Kerberos snooping → this will be overwritten.

Service Specific Configuration	
Overwrite the existing device type with the one acquired from SCCM	If set to "true" the device type (Windows operating system) retrieved from SCCM will overwrite the device type which is already in NAC. If no operating system could be retrieved from SCCM for a given end-system, then no change is performed in NAC. Be aware that this might mess up existing NAC processes if you are already retrieving and using the device type through some other mechanism like DHCP snooping → this will be overwritten. But in most cases this feature should improve your current method (at least for Windows machines managed by SCCM) since the quality of the information retrieved from SCCM is usually very good.

Adapter Installation

Extreme Connect is retrieving data from an SCCM server using an adapter. This adapter needs to be installed and configured prior to enabling the corresponding module within Extreme Connect. The adapter basically consists of a Java executable file (.jar) and a configuration file. There is currently no dedicated installer for the adapter so it's recommended that you follow these steps in order to install the adapter manually:

On the SCCM server:

1. Create a user account which the Extreme Networks adapter should use to access data on the SCCM server.
2. Install the latest Java Runtime Environment.
3. One the SSCM server, create a dedicated folder (example: C:\Program Files\Extreme Networks\SCCM Adapter) and copy the two files: FUSION_SCCM_ADAPTER_ <version>.jar and FUSION_SCCM _ADAPTER.config) into it.
4. Start the adapter by double-clicking the file FUSION_SCCM _ADAPTER.jar or running it within a shell using "java –jar FUSION_SCCM _ADAPTER.jar". AProvide at least the following access rights to this user account:
5. Verify the log file which should have been created in the same folder, where the jar file is located.
6. Make sure that the adapter is automatically started when the Windows Server starts up.

Adapter Configuration

The table below lists the configuration options for the SCCM agent.

Configuration Option	Description
LOG_LEVEL	Set the log level of the adapter to one of the following values: ERROR, WARN or DEBUG. If not set, the default will be WARN.
IP	IP address for the web service (=agent) to listen on

Configuration Option	Description
PORT	TCP Port for the web service to listen on - must NOT be used by any other application on this server!
SCCM_SERVER	The DNS name of the Configuration Manager server to connect to. So far this has only been tested with this adapter and the SCCM server running on the same server although remote connections might work as well.
SCCM_SITE_CODE	The name of the 'Site' to connect to within Configuration Manager. Example: SCCM_SITE_CODE=mysite
SLEEP_INTERVAL	Set the sleep interval in seconds - the main adapter will update all computer data from SCCM and then sleep for these many seconds before running the next update to retrieve the latest data.
PRE_SHARED_KEY	The pre-shared key used for the communication between the adapter and OFConnect. This must match the key entered when installing the OFConnect Hyper-V module
IS_PRE_SHARED_KEY_ENCRYPTED	If set to 'false' the adapter assumes that the 'PRE_SHARED_KEY' configured above is not encrypted - on the first start the adapter will automatically encrypt the key and set this value to 'true'. If you want to change this key at a later stage, change the key above, set this value back to 'false' and restart the adapter service

Verification

To verify that the data on Windows-based end-systems could be retrieved from SCCM:

1. Check the custom field within NAC's end-system table and make sure you see info on data like the netbios name, user name, detailed operating system info, etc.
2. If enabled, you will also see a more detailed operating system information within the Device Type column.
3. If enabled, you will also see the last logged on use information within the Username column.

Aruba ClearPass

The Aruba ClearPass integration is a one-way integration offering end-system data retrieval from ClearPass. ClearPass end-systems will be created and updated within Extreme Management Center. That end-system data can then be synced to Extreme Analytics and thus be mapped to flow data (username, device type, policy profile).

Note

Mapping end-system data from ClearPass to flow data within Extreme Analytics requires a correctly configured IP resolution within ClearPass since the mapping is done based on the end-system's IP address.

Module Configuration

The table below describes the configuration options available for the Aruba ClearPass module (config file: ArubaClearpassHandler.xml)

Service Configuration	Description
Server	IP Address of the Aruba ClearPass server
Port	Port of the Aruba ClearPass server API service – usually 443
Access-Token	1. Login to Aruba ClearPass Guest 2. Go to Administration [Symbol] API Services [Symbol] API Clients 3. Click on “Create an API Client” 4. Use these settings: • Enabled: true • Operator Profile: Read-Only Administrator • Grant Type: Client Credentials • Access Token Lifetime: choose a high value (long lifetime) here. Example: 52 weeks 5. Click on “Create API Client” The new client config will be shown in a list – click on that list item and click on “Generate Access Token” [Symbol] copy the HTTP authorization token which is located after the “Bearer” part of the HTTP authorization header. Example: Bearer 01279b5134e633f8df3a36b145657f4f35133f16

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the Aruba ClearPass server.
Module loglevel	Verbosity of the module. Logs are stored in Extreme Management Center's server.log file.
Module enabled	Whether or not the module is enabled.
Update local data from remote service	If this is set to “true”, data from the remote service will be used to update the internal end-system table.
Default endsystem group	The default end-system group name in NAC to assign all MAC addresses found in ClearPass. Use a non-existing group name if you don’t want this module to assign all ClearPass MAC addresses into any NAC end-system group.
Enable Data Persistence	Enabling this option will force the module to store end-system and end-system group data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use	The custom field within Extreme Management Center to update the information for end-systems retrieved from ClearPass (valid values: 1-4).
Format of the incoming data	Format of the data that gets stored in the custom data field: Syntax example: user=#user#, domain=#domain#, online=#online#, updatedAt=#updatedAt#, roles=#roles# Available variables from Aruba Clearpass: ipAddress, user, domain, spt, deviceCategory, deviceFamily,deviceName, online, updatedAt, roles
HTTP socket timeout in seconds (Clearpass API)	HTTP socket timeout in seconds for all HTTP connection sockets to the Clearpass API. Will allow the http client to timeout the established connection if there is no response from the ClearPass server after the configure amount of seconds
Enable device type overwrite	Enable this to use the device family/type retrieved from ClearPass to overwrite the device family/type in Extreme Access Control
End-system group for decommissioned Clearpass end-points	If an end-point gets deleted from Clearpass its corresponding end-system will be pushed to this end-system group
Remove end-systems from other groups on decommission	Enable this to remove a device from all other groups when it is moved to the decommission group
Delete custom data in XMC for decommissioned devices	If an end-point gets deleted from Clearpass the corresponding end-system's custom data field in XMC will be cleared
XMC Server	Hostname or IP of the XMC server. Needed to import Clearpass end-points.
XMC Port	HTTPS port of the XMC service. Default: 8443
XMC Username	Username to connect to the XMC server.
XMC Password	Password to connect to the XMC server.

Configure NAC + Analytics Integration

Ensure to enable the feature that exchanges EAC data with flow data:

Verification

The end-system data from ClearPass will be visible within the XMC end-system list and the Analytics flow data.

Within the end-system table you should see data on all ClearPass end-systems within the configured custom field:

Plus usernames and device types if available through ClearPass.

As soon as the user and device type fields for ClearPass sourced end-systems have been updated within XMC you should start seeing that information within the Analytics “Application Flows” tab as well:

Extreme Management Center Fields Updated

The following end-system table fields in Extreme Management Center are updated by the Aruba Clearpass integration:

- ipAddress
- user
- domain
- spt
- deviceCategory
- deviceFamily
- deviceName
- online
- updatedAt
- roles

MDM System Configuration

In order to be used by Extreme Networks MDM Connector plugin, the MDM software must be configured to provide the data that is imported by IAM as assessment information or end-system data.

End-System Groups

After initial installation the following groups should be present in IAM:

Group for Managed Business Mobile Devices	Managed Mobile Devices Business
Group for Managed Personal Mobile Devices	Managed Mobile Devices Personal
Group for Decommissioned Mobile Devices	Managed Mobile Devices Decommissioned

We have shown the default names for each group. These names can be changed during installation or in the configuration page.

In addition to these a fourth group will appear for the ‘wipe’ functionality:

End-system group for Managed Devices Wipe	Managed Mobile Devices Wipe

These groups contain the inventory information coming from the MDM provider. End-systems will be classified in each group depending on the ownership information from the MDM provider.

The ‘decomissioned’ group is a placeholder for devices that have been unenrolled in the MDM provider. Typically, its treatment should be the same as unregistered users.

The ‘Wipe’ group is an exception to this rule, the group is only used to trigger a wipe notification to the MDM provider. The wipe signal will reset the configuration of the ensystem to its factory settings. This option is disabled by default.

Extreme Management Center Connect Assessment Configuration

Assessment MAP Entries

All modules except McAfee EMM currently use the assessment adapter to report health results to Extreme Management Center. The assessment adapter creates 30 new assessment tests or PluginIDs to use by NAC. Each test is reported to NAC by a pluginID created as follows:

- base value = 100.000
- plugin id = base value + ENUM ID (i.e. OWNERSHIP -> 100.000 + 22 = 100.022)

The complete list of tests and its IDs is:

- EXISTS(1)
- COMPLIANT(2)
- JAILBROKEN(3)
- AUTHORIZED(4)
- WIPED(5)
- UNINSTALLED(6)
- COMPROMISED(7)
- OSOUTOFDATE(8)
- POLICYOUTOFDATE(9)

- DEVICEOUTOFDATE(10)
- BLOCKED(11)
- INFECTED(12)
- LOST(13)
- RETIRED(14)
- UDID(15)
- SERIALNUMBER(16)
- IMEI(17)
- ASSETNUMBER(18)
- NAME(19)
- LOCATION(20)
- USER(21)
- OWNERSHIP(22)
- PLATFORM(23)
- MODEL(24)
- OSVERSION(25)
- PHONENUMBER(26)
- LASTSEEN(27)
- PASSCODEPRESENT(28)
- PASSCODECOMPLIANT(29)
- DATAENCRYPTION(30)

Each one of these tests can be made to map to different variables in each MDM connector.

In JAMF Casper module's default configuration, the test EXISTS (pluginID 100001) is mapped to the value of the variable 'managed' in JAMF Casper's database.

NAC Manager can assign risk values and scores to each test using their pluginID. This is needed in order to quarantine devices based on their risk level.

Assessment Adapter

The assessment adapter infrastructure reports health results from Extreme Connect modules to NAC, if available.

The assessment adapter doesn't start automatically it has to be started with:

- Linux:

<Extreme Management CenterRootdir>/jboss/server/default/deploy/fusion_jboss.war/assessment/launchAS.sh

- Windows:

  <Extreme Management CenterRootdir>\jboss\server\default\deploy\fusion_jboss.war\assessment\launchAS.cmd

McAfee EMM uses a separate assessment plugin to gather data from the server and report it as health results to the Extreme Management Center server. This path points to the location of the MDMAdapter.jar that must be in:

- Linux:

  <Extreme Management CenterRootdir>/jboss/server/default/deploy/fusion_jboss.war/assessment/launchAS.sh

- Windows:

  <Extreme Management CenterRootdir>\jboss\server\default\deploy\fusion_jboss.war\assessment\

Before the assessment adaptor can be used in NAC manager, it has to be created as a valid assessment server.

1. From the assessment configuration (1) select assessment servers (2) and click add (3) to add a new assessment server.
2. In the new server dialog, provide the required data.
   - Assessment Server IP: IP address of the Extreme Management Center server.
   - Assessment Server Name: a Name for easily identify our server.
   - Assessment Server Port: if launched with the launchAS commands, the agent runs on server 8448.
   - Assessment Server Type: FusionAssessmentAgent
   - Max Concurrent Scans: leave empty. This can be used afterwards to increase the capacity of the server. By default the server allows 10 concurrent scans.

In order to use this server for assessment purposes, the server must be in an assessment pool and the assessment pool must be used by an assessment configuration.

3. Create a scoring override for one or more of these test cases to quarantine end-systems in case they match a certain result string within their description field.
4. If you want to quarantine all iPads with an iOS version of 5.x, make sure you have enabled “Use Quarantine Policy” in the corresponding NAC profile and that the corresponding policy on the WLAN controller has a redirect configured within that policy that points to the NAC captive portal.
5. Enable “Assisted Remediation” within the NAC configuration in order for NAC to display the remediation/self-help page.
6. Customize your remediation portal if needed. For example, you can add a remediation link that allows users to register their devices on the MDM portal.
7. Another customization that is recommended is to define the Custom Remediation Actions to improve the user experience with the help texts on the remediation page.

Extreme Management Center Connect Configuration Troubleshooting

Troubleshooting VMware vSphere Configuration

Troubleshooting Citrix XenServer Configuration with Connect

Troubleshooting Adapters for XenDesktop, Hyper-V, SCVMM and SCCM Configuration

Troubleshooting Citrix XenDesktop Configuration with Connect

Troubleshooting Microsoft Hyper-V and Virtual Machine Manager Configuration with Connect

Extreme Management Center is not responding.

Restart the Extreme Management Center services. Change directory (cd) to /usr/local/Extreme_Networks/Extreme Management Center/scripts.

cd /usr/local/Extreme_Networks/Extreme Management Center/scripts
stop Extreme Management Center service by typing:
./stopserver.sh

Wait for the prompt and then start Extreme Management Center service by typing:

./startserver.sh

Is there a log file and where do I find it?

Extreme Connect logs within the JBoss context of the Extreme Management Center server. You may find the server.log file either in the ../appdata/logs/ folder or simply by opening the server log from any Extreme Management Center Client.

What loglevels are available and how do I change them?

Every module of Extreme Connect, including the main application itself have individual loglevel settings in their respective configuration file. The default level should be ERROR and it is strongly suggested to keep it at this level, except for troubleshooting issues. The loglevels are (from least to most talkative):

- ERROR
- WARN
- INFO
- DEBUG

I am getting a lot of errors and would like to turn logging completely off for a certain module.

In addition to the four loglevels used by all modules, Log4J also supports the FATAL loglevel which is currently not used by any module without Extreme Connect. In order to set a module to use this loglevel, the configuration file has to be edited manually as this option is not provided on the web page to avoid shutting down logging by mistake.

Some modules stop working after some time and report in the log that too many errors happened.

Each module is monitored by the main Extreme Connect process regarding errors that happen during each run cycle (i.e. authentication errors). If a module produces more than 10 failures in a row, the module will be disabled to prevent any further errors. In order to restart a module, try to identify the problem source

(i.e. remote server is not responding), remedy it and update the module configuration file. As soon as the timestamp of the configuration file is changed, the configuration will be reloaded and the failure counter is reset to zero until further failures happen. The counter will also be reset, if at least one successful cycle was completed in the meantime.

The logs always note local/remote data storages. What are these?

Extreme Connect logs are always written from the Extreme Connect perspective. Local means the Extreme Connect service and remote relates to another service contacted (i.e. Extreme Control, VMware,...). Each module has its own datastore in order to track changes and update local or remote data. Therefore, if certain information for an end-system is missing from a specific module, it is always a good start to look at the datastore and log for that particular module.

What happens to a module if an error occurs?

The error is logged and the run cycle for the module will go on or end, depending on the severity of the error. If an error should crash a module, a full stack trace will be logged and the module is terminated until the JBoss service has been restarted. All other modules are not affected by this and will continue running, even if they should not receive any further updates from other modules.

After JBoss has started, I don't see any data being updated for some minutes. Is there something wrong?

No, Extreme Connect will first start all modules and wait a bit to verify that everything is running correctly. After that, the modules will enter their run cycle and start retrieving data from various sources. Depending on the delay until the information is retrieved and the interval times of each module, this might take up to a couple of minutes.

Troubleshooting VMware vSphere Configuration with Connect

Do I have to create a dedicated user for Extreme Connect to access the vSphere webservice?

No, but it is recommended to do so as it will allow you to filter events and tasks more easily within the VMware Client.

What are the least permission requirements for the webservice user?

The account should have at least all necessary permissions to:

- register the Extreme Management Center Plugin Extension

- write data to VM annotation fields

- read data from VM configurations (MAC, Network)

Although Extreme Connect seems to be running fine, I only see “n/a” in the annotation fields and no records via the Extreme Connect plugin. Why is that?

Most likely, none of the MAC addresses of the VM is listed in the end-system table of the NAC Manager. Make sure that authentication (at least MAC Auth) is set up properly on the physical switch and that the VM is actually sending some traffic.

How often will Extreme Connect update the information within vSphere (annotations, switches...etc.)?

Extreme Connect will check if the current remote data differs from its local. If so, it will update all data that is different on the remote service. This is especially true for the annotation field and it is generally recommended not to use variables like LastSeenTime in the annotation text, which will change very frequently and have a lot of updates as a result.

Is there any way to get rid of the event/task logs for every update that Extreme Connect performs within vSphere?

No. This functionality is handled by vSphere itself and Extreme Connect has no means to stop it. vSphere offers a filtering mechanism that can be used to limit the information shown and help to find specific data more efficiently.

How does Extreme Connect determine the name of the end-system group that a VM MAC address should be added to?

Extreme Connect retrieves the name of the virtual network/portgroup in its default configuration and uses the part before the first underscore as the end-system group name. This corresponds to the naming convention used if Extreme Connect is automatically creating portgroups from end-system groups. The format used there is always:

endSystemGroup_virtualSwitchName

The reason for this is the requirement within vSphere that two portgroups on the same host may not share the same name. Therefore, the (d)vSwitch name is appended to the end-system group name with an underscore. This also ensures

that vMotion is possible for VMs on two hosts which also require that both portgroups on those hosts have the same name.

Is it possible to let Extreme Connect create portgroups automatically, but to let the VM administrator handle VLAN configurations?

Yes, the configuration offers an option to turn off VLAN creation/updates.

What happens if VLAN updates are enabled and a VM administrator changes the settings of a portgroup?

Extreme Connect will update the settings using the local configuration data. It will not delete and recreate the portgroup, but simply update the existing configuration.

What happens if an end-system group is deleted and the portgroup deletion option is enabled?

Extreme Connect will move all VMs attached to that portgroup/network to the "VM Disconnected Systems" group and then delete the original portgroup/network.

If a portgroup has been deleted by Extreme Connect, can another portgroup with the same name be created manually within vSphere afterwards?

Using its local data store, Extreme Connect will put the name of the end-system group onto a special "deletion" stack. During each run cycle, every module will check the stack and remove all portgroups that use the same name until the deletion interval timer runs out. This value is set to 2 minutes per default. After those 2 minutes have passed, a VM administrator can safely create a portgroup of the same name without risking it being deleted.

Although portgroup deletion is enabled, groups are not getting deleted by Extreme Connect. What is the reason for that?

Extreme Connect will delete all groups as long as the group is on the deletion stack and the entry has not timed out. If too much time is required for each run through, try increasing the deletion interval timer so that the module has a better chance of performing the operation.

Troubleshooting Citrix XenServer Configuration with Connect

Do I have to create a dedicated user for Extreme Connect to access the XEN Server webservice?

No, you can use the root account on the XEN Server.

What are the least permission requirements for the webservice user?

The account should have at least all necessary permissions to:

- write data to VM description fields
- read data from VM configurations (MAC, Network)

How often will Extreme Connect update the information within XenCenter (descriptions, networks...etc.)?

Extreme Connect will check if the current remote data differs from its local. If so, it will update all data that is different on the remote service. This is especially true for the description field and it is generally recommended not to use variables like LastSeenTime in the annotation text, which will change very frequently and have a lot of updates as a result.

How does Extreme Connect determine the name of the end-system group that a VM MAC address should be added to?

Extreme Connect creates XEN networks with the exact same name as the corresponding Extreme Management Center end-system group. Extreme Connect then checks all XEN networks it manages and the VMs which are assigned to them. The MAC's of these VMs will then be added to the corresponding end-system group in Extreme Management Center.

Is it possible to let Extreme Connect create networks automatically, but to let the VM administrator handle VLAN configurations?

No, this feature is currently only supported for VMware, not for XEN.

What happens if a XEN administrator changes the settings of a network (VLAN ID, NIC)?

Extreme Connect will update the settings using the local configuration data. For this to take place, all VMs connected to the network will temporarily be disconnected from this network. Then the network will be reconfigured and finally all VMs priory connected to this network will be reconnected.

What happens if an end-system group is deleted and the network deletion option is enabled?

Extreme Connect will move all VMs attached to that network to the "VM Disconnected Systems" network and then delete the original network.

If a network has been deleted by Extreme Connect, can another network with the same name be created manually within XenCenter afterwards?

Using its local data store, Extreme Connect will put the name of the end-system group onto a special "deletion" stack. During each run cycle, every module will check the stack and remove all networks that use the same name until the deletion interval timer runs out. This value is set to 2 minutes per default. After those 2 minutes have passed, a XEN administrator can safely create a network of the same name without risking it being deleted.

I've set an end-system group's description to "sync=true vlan=100" but in XEN only an internal network is being created – not an external one with the corresponding VLAN ID - why?

In order for Extreme Connect to create an external network within XEN two settings are necessary: VLAN ID and physical NIC to connect the external network to.

I've set an end-system group's description to "sync=true nic=eth1" but in XEN only an internal network is being created – not an external one attached to nic eth1 without a VLAN ID - why?

In order for Extreme Connect to create an external network within XEN two settings are necessary: VLAN ID and physical NIC to connect the external network to. It is not possible to create an external XEN network without assigning a VLAN ID (all external XEN networks are tagged).

Troubleshooting Adapters for XenDesktop, Hyper-V, SCVMM and SCCM Configuration with Connect

What is the adapter doing and how?

The adapter is creating a Web Service bound to the IP and port that configure within the configuration file. OneFabric ConnectExtreme Connect is then making web service calls to this adapter to retrieve data on managed end-systems (VMs, Windows devices, etc.) and (depending on which integration is used) also update data on the remote server (for example: update description fields for VMs).

What ports are needed to communicate between the OneFabric ConnectExtreme Connect and the adapter?

Only one port is required and this is the one configured on the adapter side within its configuration file.

Is the communication secure?

All data sent and retrieved from/to the adapter is encrypted using the pre-shared key which the admin defines when setting up the adapter and installing OneFabric ConnectExtreme Connect. The key itself is then automatically encrypted.

No information is synchronized – what else can I check?

Check the adapter's logfile. It will show you when the adapter has been "called" by OneFabric ConnectExtreme Connect, what powershell commands it tries to execute and what the return values of these commands were. You need to set the log level to "DEBUG" and restart the adapter in order for this to print detailed logging information.

How can I check whether the adapter's web service is working and reachable?

Depending on whether your NetSightExtreme Control CenterExtreme Management Center server is installed on a Windows server or on a Linux-based appliance you can use a standard browser or a Linux tool like wget to request one of the following web URLs (depending on the integration (adapter) you are trying to troubleshoot):

- XenDesktop: http://<IPofAdpater>:<PortOfAdapter>/DCM_XENDESKTOP_ADAPTER
- Hyper-V: http://<IPofAdpater>:<PortOfAdapter>/DCM_HYPERV_ADAPTER
- SCVMM: http://<IPofAdpater>:<PortOfAdapter>/DCM_SCVMM_ADAPTER
- SCCM: http://<IPofAdpater>:<PortOfAdapter>/FUSION_SCCM_ADAPTER

If you get a browser error that it cannot connect or the page is not existing you either have an issue with a firewall along the communication path or the adapter's web service did not start properly on the configured IP and port. Also make sure that the configured port for the adapter is not yet used by another service on your Microsoft server.

Troubleshooting Citrix XenDesktop Configuration with Connect

Why do the usernames within Extreme Management Center NAC Manager appear as “Kerberos” usernames?

The XenDesktop adapter uses the same webservice call as the Kerberos snooping process. For the system’s functionality this makes no difference: you can create user groups, rules and profiles based on these usernames.

After some time the usernames are deleted or disappear in NAC Manager - why?

1. The corresponding XenDesktop session has ended. In this case, the adapter resets the username on the corresponding end-system VM which will also trigger any existing rule / NAC profile changes.
2. The Kerberos aging timer was triggered. Within NAC Manager you can configure a period after which the Kerberos usernames will automatically age out. If you don’t want this timer to interfere with the XenDesktop adapter functionality make sure to set a very high value or disable this feature.

Although some users have disconnected from their XenDesktop session the usernames are still active within NAC Manager - why?

XenDesktop distinguishes between a closed/non-existing session and a disconnected one. A session is first active, then disconnected and then deleted. As long as the session is in the disconnected state, the adapter still doesn’t reset the username within Extreme Management Center. In case the user re-activates his/her session, there is no need for the adapter to set the username and the corresponding user-profile is already active within NAC.

Troubleshooting Microsoft Hyper-V and Virtual Machine Manager Configuration with Connect

How often will Extreme Connect update the information within the notes field?

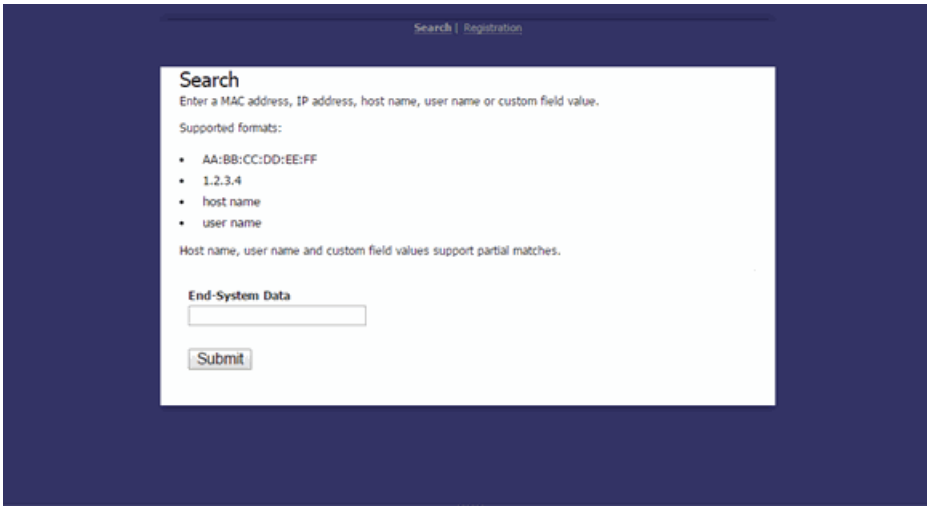
Extreme Connect will check if the current remote data differs from its local. If so, it will update all data that is different on the remote service. This is especially true for the notes field and it is generally recommended not to use variables like LastSeenTime in the notes text, which will change very frequently and have a lot of updates as a result.

How does Extreme Connect determine the name of the end-system group that a VM MAC address should be added to?

Extreme Connect reads the virtual networks (virtual switches) each VM belongs to and puts its MAC address into the corresponding end-system group in Extreme Management Center. For this feature to work, end-system groups with the exact same name as the virtual networks from Hyper-V must exist within Extreme Management Center and the description field must contain “sync=true”.

Connect Domains

The Domains tab allows you to search for a particular end-system in all of the network monitoring modules on your network across multiple instances of Extreme Management Center based on a variety of criteria. In addition, you can configure user membership in end-system groups based on MAC address, allowing you to quickly authorize end-systems in your Extreme Access Control solution to allow network access across all modules.



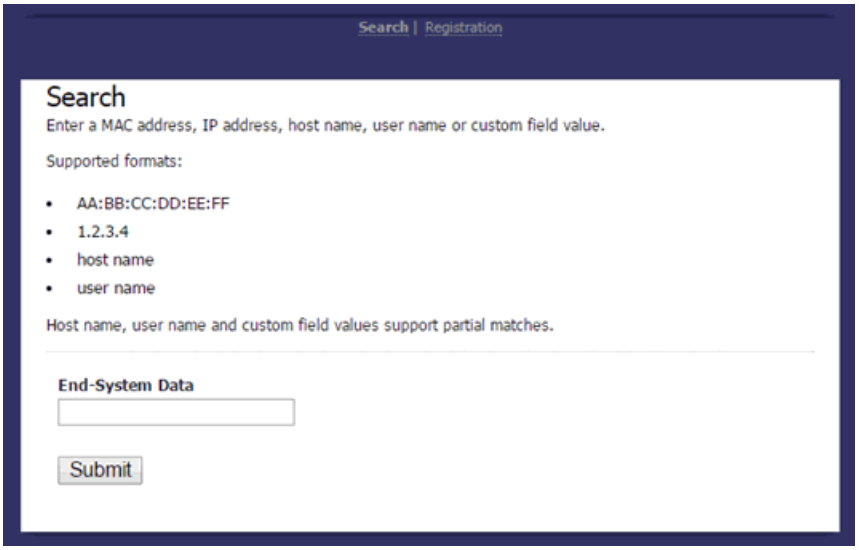
The Domains tab contains two sub-tabs:

- Search — Allows you to search for an end-system across multiple versions of Extreme Management Center in all modules using the following criteria:
  - MAC address
  - IP address
  - Hostname
  - Username
  - Custom Field (user-defined value)

- Registration — Allows you to add a MAC address to an end-system group or remove existing MAC addresses from an end-system group. These end-system groups can then be used to allow or deny access in all modules.

Search

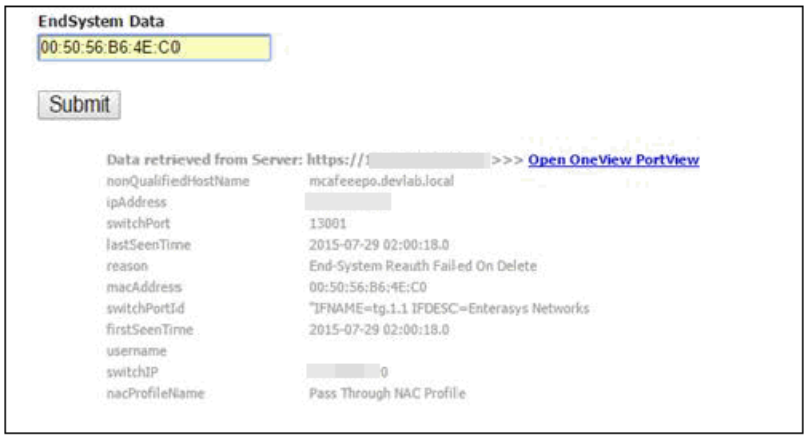
The Search tab allows you to search for a particular end-system in all of your supported network monitoring and network control modules in all versions of Extreme Management Center on your network.



End-System Data

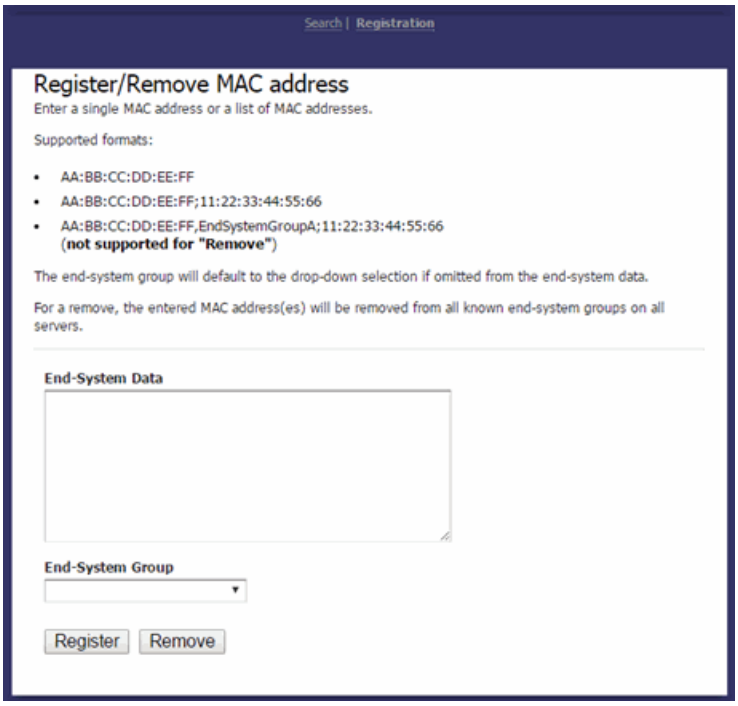
Enter a MAC address, hostname, username, or custom field value (a user-defined field) and click Submit to find an end-system on your network.

Once an end-system is returned, you can open the device to which it is connected in PortView.



Registration

The **Registration** tab allows you to add end-systems to end-system groups by entering lists of MAC addresses or remove end-systems from existing groups. End-system groups allow you to quickly create rules for different groups of end-systems you can use to configure appropriate network access in your Extreme Access Control solution.



End-System Data

Enter a MAC address or multiple MAC addresses separated by a semi-colon to add them to the end-system group selected in the End-System Group drop-down menu.

You can also enter end-systems with the end-system groups to which they are being added separated by a comma (e.g. AA:BB:CC:DD:EE:FF,*<End-SystemGroupName>*). Any end-systems added without their end-system group specifically listed are added to the group selected in the **End-System Group** drop-down menu.

End-System Group

Select the end-system group into which you are adding the end-systems associated with the MAC addresses listed in the End-System Data field. This field displays all end-system groups from all servers in Extreme Management Center.

Register Button

Click the **Register** button to add the end-system MAC addresses to the end-system group listed in the **End-System Data** field or selected in the **End-System Group** drop-down menu.

Remove Button

Click the **Remove** button to remove the end-system MAC addresses from the end-system group listed in the **End-System Data** field or selected in the **End-System Group** drop-down menu.

Once the end-system group is created, use the Extreme Access Control tab to configure network access rules for the end-systems in the group.

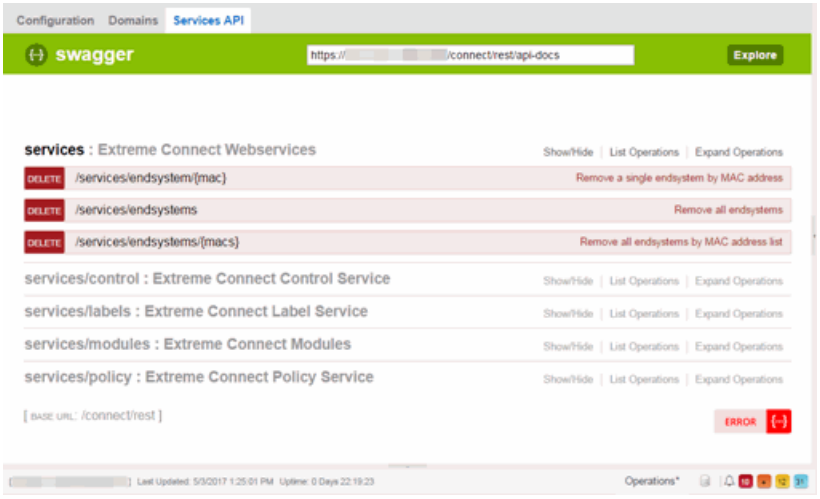
Related Information

For information on related tabs:

- Extreme Management Center Connect Overview
- Configuration

Connect Services API

The **Services API** tab allows you to execute a client/server application, known as a web service.



The available web services are organized based on the type of function they perform:

- Inventory Web Services — Perform Inventory Manager functions (e.g. backups or retrieving device properties).
- NAC Configuration Web Services — Perform Extreme Access Control configuration functions.
- NAC End-System Web Services — Retrieve and modify Extreme Access Control services, with a focus on accessing end-systems.
- NAC Web Services — Retrieve and modify general Extreme Access Control services.
- NetSight Device Web Services — Retrieve and modify the devices in the Extreme Management Center database.
- Policy Web Services — Perform Policy Manager functions.
- Purview Web Services — Retrieve and modify Application Analytics data and configuration.
- Reporting Web Services — Retrieve and modify the Extreme Management Center reporting engine data configuration.

Related Information

For information on related tabs:

- Extreme Management Center Connect Overview
- Configuration

Inventory Web Service

The Inventory web service provides an external interface to expose Inventory Manager functions such as performing backups or retrieving device properties. The Inventory web service description language is available at:

https://<ManagementCenterServerIP>:<Port>/axis/services/InventoryWebService?wsdl

Method: backupDeviceConfiguration

Method: backupDeviceConfigurationArchive

Method: getDeviceProperties

Method: backupDeviceConfiguration

Backup device configuration.

Parameters

Name	Type	Description
ipAddress	string	IP address of the device

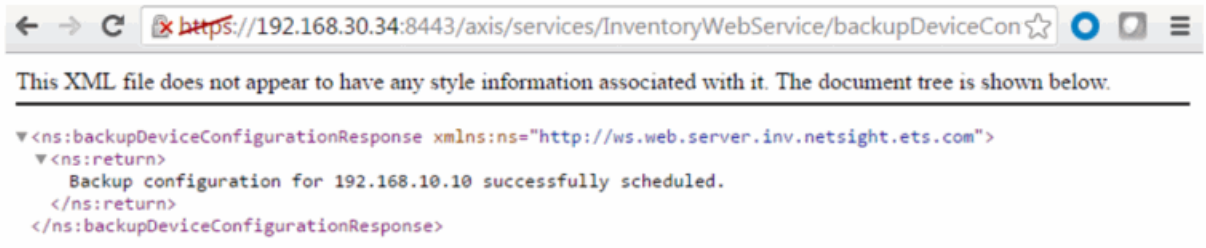
Returns

Returns status message.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/InventoryWebService/backupDeviceConfiguration?ipAddress=192.168.10.10



Method: backupDeviceConfigurationArchive

Backup device configuration.

Parameters

Name	Type	Description
ipAddress	string	IP address of the device
archiveName	string	Archive name

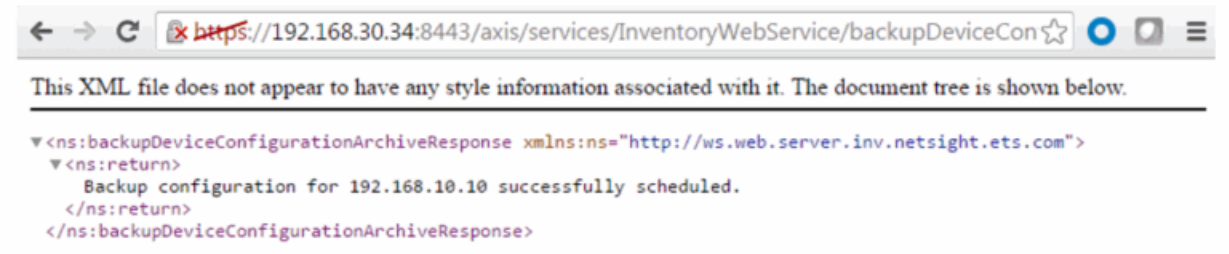
Returns

Returns status message.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/InventoryWebService/backupDeviceConfigurationArchive?ipAddress=192.168.10.10&archiveName=Web Service Archive



Method: getDeviceProperties

Returns device information/properties.

Parameters

Name	Type	Description
ipAddress	string	IP address of the device

Returns

Returns a WsDeviceProperty with a structure defined by the following table.

Name	Type	Description
baseMac	string	Base MAC address of the switch
chassisId	string	Chassis ID of the switch
chassisType	string	Chassis type
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text

Name	Type	Description
firmware	string	Firmware version installed on the switch
hostName	string	Hostname of the switch
ip	string	IP address of the switch
module	WsModulePropertyResult	Additional switch data
success	boolean	True if operation is successful
sysLocation	string	Switch sysLocation value

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/InventoryWebService/getDeviceProperties?ipAddress=192.168.10.10

Method: getDevicePropertiesWithRefresh

Force a refresh and return the device information/properties.

Parameters

Name	Type	Description
ipAddress	string	IP address of the device

Returns

Returns a WsDeviceProperty with a structure defined by the following table.

Name	Type	Description
baseMac	string	Base MAC address of the switch
chassisId	string	Chassis ID of the switch
chassisType	string	Chassis type
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
firmware	string	Firmware version installed on the switch
hostName	string	Hostname of the switch
ip	string	IP address of the switch
module	WsModulePropertyResult	Additional switch data
success	boolean	True if operation is successful
sysLocation	string	Switch sysLocation value

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/InventoryWebService/getDevicePropertiesWithRefresh?ipAddress=192.168.10.10

Method: refreshDevice

Refresh the device.

Parameters

Name	Type	Description
ipAddress	string	IP address of the switch

Returns

Returns a NsWsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

Method: test

Test operation that returns back the current time.

Returns

Returns current time.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/InventoryWebService/test

NAC Configuration Web Service

The NAC configuration web service provides an external interface to manage Extreme Access Control's configuration data. The NAC configuration web service description language is available at:

https://<ExtremeManagementCenterServer>:<port>/axis/services/NACConfigurationWebService?wsdl

Method: createDCMVirtualAndPhysicalNetwork

Create a virtual and physical network configuration. This operation creates Extreme Access Control rules, profile, policy mapping, policy role, and VLANs for the Extreme Management Center configuration and domain. Enforce the configuration changes after executing the web service.

Parameters

Name	Type	Description
name	string	Name used for the Extreme Access Control rule, profile, and policy mapping
nacConfig	string	Extreme Access Control configuration name
domain	string	Domain name
isPrivateVlan	boolean	Set to **true** if it is a private VLAN
primaryVlanId	int	Primary VLAN ID
secondaryVlanId	int	Secondary VLAN ID, only required if **isPrivateVlan** is set to **true**. Otherwise it can be set to **-1**
mode	string	VLAN type, available options are: -promiscuous -isolated -community
forwardAsTagged	boolean	Set to **true** for forwarding tagged packets
swGroup	string	Switch group name
nic	string	Network adapter name
isSync	boolean	Set to **true** to synchronize physical and virtual fabric
isApproval	boolean	Set to **true** to approve workflow

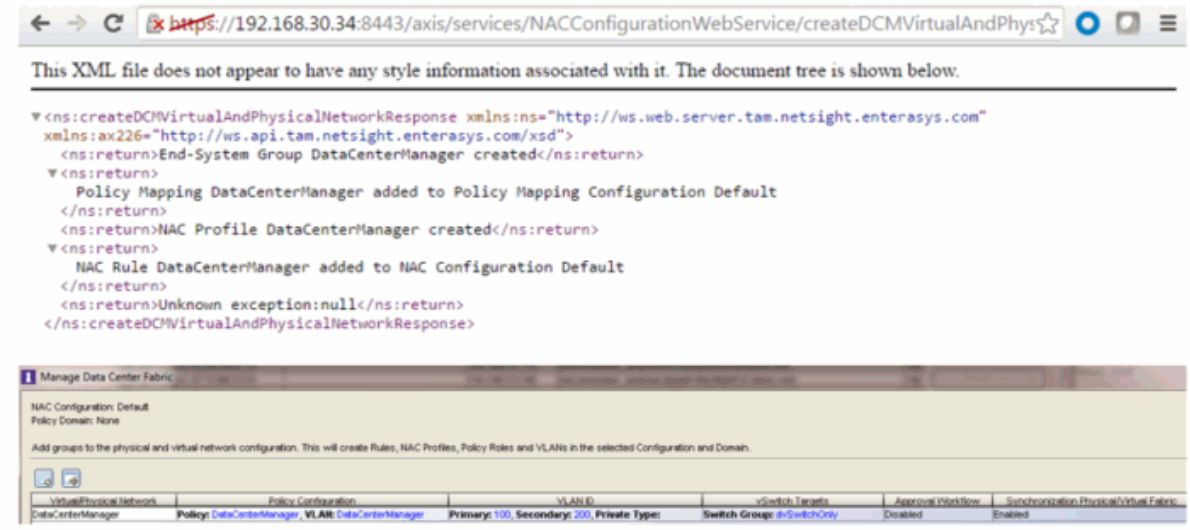
Returns

Returns a string status describing whether the operation is successful.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACConfigurationWebService/createDCMVirtualAndPhysicalNetwork?name=DataCenterManager&nacConfig=Default&domain=Default&isPrivateVlan=true&primaryVlanId=100&secondaryVlanId=200&mode=promiscuous&forwardAsTagged=true&swGroup=dvSwitchOnly&nic=Default&isSync=true&isApproval=false



Method: createSwitch

Create a switch in the Extreme Access Control configuration.

Parameters

Name	Type	Description
nacApplianceGroup	string	Extreme Access Control engine group for the switch
ipAddress	string	IP address of the switch

Name	Type	Description
switchType	string	Type of switch, a null or empty value will default to Layer 2 Out of Band. Available options are: -Layer 2 Out-Of-Band -Layer 2 Out-Of-Band Data Center -Layer 2 Out-Of-Band with PEPs -Layer 2 Controller PEP -Layer 2 RADIUS Only -Layer 3 Out-Of-Band -Layer 3 Controller PEP -VPN
primaryGateway	string	IP address of primary Extreme Access Control engine
secondaryGateway	string	IP address of secondary Extreme Access Control engine
tertiaryGateway	string	IP address of the third Extreme Access Control engine
quaternaryGateway	string	IP address of the fourth Extreme Access Control engine
authType	string	Authentication type, a null or empty value defaults to Network Access. Available options are: -Any Access -Management Access -Network Access -Monitoring - RADIUS -Accounting -Manual RADIUS Configuration
attrsToSend	string	Gateway RADIUS attributes to send, a null or empty value defaults to Extreme Policy
isRadiusAccountingEnabled	boolean	Set to true to enable RADIUS accounting
managementRadiusServer1	string	Management RADIUS server 1, only available when **authType** is set to **Network Access**

Name	Type	Description
managementRadiusServer2	string	Management RADIUS server 2, only available when **authType** is set to **Network Access**
policyDomain	string	Policy domain
pep1	string	Policy enforcement point 1, only available when **switchType** is set to **VPN**
pep2	string	Policy enforcement point 2, only available when **switchType** is set to **VPN**

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Method: createVirtualAndPhysicalNetwork

Create a virtual and physical network configuration. This operation creates an Extreme Access Control rule, profile, policy mapping, policy role, and VLANs for the Extreme Access Control configuration and domain. Enforce configuration changes after executing the web service.

Parameters

Name	Type	Description
name	string	Name used for the Extreme Access Control rule, profile, and policy mapping
nacConfig	string	Extreme Access Control configuration name
domain	string	Domain name
isPrivateVlan	boolean	Set to **true** if it is a private VLAN
primaryVlanId	int	Primary VLAN ID

Name	Type	Description
secondaryVlanId	int	Secondary VLAN ID, only required if **isPrivateVlan** is set to **true**. Otherwise it can be set to -1
mode	string	VLAN type, available options are: -promiscuous -isolated -community
forwardAsTagged	boolean	Set to **true** for forwarding tagged packets

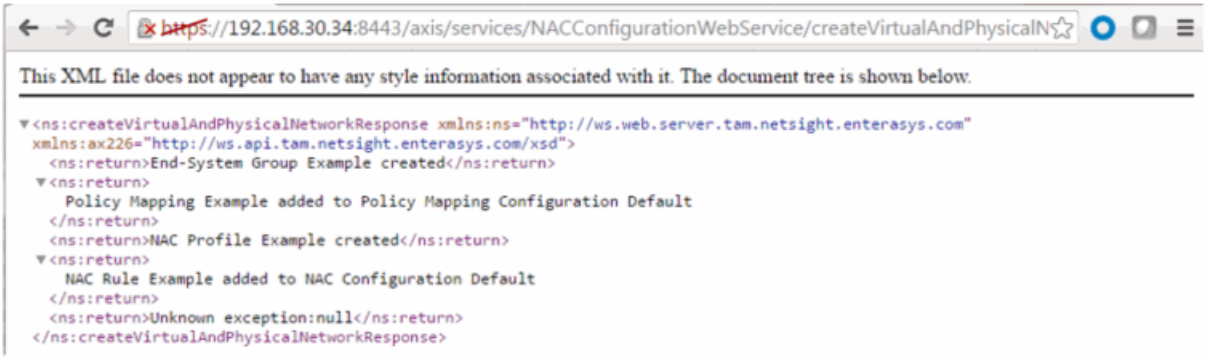
Returns

Returns a string status describing whether the operation is successful.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACConfigurationWebService/createVirtualAndPhysicalNetwork?name=Example&nacConfig=Default&domain=Default&isPrivateVlan=true&primaryVlanId=100&secondaryVlanId=200&mode=promiscuous&forwardAsTagged=true



Method: deleteSwitch

Delete switch from Extreme Access Control configuration.

Parameters

Name	Type	Description
ipAddress	string	IP address of the switch

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACConfigurationWebService/deleteSwitch?ipAddress=192.168.10.10

Method: updateSwitch

Update switch in the Extreme Access Control configuration.

Parameters

Name	Type	Description
nacApplianceGroup	string	Extreme Access Control engine group for the switch
ipAddress	string	IP address of the switch

Name	Type	Description
switchType	string	Type of switch, a null or empty value defaults to Layer 2 Out of Band. Available options are: -Layer 2 Out-Of-Band -Layer 2 Out-Of-Band Data Center -Layer 2 Out-Of-Band with PEPs -Layer 2 Controller PEP -Layer 2 RADIUS Only -Layer 3 Out-Of-Band -Layer 3 Controller PEP -VPN
primaryGateway	string	IP address of primary Extreme Access Control engine
secondaryGateway	string	IP address of secondary Extreme Access Control engine
tertiaryGateway	string	IP address of a third Extreme Access Control engine
quaternaryGateway	string	IP address of a fouth Extreme Access Control engine
authType	string	Authentication type, a null or empty value defaults to Network Access. Available options are: -Any Access -Management Access -Network Access -Monitoring - RADIUS Accounting -Manual RADIUS Configuration
attrsToSend	string	Gateway RADIUS attributes to send, a null or empty value defaults to Extreme Policy
isRadiusAccountingEnabled	boolean	Set to true to enable RADIUS accounting
managementRadiusServer1	string	Management RADIUS server 1, only available when **authType** is set to **Network Access**

Name	Type	Description
managementRadiusServer2	string	Management RADIUS server 2, only available when **authType** is set to **Network Access**
policyDomain	string	Policy domain
pep1	string	Policy enforcement point 1, only available when **switchType** is set to **VPN**
pep2	string	Policy enforcement point 2, only available when **switchType** is set to **VPN**

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation was successful

NAC End System Web Service

The NAC end system web service provides an external interface to retrieve and modify Extreme Management Center services. The end-system web service is very similar to the NAC web service; there are, however, additional operations for accessing end-systems. The NAC end-system web service description language is available at:

https://<Extreme Management Center IP>:<port>/axis/services/NACEndSystemWebService?wsdl

Method: addHostnameToEndSystemGroup

Add an end-system hostname to an Extreme Access Control end-system group. You can remove the hostname from other end-system groups.

Parameters

Name	Type	Description

Method: addIPToEndSystemGroup

Add an end-system IP address to an Extreme Access Control end-system group. You can remove the IP address from other end-system groups.

Parameters

Name	Type	Description
endSystemGroup	string	The end system group name changing
ipAddress	string	The IP address of the end-system

Name	Type	Description
description	string	Optional information stored in the end-system group with the IP address
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the IP address from other end-system groups

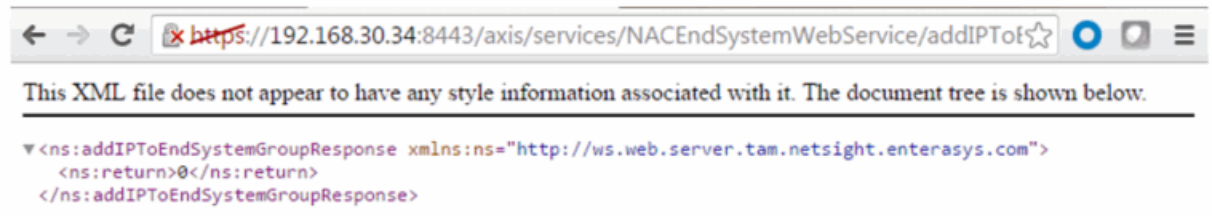
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/addIPToEndSystemGroup?endSystemGroup=Administrator-IP&ipAddress=192.168.10.180&description=Example-Web-Service&reauthorize=true&removeFromOtherGroups=true



Method: addMACsToEndSystemGroup

Add an end-system MAC address to an Extreme Access Control end-system group. You can remove the MAC address from other end-system groups and set the custom fields.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name changing
macs	string	The MAC address(es) of the end-system(s)
description	string	Optional information stored in the end-system group with the MAC address(es)
reauthorize	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the MAC address from other end-system groups

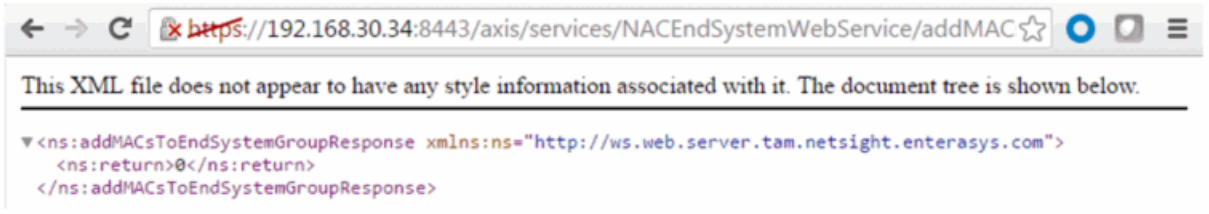
Returns

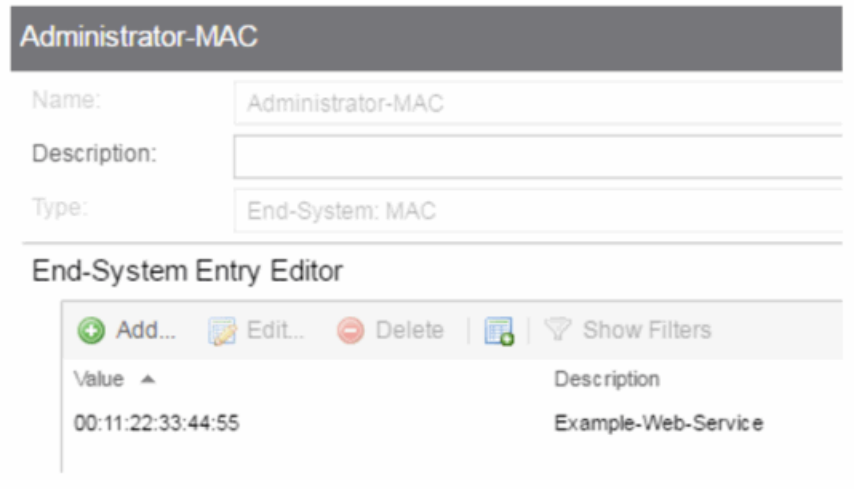
The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/addMACsToEndSystemGroup?endSystemGroup=Administrator-MAC&macs=00:11:22:33:44:55&descriptions=Example-Web-Service&reauthorize=true&removeFromOtherGroups=true





Method: addMACToBlacklist

Add an end-system MAC address to the Extreme Access Control blacklist end-system group. Force reauthentication on the end-system once it is blacklisted to limit network access.

Parameters

Name	Type	Description
mac	string	The MAC address of the end-system
description	string	Optional information stored in the end-system group with the MAC address
reauthorize	boolean	Set to **true** to force reauthentication on the affected end-system

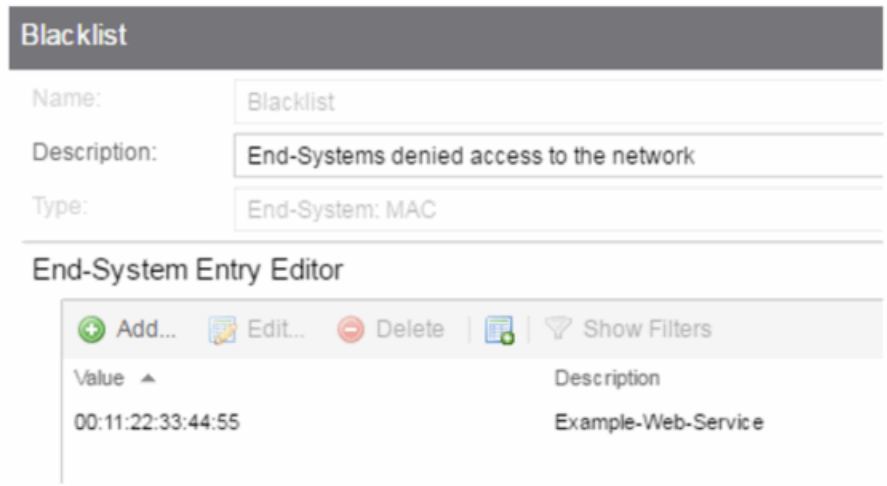
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/addMACToBlacklist?mac=00:11:22:33:44:55&description=Example-Web-Service&reauthorize=true



Method: addMACToEndSystemGroup

Add an end-system MAC address to an Extreme Access Control end-system group. You can remove the MAC address from other end-system groups and set the custom fields.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name changing
mac	string	The MAC address of the end-system
description	string	Optional information stored in the end-system group with the MAC address
reauthorize	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the MAC address from other end-system groups

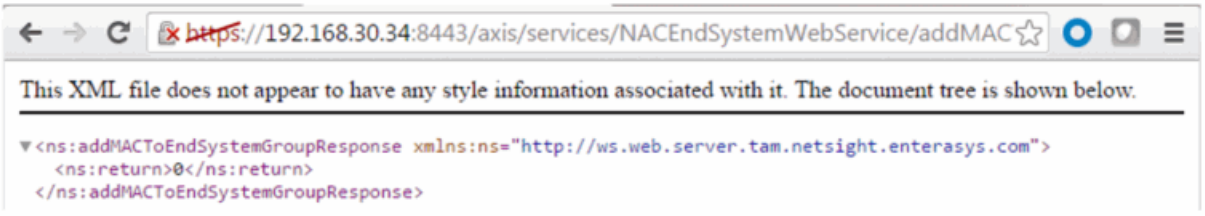
Returns

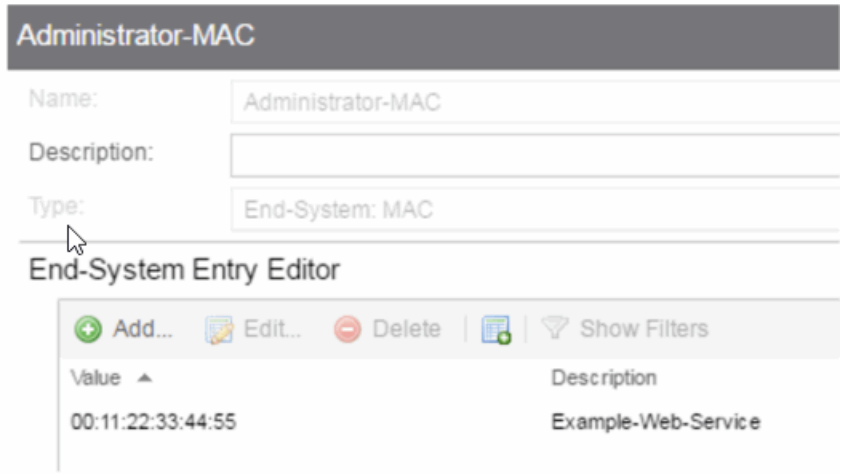
The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/addMACToEndSystemGroup?endSystemGroup=Administrator-MAC&mac=00:11:22:33:44:55&description=Example-Web-Service&reauthorize=true&removeFromOtherGroups=true





Method: addUsernameToUserGroup

Add an end-system username to an Extreme Access Control end-system group. You can remove the username from other end system groups.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name changing

Name	Type	Description
username	string	The username of the end-system
description	string	Optional information stored in the end-system group with the username
username	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the username from other end-system groups

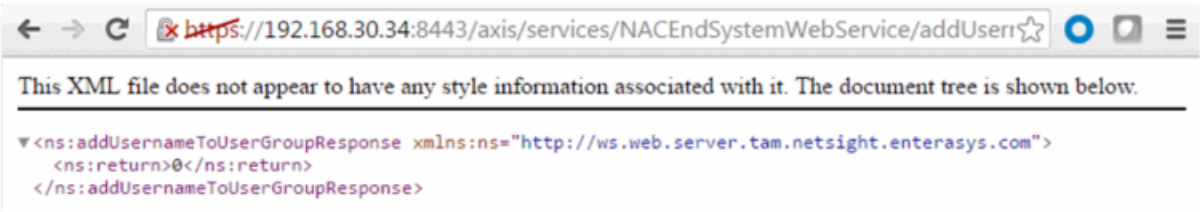
Returns

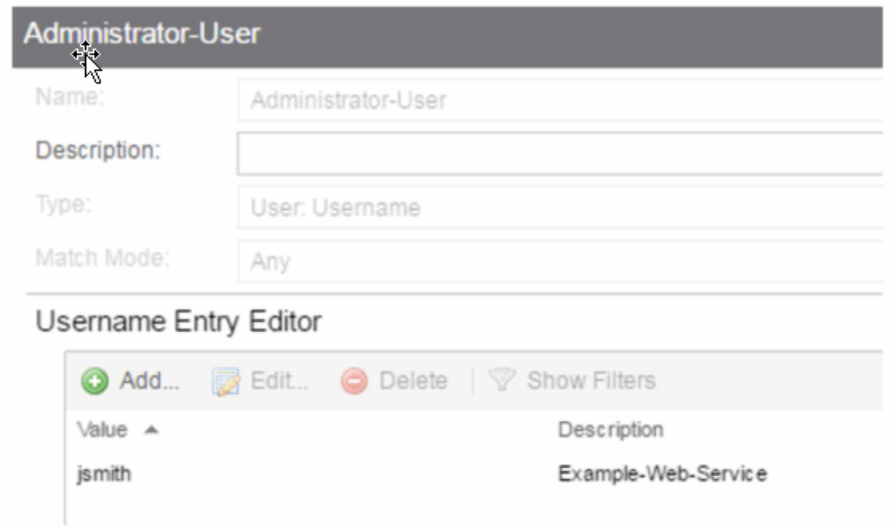
The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/addUsernameToUserGroup?endSystemGroup=Administrator-User&username=jsmith&description=Example-Web-Service&reauthorize=true&removeFromOtherGroups=true





Method: addValueToNamedList

Add a value to an Extreme Access Control end-system group. This is a generic operation so ensure you enter the correct value and end-system group. Adding to a MAC address based end-system group requires the value to be in a MAC address format. Adding an IP address to an IP based end-system group requires the value to be in an IP address format. Failure to use the correct value and end-system group can cause network access issues.

Parameters

Name	Type	Description
list	string	The end-system group changing
value	string	The value to add
description	string	Optional information stored in the end-system group with the value
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/addValueToNamedList?list=Administrator-User&value=jdoe&description=Example-Web-Service-ListName&reauthenticate=true&removeFromOtherGroups=true

Method: addValueToNamedListByWho

Add a value to an Extreme Access Control end-system group. This is a generic operation so ensure you enter the correct value and end-system group. Adding to a MAC address based end-system group requires the value to be in a MAC address format. Adding an IP address to an IP based end system group requires the value to be in an IP address format. Failure to use the correct value and end-system group can cause network access issues.

Parameters

Name	Type	Description
list	string	The end-system group changing
value	string	The value to add
description	string	Optional information stored in the end-system group with the value
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
byWho	string	User requesting the operation
fromWhere	string	Location of the request

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/addValueToNamedListByWho?list=Administrator-User&value=jdoe&description=Example-Web-Service-ListName&reauthenticate=true&removeFromOtherGroups=true&byWho=root&fromWhere=Extreme

Method: clearOldestEndSystemIp

Clear the IP address on all end-systems with the matching parameter.

Parameters

Name	Type	Description
ipAddress	string	IP address to clear

Returns

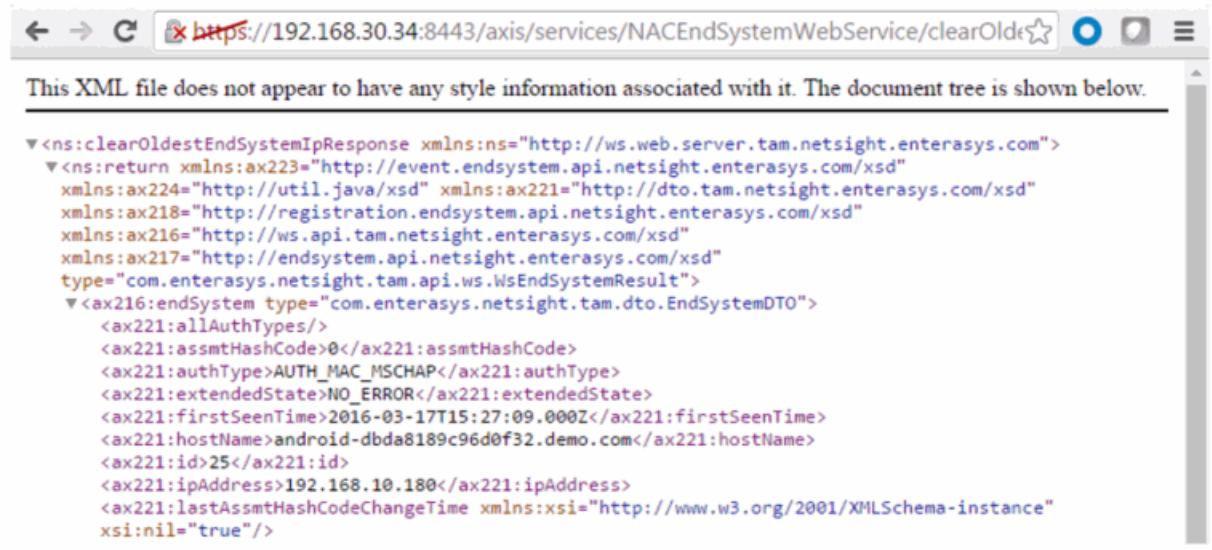
Returns WsEndSystemResult with a structure defined by the following table.

Name	Type	Description
endSystem	EndSystemDTO	End-system data
endSystemSwitchSupportsReauth	boolean	**True** if end-system supports reauthentication
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

The following web service is executed with a web browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/clearOldestEndSystemIp?ipAddress=192.168.10.180



Method: collectOsFamilyDataPointStats

Collect the current device types from the Extreme Access Control end-system table and store the results to the reporting database table.

Parameters

Name	Type	Description
overrideTimeStamp	long	Timestamp to store in the reporting database, in milliseconds

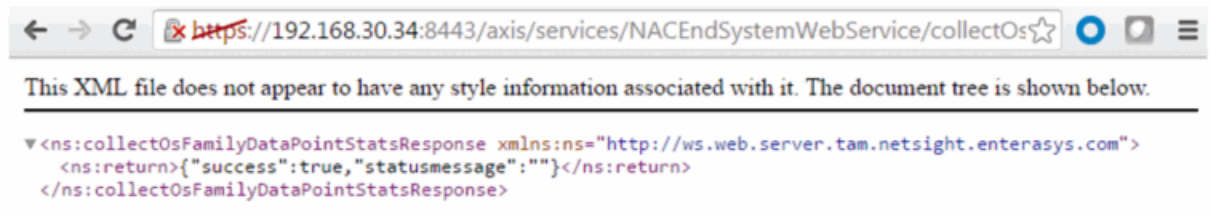
Returns

Returns a string status.

Example

The following web service is executed with a web browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/collectOsFamilyDataPointStats?overrideTimeStamp=1464015739000



Method: collectOsNameDataPointStats

Collect the current device families from the Extreme Access Control end-system table and store the results to the reporting database table.

Parameters

Name	Type	Description
overrideTimeStamp	long	Timestamp to store in the reporting database, in milliseconds

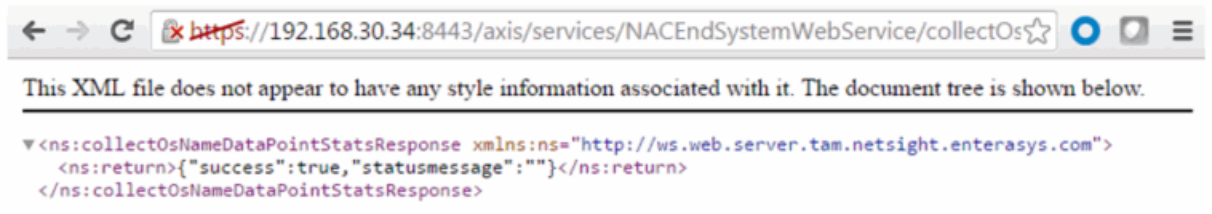
Returns

Returns a string status.

Example

The following web service is executed with a web browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/collectOsNameDataPointStats?overrideTimeStamp=1464015739000



method: createNamedList

Create a named list.

Parameters

Name	Type	Description
listName	string	Name of the named list
listType	string	The named list type, available options are: USERNAME LDAPUSERGROUP RADIUSUSERGROUP MAC IP HOSTNAME LOCATION TIMEOFWEEK
description	string	Description of the named list

Returns

The operation returns an integer error code.

Example

The following web service is executed with a web browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/createNamedList?listName=Example&listType=MAC&description=Web-Service-Example

Method: deleteEndSystemByMac

Delete end-system based on the end-system's MAC address.

Parameters

Name	Type	Description
mac	string	MAC address of the end-system to delete

Name	Type	Description
deleteOptionsMask	int	0x01 – Delete values in named lists 0x02 – Delete MAC locks 0x04 – Delete end-system information 0x08 – Delete registered devices 0x10 – Force delete of end-system

Returns

A return element having the structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/deleteEndSystemByMac?mac=50:7A:55:6F:24:35&deleteOptionsMask=16

Method: deleteEndSystemInfoByHostname

Delete end-system information record based on the end-system's hostname.

Parameters

Name	Type	Description
hostname	string	The hostname of the end-system

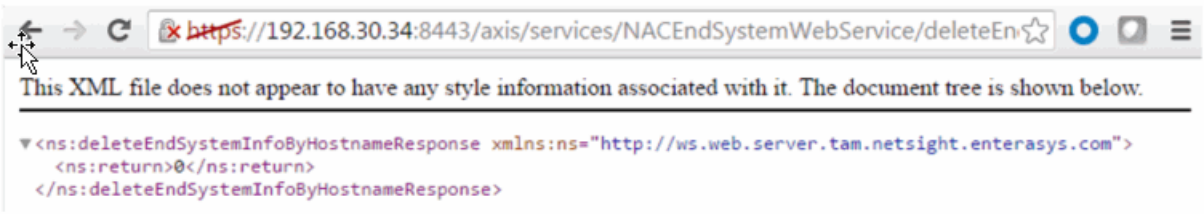
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/deleteEndSystemInfoByHostname?hostname=Captain-Obvious.demo.com



Method: deleteEndSystemInfoByIp

Delete end-system information record based on the end-system's IP address.

Parameters

Name	Type	Description
ipAddress	string	The IP address of the end-system

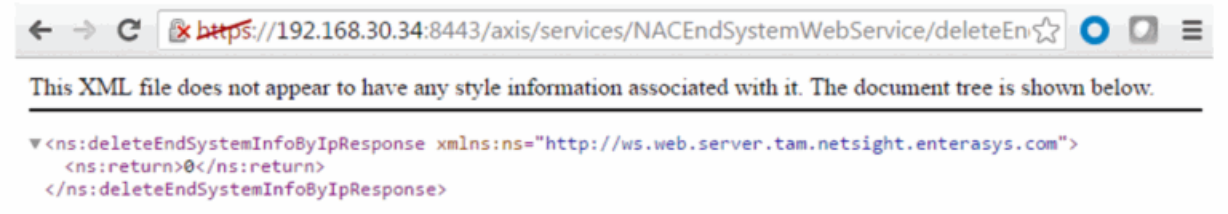
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/deleteEndSystemInfoByIp?ipAddress=192.168.10.180



Method: deleteEndSystemInfoByMac

Delete end-system information record based on the end-system's MAC address.

Parameters

Name	Type	Description
mac	string	The MAC address of the end-system

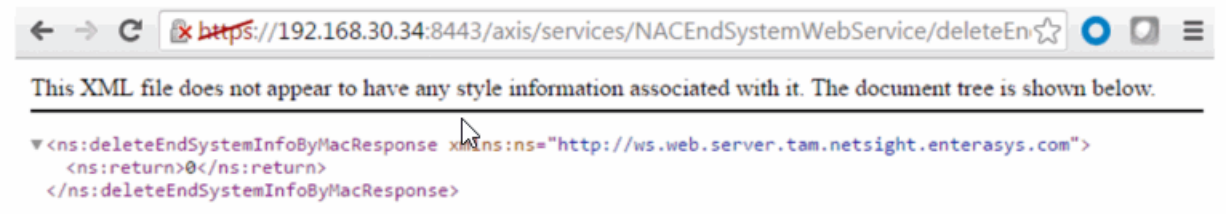
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/deleteEndSystemInfoByMac?mac=14:7D:C5:97:70:CB



Method: deleteEndSystemInfoEx

Delete end-system information record based on the end-system's MAC address. This operation is similar to deleteEndSystemInfoByMac but returns a verbose message.

Parameters

Name	Type	Description
macAddress	string	The MAC address of the end-system

Returns

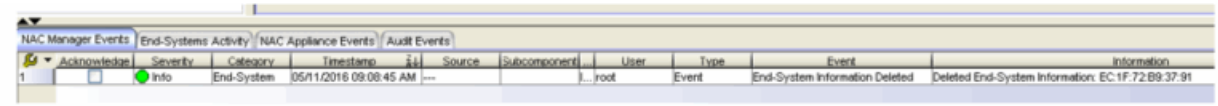
Returns a WsEndSystemInfoResult with a structure defined by the following table.

Name	Type	Description
endSystemInfo	EndSystemInfo	End-system from which information is deleted
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/deleteEndSystemInfoEx?macAddress=EC:1F:72:B9:37:91



Method: findEndSystem

Find end-systems in the database that match the given search criteria.

Parameters

Name	Type	Description
search	string	Search string, accept values are an IP address, MAC address, or username

Returns

Returns an array of end-systems that match the search criteria.

Example

Execute the following web-service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/findEndSystem?search=18:F6:43:0D:BE:59

Method: getAllEndSystemsAsProperties

Retrieve all end-system information as properties. Use the firstResult and maxResults parameters to paginate the end-systems returned by the web service.

Parameters

Name	Type	Description
firstResult	int	The first index in the query
maxResults	int	The maximum number of end-systems to return

Returns

Returns an array of end-systems.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getAllEndSystemsAsProperties?firstResult=0&maxResults=100

Method: getAllNacApplianceIpAddresses

Retrieve the IP addresses of all Extreme Access Control engines.

Returns

Returns an array of IP addresses.

Example

Execute the following web service with a browser:
https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getAllNacApplianceIpAddresses

Method: getAllNamedLists

Retrieve all the named lists and their descriptions.

Returns

Returns an array of named lists and their descriptions.

Example

Execute the following web service with a browser:
https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getAllNamedLists

Method: getDefaultConfigPolicyMappingEntries

Retrieve the policy mappings defined in the default policy mapping configuration.

Returns

Returns a list of policyMappingEntry objects.

Method: getEndSystemAgentServerList

Obtain a list of servers to which an agent connects to provide Extreme Management Center with information about end-systems known by the Extreme

Management Center server.

Parameters

Name	Type	Description
endSystemIp	string	IP address of the end-system
rawMacs	string	MAC addresses of the end-systems

Returns

Returns a list of assessment servers.

Method: getEndSystemAndHrByMac

Returns end system data, based on a MAC address, and it's most recent health result and vulnerabilities.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end system

Returns

Returns end-system data and most recent health result.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemAndHrByMac?macAddress=00:88:65:66:03:C1

Method: getEndSystemByIP

Return end-system data based on an IP address.

Parameters

Name	Type	Description
ipAddress	string	IP address of the end-system

Returns

Returns end-system data.

Example

Execute the following web-service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemByIP?ipAddress=192.168.10.190

Method: getEndSystemByIpEx

Return end-system data based on an IP address. The operation is similar to getEndSystemByIP, but returns additional information.

Parameters

Name	Type	Description
ipAddress	string	IP address of the end-system

Returns

Returns WsEndSystemResult with a structure defined by the following table.

Name	Type	Description
endSystem	EndSystemDTO	End-system data
endSystemSwitchSupportsReauth	boolean	**True** if end system supports reauthentication
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getEndSystemByIpEx?ipAddress=192.168.10.190

Method: getEndSystemByMac

Return end system data based on a MAC address.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end system

Returns

Returns end system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemByMac?macAddress=00:88:65:66:03:C1

Method: getEndSystemByMacEx

Return end-system data based on a MAC address. The operation is similar to getEndSystemByMac, but returns additional information.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

Returns

Returns WsEndSystemResult with a structure defined by the following table.

Name	Type	Description
endSystem	EndSystemDTO	End-system data
endSystemSwitchSupportsReauth	boolean	End-system data
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text

Name	Type	Description
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemByMacEx?macAddress=00:88:65:66:03:C1

Method: getEndSystemInfoByMacEx

Return end-system data based on a MAC Address. The data is returned as a set of comma-delimited key=value pairs. If there is an error, errorCode and errorString properties are encoded in the result.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

Returns

Returns a WsEndSystemInfoResult with a structure defined by the following table.

Name	Type	Description
endSystem	EndSystemDTO	End-system data
endSystemSwitchSupportsReauth	boolean	**True** if end-system supports reauthentication
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text

Method: getEndSystems

Retrieve 1 or more end-systems based on the MAC address.

Parameters

Name	Type	Description
macs	string	MAC addresses of the end-systems

Returns

Returns end system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystems?macs=00:88:65:66:03:C1&macs=80:D6:05:4A:D6:C4

Method: getEndSystemsByCustomFieldsFuzzy

Retrieve end-systems with custom fields that contain the specified search query.

Parameters

Name	Type	Description
search	string	Custom field string

Returns

Returns end-system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemsByCustomFieldsFuzzy?search=Custom

Method: getEndSystemsByLocationFuzzy

Retrieve end-systems connected to a device with the specified location (sysLocation).

Parameters

Name	Type	Description
search	string	sysLocation string

Returns

Returns end-system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemsByLocationFuzzy?search=AP

Method: getEndSystemsByQuery

Retrieve end-systems with custom fields that contain the specified search query. The search criteria is in the key=value,key=value format.

Parameters

Name	Type	Description
whereClause	string	Query string in key=value format

Returns

Returns end-system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemsByQuery?whereClause=custom4=Custom4

Method: getEndSystemsByUserName

Return end-system data based on a username.

Parameters

Name	Type	Description
userName	string	Username of the end system

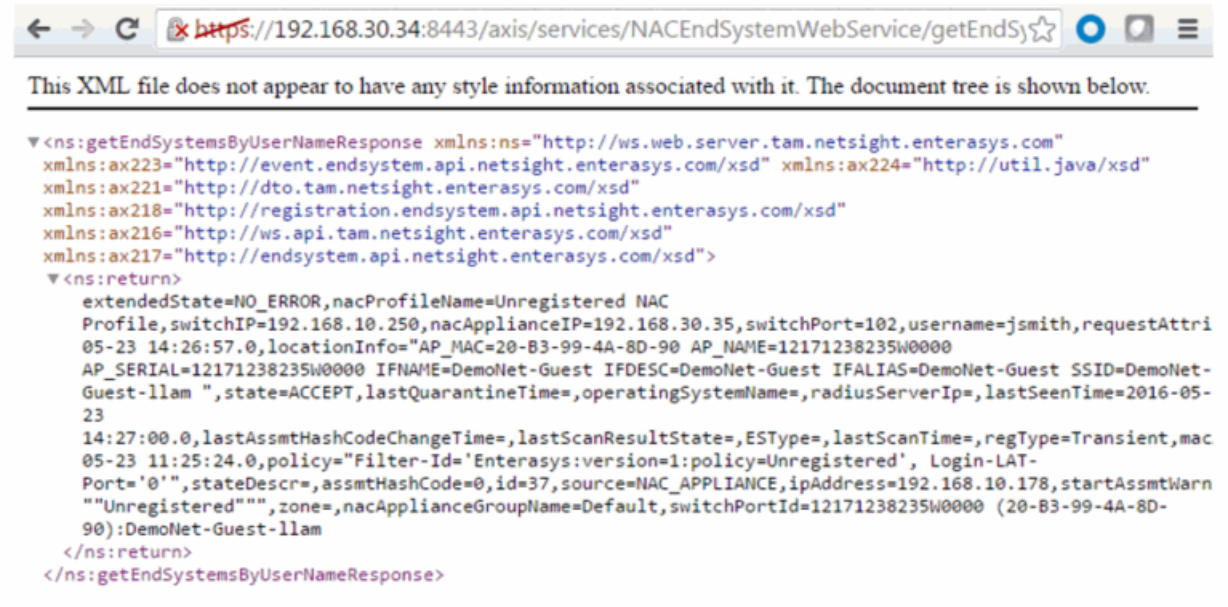
Returns

Returns end-system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemsByUserName?userName=jsmith



Method: getEndSystemsByUserNameEx

Return end-system data based on a username. This operation is similar to getEndSystemsByUserName, but returns a verbose message.

Parameters

Name	Type	Description
userName	string	Username of the end-system

Returns

Returns WsEndSystemListResult with a structure defined by the following table.

Name	Type	Description
endSystem	EndSystemDTO	End-system data
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation was successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemsByUserName?userName=jsmith

Method: getEndSystemsByUserNameFuzzy

Return end-system data that contains the specified username.

Parameters

Name	Type	Description
userName	string	Username of the end-system

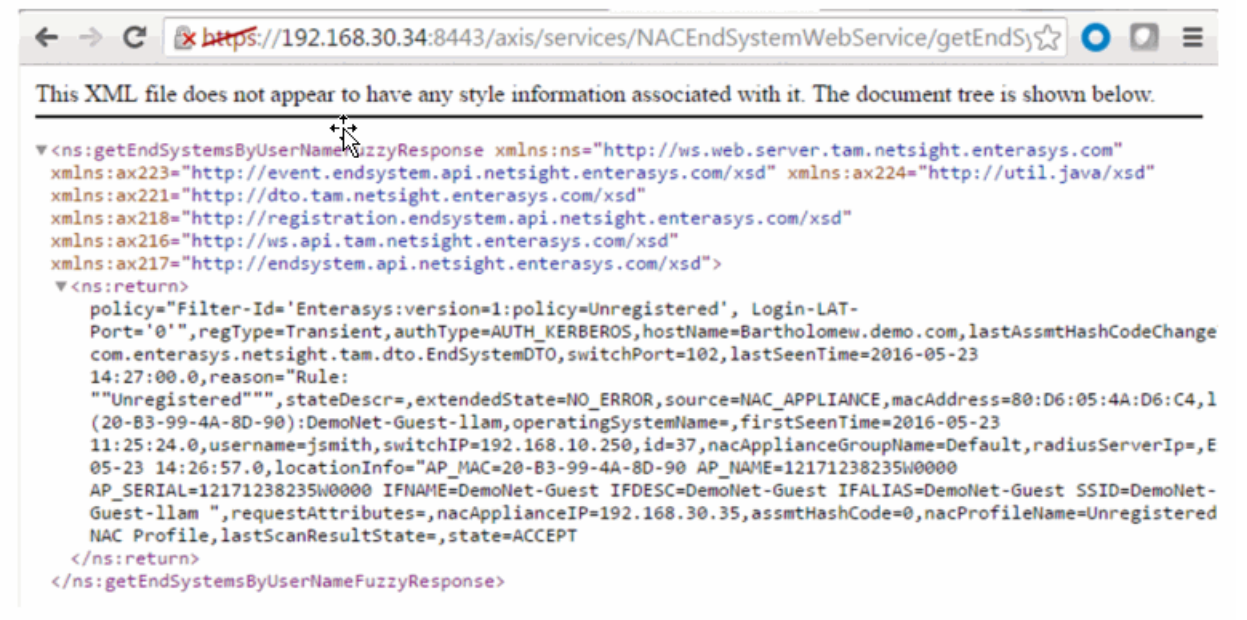
Returns

Returns end-system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemsByUserNameFuzzy?userName=smith



Method: getEndSystemTableData

Retrieve end-system table data as a JSON string.

Parameters

Name	Type	Description
start	int	Starting record index
limit	int	Number of end-systems to return
sort	string	Column ID to sort on
dir	string	Sort direction, options are: ASC – ascending DESC – descending
search	string	Search string
userName	string	Username used to determine zone access

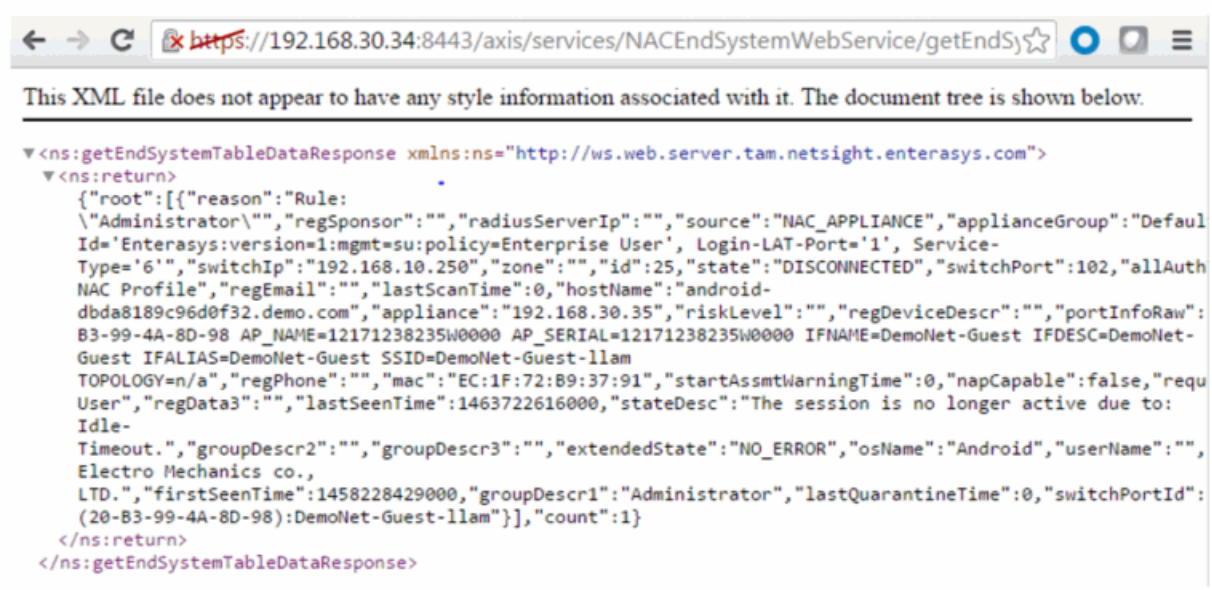
Returns

Returns end-system data in JSON format.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getEndSystemTableData?start=0&limit=100&sort=ipAddress&dir=ASC&search=180&userName=root



Method: getExtendedEndSystemArrByMac

Return an extended set of data (e.g. ELIN, portAlias) for an end-system based on a MAC address. The data is returned as a set of comma-delimited key=value pairs. If there is an error, errorCode and errorString properties will be encoded into the result.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

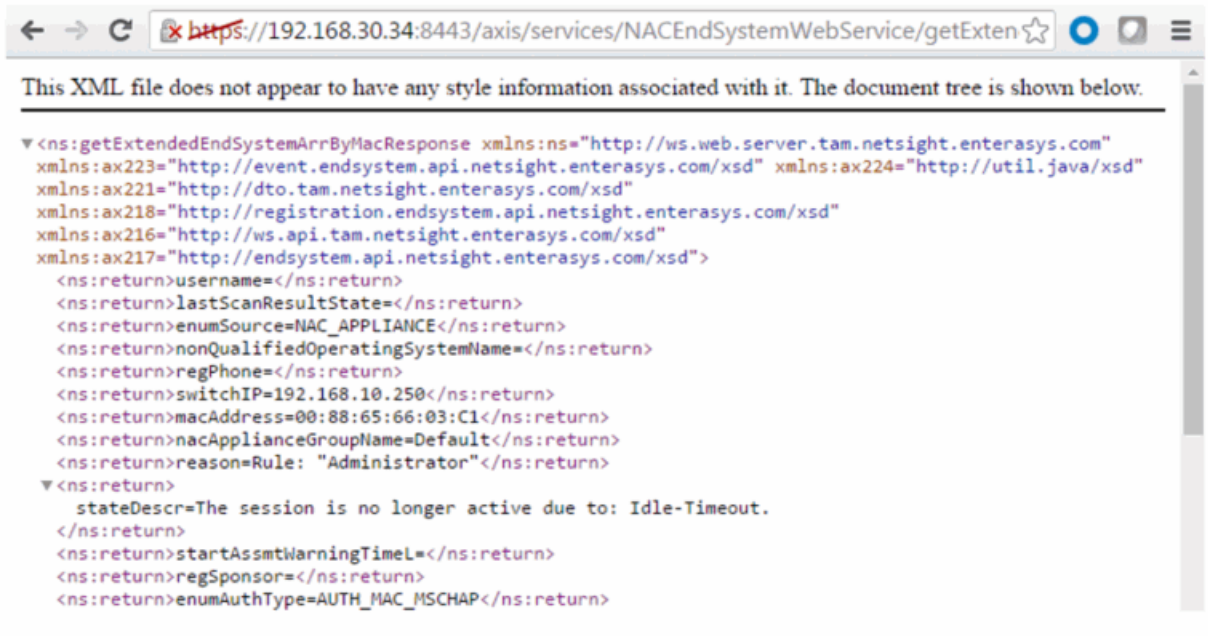
Returns

Returns an array of end-system data in key=value pair format.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getExtendedEndSystemArrByMac?macAddress=00:88:65:66:03:C1



I Method: getExtendedEndSystemByMac

Return an extended set of data (e.g. ELIN, portAlias) for an end-system based on a MAC address. The data is returned as a set of comma-delimited key=value pairs. If there is an error, errorCode and errorString properties are encoded into the result.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

Returns

Returns an extended set of end-system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getExtendedEndSystemByMac?macAddress=00:88:65:66:03:C1

Method: getNACVersion

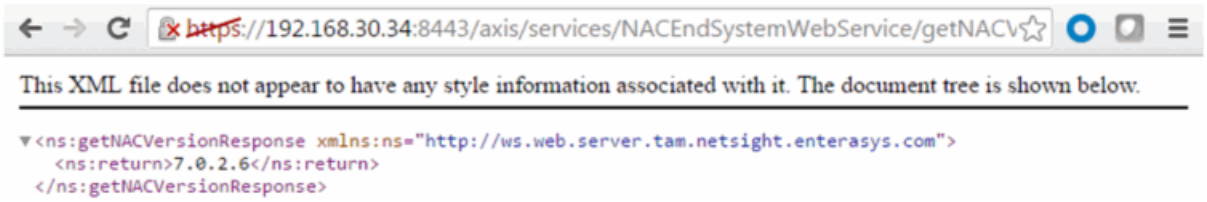
Return the Extreme Access Control version.

Returns

Returns Extreme Access Control version.

Example

Execute the following web service with a browser:
https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getNACVersion



Method: getNamedList

Retrieve a named list.

Parameters

Name	Type	Description
listName	string	Name of the named list

Returns

Returns a named list and its properties.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getNamedList?listName=Administrator

Method: getPollerStatus

Return the last polling status of an Extreme Access Control engine.

Parameters

Name	Type	Description
nacIP	string	IP address of an Extreme Access Control engine

Returns

Returns **true**/**false** for the Extreme Access Control engine's last polling status.

Example

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getPollerStatus?nacIP=192.168.30.35

Method: getUnsurfacedNamedList

Return the contents of a named list/end system group without manipulation.

Parameters

Name	Type	Description
listName	string	End-system group name

Returns

Returns a string array that contains the XML representation of values, description, and data.

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/getUnsurfacedNamedList?listName=Registered Guests

Method: processFlattenedWsEndSystemEvents

Method to process incoming end-system events from a source. These events are passed as a flattened end-system events.

Parameters

Name	Type	Description
flattenedEvents	string	List of flattened end-system events

Returns

Returns null for a successful operation or an error message.

Method: processNacRequestArrFromCsv

Process Extreme Access Control requests from a CSV file.

Parameters

Name	Type	Description
csvData	string	The CSV data must be in the following format: Reauthentication operation – MAC address End system override (FULL_MAC) – MAC address, end system group, description End system override (FULL_IP) – IP address, end system group, description End system override (HOSTNAME) – hostname, end system group, description User override – username, user group, description
oper	string	Operation request, available options are: reauth – force reauthentication esoverride – end system override useroverride – user override
isAdd	boolean	**True** for adding the request, **false** for deleting it
type	string	End system types, options are: FULL_MAC FULL_IP HOSTNAME

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation was successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/processNacRequestArrFromCsv?csvData=50:7A:55:6F:24:35,iOS,Web-Service-Example&oper=esoverride&isAdd=true&type=FULL_MAC

Method: processNacRequestFromCsv

Process Extreme Access Control requests from a CSV file.

Parameters

Name	Type	Description
csvData	string	The CSV data must be in the following format: Reauthentication operation – MAC address End-system override (FULL_MAC) – MAC address, end system group, description End-system override (FULL_IP) – IP address, end system group, description End-system override (HOSTNAME) – hostname, end system group, description User override – username, user group, description
oper	string	Operation request, available options are: reauth – force reauthentication esoverride – end system override useroverride – user override
isAdd	boolean	**True** for adding the request, **false** for deleting it
type	string	End-system types, options are: FULL_MAC FULL_IP HOSTNAME

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation was successful

Example

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/processNacRequestFromCsv?csvData=50:7A:55:6F:24:35,iOS,Web-Service-Example&oper=esoverride&isAdd=true&type=FULL_MAC

Method: processWsEndSystemEvents

Method to process incoming end-system events from a source. These events are passed in as flattened end-system events.

Parameters

Name	Type	Description
events	WsEndSystemEvent	List of flattened end system events

Returns

Returns null for a successful operation or an error message.

Method: reauthenticate

Force an end system to reauthenticate.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system
assess	boolean	True to reassess the end-system

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/reauthenticate?macAddress=80:D6:05:4A:D6:C4&assess=false

Method: reauthenticateMacs

Force reauthentication on multiple end-systems.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system
assess	boolean	True to reassess the end-system

Returns

Returns an array of error codes.

Example

Execute the following web service with a web browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/reauthenticateMacs?macAddresses=80:D6:05:4A:D6:C4&macAddresses=50:7A:55:6F:24:35&assess=false

Method: reauthenticateMacsBulk

Force reauthentication on multiple end-systems.

Parameters

Name	Type	Description
macAddresses	string	MAC address of the end-systems
reason	string	Brief reason for the reauthentication
assess	boolean	True to reassess the end-system

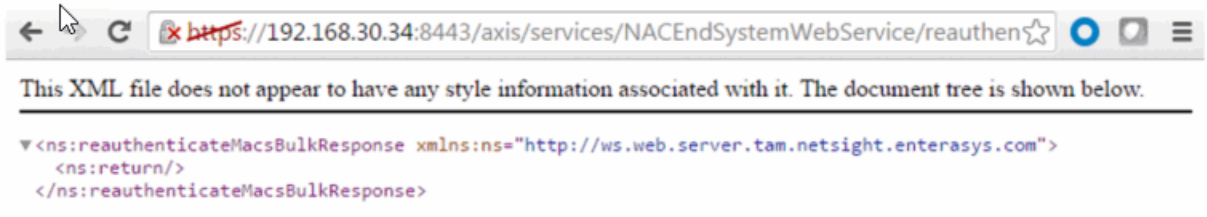
Returns

Returns an empty status.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/reauthenticateMacsBulk?macAddresses=80:D6:05:4A:D6:C4&macAddresses=50:7A:55:6F:24:35&reason=Example-Web-Service&assess=false



Method: reauthenticateMacsWithReason

Force reauthentication on multiple end-systems.

Parameters

Name	Type	Description
macAddresses	string	MAC address of the end-systems
reauthReasonStr	string	Brief reason for the reauthentication
assess	boolean	True to reassess the end-system

Returns

Returns an array of error codes.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/reauthenticateMacsWithReason?macAddresses=80:D6:05:4A:D6:C4&macAddresses=50:7A:55:6F:24:35&reauthReasonStr=Example-Web-Service&assess=false

Method: reauthenticateWithReason

Force an end-system to reauthenticate.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system
reauthReasonStr	string	Brief reason for the reauthentication
assess	boolean	True to reassess the end-system

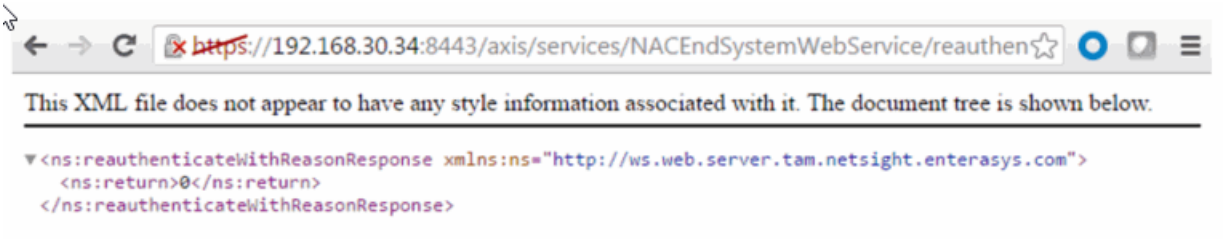
Returns

Returns an array of error codes.

Example

Execute the following web service with a web browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/reauthenticateWithReason?macAddress=80:D6:05:4A:D6:C4&reauthReasonStr=Example-Web-Service&assess=false



Method: registerAgentMacs

Register assessment agent MAC address.

Parameters

Name	Type	Description
macs	string	MAC address of the assessment agents
description	string	Description of the assessment agent(s)

Returns

Returns true for a successful registration.

Method: removeHostnameFromEndSystemGroup

Remove an end-system hostname from an Extreme Access Control end-system group.

Parameters

Name	Type	Description
endSystemGroup	string	End-system group name changing
hostname	string	The hostname of the end-system
reauthorize	boolean	Set to **true** to force reauthentication on the affected end-system

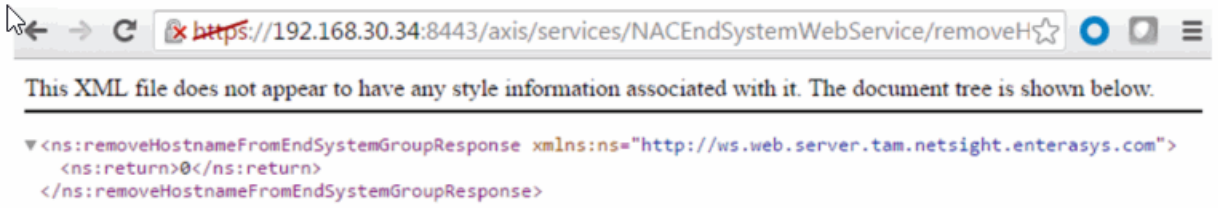
Returns

The operation returns an integer error code.

Example

Execute the following web service with a web browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/removeHostnameFromEndSystemGroup?endSystemGroup=iPhone&hostname=jdoe-iPhone&reauthorize=true



Method: removeIPFromEndSystemGroup

Remove an end-system IP address from an Extreme Access Control end-system group.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name changing
ip	string	IP address of the end-system
reauthorize	boolean	Set to **true** to force reauthentication on the affected end-system

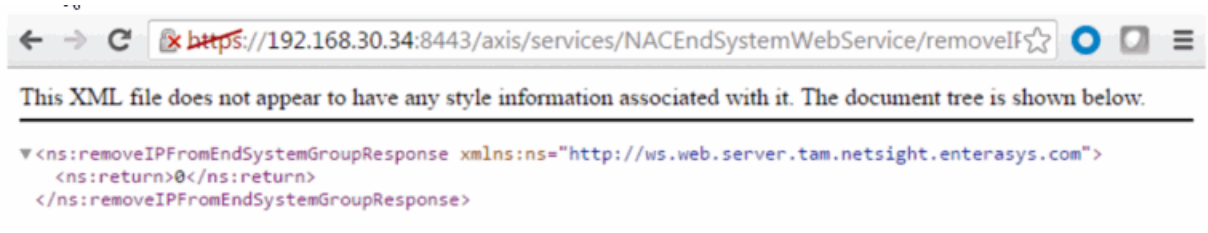
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/removeIPFromEndSystemGroup?endSystemGroup=Administrator-IP&ip=192.168.10.180&reauthorize=true



Method: removeMACFromBlacklist

Remove an end-system MAC address from the blacklist end-system group.

Parameters

Name	Type	Description
mac	string	MAC address of the end-system
reauthorize	boolean	Set to **true** to force reauthentication on the affected end-system

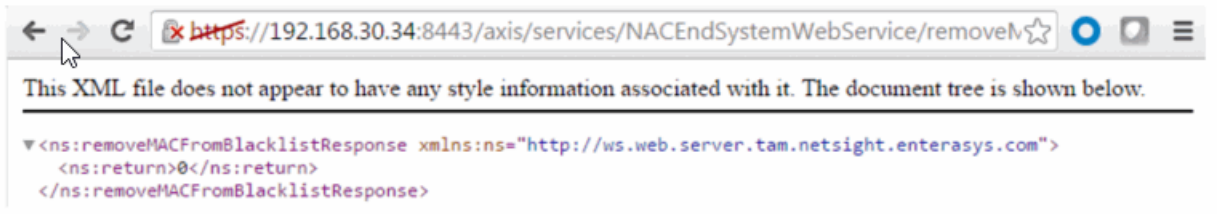
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/removeMACFromBlacklist?mac=00:11:22:33:44:55&reauthorize=true



Method: removeMACFromEndSystemGroup

Remove an end-system MAC address from an Extreme Access Control end-system group

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name changing
mac	string	MAC address of the end-system
reauthorize	boolean	Set to **true** to force reauthentication on the affected end-system

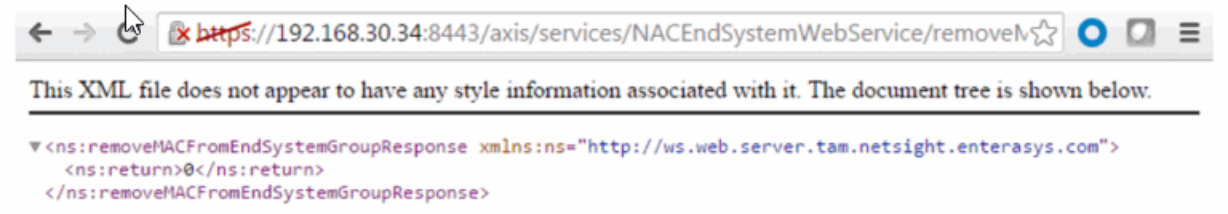
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/removeMACFromEndSystemGroup?endSystemGroup=iOS&mac=00:11:22:33:44:55&reauthorize=true



Method: removeMACsFromEndSystemGroup

Remove multiple end system MAC addresses from an Extreme Access Control end-system group

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name changing
macs	string	MAC address of the end-systems
reauthorize	boolean	Set to **true** to force reauthentication on the affected end-system

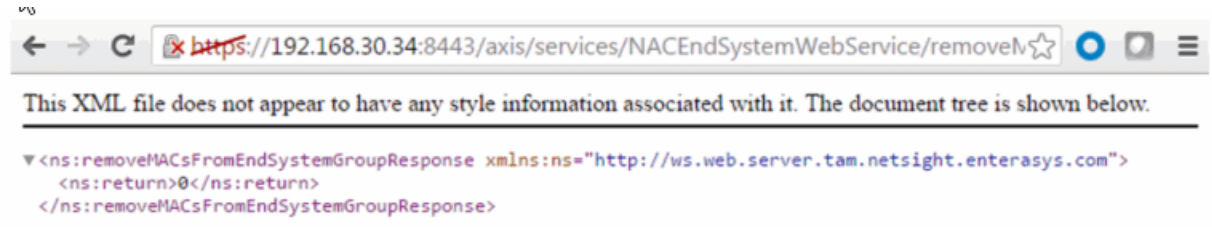
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/removeMACsFromEndSystemGroup?endSystemGroup=iOS&macs=00:11:22:33:44:55&macs=00:11:22:33:44:66&reauthorize=true



Method: removeNamedList

Remove a named list.

Parameters

Name	Type	Description
listName	string	Name of the named list

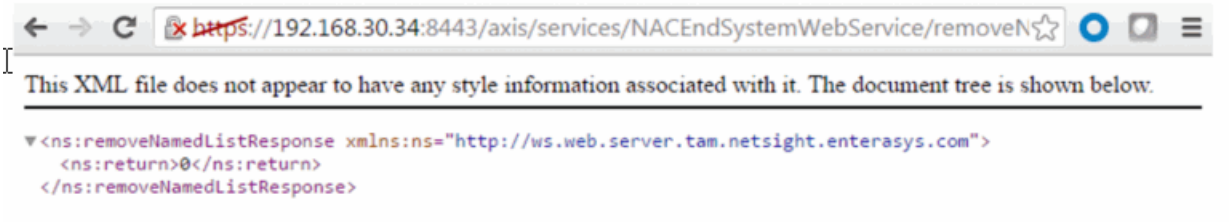
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/removeNamedList?listName=iPhone



Method: removeUsernameFromUserGroup

Remove a username from an Extreme Access Control end-system group.

Parameters

Name	Type	Description
endSystemGroup	string	The name of the end-system group you are changing
username	string	Username of the end-system
reauthorize	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/removeUsernameFromUserGroup?endSystemGroup=Administrator-User&username=jsmith&reauthorize=true

Method: removeValueFromNamedList

Remove a value to an Extreme Access Control end-system group. This is a generic operation so ensure you enter the correct value and end-system group.

Parameters

Name	Type	Description
list	string	The end-system group changing
value	string	The value to add
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

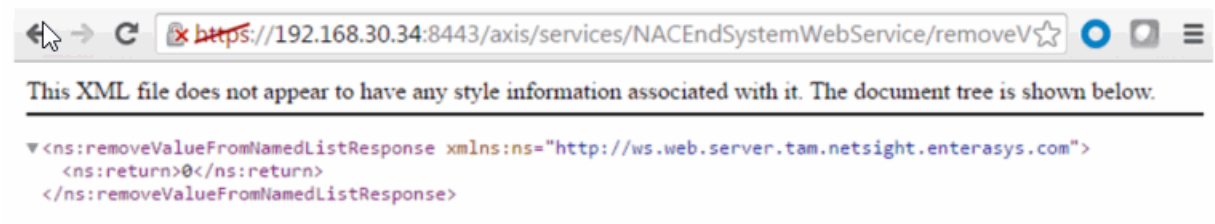
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/removeValueFromNamedList?list=iOS&value=50:7A:55:6F:24:35&reauthenticate=true



Method: removeValueFromNamedListByWho

Remove a value to an Extreme Access Control end-system group. This is a generic operation, so ensure you use the correct value and end-system group.

Parameters

Name	Type	Description
list	string	The end system group you are changing
value	string	The value to add
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
byWho	string	User requesting the operation
fromWhere	string	Location of the request

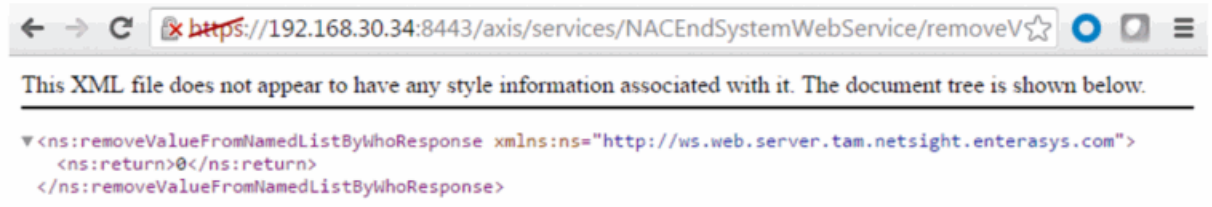
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/removeValueFromNamedListByWho?list=iOS&value=50:7A:55:6F:24:35&reauthenticate=true&byWho=root&fromWhere=Extreme



Method: saveEndSystemInfo

Update end system information. The end-system is identified by using the macAddress, ipAddress, or hostname property.

Parameters

Name	Type	Description
propString	string	Custom field data in custom1=value1,custom2=value2,custom3=value3,custom4=value4 format

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/saveEndSystemInfo?propString=macAddress=EC:1F:72:B9:37:91,custom1=Custom1,custom2=Custom2,custom3=Custom3,custom4=Custom4

Method: saveEndSystemInfoByHostname

Update end system information.

Parameters

Name	Type	Description
hostname	string	The hostname of the end-system
custom1	string	Custom field 1 value
custom2	string	Custom field 2 value
custom3	string	Custom field 3 value
custom4	string	Custom field 4 value

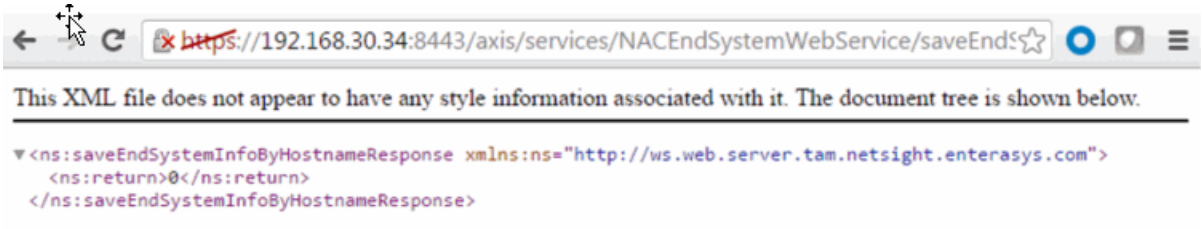
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/saveEndSystemInfoByHostname?hostname=MacBookPro.demo.com&custom1=Custom1&custom2=Custom2&custom3=Custom3&custom4=Custom4



Method: saveEndSystemInfoByIp

Update end system information.

Parameters

Name	Type	Description
ipAddress	string	The IP address of the end system
custom1	string	Custom field 1 value
custom2	string	Custom field 2 value
custom3	string	Custom field 3 value
custom4	string	Custom field 4 value

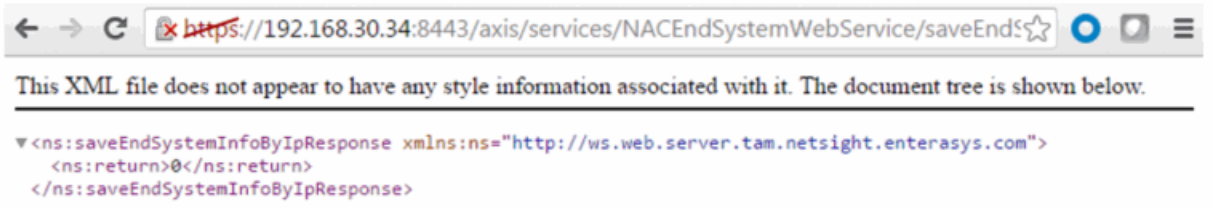
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/saveEndSystemInfoByIp?ipAddress=192.168.10.178&custom1=Custom1&custom2=Custom2&custom3=Custom3&custom4=Custom4



Method: saveEndSystemInfoByMac

Update end system information.

Parameters

Name	Type	Description
mac	string	The MAC address of the end-system
custom1	string	Custom field 1 value
custom2	string	Custom field 2 value
custom3	string	Custom field 3 value
custom4	string	Custom field 4 value

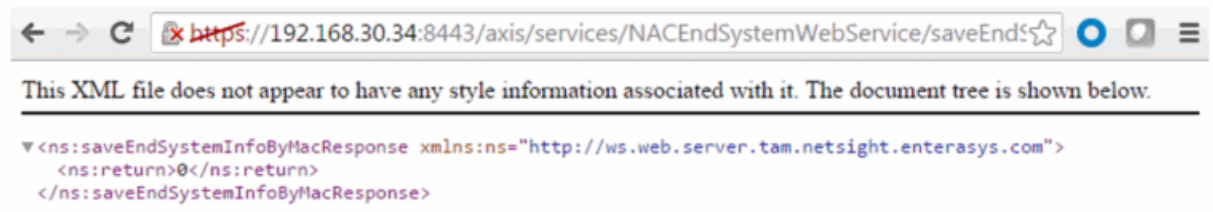
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/saveEndSystemInfoByMac?mac=80:A5:89:33:67:37&custom1=Custom1&custom2=Custom2&custom3=Custom3&custom4=Custom4



Method: saveEndSystemInfoEx

Update end system information

Parameters

Name	Type	Description
info	EndSystemInfo	End-system information to save

Returns

Returns a WsEndSystemInfoResult with a structure defined by the following table.

Name	Type	Description
endSystemInfo	EndSystemInfo	End-system that had information saved
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation was successful

Method: sendKerberosMessageByIp

Send Kerberos messages to all Extreme Access Control engine.

Parameters

Name	Type	Description
ipAddress	string	IP address of the end-system
userName	string	Username of the end-system
hostName	string	Hostname of the end-system
lastSeenTime	long	The timestamp, in milliseconds, at which the Keberos message is snooped. Set to 0 to use Extreme Management Center's current time
lastAuthTime	long	The timestamp, in milliseconds, at which the Keberos message is snooped. Set to 0 to use Extreme Management Center's current time
sourceIp	string	Source IP address of the Keberos message

Name	Type	Description
clearUserName	boolean	Setting to **true** clears the end-system's username

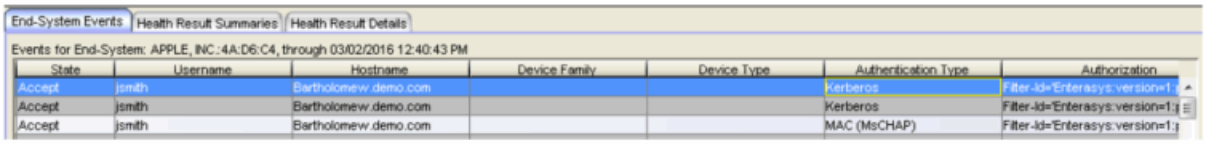
Returns

The operation does not return a value.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/sendKerberosMessageByIp?ipAddress=192.168.10.178&userName=jsmith&hostName=jsmith-test-system&lastSeenTime=0&lastAuthTime=0&sourceIp=192.168.30.34&clearUserName=false



Method: sendKerberosMessageByMAC

Send Kerberos message to all Extreme Access Control engines.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system
userName	string	Username of the end-system
hostName	string	Hostname of the end-system
lastSeenTime	long	The timestamp, in milliseconds, at which the Keberos message is snooped. Set to **0** to use Extreme Management Center's current time
lastAuthTime	long	The timestamp, in milliseconds, the Keberos message was snooped at. Set to **0** to use Extreme Management Center's current time
sourceIp	string	Source IP address of the Keberos message
clearUserName	boolean	Set to **true** to clear the end-system's username

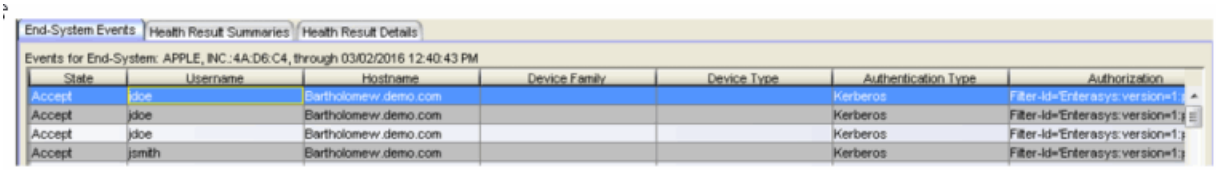
Returns

The operation does not return a value.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/sendKerberosMessageByMAC?macAddress=80:D6:05:4A:D6:C4&userName=jdoe&hostName=jdoe-test-system&lastSeenTime=0&lastAuthTime=0&sourceIp=192.168.30.34&clearUserName=false



Method: setDeviceTypeByIp

Update the end-system's device type.

Parameters

Name	Type	Description
ipAddress	string	IP address of the end-system
deviceType	string	New device type value
isAccurate	boolean	Set to **true** if you know the new device type is accurate
reason	string	A brief description as to the reason for the Extreme Access Control event

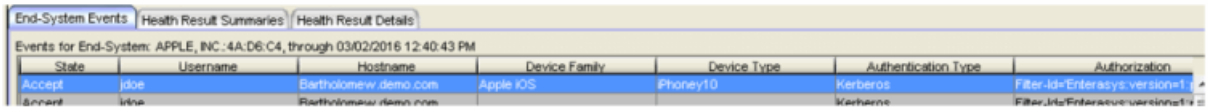
Returns

Returns a string status indicating whether the operation is successful.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/setDeviceTypeByIp?ipAddress=192.168.10.178&deviceType=iPhoney10&isAccurate=true&reason=Web-Service-Example



Method: setDeviceTypeByMAC

Update the end-system's device type.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system
deviceType	string	New device type value
isAccurate	boolean	Set to **true** if you know the new device type is accurate
reason	string	A brief description as to the reason for the Extreme Access Control event

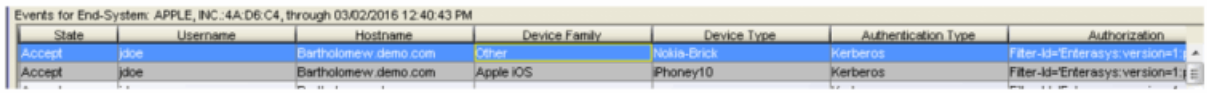
Returns

Returns a string status describing whether the operation is successful.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/setDeviceTypeByMAC?macAddress=80:D6:05:4A:D6:C4&deviceType=Nokia-Brick&isAccurate=true&reason=Web-Service-Example



Method: updateNamedListDescription

Update the named list description with the new provided description.

Parameters

Name	Type	Description
listName	string	Named list to update
descr	string	Named list description

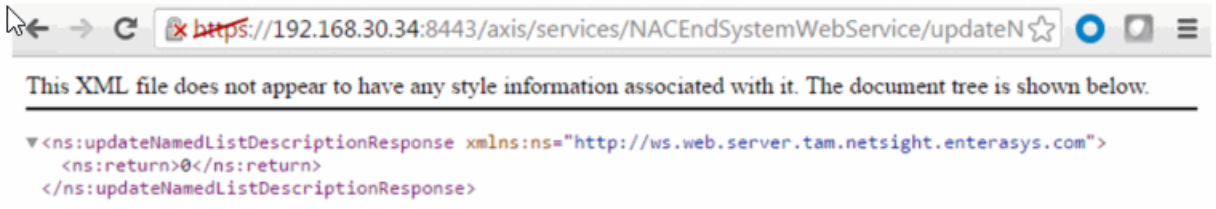
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/updateNamedListDescription?listName=iOS&descr=Example-Web-Service



Method: updateNamedListDescriptionEx

Update the named list description with the new provided description. This operation is similar to updateNamedListDescription, but returns a verbose message.

Parameters

Name	Type	Description
listName	string	Named list to update
descr	string	Named list description

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorCode	string	Error message in readable text
success	boolean	True if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACEndSystemWebService/updateNamedListDescriptionEx?listName=iOS&descr=Example-Web-Service

NAC Web Service

The NAC web service provides an external interface to retrieve and modify the Extreme Access Control services. The NAC web service description language is available at:

https://<Extreme Management Center Server IP>:<port>/axis/services/NACWebService?wsdl

Method: addHostnameToEndSystemGroup

Add an end-system hostname to an Extreme Access Control end-system group. You can remove the hostname from other end-system groups.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
hostname	string	The hostname of the end-system
description	string	Optional information stored in the end-system group with the hostname
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the hostname from other end-system groups

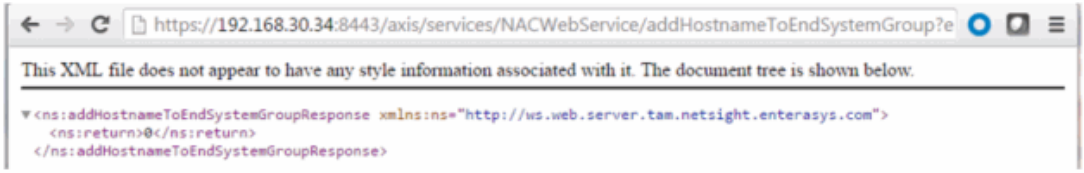
Returns

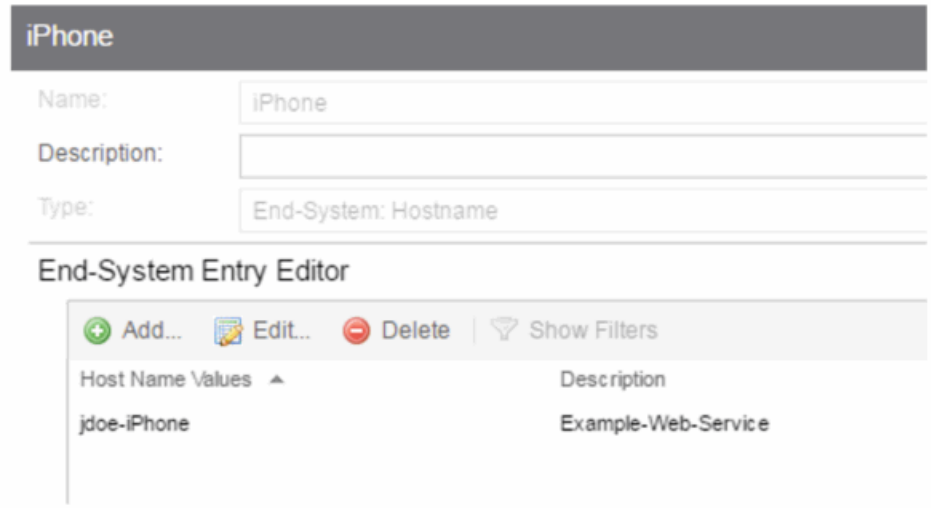
The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addHostnameToEndSystemGroup?endSystemGroup=iPhone&hostname=jdoe-iPhone&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=true





Method: addHostnameToEndSystemGroupEx

Add an end-system hostname to an Extreme Access Control end-system group. You can remove the hostname from other end-system groups. This operation is similar to addHostnameToEndSystemGroup, but returns a verbose message.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
hostname	string	The hostname of the end-system
description	string	Optional information stored in the end-system group with the hostname
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the hostname from other end-system groups

Returns

Returns a WsResult with a structure defined by the following table.

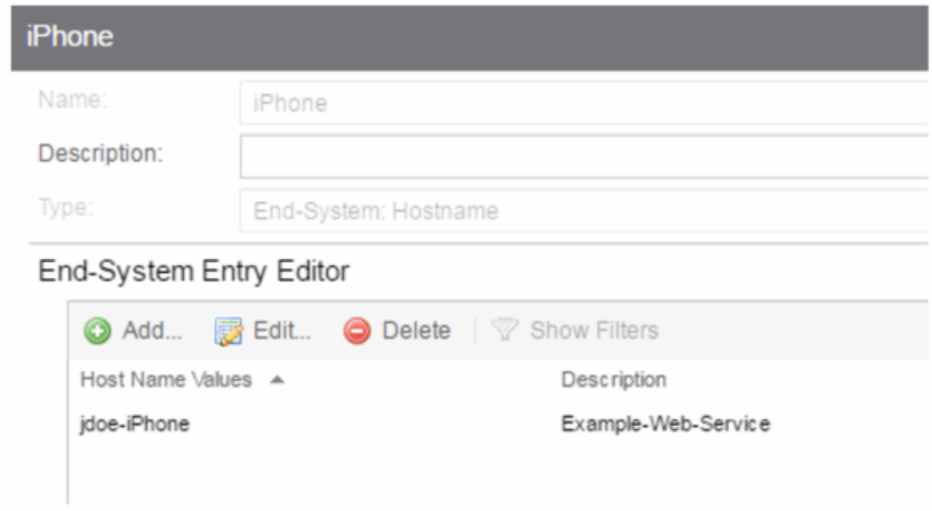
Name	Type	Description
errorCode	int	Please see the Web Service Error Codes

Name	Type	Description
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addHostnameToEndSystemGroupEx?endSystemGroup=iPhone&hostname=jdoe-iPhone&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=



Method: addHostnameToEndSystemGroupWithCustomDataEx

Add an end-system hostname to an Extreme Access Control end-system group. You can remove the hostname from other end-system groups and set the custom fields.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
hostname	string	The hostname of the end-system
description	string	Optional information stored in the end-system group with the hostname
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the hostname from other end-system groups
custom	string	The end-system's new custom fields

Returns

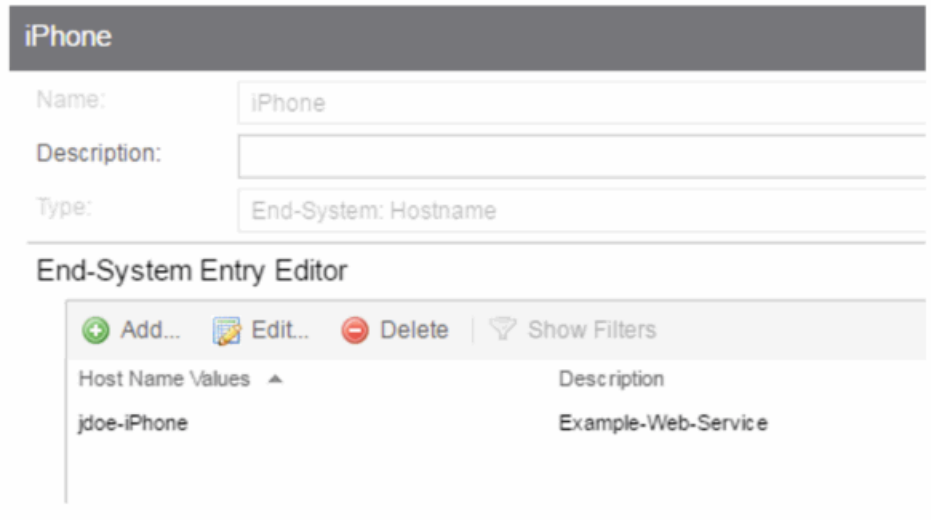
Returns a WsResult with a structure defined by the following table.

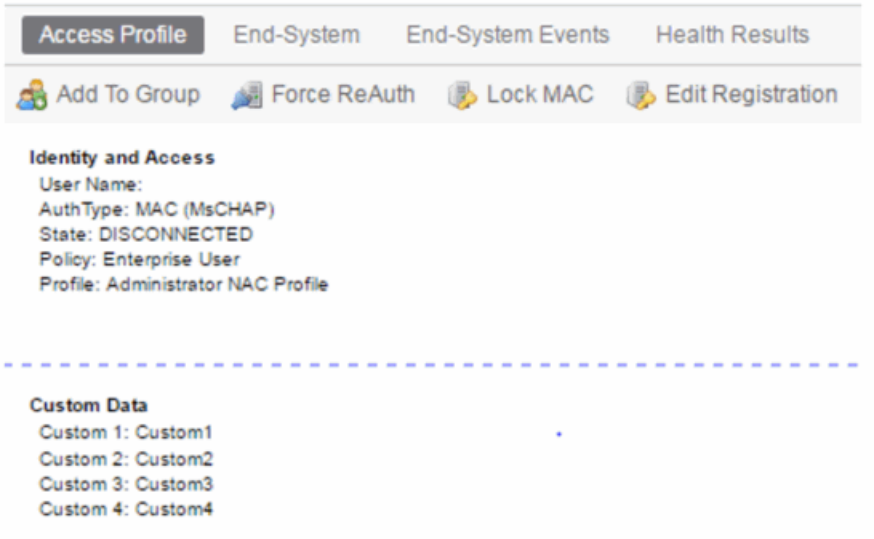
Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	Displays **True** if the operation occurred successfully

Example

Execute the following web service with a browser. Note the custom field parameter is an array. The 1st custom parameter is associated to **Custom Field 1**, the 2nd custom parameter is associated to **Custom Field 2**, the 3rd custom parameter is associated to **Custom Field 3**, and the 4th is associated to **Custom Field 4**.

https://192.168.30.34:8443/axis/services/NACWebService/addHostnameToEndSystemGroupWithCustomDataEx?endSystemGroup=iPhone&hostname=jdoe-iPhone&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=true&custom=Custom1&custom=Custom2&custom=Custom3&custom=Custom4





Method: addIPToEndSystemGroup

Add an end-system IP address to an Extreme Access Control end-system group. You can remove the IP address from other end-system groups.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
ipAddress	string	The IP address of the end-system
description	string	Optional information stored in the end-system group with the hostname
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the hostname from other end-system groups

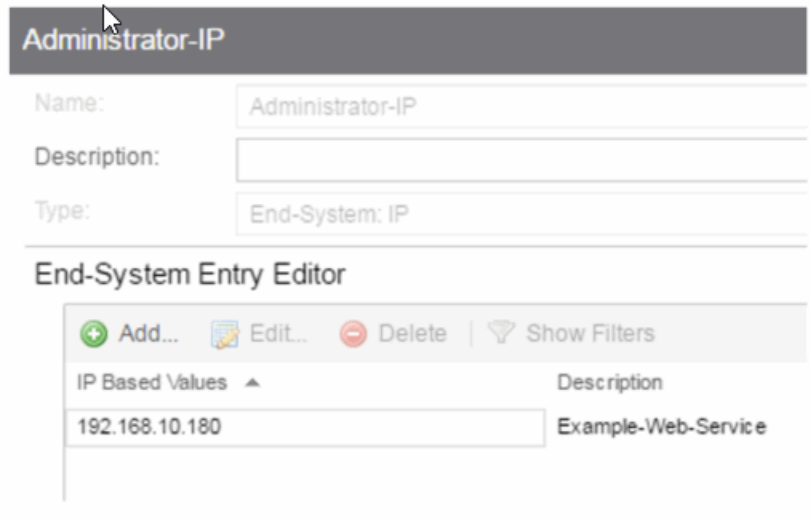
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addIPToEndSystemGroup?endSystemGroup=Administrator-IP&ipAddress=192.168.10.180&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=true



Method: addIPToEndSystemGroupEx

Add an end-system IP address to an Extreme Access Control end-system group. You can remove the IP address from other end-system groups. This operation is similar to addIPToEndSystemGroup, but returns a verbose message.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
ipAddess	string	The IP address of the end-system
description	string	Optional information stored in the end-system group with the hostname

Name	Type	Description
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the hostname from other end system groups

Returns

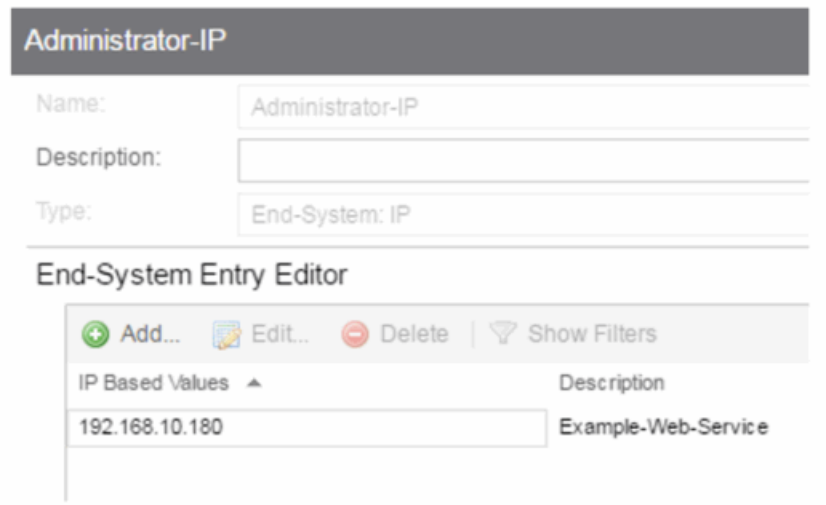
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation was successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addIPToEndSystemGroupEx?endSystemGroup=Administrator-IP&ipAddress=192.168.10.180&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=true



Method: addIPToEndSystemGroupWithCustomDataEx

Add an end-system IP address to an Extreme Access Control end-system group. You can remove the IP address from other end-system groups and configure the custom fields.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
ipAddress	string	The IP address of the end-system
description	string	Optional information stored in the end-system group with the hostname
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the hostname from other end-system groups
custom	string	The end-system's new custom fields

Returns

Returns a WsResult with a structure defined by the following table.

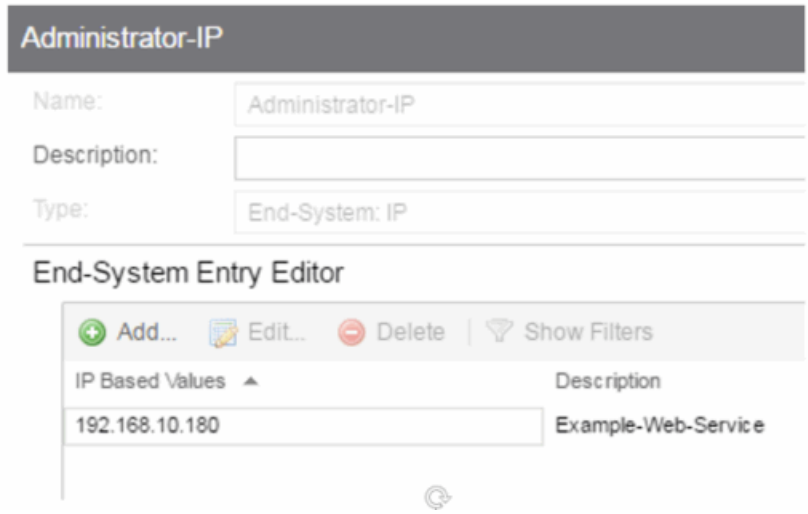
Name	Type	Description
errorCode	int	Please see the Web Service Error Codes

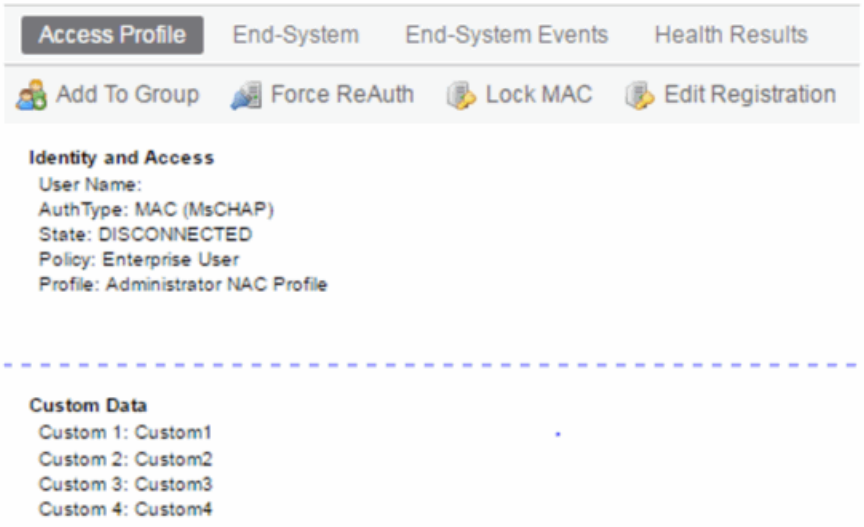
Name	Type	Description
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser. Note the custom field parameter is an array. The 1st custom parameter is associated to **Custom Field 1**, the 2nd custom parameter is associated to **Custom Field 2**, the 3rd custom parameter is associated to **Custom Field 3**, and the 4th is associated to **Custom Field 4**.

https://192.168.30.34:8443/axis/services/NACWebService/addIPToEndSystemGroupWithCustomDataEx?endSystemGroup=Administrator-IP&ipAddress=192.168.10.180&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=true&custom=Custom1&custom=Custom2&custom=Custom3&custom=Custom4





Method: addMACToBlacklist

Add an end-system MAC address to the Extreme Access Control blacklist end-system group. Force reauthentication on the end-system once it is blacklisted to limit network access.

Parameters

Name	Type	Description
macAddress	string	The MAC address of the end-system
description	string	Optional information stored in the end-system group with the MAC address
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

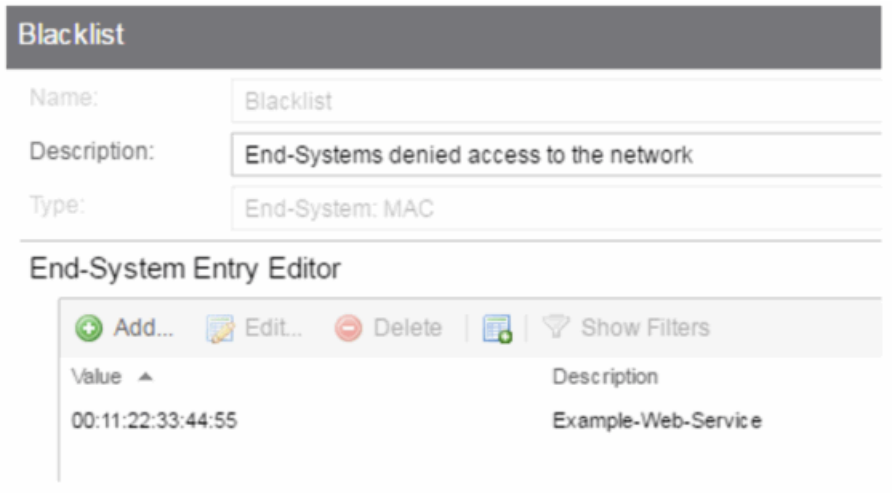
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addMACToBlacklist?macAddress=00:11:22:33:44:55&description=Example-Web-Service&reauthenticate=true



Method: addMACToBlacklistEx

Add an end-system MAC address to the Extreme Access Control blacklist end-system group. This operation is similar to the addMACToBlackList, but returns a verbose message. Force reauthentication on the end-system once it is blacklisted to limit network access.

Parameters

Name	Type	Description
macAddress	string	The MAC address of the end-system
description	string	Optional information stored in the end-system group with the MAC address
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

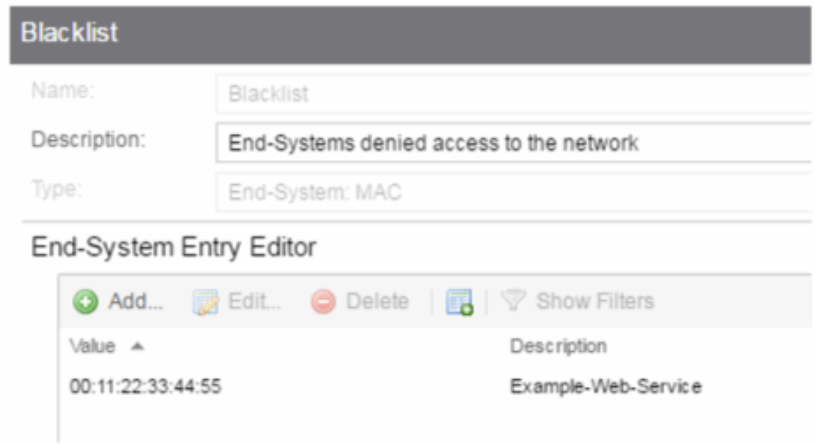
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addMACToBlacklistEx?macAddress=00:11:22:33:44:55&description=Example-Web-Service&reauthenticate=true



Method: addMACToBlacklistWithCustomDataEx

Add an end-system MAC address to the Extreme Access Control blacklist end-system group. You can configure the custom fields. Force reauthentication on the end-system once it is blacklisted to limit network access.

Parameters

Name	Type	Description
macAddress	string	The MAC address of the end-system
description	string	Optional information stored in the end-system group with the MAC address
reauthenticate	boolean	Set to true to force reauthentication on the affected end-system
custom	string	The end-system's new custom fields

Returns

Returns a WsResult with a structure defined by the following table.

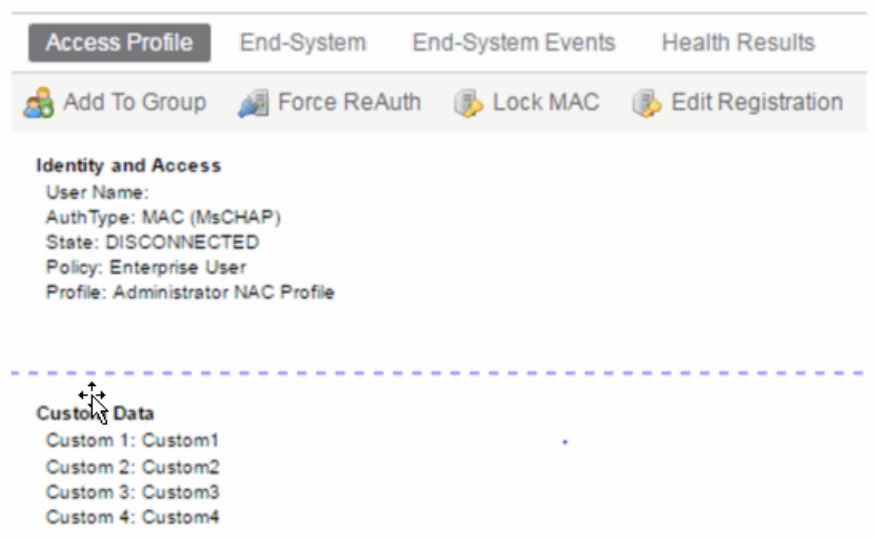
Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser.

Note the custom field parameter is an array. The 1st custom parameter is associated to **Custom Field 1**, the 2nd custom parameter is associated to **Custom Field 2**, the 3rd custom parameter is associated to **Custom Field 3**, and the 4th is associated to **Custom Field 4**.

https://192.168.30.34:8443/axis/services/NACWebService/addMACToBlacklistWithCustomDataEx?macAddress=00:11:22:33:44:55&description=Example-Web-Service&reauthenticate=true&custom=Custom1&custom=Custom2&custom=Custom3&custom=Custom4



Method: addMACToEndSystemGroup

Add an end-system MAC address to an Extreme Access Control end-system group. You can remove the MAC address from other end-system groups and configure custom fields.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
macAddress	string	The MAC address of the end-system
description	string	Optional information stored in the end-system group with the MAC address

Name	Type	Description
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the MAC address from other end-system groups

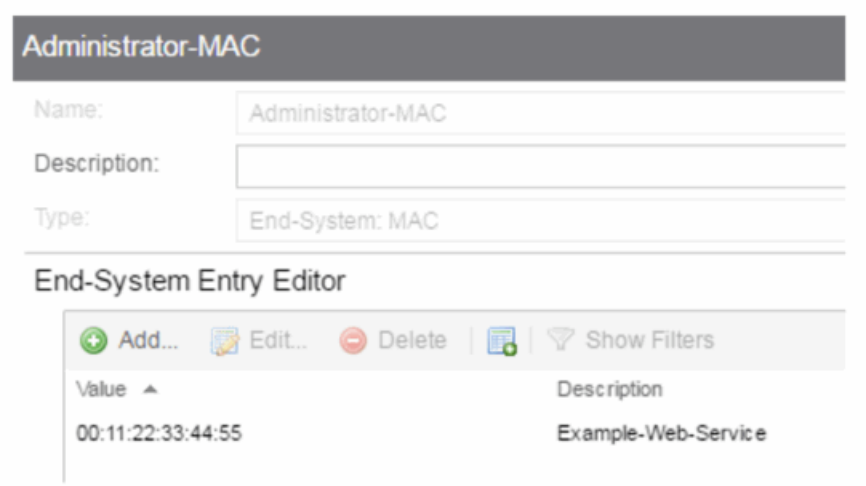
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addMACToEndSystemGroup?endSystemGroup=Administrator-MAC&macAddress=00:11:22:33:44:55&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=true



Method: addMACToEndSystemGroupEx

Add an end system MAC address to an Extreme Access Control end-system group. You can remove the MAC address from other end-system groups. This operation is similar to addMACToEndSystemGroup, but returns a verbose message.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
macAddress	string	The MAC address of the end-system
description	string	Optional information stored in the end-system group with the MAC address
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the MAC address from other end-system groups

Returns

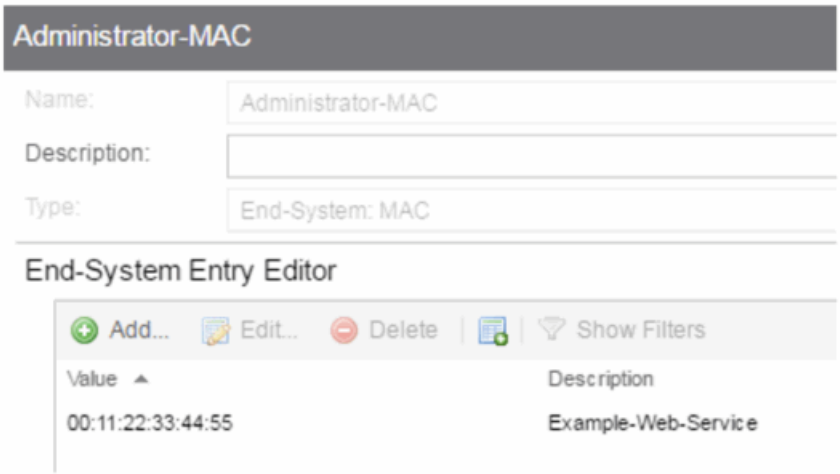
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addMACToEndSystemGroupEx?endSystemGroup=Administrator-MAC&macAddress=00:11:22:33:44:55&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=true



Method: addMACToEndSystemGroupWithCustomDataEx

Add an end-system MAC address to an Extreme Access Control end-system group. You can remove the MAC address from other end-system groups and configure the custom fields.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
macAddress	string	The MAC address of the end-system
description	string	Optional information stored in the end-system group with the MAC address
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Name	Type	Description
removeFromOtherGroups	boolean	Set to **true** to remove the MAC address from other end-system groups
custom	string	The end-system's new custom fields

Returns

Returns a WsResult with a structure defined by the following table.

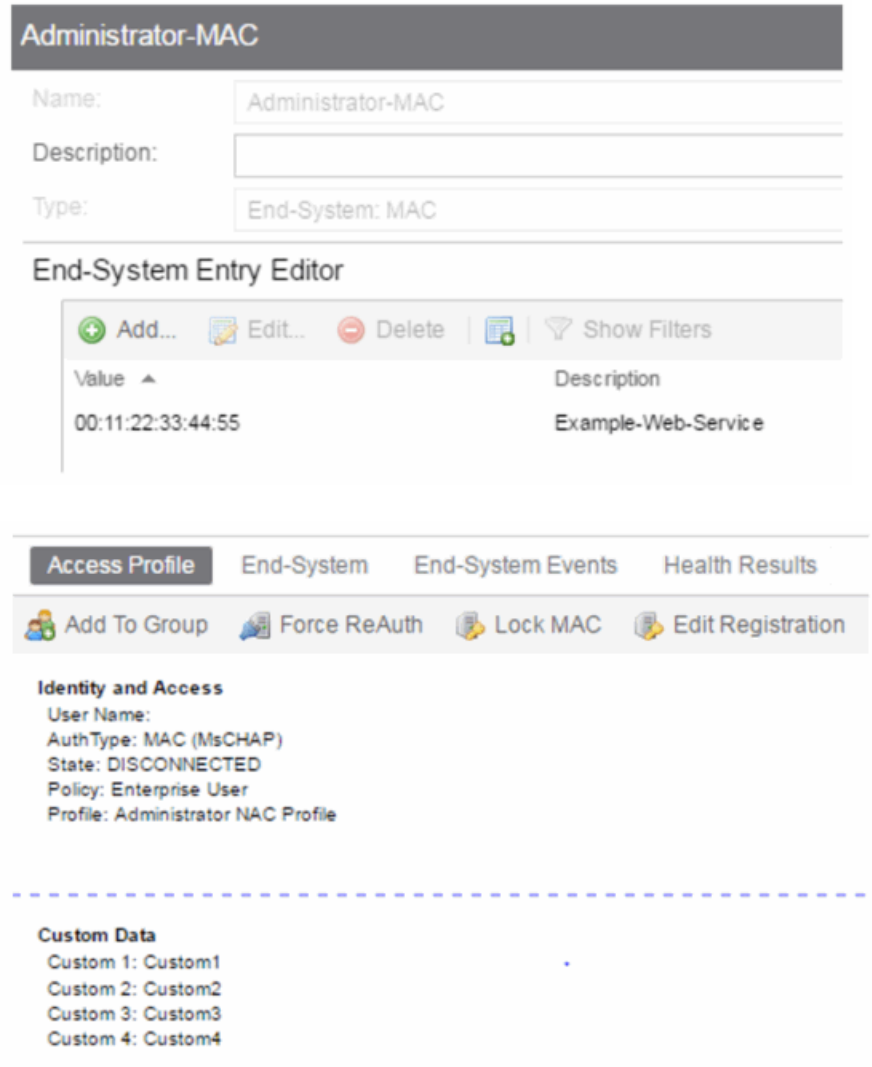
Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser.

Note the custom field parameter is an array. The 1st custom parameter is associated to **Custom Field 1**, the 2nd custom parameter is associated to **Custom Field 2**, the 3rd custom parameter is associated to **Custom Field 3**, and the 4th is associated to **Custom Field 4**.

https://192.168.30.34:8443/axis/services/NACWebService/addMACToEndSystemGroupWithCustomDataEx?endSystemGroup=Administrator-MAC&macAddress=00:11:22:33:44:55&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=true&custom=Custom1&custom=Custom2&custom=Custom3&custom=Custom4



Method: addUsernameToUserGroup

Add an end-system username to an Extreme Access Control end-system group. You can remove the username from other end-system groups.

Parameters

Name	Type	Description
userGroup	string	The end-system group name you are changing
username	string	The username of the end-system
description	string	Optional information stored in the end-system group with the username

Name	Type	Description
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the username from other end-system groups

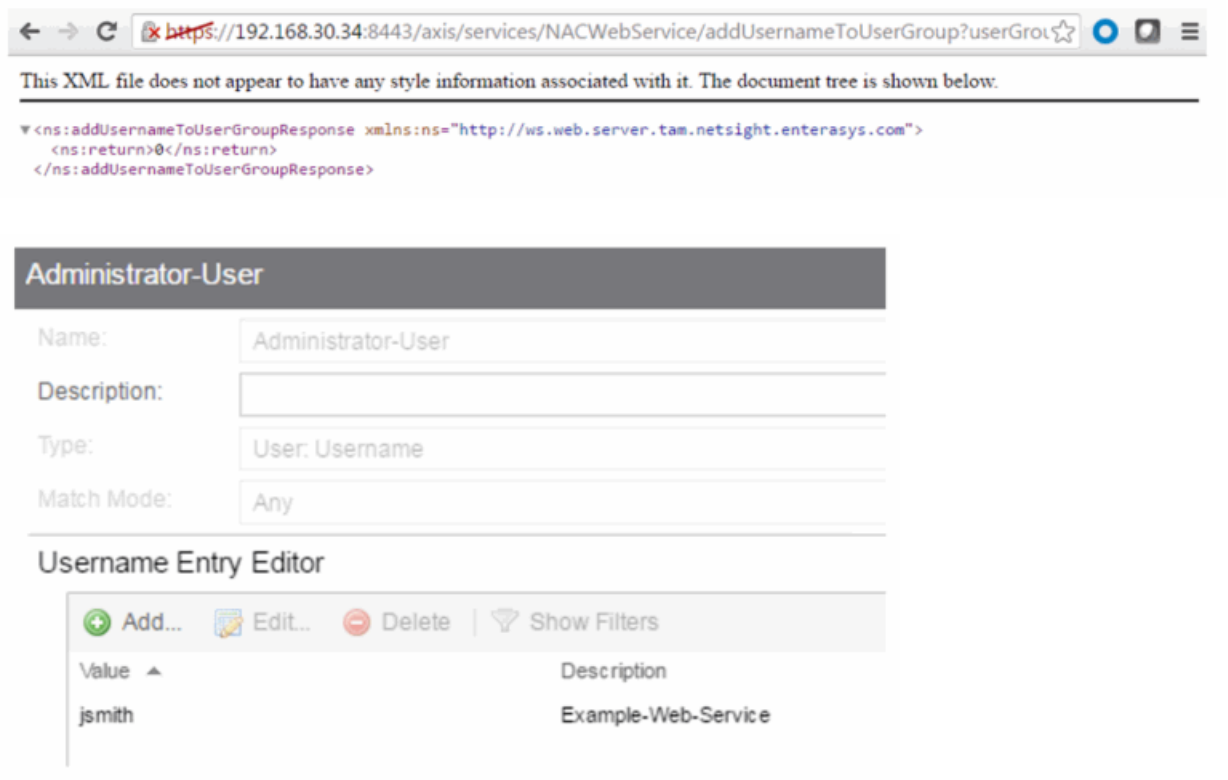
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addUsernameToUserGroup?userGroup=Administrator-User&username=jsmith&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=true



Method: addUsernameToUserGroupEx

Add an end-system username to an Extreme Access Control end-system group. You can remove the username from other end-system groups. This operation is similar to addUsernameToEndSystemGroup, but returns a verbose message.

Parameters

Name	Type	Description
userGroup	string	The end-system group name you are changing
username	string	The username of the end-system
description	string	Optional information stored in the end-system group with the username
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system
removeFromOtherGroups	boolean	Set to **true** to remove the username from other end-system groups

Returns

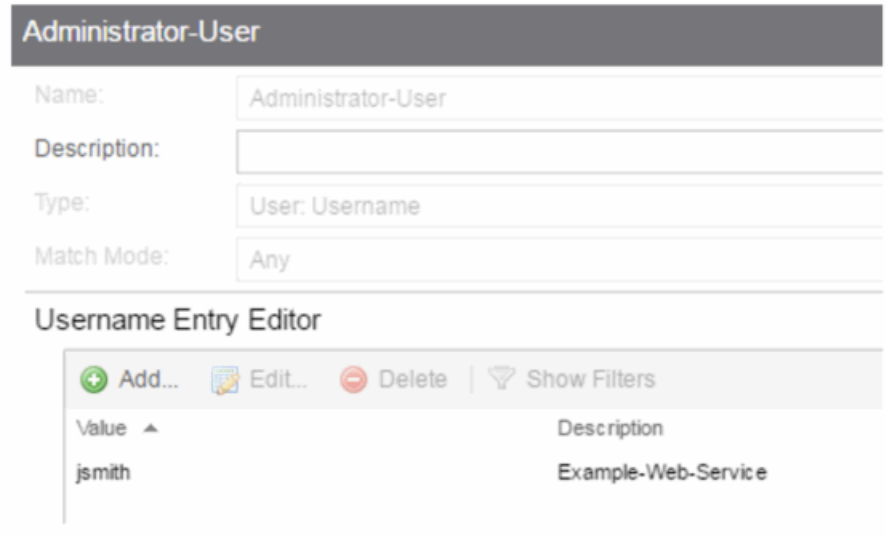
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addUsernameToUserGroupEx?userGroup=Administrator-User&username=jsmith&description=Example-Web-Service&reauthenticate=true&removeFromOtherGroups=true



Method: addValueToNamedList

Add a value to an Extreme Access Control end-system group. This is a generic operation, so ensure you use the correct value and end-system group. Adding to a MAC address based end-system group requires the value to be in a MAC address format. Adding an IP address to an IP based end-system group requires the value to be in an IP address format. Failure to use the correct value and end-system group can cause network access issues.

Parameters

Name	Type	Description
list	string	The end system group you are changing
list	string	The value to add

Name	Type	Description
description	string	Optional information stored in the end-system group with the value
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

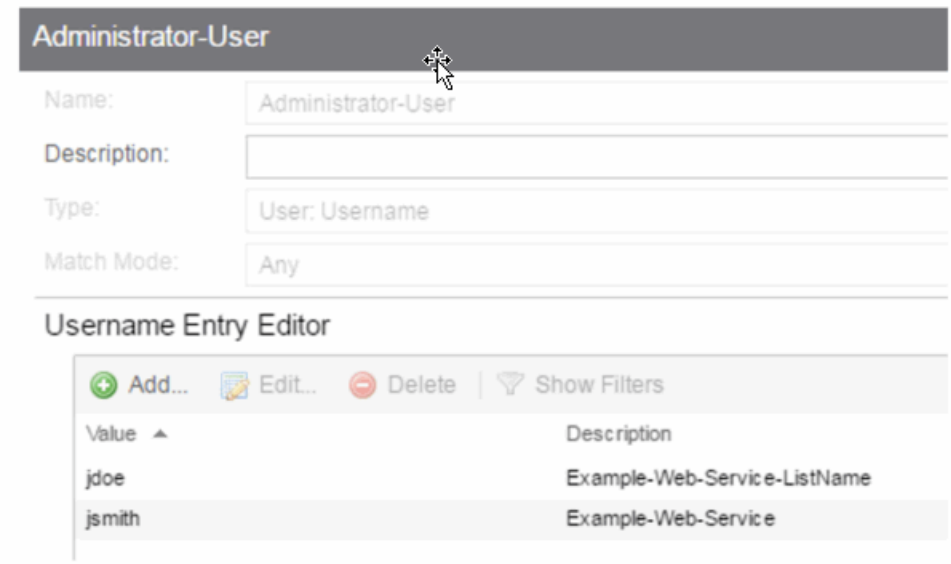
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addValueToNamedList?list=Administrator-User&value=jdoe&description=Example-Web-Service-ListName&reauthenticate=true&removeFromOtherGroups=true



Method: addValueToNamedListEx

Add a value to an Extreme Access Control end-system group. This is a generic operation, so ensure you use the correct value and end-system group. This operation is similar to addValueToNamedList, but returns a verbose message. Adding to a MAC address based end-system group requires the value to be in a MAC address format. Adding an IP address to an IP based end-system group requires the value to be in an IP address format. Failure to use the correct value and end-system group can cause network access issues.

Parameters

Name	Type	Description
list	string	The end-system group you are changing
Value	string	The value to add
description	string	Optional information stored in the end-system group with the value
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

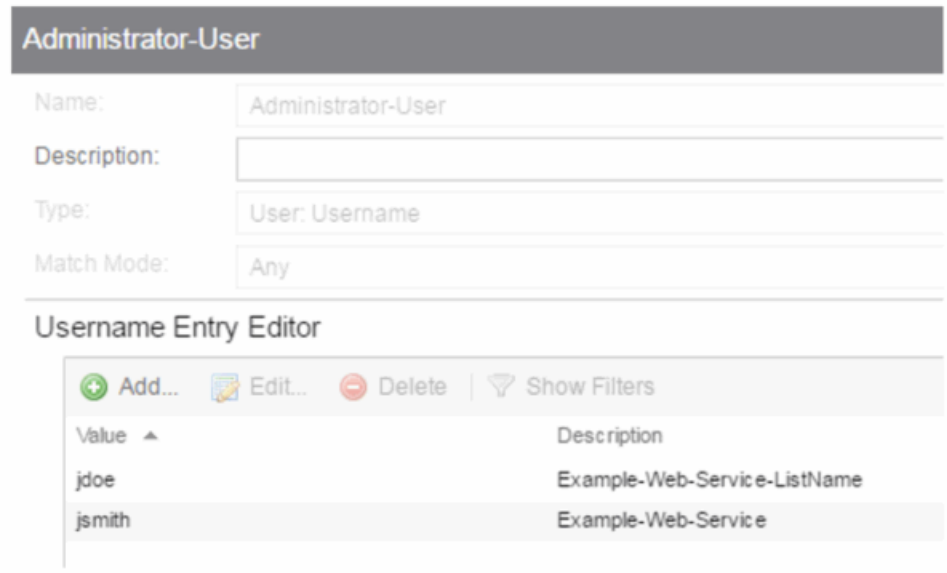
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/addValueToNamedListEx?list=Administrator-User&value=jdoe&description=Example-Web-Service-ListName&reauthenticate=true&removeFromOtherGroups=true



Method: auditEnforceNacAppliances

Enforce changes to a list of Extreme Access Control engines.

Parameters

Name	Type	Description
nacAppliances	string	List of Extreme Access Control engines.

Returns

Returns a WsEnforceApplianceResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/auditEnforceNacAppliances?nacAppliances=192.168.30.35

Method: createMacLock

Create a MAC lock to limit a device to a single switch port.

Parameters

Name	Type	Description
mac	string	MAC address of the end-system
switchIp	string	IP address of the switch to which the end-system is limited
switchPort	string	Switch port to which the end-system is limited

Name	Type	Description
reject	boolean	Set to **true** to reject the authentication request if the end system tries to authentication on a different switch or port
policy	string	Policy that applies if the end-system tries to authenticate to a different switch or port

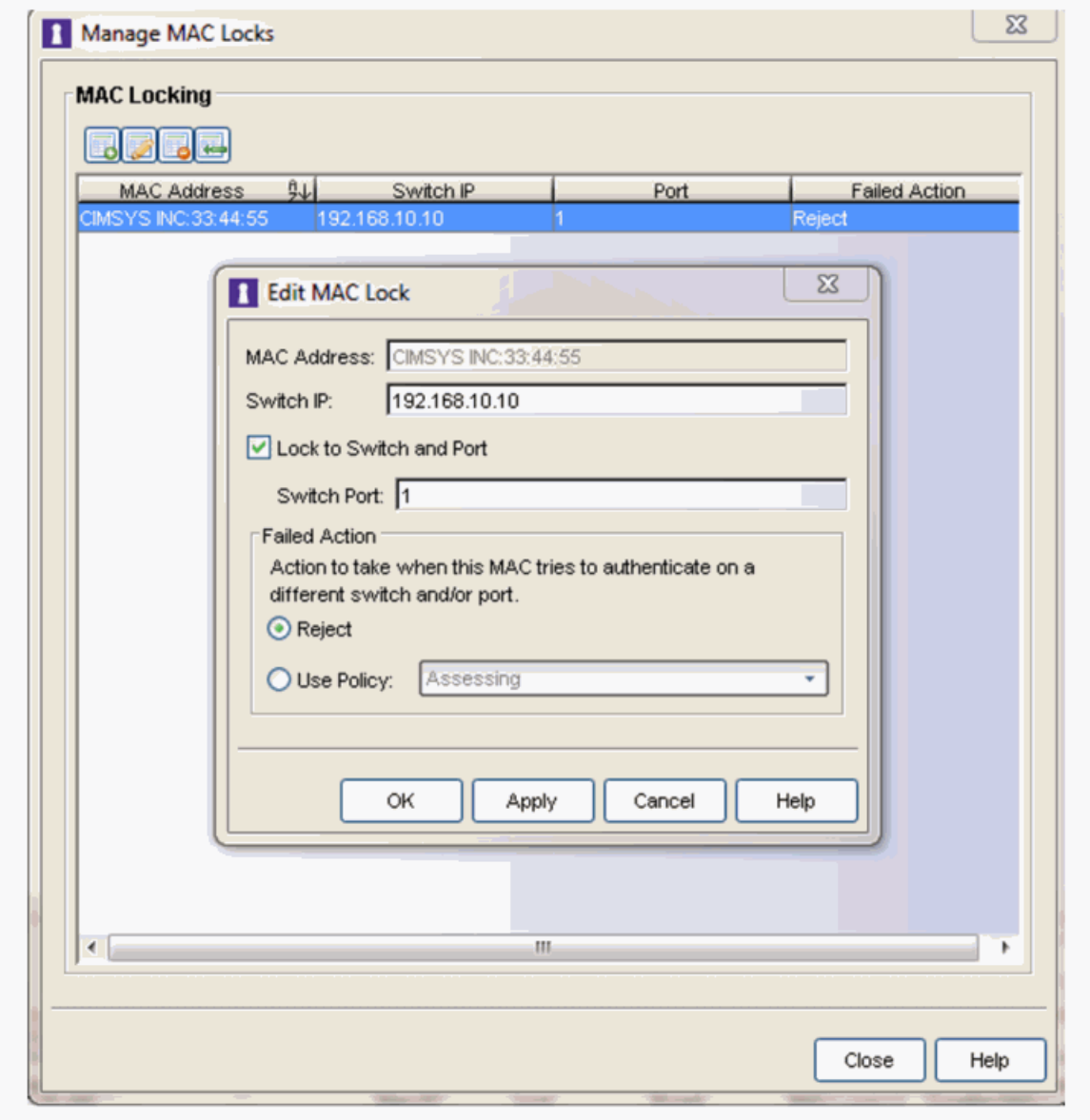
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/createMacLock?mac=00:11:22:33:44:55&switchIp=192.168.10.10&switchPort=1&reject=true



Method: deleteEndSystemByMac

Delete end system based on the end system's MAC address.

Parameters

Name	Type	Description
mac	string	MAC address of the end-system to delete

Name	Type	Description
deleteOptionsMask	int	0x01 – Delete values in named lists 0x02 – Delete MAC locks 0x04 – Delete end-system information 0x08 – Delete registered devices 0x10 – Force delete of end-system

Returns

A return element having the structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/deleteEndSystemByMac?mac=78:E4:00:44:7E:E6&deleteOptionsMask=16

Method: deleteEndSystemInfoByHostname

Delete end-system information record based on the end-system's hostname.

Parameters

Name	Type	Description
hostname	string	The hostname of the end-system

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/deleteEndSystemInfoByHostname?hostname=Captain-Obvious.demo.com

Method: deleteEndSystemInfoByIp

Delete end system information record based on the end system's IP address.

Parameters

Name	Type	Description
ipAddress	string	The IP address of the end-system

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/deleteEndSystemInfoByIp?ipAddress=192.168.10.181

Method: deleteEndSystemInfoByMac

Delete end-system information record based on the end-system's MAC address.

Parameters

Name	Type	Description
macAddress	string	The MAC address of the end-system

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/deleteEndSystemInfoByMac?macAddress=14:7D:C5:97:70:CB

method: deleteEndSystemInfoEx

Delete end-system information record based on the end system's MAC address. This operation is similar to deleteEndSystemInfoByMac, but returns a verbose

message.

Parameters

Name	Type	Description
macAddress	string	The MAC address of the end-system

Returns

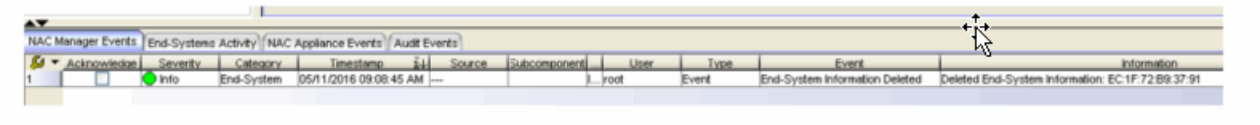
Returns a WsEndSystemInfoResult with a structure defined by the following table.

Name	Type	Description
endSystemInfo	EndSystemInfo	End-system from which you are deleting information
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/deleteEndSystemInfoEx?macAddress=EC:1F:72:B9:37:91



Method: deleteLocalUsers

Delete users from the local user database, specifying the users by a list of local user IDs.

Parameters

Name	Type	Description
localUserIdsCSV	string	The list of local user IDs separated by commas
requestingUser	string	The name of the user requesting this operation

Returns

The operation returns an integer error code.

Example

https://192.168.30.34:8443/axis/services/NACWebService/deleteLocalUsers?localUserIdsCSV=3,4&requestingUser=root

Method: deleteLocalUsersbyLoginIdEx

Delete users from the local user database, specifying the repository and list of usernames.

Parameters

Name	Type	Description
repository	string	The name of the password repository from which you are deleting the user
localUserLoginIdsCSV	string	The list of local usernames separated by commas
requestingUser	string	The name of the user requesting this operation

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/deleteLocalUsersbyLoginIdEx?repository=Default&localUserLoginIdsCSV=jdoe&requestingUser=root

Method: deleteLocalUsersEx

Delete users from the local user database, specifying the users by a list of local user IDs. This operation is similar to deleteLocalUsers, but returns a verbose message.

Parameters

Name	Type	Description
localUserIdsCSV	string	The list of local user IDs separated by commas
requestingUser	string	The name of the user requesting this operation

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/deleteLocalUsersEx?localUserIdsCSV=7&requestingUser=root

Method: deleteMacLock

Delete MAC lock.

Parameters

Name	Type	Description
mac	string	MAC address of the end-system

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/deleteMacLock?mac=00:11:22:33:44:55

Method: deleteRegisteredDevice

Remove a registered device with the matching properties from the database.

Parameters

Name	Type	Description
propString	string	The properties string used to delete the device, string is in the following format: userName=value1,macAdress=value2,applianceGroup=value3
requestingUser	string	The user requesting the deletion

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/deleteRegisteredDevice?propString=userName=jane.smith,macAddress=80:D6:05:4A:D6:C4,applianceGroup=Default&requestingUser=root

Method: deleteRegisteredDevices

Remove registered devices with the matching properties from the database.

Parameters

Name	Type	Description
propStrings	string	The properties string used to delete the device, string is in the following format: userName=value1,macAdress=value2,applianceGroup=value3
requestingUser	string	The user requesting the deletion

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/deleteRegisteredDevices?propStrings=userName=jane.smith,macAddress=80:D6:05:4A:D6:C4,applianceGroup=Default&propStrings=userName=jane.smith,macAddress=50:7A:55:6F:24:35,applianceGroup=Default&requestingUser=root

Method: deleteRegisteredUserAndDevices

Remove a registered user and their associated devices from the database.

Parameters

Name	Type	Description
propString	string	The properties string used to delete the user, string is in the following format: userName=value1,userType=value2,applianceGroup=value3
requestingUser	string	The user requesting this user to be deleted

Returns

The operation returns an integer error code.

Method: deleteRegisteredUsers

Delete a set of registered users in the database.

Parameters

Name	Type	Description
propStrings	string	A list of property strings of users to be deleted from the database, string is in the following format: userName=value1,userType=value2,applianceGroup=value3
requestingUser	string	The user requesting the operation

Returns

The operation returns an integer error code.

Method: enforceNacAppliances

Enforce changes to a list of Extreme Access Control engines.

Parameters

Name	Type	Description
nacAppliances	string	List of Extreme Access Control engines
forceMask	long	Mask to disable enforce optimizations, forcing a reset behavior. Options are: 0x0000 – default behavior 0x0001 - force reconfiguration for all switches 0x0002 – force reconfiguration for captive portal
ignoreWarnings	boolean	**True** to ignore configuration warnings

Returns

Returns a WsEnforceResult with the structure defined by the following table.

Name	Type	Description
applianceEnforceResults	WsEnforceApplianceResult	Extreme Access Control engine errors or warnings encountered during an enforcement
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/enforceNacAppliances?nacAppliances=192.168.30.35&forceMask=0&ignoreWarnings=true

Method: getAllEndSystemMacs

Return a list of end-system MAC addresses known to Extreme Management Center and Extreme Access Control.

Returns

Returns a list of MAC addresses.

Name	Type	Description
Return	string	List of MAC addresses

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getAllEndSystemMacs

Method: getAllEndSystems

Returns data for all end-systems known to Extreme Management Center and Extreme Access Control. This operation can be data intensive on both the Extreme Management Center server and client requesting the operation. The response is stored in memory, so the client (PHP) may need to increase memory.

Returns

Returns a list of end-system data.

Name	Type	Description
Return	string	List of end-system data

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getAllEndSystems

Method: getEndSystemAndHrByMac

Returns end-system data, based on a MAC address, and it's most recent health result and vulnerabilities.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

Returns

Returns end-system data and most recent health result.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getEndSystemAndHrByMac?macAddress=00:88:65:66:03:C1

Method: getEndSystemByIp

Return end-system data based on an IP address.

Parameters

Name	Type	Description
ipAddress	string	IP address of the end-system

Returns

Returns end-system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getEndSystemByIp?ipAddress=192.168.10.190

Method: getEndSystemByIpEx

Return end-system data based on an IP address. The operation is similar to getEndSystemByIp, but returns additional information.

Parameters

Name	Type	Description
ipAddress	string	IP address of the end-system

Returns

Returns WsEndSystemResult with a structure defined by the following table.

Name	Type	Description
endSystem	EndSystemDTO	End-system data
endSystemSwitchSupportsReauth	boolean	**True** if end-system supports reauthentication
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text

Name	Type	Description
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getEndSystemByIpEx?ipAddress=192.168.10.190

Method: getEndSystemByMac

Return end-system data based on a MAC address.

Parameters

Name	Type	Description
ipAddress	string	MAC address of the end-system

Returns

Returns end-system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getEndSystemByMac?macAddress=00:88:65:66:03:C1

Method: getEndSystemByMacEx

Return end-system data based on a MAC address. The operation is similar to getEndSystemByMac, but returns additional information.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

Returns

Returns WsEndSystemResult with a structure defined by the following table.

Name	Type	Description
endSystem	EndSystemDTO	End-system data

Name	Type	Description
endSystemSwitchSupportsReauth	boolean	**True** if end-system supports reauthentication
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getEndSystemByMacEx?macAddress=00:88:65:66:03:C1

Method: getEndSystemInfoArrByMac

Return end-system data based on a MAC Address. The data is returned, in an array, as a set of comma-delimited key=value pairs. If there is an error, errorCode and errorString properties are encoded into the result.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

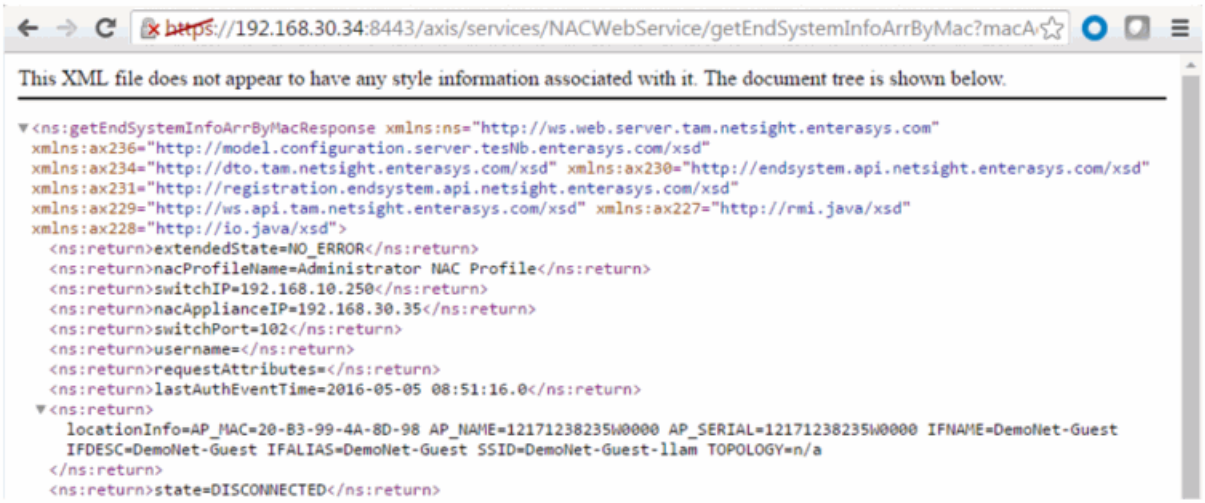
Returns

Returns an array of end-system data in key=value pair format.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getEndSystemInfoArrByMac?macAddress=00:88:65:66:03:C1



Method: getEndSystemInfoByMac

Return end-system data based on a MAC Address. The data is returned as a set of comma-delimited key=value pairs. If there is an error, errorCode and errorString properties are encoded into the result.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

Returns

Returns end-system data in key=value pair format.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getEndSystemInfoByMac?macAddress=00:88:65:66:03:C1

Method: getEndSystemInfoByMacEx

Return end-system data based on a MAC Address. The data is returned as a set of comma-delimited key=value pairs. If there is an error, errorCode and errorString properties are encoded into the result. The operation is similar to getEndSystemInfoByMac, but returns additional information.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

Returns

Returns a WsEndSystemInfoResult with a structure defined by the following table.

Name	Type	Description
endSystem	EndSystemDTO	End-system data

Name	Type	Description
endSystemSwitchSupportsReauth	boolean	**True** if end-system supports reauthentication
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text

Method: getEndSystemsByMacEx

Return end-system data based on a MAC address(es).

Parameters

Name	Type	Description
macAddresses	string	MAC addresses of the end-systems

Returns

Returns a WsEndSystemList with a structure defined by the following table.

Name	Type	Description
endSystem	EndSystemDTO	End-system data
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getEndSystemsByMacEx?macAddresses=00:88:65:66:03:C1&macAddresses=EC:1F:72:B9:37:91

Method: getExtendedEndSystemArrByMac

Return an extended set of data for an end-system based on a MAC address. The data includes additional information such as ELIN, portAlias, etc. The data is returned as a set of comma-delimited key=value pairs. If there is an error, errorCode and errorString properties are encoded into the result.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

Returns

Returns an array of end system data in key=value pair format.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getExtendedEndSystemArrByMac?macAddress=00:88:65:66:03:C1

Method: getExtendedEndSystemByMac

Return an extended set of data for an end-system based on a MAC address. The data includes additional information such as ELIN, portAlias, etc. The data is returned as a set of comma-delimited key=value pairs. If there is an error, errorCode and errorString properties are encoded into the result.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system

Returns

Returns an extended set of end-system data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getExtendedEndSystemByMac?macAddress=00:88:65:66:03:C1

Method: getLocalUser

Return a local user from the user database.

Parameters

Name	Type	Description
passwordRepository	string	Password repository in which the user is saved
loginId	string	The username of the user

Returns

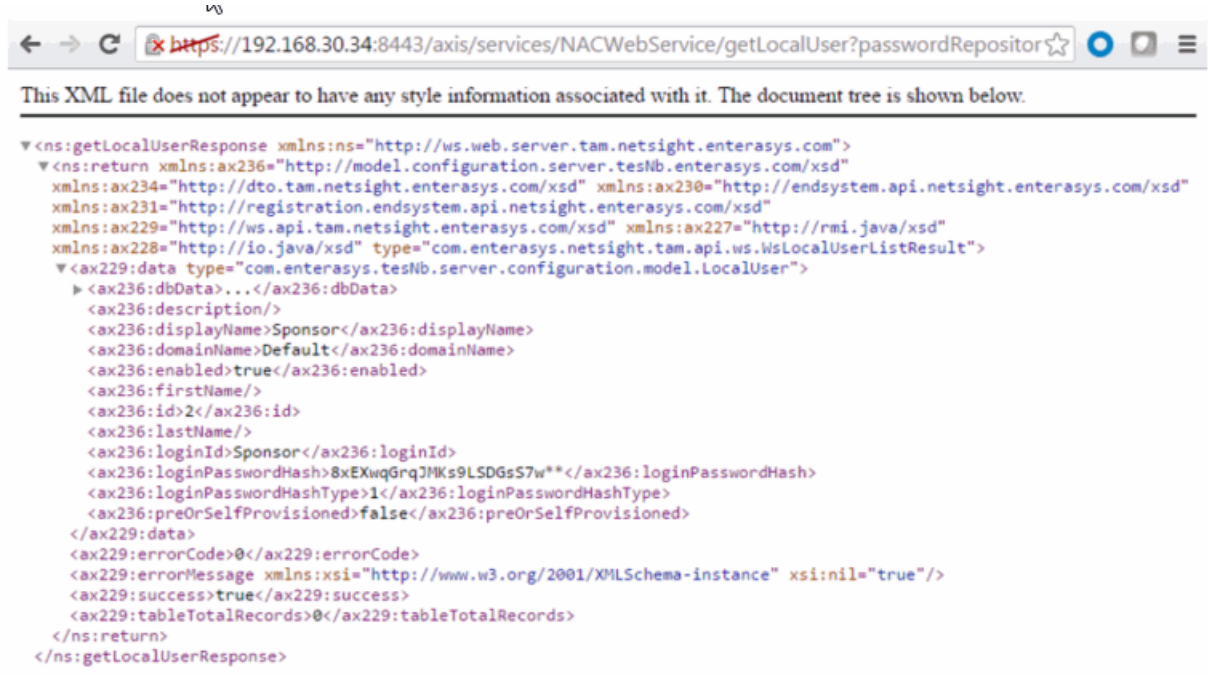
Returns a WsLocalUserListResult with a structure defined by the following table.

Name	Type	Description
data	LocalUser	User information
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful
tableTotalRecords	int	Total number of available records

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getLocalUser?passwordRepository=Default&loginId=Sponsor



Method: getNACVersion

Return the Extreme Access Control version.

Returns

Returns Extreme Access Control version.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getNACVersion

Method: getPollerStatus

Return the last polling status of an Extreme Access Control engine.

Parameter

Name	Type	Description
nacIP	string	IP address of an Extreme Access Control engine

Returns

Returns true/false for the Extreme Access Control engine's last polling status.

Example

https://192.168.30.34:8443/axis/services/NACWebService/getPollerStatus?nacIP=192.168.30.35

Method: getRegisteredDevicesByMacAddress

Retrieve an array of registered devices as KEY=VALUE comma separated string based on a MAC address.

Parameters

Name	Type	Description
macAddress	string	MAC address of the registered device

Returns

Returns an array of key=value comma separated string.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getRegisteredDevicesByMacAddress?macAddress=50:7A:55:6F:24:35

Method: getRegisteredUsersByUsername

Retrieve an array of registered users as KEY=VALUE comma separated string.

Parameters

Name	Type	Description
username	string	Username of the registered user

Returns

Returns an array of key=value comma separated string.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getRegisteredUsersByUsername?username=jane.smith

Method: getRegistredDevicesByUsername

Retrieve an array of registered devices as KEY=VALUE comma-separated string based on a username.

Parameters

Name	Type	Description
username	string	Username of the registered user

Returns

Returns an array of key=value comma separated string.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getRegistredDevicesByUsername?username=jane.smith

Method: getRegistredUsersByMacAddress

Retrieve an array of registered users as KEY=VALUE comma separated string based on a MAC address.

Parrameters

Name	Type	Description
macAddress	string	MAC address of the registered device

Returns

Returns an array of key=value comma separated string.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getRegistredUsersByMacAddress?macAddress=50:7A:55:6F:24:35

Method: getUnsurfacedNamedList

Return the contents of a named list/end-system group without manipulation.

Parameters

Name	Type	Description
listName	string	End-system group name

Returns

Returns a string array that contains the XML representation of values, description, and data.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/getUnsurfacedNamedList?listName=Registered Guests

Method: hashLocalUserPassword

Generate a hashed password for a local user.

Parameters

Name	Type	Description
password	string	Password in clear text

Returns

Returns a hashed password.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/hashLocalUserPassword?password=MySuperDuperSecurePassword

Method: hashLocalUserPasswordEx

Generate a hashed password for a local user.

Parameters

Name	Type	Description
Password in clear text	Password in clear text	Password in clear text
hashAlgorithm	int	Hashing algorithm, available options are: 0 - SHA1 non reversible hash 1 - PKCS5 reversible hash

Returns

Returns a hashed password.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/hashLocalUserPasswordEx?password=MySuperDuperSecurePassword&hashAlgorithm=1

Method: importEndSystemInfoEx

Save a batch of end system information.

Parameters

Name	Type	Description
infoList	EndSystemInfo	An array of end-system information
isSave	Boolean	**True** to save end-system information, **false** to delete it

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Method: importEndSystemInfoFromCsv

Save a batch of end-system information provided by a CSV file.

Parameters

Name	Type	Description
csvData	string	A string version of CSV file with new line delimiters
isSave	boolean	**True** to save end-system information, **false** to delete it

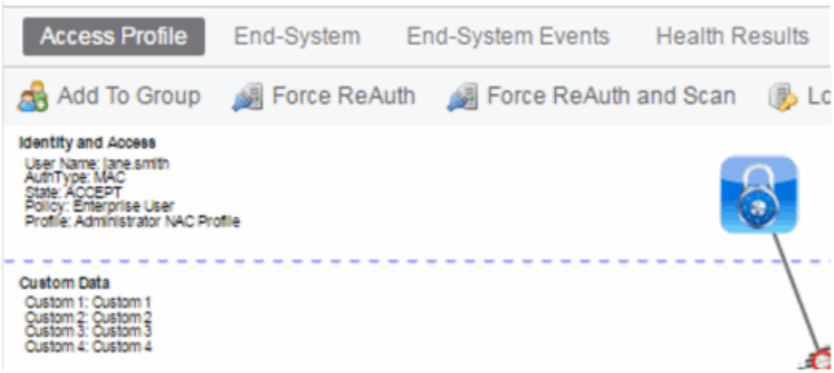
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/importEndSystemInfoFromCsv?csvData=50:7A:55:6F:24:35,Custom 1,Custom 2,Custom 3,Custom 4&isSave=true



Method: processNacRequestArrFromCsv

Process Extreme Access Control requests from a CSV file.

Parameters

Name	Type	Description
csvData	string	The CSV data must be in the following format: Reauthentication operation – MAC address End-system override (FULL_MAC) – MAC address, end-system group, description End-system override (FULL_IP) – IP address, end-system group, description End-system override (HOSTNAME) – hostname, end-system group, description User override – username, user group, description
oper	string	Operation request, available options are: reauth – force reauthentication esoverride – end-system override useroverride – user override
isAdd	Boolean	**True** for adding the request, **false** for deleting it
type	string	End-system types, options are: FULL_MAC FULL_IP HOSTNAME

Returns

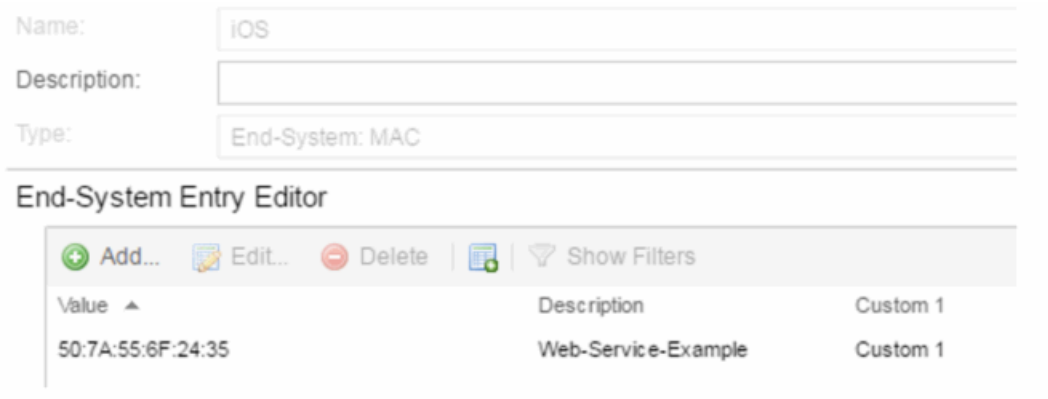
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/processNacRequestArrFromCsv?csvData=50:7A:55:6F:24:35,iOS,Web-Service-Example&oper=esoverride&isAdd=true&type=FULL_MAC



Method: processNacRequestFromCsv

Process Extreme Access Control requests from a CSV file.

Parameters

Name	Type	Description
csvData	string	The CSV data must be in the following format: Reauthentication operation – MAC address End system override (FULL_MAC) – MAC address, end-system group, description End system override (FULL_IP) – IP address, end-system group, description End system override (HOSTNAME) – hostname, end-system group, description User override – username, user group, description
oper	string	Operation request, available options are: reauth – force reauthentication esoverride – end-system override useroverride – user override
isAdd	Boolean	**True** for adding the request, **false** for deleting it
type	string	End-system types, options are: FULL_MAC FULL_IP HOSTNAME

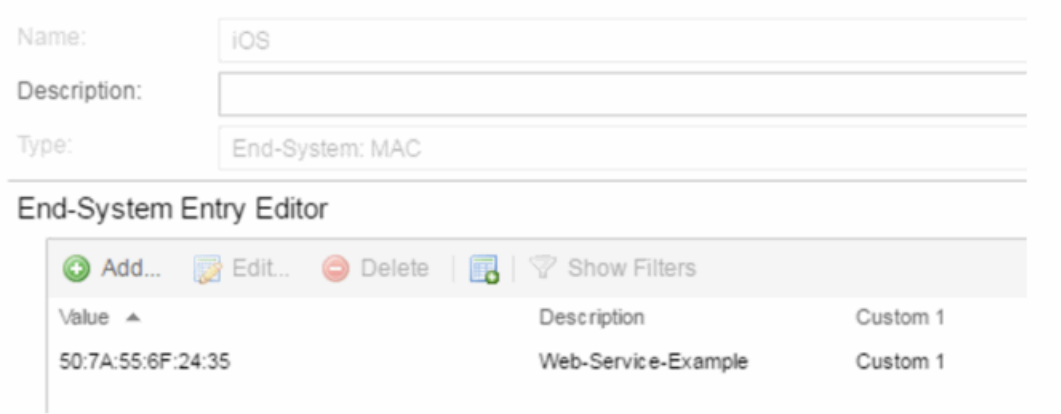
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/processNacRequestFromCsv?csvData=50:7A:55:6F:24:35,iOS,Web-Service-Example&oper=esoverride&isAdd=true&type=FULL_MAC



Method: reauthenticate

Force an end-system to reauthenticate.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system
assess	boolean	True to reassess the end-system

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/reauthenticate?macAddress=50:7A:55:6F:24:35&assess=false

Method: reauthenticateEx

Force an end-system to reauthenticate. This operation is similar to reauthenticate, but returns a verbose message.

Parameters

Name	Type	Description
macAddress	string	MAC address of the end-system
assess	boolean	**True** to reassess the end-system

Returns

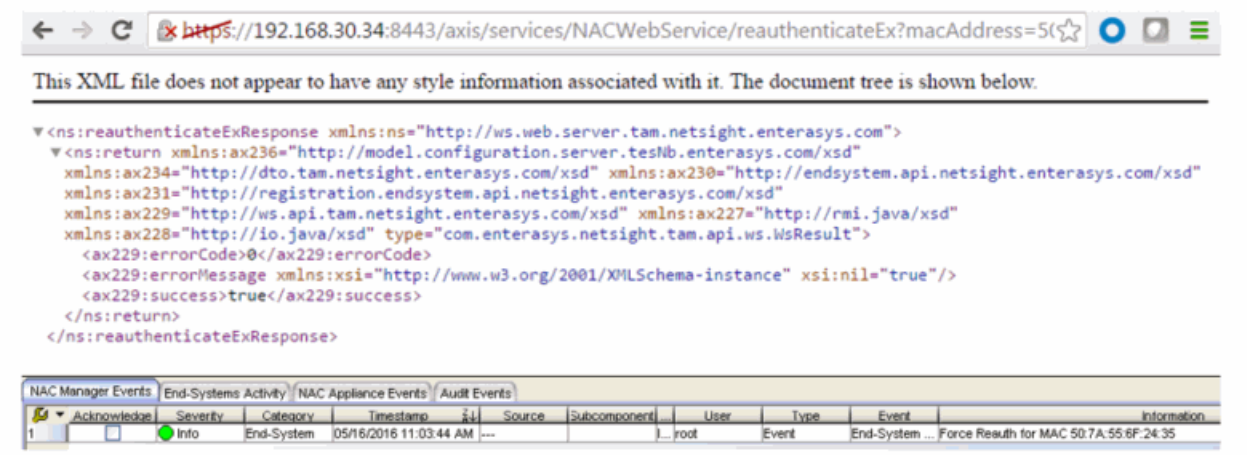
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/reauthenticateEx?macAddress=50:7A:55:6F:24:35&assess=false



Method: removeHostnameFromEndSystemGroup

Remove an end-system hostname from an Extreme Access Control end-system group.

Parameters

Name	Type	Description
endSystemGroup	string	End-system group name you are changing
hostname	string	The hostname of the end-system
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

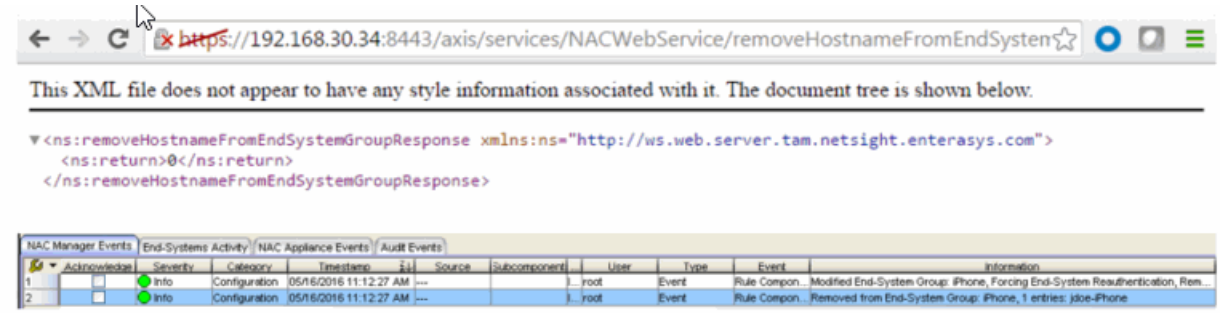
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeHostnameFromEndSystemGroup?endSystemGroup=iPhone&hostname=jdoe-iPhone&reauthenticate=true



Method: removeHostnameFromEndSystemGroupEx

Remove an end-system hostname from an Extreme Access Control end-system group. This operation is similar to removeHostnameFromEndSystemGroup, but returns a verbose message.

Parameters

Name	Type	Description
endSystemGroup	string	End-system group name you are changing
hostname	string	The hostname of the end-system
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

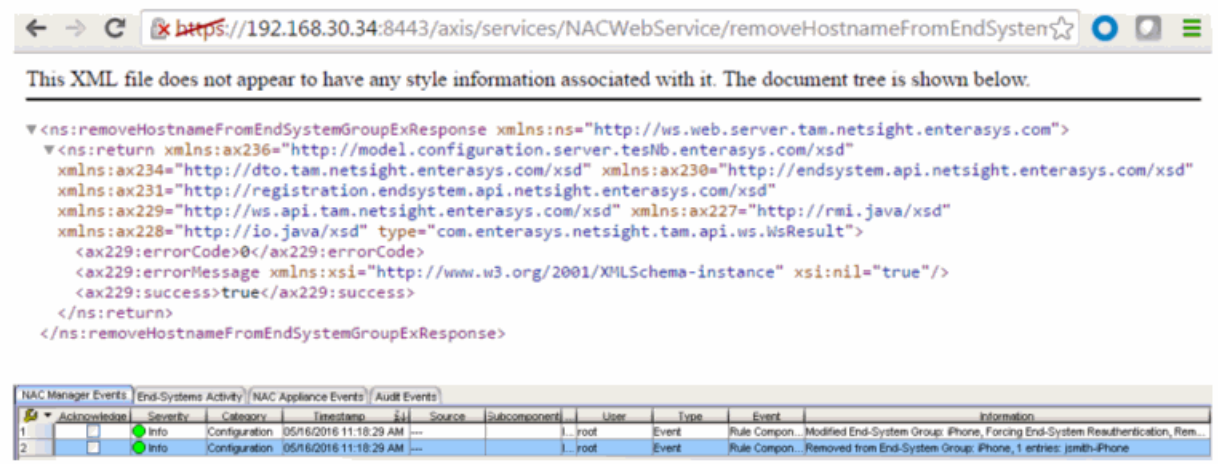
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeHostnameFromEndSystemGroupEx?endSystemGroup=iPhone&hostname=jsmith-iPhone&reauthenticate=true



Method: removeIPFromEndSystemGroup

Remove an end system IP address from an Extreme Access Control end-system group.

Parameters

Name	Type	Description
endSystemGroup	string	End-system group name you are changing
ipAddress	string	IP address of the end-system
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

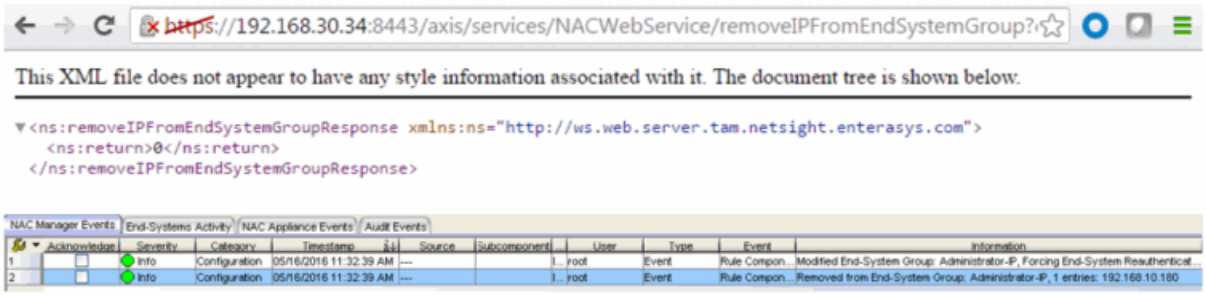
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeIPFromEndSystemGroup?endSystemGroup=Administrator-IP&ipAddress=192.168.10.180&reauthenticate=true



Method: removeIPFromEndSystemGroupEx

Remove an end-system IP address from an Extreme Access Control end-system group. This operation is similar to removeIPFromEndSystemGroup, but returns a verbose message.

Parameters

Name	Type	Description
endSystemGroup	string	End-system group name you are changing
ipAddress	string	IP address of the end-system
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

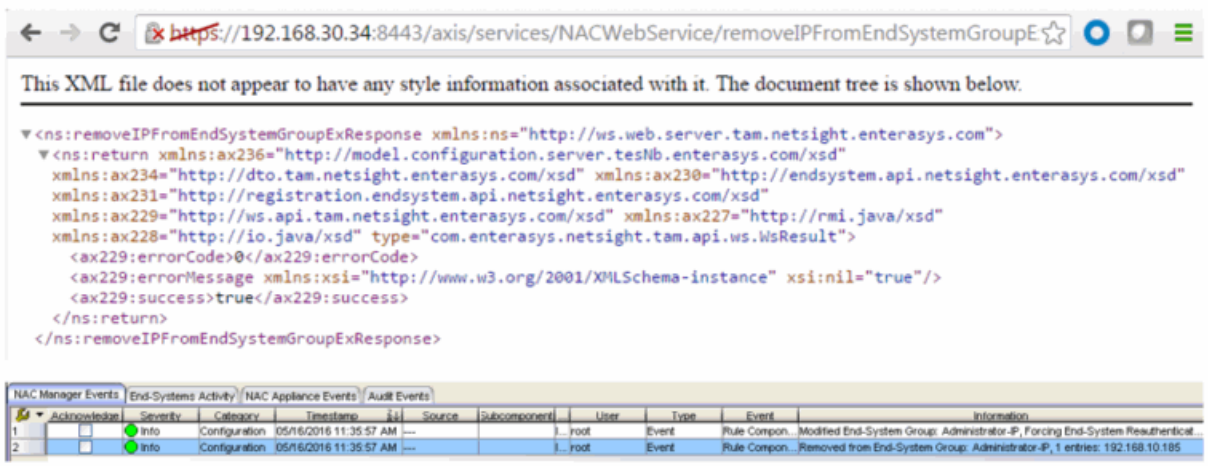
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeIPFromEndSystemGroupEx?endSystemGroup=Administrator-IP&ipAddress=192.168.10.185&reauthenticate=true



Method: removeMACFromBlacklist

Remove an end-system MAC address from the blacklist end-system group.

Parameters

Name	Type	Description
macAddress	string	The MAC address of the end-system
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

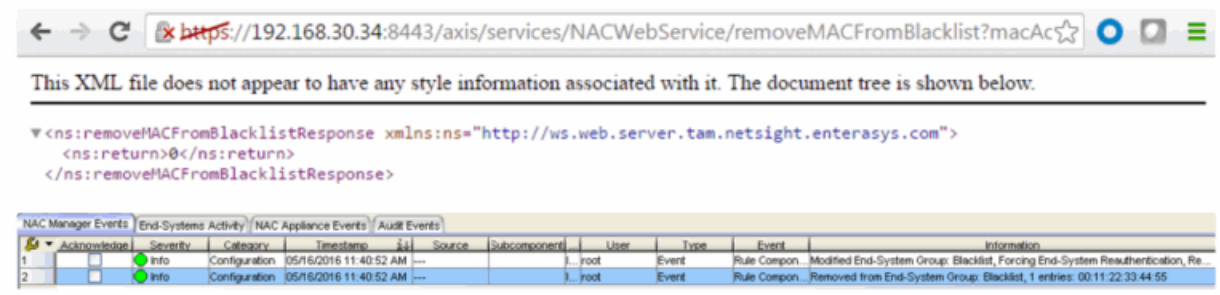
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeMACFromBlacklist?macAddress=00:11:22:33:44:55&reauthenticate=true



Method: removeMACFromBlacklistEx

Remove an end-system MAC address from the blacklist end-system group. This operation is similar to removeMACFromBlacklist, but returns a verbose message.

Parameters

Name	Type	Description
macAddress	string	The MAC address of the end-system
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

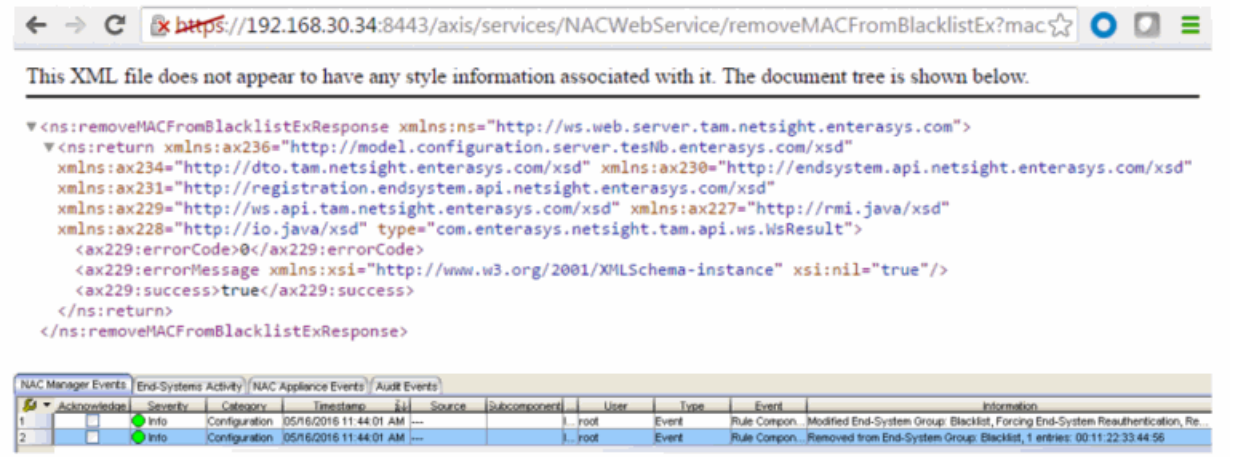
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeMACFromBlacklistEx?macAddress=00:11:22:33:44:56&reauthenticate=true



Method: removeMACFromEndSystemGroup

Remove an end-system MAC address from an Extreme Access Control end-system group.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
macAddress	string	The MAC address of the end-system
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeMACFromEndSystemGroup?endSystemGroup=iOS&macAddress=00:11:22:33:44:55&reauthenticate=true

Method: removeMACFromEndSystemGroupEx

Remove an end-system MAC address from an Extreme Access Control end-system group. This operation is similar to removeMACFromEndSystemGroup, but returns a verbose message.

Parameters

Name	Type	Description
endSystemGroup	string	The end-system group name you are changing
macAddress	string	The MAC address of the end-system
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

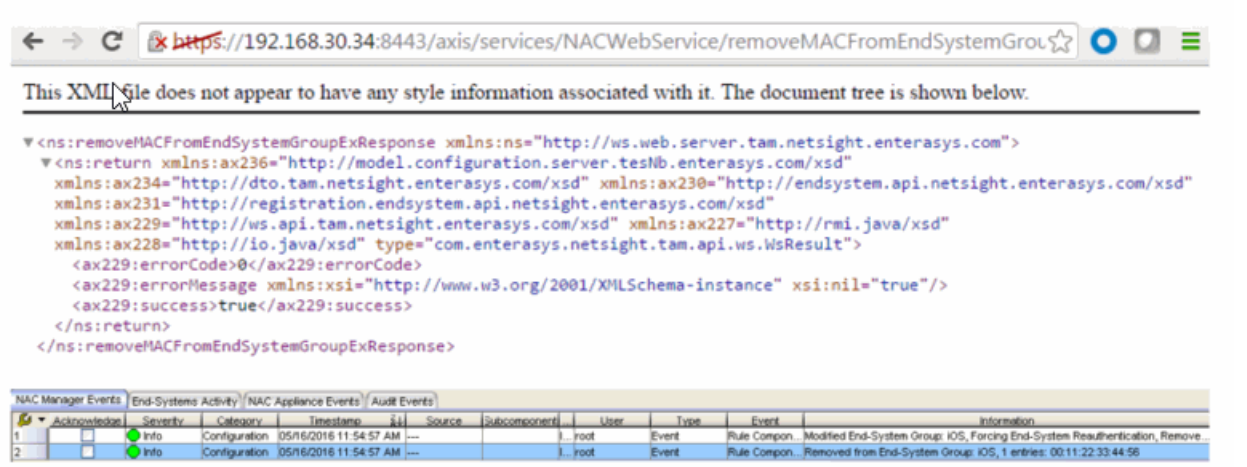
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeMACFromEndSystemGroupEx?endSystemGroup=iOS&macAddress=00:11:22:33:44:56&reauthenticate=true



Method: removeUsernameFromUserGroup

Remove a username from an Extreme Access Control end-system group.

Parameters

Name	Type	Description
usergroup	string	The username group name you are changing
username	string	Username of the end-system
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

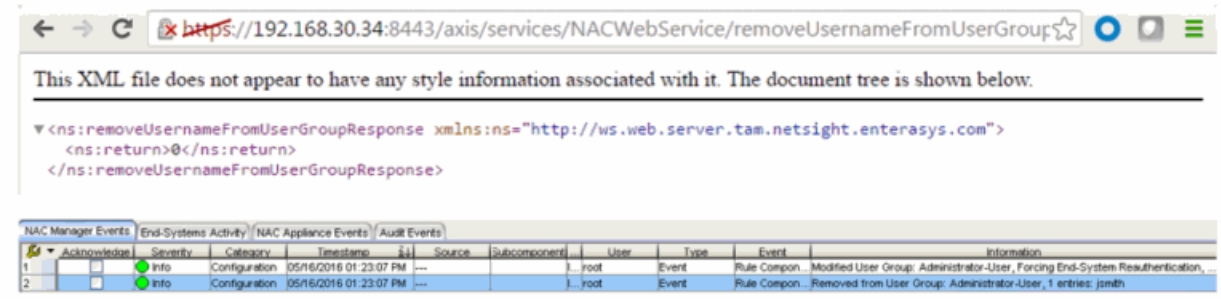
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeUsernameFromUserGroup?userGroup=Administrator-User&username=jsmith&reauthenticate=true



Method: removeUsernameFromUserGroupEx

Remove a username from an Extreme Access Control end-system group. This operation is similar to removeUsernameFromUserGroup, but returns a verbose message.

Parameters

Name	Type	Description
userGroup	string	The username group name you are changing
username	string	Username of the end-system
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

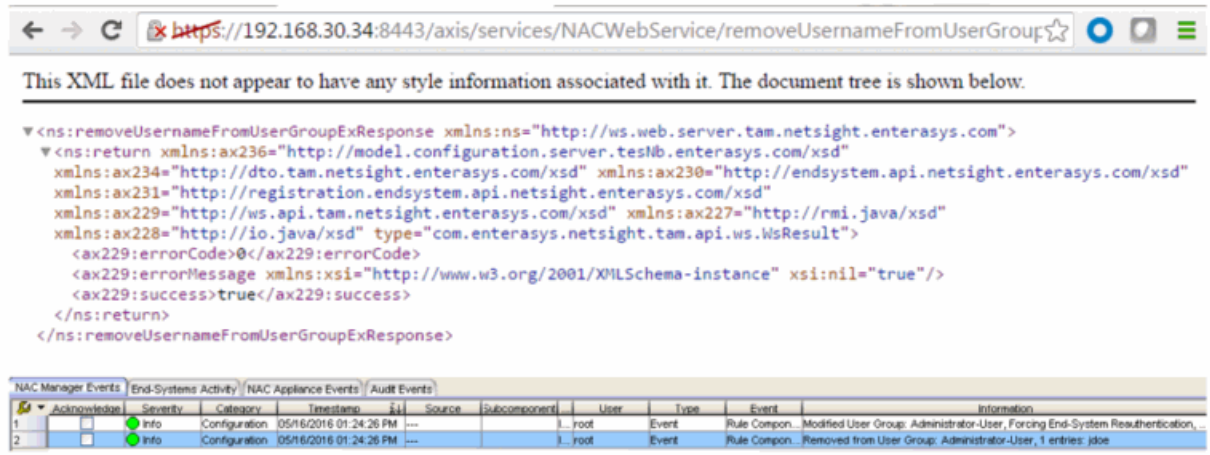
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeUsernameFromUserGroupEx?userGroup=Administrator-User&username=jdoe&reauthenticate=true



Method: removeValueFromNamedList

Remove a value to an Extreme Access Control end-system group. This is a generic operation, so ensure you use the correct value and end-system group.

Parameters

Name	Type	Description
list	string	The end-system group you are changing
value	string	The value to add
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

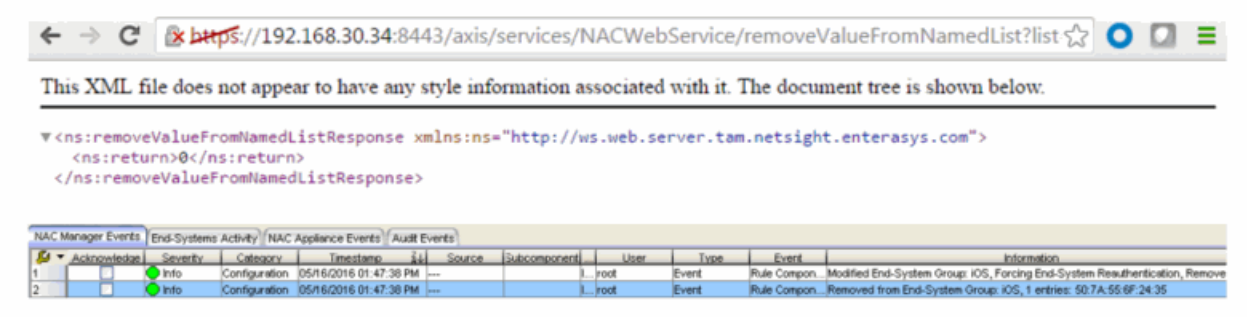
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeValueFromNamedList?list=iOS&value=50:7A:55:6F:24:35&reauthenticate=true



Method: removeValueFromNamedListEx

Remove a value to an Extreme Access Control end-system group. This operation is similar to removeValueFromNamedList, but returns a verbose message.

Parameters

Name	Type	Description
list	string	The end-system group you are changing
value	string	The value to add
reauthenticate	boolean	Set to **true** to force reauthentication on the affected end-system

Returns

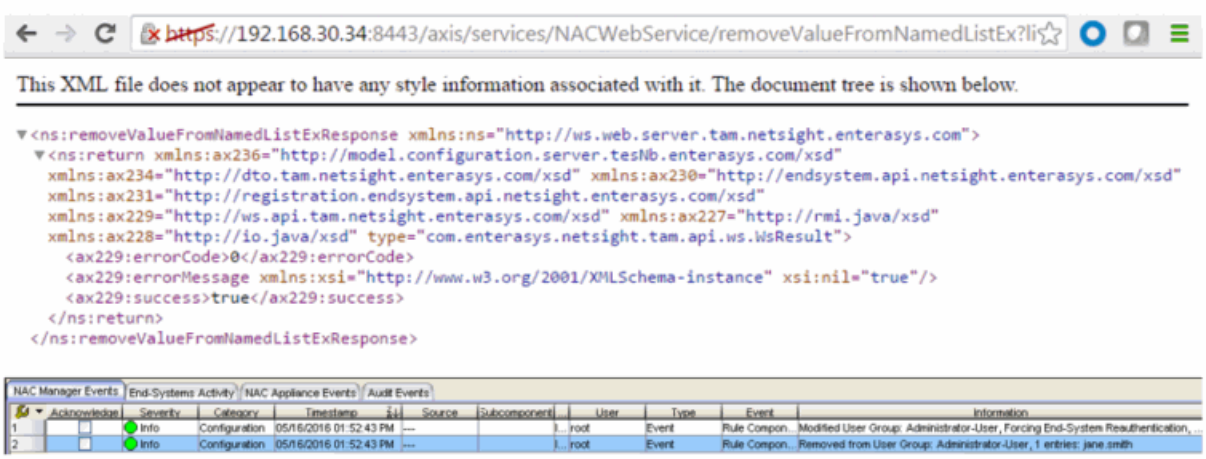
Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/removeValueFromNamedListEx?list=Administrator-User&value=jane.smith&reauthenticate=true



Method: saveEndSystemInfo

Update end-system information. The end-system is identified by using the macAddress, ipAddress, or hostname property.

Parameters

Name	Type	Description
properties	string	Custom field data in custom1=value1,custom2=value2,custom3=value3,custom4=value4 format

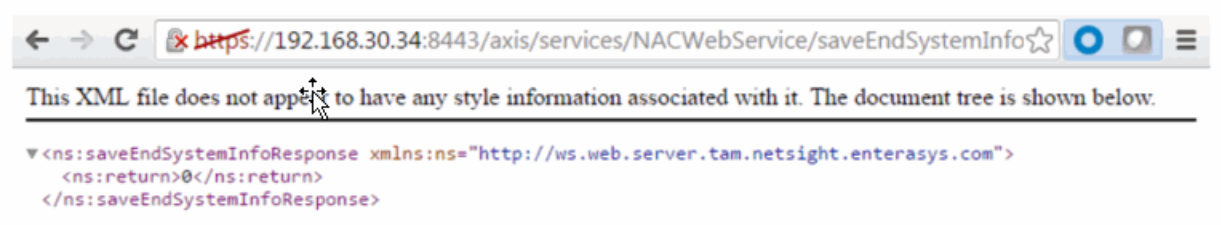
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/saveEndSystemInfo?properties=macAddress=EC:1F:72:B9:37:91,custom1=Custom1,custom2=Custom2,custom3=Custom3,custom4=Custom4



Method: saveEndSystemInfoByHostname

Update end-system information.

Parameters

Name	Type	Description
hostname	string	The hostname of the end-system
custom1	string	Custom field 1 value
custom2	string	Custom field 2 value
custom3	string	Custom field 3 value
custom4	string	Custom field 4 value

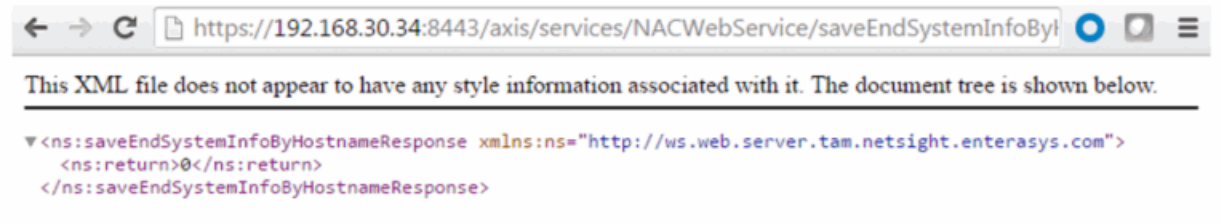
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/saveEndSystemInfoByHostname?hostname=MacBookPro.demo.com&custom1=Custom1&custom2=Custom2&custom3=Custom3&custom4=Custom4



Method: saveEndSystemInfoByIp

Update end-system information.

Parameters

Name	Type	Description
ipAddress	string	The IP address of the end-system
custom1	string	Custom field 1 value
custom2	string	Custom field 2 value
custom3	string	Custom field 3 value
custom4	string	Custom field 4 value

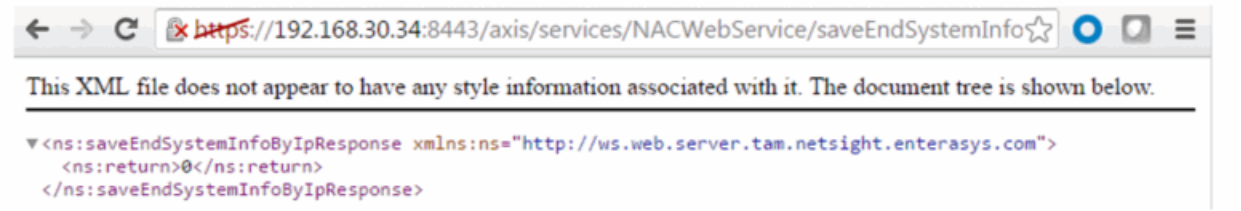
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/saveEndSystemInfoByIp?ipAddress=192.168.10.178&custom1=Custom1&custom2=Custom2&custom3=Custom3&custom4=Custom4



Method: saveEndSystemInfoByMac

Update end-system information.

Parameters

Name	Type	Description
macAddress	string	The MAC address of the end-system

Name	Type	Description
custom1	string	Custom field 1 value
custom2	string	Custom field 2 value
custom3	string	Custom field 3 value
custom4	string	Custom field 4 value

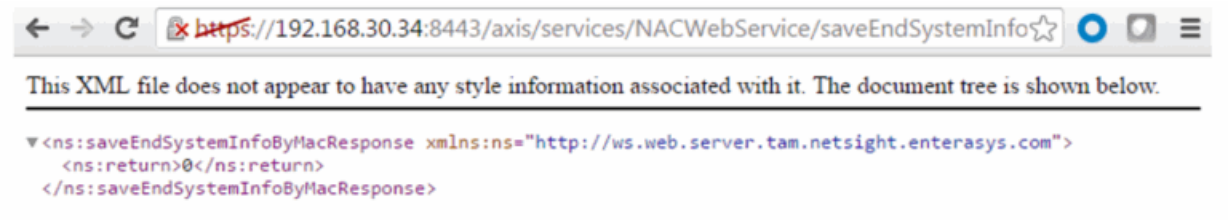
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/saveEndSystemInfoByMac?macAddress=80:A5:89:33:67:37&custom1=Custom1&custom2=Custom2&custom3=Custom3&custom4=Custom4



Method: saveEndSystemInfoEx

Update end-system information.

Parameters

Name	Type	Description
info	EndSystemInfo	End-system information you are saving

Returns

Returns a WsEndSystemInfoResult with a structure defined by the following table.

Name	Type	Description
endSystemInfo	EndSystemInfo	End-system for which information is saved

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Method: saveLocalUser

Create or update a user in the local user database.

Parameters

Name	Type	Description
propString	string	The properties string used to create/update the user, string is in the following format: loginId=value1,domainName=value2,description =value3,enabled=true,password=value4
propString	string	The user requesting the operation

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/saveLocalUser?propString=loginId=jdoe,domainName=Default,description=Sample-User,enabled=true,password=mysuperduperpassword

Method: saveLocalUserEx

Create or update a user in the local user database.

Parameters

Name	Type	Description
user	LocalUser	Local user to save in the database
requestingUser	string	The user requesting the operation

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Method: saveRegisteredDevice

Create a new registered device.

Parameters

Name	Type	Description
propString	string	The properties string used to register the device, string is in the following format: userName=value1,macAddress= value2,ipAddress=value3,state= Approved,description =value4,applianceGroup=value5
requestingUser	string	The user requesting the operation

Returns

The operation returns an integer error code.

Method: saveRegisteredDeviceEx

Create a new registered device.

Parameters

Name	Type	Description
device	RegisteredDevice	Device to register
requestingUser	string	The user requesting the operation

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Method: saveRegisteredDevices

Create a new registered device.

Parameters

Name	Type	Description
propStrings	string	The properties string used to register the device, string is in the following format: userName=value1,macAddress= value2,ipAddress=value3,state= Approved,description=value4, applianceGroup=value5
requestingUser	string	The user requesting the operation

Returns

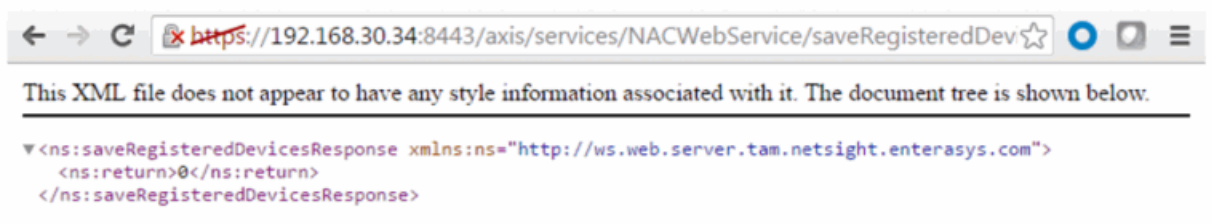
The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/saveRegisteredDevi

ces?propStrings=userName=jane.smith,macAddress=80:D6:05:4A:D6:C5,state=Approved,applianceGroup=Default&requestingUser=root



Method: saveRegisteredDeviceWithSponsorship

Create a new registered device with sponsorship.

Parameters

Name	Type	Description
propString	string	The properties string used to register the device, string is in the following format: userName=value1,macAddress= value2,ipAddress=value3,state=Approved, description=value4,applianceGroup=value5
requestingUser	string	The user requesting the operation
defaultSponsorEmail	string	Sponsor email address
nacApplianceIp	string	Extreme Access Control engine IP address

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/saveRegisteredDeviceWithSponsorship?propString=userName=jane.smith,macAddress=80:D6:05:4A:D6:C5,state=Approved,applianceGroup=Default&requestingUser=root&defaultSponsorEmail=jdoe@jdoe.com&nacApplianceIp=192.168.30.35

Method: saveRegisteredDeviceWithSponsorshipEx

Create a new registered device with sponsorship.

Parameters

Name	Type	Description
device	RegisteredDevice	Device to register
requestingUser	string	The user requesting the operation
defaultSponsorEmail	string	Sponsor email address
nacApplianceIp	string	Extreme Access Control engine IP address

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Method: saveRegisteredUser

Create a new registered user.

Parameters

Name	Type	Description
propString	string	The properties string used to register the device, string is in the following format: userName=value1,applianceGroup=value2

Name	Type	Description
requestingUser	string	The user requesting the operation

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/saveRegisteredUser?propString=userName=john.doe,applianceGroup=Default&requestingUser=root

Method: saveRegisteredUserEx

Create a new registered user.

Parameters

Name	Type	Description
user	RegisteredUser	User to register
requestingUser	string	The user requesting the operation

Returns

Returns a WsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Method: saveRegisteredUsers

Create a new registered user.

Parameters

Name	Type	Description
propStrings	string	The properties string used to register the device, string is in the following format: userName=value1,applianceGroup=value2
requestingUser	string	The user requesting the operation

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/saveRegisteredUsers?propStrings=userName=john.smith,applianceGroup=Default&requestingUser=root

Method: updateRegisteredDevice

Update an existing registered device.

Parameters

Name	Type	Description
propString	string	The properties string used to register the device, string is in the following format: userName=value1,macAddress=value2, ipAddress=value3,state=Approved, description=value4,applianceGroup=value5
requestingUser	string	The user requesting the operation

Returns

The operation returns an integer error code.

Method: updateRegisteredUser

Update an existing registered user.

Parameters

Name	Type	Description
propString	string	The properties string used to register the device, string is in the following format: userName=value1,applianceGroup=value2
requestingUser	string	The user requesting the operation

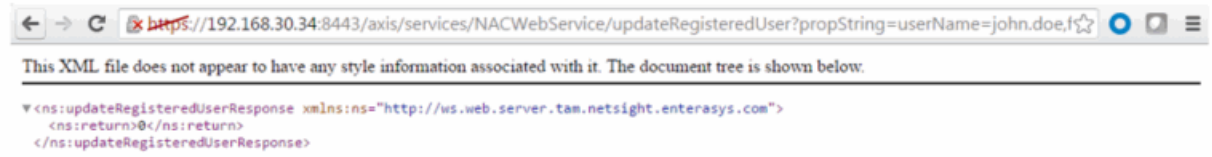
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NACWebService/updateRegisteredUser?propString=userName=john.doe,firstName=John,lastName=Doe,applianceGroup=Default&requestingUser=root



Netsight Device Web Service

The NetSight device web service provides an external interface to retrieve and modify the managed devices in the database.

https://<Extreme Management Center Server IP>:<port>/axis/services/NetSightDeviceWebService?wsdl

- Method: addAuthCredential
- Method: addAuthCredentialEx
- Method: addCredentialEx
- Method: addDeviceEx
- Method: addProfileEx
- Method: deleteDeviceByIpEx
- Method: exportDevicesAsNgf
- Method: getAllDevices
- Method: getDeviceByIpAddressEx
- Method: getSnmpCredentialAsNgf
- Method: importDevicesAsNgfEx
- Method: isIpV6Enabled
- Method: isNetSnmpEnabled
- Method: updateAuthCredential
- Method: updateAuthCredentialEx
- Method: updateCredential
- Method: updateCredentialEx
- Method: updateDevicesEx
- Method: updateProfile
- Method: updateProfileEx

Method: addAuthCredential

Add a command line interface credential to the database.

Parameters

Name	Type	Description
username	string	Username for the credential
description	string	Brief description of the credential
loginPassword	string	Password for the credential
enablePassword	string	Enable password for the credential
configurationPassword	string	Configuration password for the credential
type	string	Type of login session, available options are: -SSH -Telnet

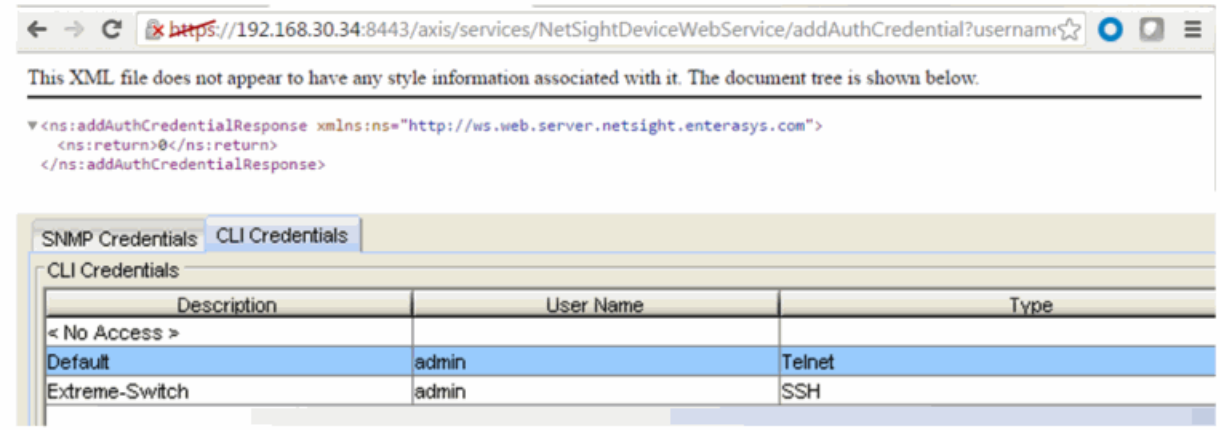
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/addAuthCredential?username=admin&description=Extreme-Switch&loginPassword=password&enablePassword=&configurationPassword=&type=SSH



Method: addAuthCredentialEx

Add a command line interface credential to the database. This operation is similar to addAuthCredential, but returns a verbose message.

Parameters

Name	Type	Description
username	string	Username for the credential
description	string	Brief description of the credential
loginPassword	string	Password for the credential
enablePassword	string	Enable password for the credential
configurationPassword	string	Configuration password for the credential
type	string	Type of login session, available options are: -SSH -Telnet

Returns

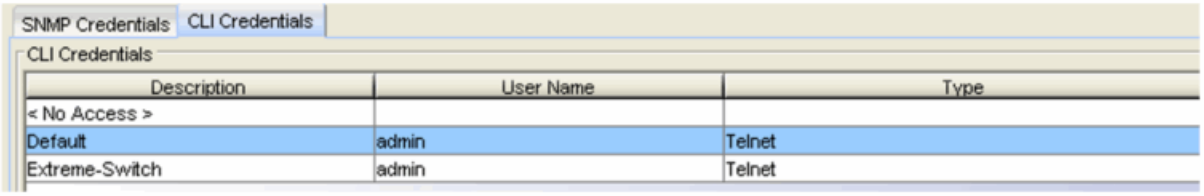
Returns a NsWsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/addAuthCredentialEx?username=admin&description=Extreme-Switch&loginPassword=password&enablePassword=&configurationPassword=&type=Telnet



Method: addCredentialEx

Add a SNMP credential to the database.

Parameters

Name	Type	Description
name	string	Name of the credential
snmpVersion	int	SNMP version
communityName	string	SNMP community name
userName	string	SNMPv3 username
authPassword	string	SNMPv3 authentication password
authType	string	SNMPv3 authentication type, available options are: -MD5 -SHA
privPassword	string	SNMPv3 privacy password
privType	string	SNMPv3 privacy type, available options are: -AED -DES

Returns

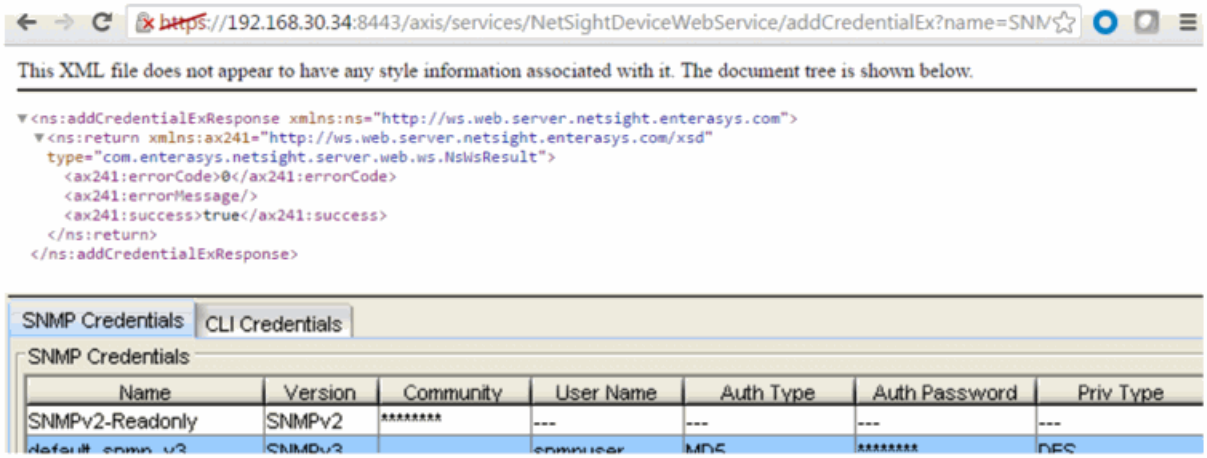
Returns a NsWsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/addCredentialEx?name=SNMPv2-Readonly&snmpVersion=2&communityName=readonly&userName=&authPassword=&authType=&privPasswod=&privType=



Method: addDeviceEx

Add a device to the database.

Parameters

Name	Type	Description
ipAddress	string	IP address of the device
profileName	string	Profile name associated to the device
snmpContext	string	SNMP context associated to the device
nickName	string	Device nickname

Returns

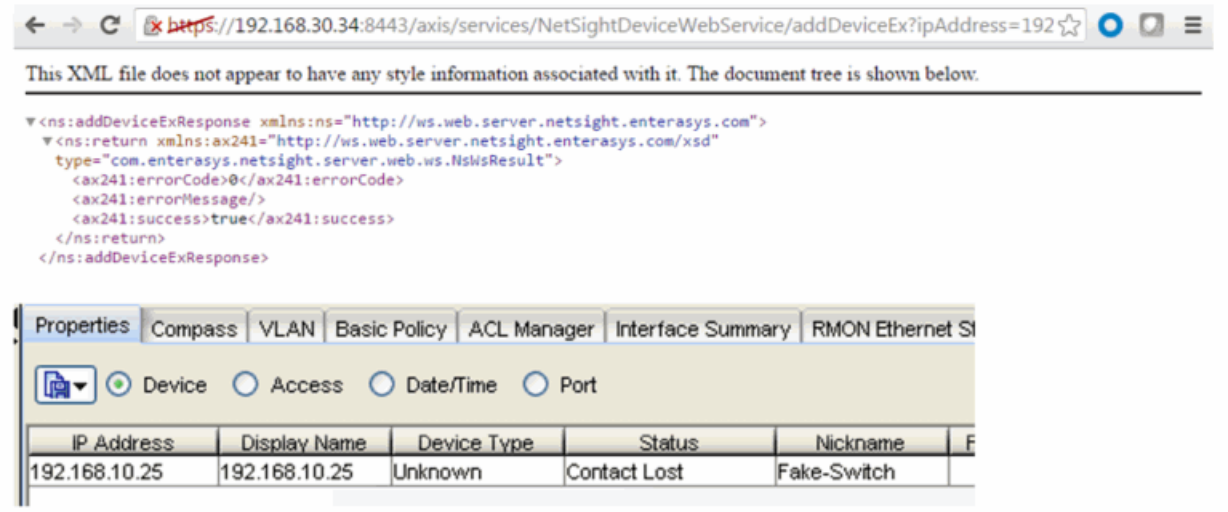
Returns a NsWsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/addDeviceEx?ipAddress=192.168.10.25&profileName=public_v1_Profile&snmpContext=&nickName=Fake-Switch



Method: addProfileEx

Add credential profile to the database.

Parameters

Name	Type	Description
name	string	Name of the profile
snmpVersion	int	SNMP version

Name	Type	Description
read	string	SNMP read only credential
write	string	SNMP read/write credential
maxAccess	string	SNMP max access credential
auth	string	CLI credential

Returns

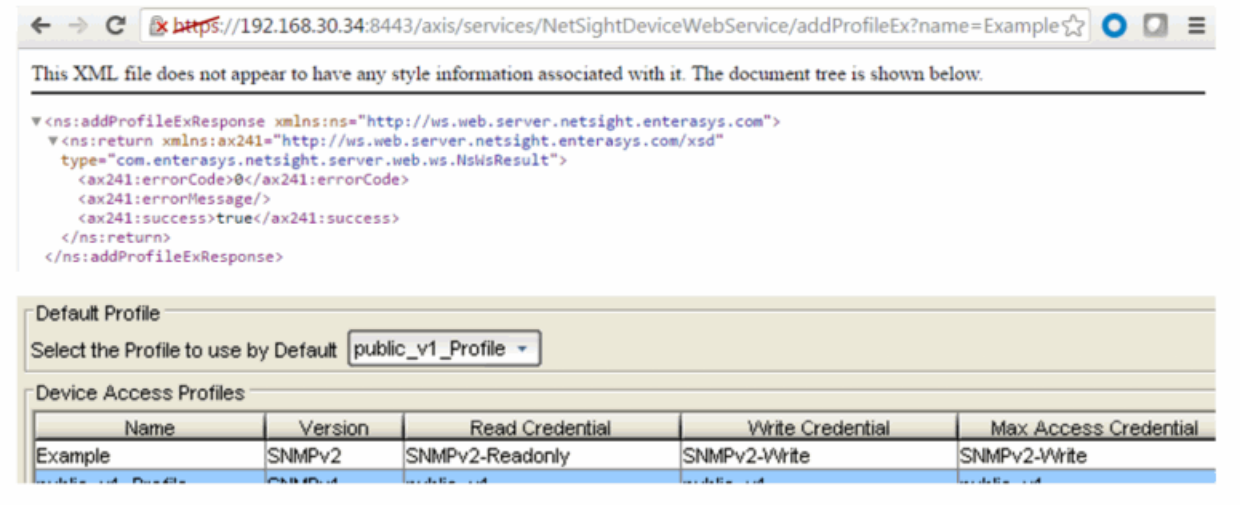
Returns a NsWsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/addProfileEx?name=Example&snmpVersion=2&read=SNMPv2-Readonly&write=SNMPv2-Write&maxAccess=SNMPv2-Write&auth=Extreme-Switch



Method: deleteDeviceByIpEx

Delete a device from the database.

Parameters

Name	Type	Description
ipAddress	string	IP address of the device

Returns

Returns a NsWsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/deleteDeviceByIpEx?ipAddress=192.168.10.25

Method: exportDevicesAsNgf

Export all devices in a NetSight grouping format.

Returns

Returns a string representation of all devices from the database.

Example

Execute the following web service with a browser:
https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/exportDevicesAsNgf

Method: getAllDevices

Retrieve all the devices from the database.

Returns

Returns a WsDeviceListResult with a structure defined by the following table.

Name	Type	Description
data	WsDevice	Device Information
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful
tableTotalRecords	int	Total number of available records

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/getAllDevices

Method: getDeviceByIpAddressEx

Retrieve the device based on an IP address.

Parameters

Name	Type	Description
ipAddress	string	IP address of the device

Returns

Returns a WsDeviceListResult with a structure defined by the following table.

Name	Type	Description
data	WsDevice	Device Information
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful
tableTotalRecords	int	Total number of available records

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/getDeviceByIpAddressEx?ipAddress=192.168.10.10

Method: getSnmpCredentialAsNgf

Retrieve SNMP credentials, in NetSight Grouping Format, for a device.

Parameters

Name	Type	Description
ipAddress	string	

Returns

Returns a string representation of device settings from the database.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/getSnmpCredentialAsNgf?ipAddress=192.168.10.10

Method: importDevicesAsNgfEx

Import a list of devices, in NetSight grouping format, to the database.

Parameters

Name	Type	Description
ngfDevices	string	Devices in NetSight grouping format

Returns

Returns a NsWsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/importDevicesAsNgfEx?ngfDevices=cliUsername=admin cliType=Telnet snmp=v1 dev=192.168.10.25 mt=2 pg=1 ro=public rw=public su=public cliDesc=Default cliUsername=admin cliType=Telnet snmp=v1

Method: isIpV6Enabled

Queries the Extreme Management Center server to determine if IPv6 support is enabled.

Returns

Returns **true** if IPv6 is supported.

Example

Execute the following web service with a browser:
https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/isIpV6Enabled

Method: isNetSnmpEnabled

Queries the Extreme Management Center server to determine if the Net SNMP stack is enabled.

Returns

Returns true if IPv6 is supported.

Example

Execute the following web service with a browser:
https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/isNetSnmpEnabled

Method: updateAuthCredential

Update command line interface credentials.

Parameters

Name	Type	Description
username	string	Username for the credential
description	string	Brief description of the credential
loginPassword	string	Password for the credential
enablePassword	string	Enable password for the credential
configurationPassword	string	Configuration password for the credential
type	string	Type of login session, available options are: -SSH -Telnet

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/updateAuthCredential?username=admin&description=Extreme-Switch&loginPassword=login&enablePassword=enable&configurationPassword=config&type=SSH

Method: updateAuthCredentialEx

Update command line interface credentials. This operation is similar to updateAuthCredential, but returns a verbose message.

Parameters

Name	Type	Description
username	string	Username for the credential

Name	Type	Description
description	string	Brief description of the credential
loginPassword	string	Password for the credential
enablePassword	string	Enable password for the credential
configurationPassword	string	Configuration password for the credential
type	string	Type of login session, available options are: -SSH -Telnet

Returns

Returns a NsWsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	True if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/updateAuthCredentialEx?username=admin&description=Extreme-Switch&loginPassword=login&enablePassword=enable&configurationPassword=config&type=Telnet

Method: updateCredential

Update SNMP credential.

Parameters

Name	Type	Description
name	string	Name of the credential
communityName	string	SNMP version
userName	string	SNMP community name
authPassword	string	SNMPv3 username
authType	string	SNMPv3 authentication password
privPassword	string	SNMPv3 authentication type, available options are: -MD5 -SHA
privType	string	SNMPv3 privacy password
		SNMPv3 privacy type, available options are: -AED -DES

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/updateCredential?name=SNMPv2-Readonly&snmpVersion=2&communityName=public&userName=&authPassword=&authType=&privPasswod=&privType=

Method: updateCredentialEx

Update SNMP credential. This operation is similar to updateCredential, but returns a verbose message.

Parameters

Name	Type	Description
name	string	Name of the credential
communityName	string	SNMP version
userName	string	SNMP community name
authPassword	string	SNMPv3 username
authType	string	SNMPv3 authentication password
privPassword	string	SNMPv3 authentication type, available options are: -MD5 -SHA
privType	string	SNMPv3 privacy password
		SNMPv3 privacy type, available options are: -AED -DES

Returns

Returns a NsWsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/updateCredentialEx?name=SNMPv2-Readonly&snmpVersion=2&communityName=Read_Only&userName=&authPassword=&authType=&privPasswod=&privType=

Method: updateDevicesEx

Update a set of devices in the database.

Parameters

Name	Type	Description
devices	string	Updated devices to be saved in the database

Returns

Returns a NsWsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Method: updateProfile

Update credential profile in the database.

Parameters

Name	Type	Description
name	string	Name of the profile
read	string	SNMP read only credential
write	string	SNMP read/write credential
maxAccess	string	SNMP max access credential
authCred	string	CLI credential

Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/updateProfile?name=Example&read=public_v2&write=SNMPv2-Write&maxAccess=SNMPv2-Write&authCred=Default

Method: updateProfileEx

Update credential profile in the database. This operation is similar to updateProfile, but returns a verbose message.

Parameters

Name	Type	Description
name	string	Name of the profile
read	string	SNMP read only credential
write	string	SNMP read/write credential
maxAccess	string	SNMP max access credential
authCredName	string	CLI credential

Returns

Returns a NsWsResult with a structure defined by the following table.

Name	Type	Description
errorCode	int	Please see the Web Service Error Codes
errorMessage	string	Error message in readable text
success	boolean	**True** if operation is successful

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/NetSightDeviceWebService/updateProfileEx?name=Example&read=public_v2&write=public_v2&maxAccess=SNMPv2-Write&authCredName=Extreme-Switch

Policy Web Service

The Policy web service provides an external interface to Policy Manager.

https://<Extreme Management Center Server IP>:<port>/axis/services/PolicyService?wsdl

- Method: addRoleMapping
- Method: addRule
- Method: addSwitchesToDomain
- Method: getRoleMapping
- Method: removeRoleMapping

Method: addRoleMapping

Add an IP or MAC role mapping to the specified switches.

Parameters

Name	Type	Description
station	string	IP/MAC address to add
role	string	Role name to map station to
devices	string	IP address of the switches

Returns

The operation returns an integer error code.

Error Code	Description
0	Operation successful
1	General error
2	Truststore missing
3	Bad parameters
4	Timeout
5	Connection refused
6	Connection reset
7	No server
8	Unauthorized transport
9	Server communication failed
10	Policy domain lock failure
11	Policy domain save failure
12	Nonvolatile mapping exists
13	Mapping role not found
14	Mapping unknown device

Method: addRule

Add a rule to a service in a specified policy domain. The policy domain and service you are creating if they do not exist.

Parameters

Name	Type	Description
domainName	string	Policy domain to which to add the rule
serviceName	string	Service to which to add the rule
ruleName	string	Rule name, a null or AUTO value generates the name based on the traffic description data

Name	Type	Description
trafficDescrType	string	Rule type, available options are: 1 – Ethernet type 2 – LLC DSAP SSAP 3 – IP type of service 4 – IP protocol 5 – IPX class of service 6 – IPX packet type 7 – Source IP address 8 – Destination IP address 9 – Bilateral IP address 10 – Source IPX network 11 – Destination IPX network 12 – Bilateral IPX network 13 – UDP source port 14 – UDP destination port 15 – UDP bilateral port 16 – TCP source port 17 – TCP destination port 18 – TCP bilateral port 19 – IPX source socket 20 – IPX destination socket 21 – IPX bilateral socket 22 – Source MAC address 23 – Destination MAC address 24 – Bilateral MAC address 25 – IP fragment 26 – IP UDP source port range 27 – IP UDP destination port range 28 – IP UDP bilateral port range 29 – IP TCP source port range 30 – IP TCP destination port range 31 – IP TCP bilateral port range 32 – ICMP Type 33 – VLAN ID 34 – TCI 43 – IPv6 source address 44 – IPv6 destination address 45 – IPv6 bilateral address

Name	Type	Description
		46 – IPv6 source socket 47 – IPv6 destination socket 48 – IPv6 bilateral socket 49 – IPv6 type 50 – IPv6 flow label
trafficDescrValue	string	Value associated with the rule
trafficDescrMask	string	Mask associated with value, use 0 for no mask
expandedTrafficDescrValue	string	Additional value for rules that require multiple values i.e. TCP port + IP address
expandedTrafficDescrMask	string	Mask associated to the additional value, only applicable to multiple value rules
vlanAction	string	VLAN action, available options are: -1 – None 0 – Discard 4095 – Permit

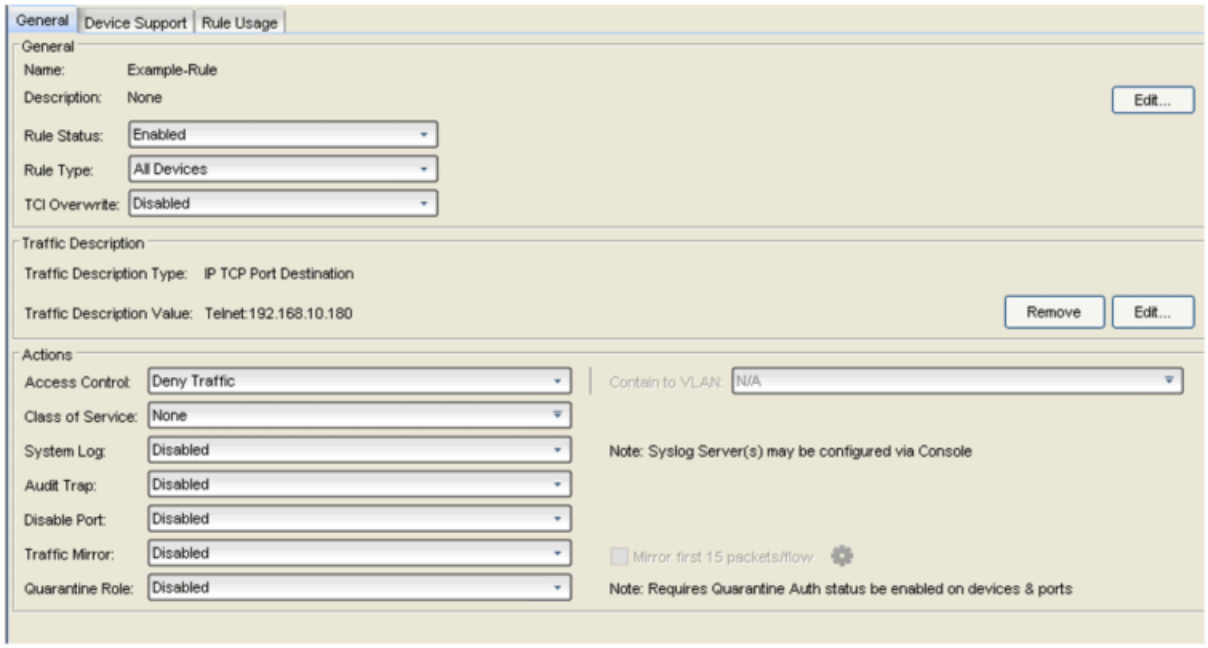
Returns

The operation returns an integer error code.

Example

Execute the following web service with a browser. The web service creates a policy rule that drops all telnet (port 23) from 192.168.10.180.

https://192.168.30.34:8443/axis/services/PolicyService/addRule?domainName=Default Policy Domain&serviceName=Example-Service&ruleName=Example-Rule&trafficDescrType=17&trafficDescrValue=23&trafficDescrMask=0&expandedTrafficDescrValue=192.168.10.180&expandedTrafficDescrMask=0&vlanAction=0



Method: addSwitchesToDomain

Add switches to the policy domain.

Parameters

Name	Type	Description
domainName	string	Policy domain to add switches to
switches	string	IP address of the switches

Returns

The operation returns an integer error code.

Method: getRoleMapping

Retrieve an IP or MAC role mapping for the specified switch.

Parameters

Name	Type	Description
station	string	Mapping you are retrieving
device	string	IP address of the switch

Returns

Returns a string array role mapping.

Method: removeRoleMapping

Remove an IP or MAC role mapping for the specified switches.

Parameters

Name	Type	Description
station	string	Mapping you are removing
devices	string	IP address of the switches

Returns

The operation returns an integer error code.

Purview Web Service

The Purview web service provides an external interface to retrieve and modify the Application Analytics data and configuration. The Purview web service description language is available at:

https://<Extreme Management Center Server IP>:<port>/axis/services/PurviewWebService?wsdl

Method: addLocation

Create a new location with the specified name.

Parameters

Name	Type	Description
locationGroup	string	Location group name
name	string	Name of new location
description	string	Location description
masks	string	IP subnets and masks of location

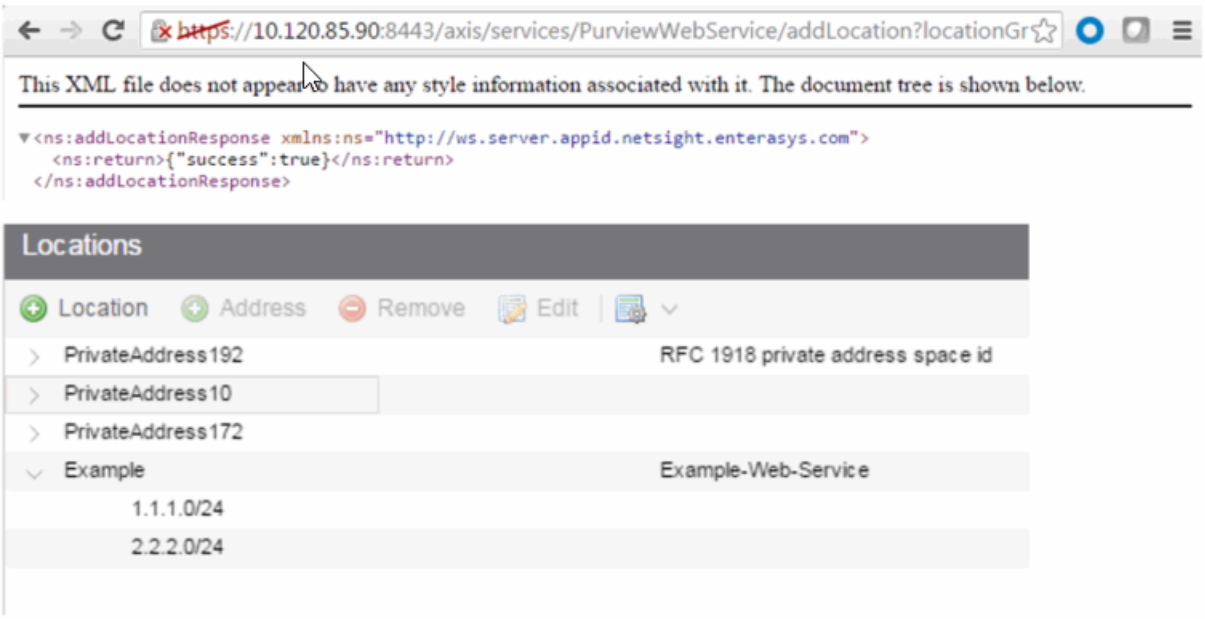
Returns

Returns a string status.

Example

Execute the following web service with a browser:

https://10.120.85.90:8443/axis/services/PurviewWebService/addLocation?locationGroup=Default&name=Example&description=Example-Web-Service&masks=1.1.1.0/24&masks=2.2.2.0/24



Method: addLocationGroup

Create a new location group.

Parameters

Name	Type	Description
name	string	Name of new location group
description	string	Description of location group

Returns

Returns a string status.

Example

Execute the following web service with a browser:

https://10.120.85.90:8443/axis/services/PurviewWebService/addLocationGroup?name=Example Location Group&Description=Example-Web-Service

Method: getAppliances

Retrieve the list of Extreme Management Center engines.

Returns

Returns a list of Extreme Management Center engines in JSON format.

Example

Execute the following web service with a browser:

https://10.120.85.90:8443/axis/services/PurviewWebService/getAppliances

Method: getApplicationBrowserTableData

Retrieve data from the application browser.

Parameters

Name	Type	Description
tableId	int	The table to retrieve the data from, available options are: 0 – appid_attribute (client & server data) 1 – appid_datapoint (application data) 2 – topn_tables 3 – application_usage_default (hourly application data) 4 – application_usage_hr_default (high rate application data)

Name	Type	Description
target	string	The target to retrieve data from, available options are: application application_group location profile target_address client target source target_type datafamily user_data TopN specific targets: appsByClient server
statistics	string	The statistic to retrieve, available options are: byte_count – total byte count flow_count – total flow count target_address – client/server IP address app_rsp_time – application response time tcp_rsp_time – network response time total – total clients, used with TopN tx_byte_count – transmit byte count rx_byte_count – receive byte count tx_flow_count – transmit flow count rx_flow_count – receive flow count client_count – client count server_count – server count application_count – application count user_data – user data contains different fields based on the tableId all_stats – all the above stats
searchCriteria	string	Key value (key=value) pair used in the database query. The available targets, with the exception of TopN, and statistics can be used as a key.

Name	Type	Description
start	long	Starting timestamp for the query in milliseconds
end	long	Ending timestamp for the query in milliseconds
limit	int	Number of results to return
queryType	string	Query type, available options are: grid chartovertime
aggType	string	Aggregation type, available options are: SUM – sum AVG - average

Returns

Returns a TableData with a structure defined by the following table.

Name	Type	Description
extraData	anyType	Additional data from the operation
lastChange	long	Timestamp of last valid data
noChange	boolean	**True** if the data is being stored
success	boolean	**True** if operation is successful
tableData	string	JSON data

Example

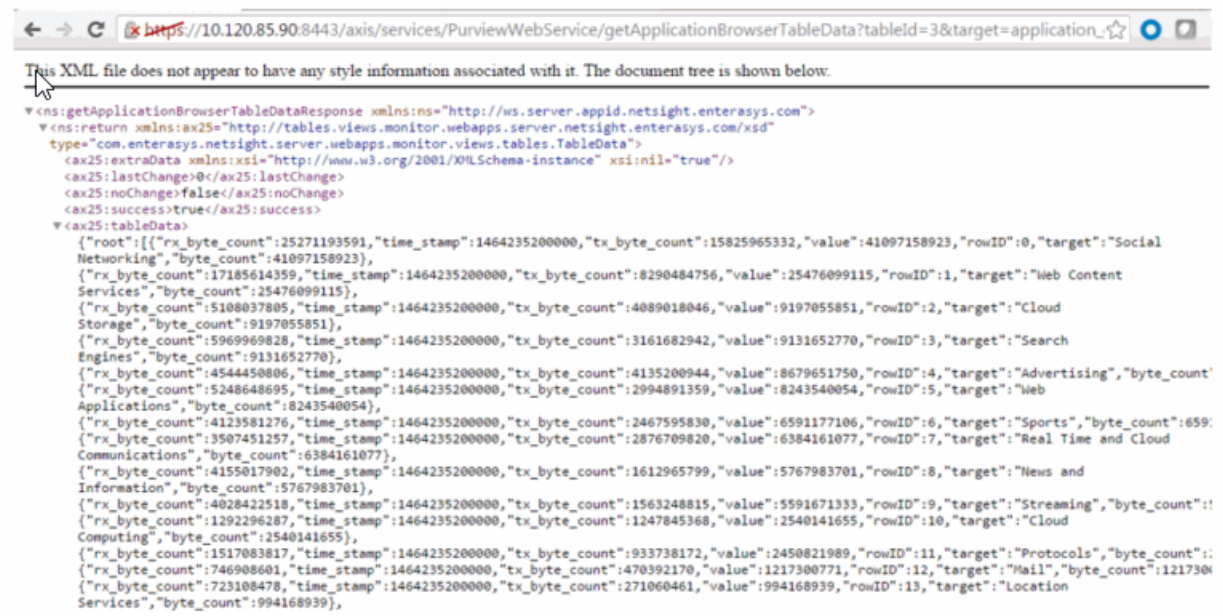
Execute the following web service with a browser:

Retrieve all the statistics for Facebook from the hourly table.

https://10.120.85.90:8443/axis/services/PurviewWebService/getApplicationBrowserTableData?tableId=3&target=application&statistics=all_stats&searchCriteria=application=Facebook&start=1464235200000&end=1464321600000&limit=100&queryType=grid&aggType=AVG

Retrieve the total bytes for the top application groups from the hourly table.

https://10.120.85.90:8443/axis/services/PurviewWebService/getApplicationBrowserTableData?tableId=3&target=application_group&statistics=byte_count&searchCriteria=&start=1464235200000&end=1464321600000&limit=100&queryType=grid&aggType=SUM



Method: getBidirectionalFlowsData

Retrieve the latest filtered bidirectional flow data from an Application Analytics engine.

Parameters

Name	Type	Description
maxRows	int	Maximum number of flows to return
searchString	string	Search string used to query the data
source	string	Application Analytics engine IP address

Returns

Returns flow data in JSON format.

Example

Execute the following web service with a browser:

Retrieve the latest 100 flows.

https://10.120.85.90:8443/axis/services/PurviewWebService/getBidirectionalFlowsData?maxRows=100&searchString=&source=10.120.85.91

Retrieve the latest Facebook flows.

https://10.120.85.90:8443/axis/services/PurviewWebService/getBidirectionalFlowsData?maxRows=100&searchString=Facebook&source=10.120.85.91

Method: getLocations

Retrieve the list of location groups and locations.

Returns

Returns a list of location groups and locations in JSON format.

Example

Execute the following web service with a browser:

https://10.120.85.90:8443/axis/services/PurviewWebService/getLocations

Method: getUnidirectionalFlowsData

Retrieve latest flow data from an Application Analytics engine.

Parameters

Name	Type	Description
maxRows	int	Maximum number of flows to return
searchString	string	Search string used to query the data
source	string	Extreme Analytics appliance IP address

Returns

Returns flow data in JSON format.

Example

Execute the following web service with a browser:

Retrieve the latest 100 flows.

https://10.120.85.90:8443/axis/services/PurviewWebService/getUnidirectionalFlowsData?maxRows=100&searchString=&source=10.120.85.91

Retrieve the latest Instagram flows.

https://10.120.85.90:8443/axis/services/PurviewWebService/getUnidirectionalFlowsData?maxRows=100&searchString=Instagram&source=10.120.85.91

Method: getVersion

Retrieve Application Analytics version.

Returns

Returns version in string format.

Example

Execute the following web service with a browser:

https://10.120.85.90:8443/axis/services/PurviewWebService/getVersion

Method: importLocationCSV

Create locations with a provided CSV string.

Parameters

Name	Type	Description
locationGroup	string	Location group name
csv	string	CSV data, data must be in a format where line 1 contains “name,ipmask” without quotes. Subsequent lines contain the “<location name>,<IP subnet/mask>” without quotes.
overwrite	boolean	**True** to replace locations with the same name
purge	boolean	**True** to remove locations not imported
protect	boolean	**True** to prevent a location from being overwritten

Returns

Returns a string status.

Reporting Web Service

The Reporting web service provides an external interface to retrieve and modify the Extreme Management Center reporting engine data and configuration. The Reporting web service description language is available at:

https://<Extreme Management Center Server IP>:<port>/axis/services/Reporting?wsdl

The Reporting web services use complex data types. It is recommended to use a WSDL converter to generate the source code to execute the web service operations. In these examples, the Java source code is generated via the Axis2 1.6.2 wsdl2java utility.

Method: addDataPointObj

Add a data point to the reporting table.

Parameters

Name	Type	Description
dp	DataPoint	The raw statistic which contains the target ID, statistic ID, value, and timestamp

Returns

Returns a RptResult with a structure defined by the following table.

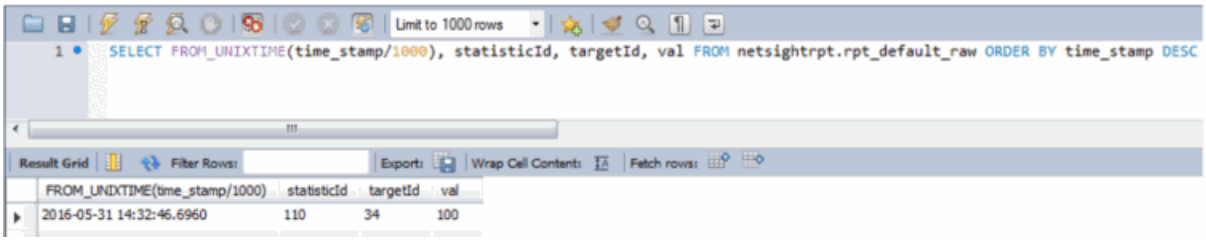
Name	Type	Description
errorMessage	string	Error message in readable text

Name	Type	Description
returnCode	int	Web service error code, **0** if the operation is successful
success	boolean	Displays **True** if the operation occurred successfully

Example

This example sets the SsidAssociatedClients, with statisticID 100, on Fake SSID, with targetID 34, to 100.

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddDataPointObjDocument document = AddDataPointObjDocument.Factory.newInstance();
AddDataPointObj dpObj = document.addNewAddDataPointObj();
DataPoint dp = dpObj.addNewDp();
Domain domain = Domain.Factory.newInstance();
domain.setName("Default");
dp.setDomain(domain);
dp.setStatisticID(110);
dp.setTargetID(34);
dp.setValue(100);
dp.setTimeStamp(System.currentTimeMillis());
stub.addDataPointObj(document);
```



Method: addDataPointObjs

Add multiple data samples to the reporting table.

Parameters

Name	Type	Description
dp	DataPoint	The raw statistic which contains the target ID, statistic ID, value, and timestamp

Returns

Returns a MultiObjRptResult with a structure defined by the following table.

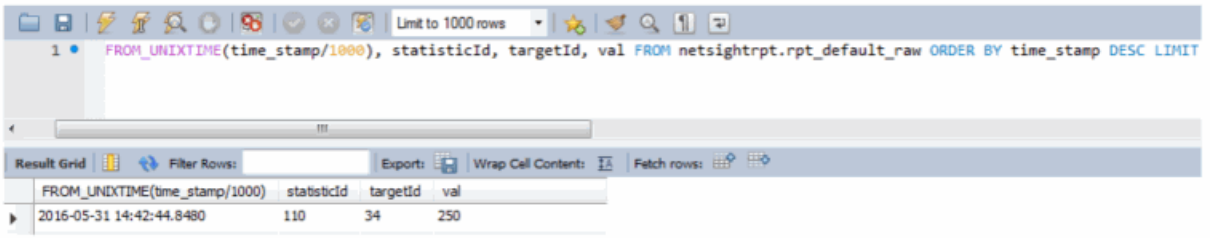
Name	Type	Description
errorMessage	string	Error message in readable text
numFailures	int	Number of operation failures
partialFailure	boolean	**True** if the operation does not complete
returnCode	int	Web service error code, **0** if the operation is successful

Name	Type	Description
success	boolean	Displays **True** if the operation occurred successfully

Example

This example sets the SsidAssociatedClients, with statisticID 100, on Fake SSID, with targetID 34, to 250.

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddDataPointObjsDocument document = AddDataPointObjsDocument.Factory.newInstance();
AddDataPointObjs dpObj = document.addNewAddDataPointObjs();
DataPoint dp = dpObj.addNewDp();
Domain domain = Domain.Factory.newInstance();
domain.setName("Default");
dp.setDomain(domain);
dp.setStatisticID(110);
dp.setTargetID(34);
dp.setValue(250);
dp.setTimeStamp(System.currentTimeMillis());
stub.addDataPointObjs(document);
```



Method: addDataSample

Add a data sample to the reporting table.

Parameters

Name	Type	Description
newSample	DataSample	The raw statistic which contains the target name, statistic name, value, and timestamp

Returns

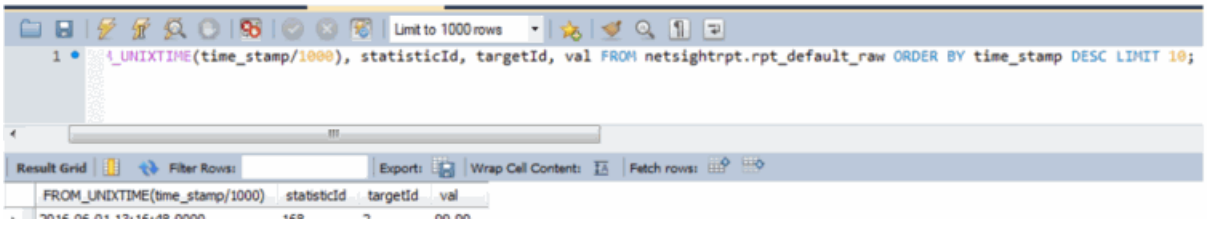
Returns a RptResult with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
success	boolean	Displays True if the operation occurred successfully

Example

This example sets the NsServerDiskUsedPercent statistic on the NetsightServer to 99.99.


```
eportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
ttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddDataSampleDocument document = AddDataSampleDocument.Factory.newInstance();
AddDataSample data = document.addNewAddDataSample();
DataSample ds = data.addNewNewSample();
ds.setDomainName("Default");
ds.setSingleValue(BigDecimal.valueOf(99.99));
ds.setStatName("NsServerDiskUsedPercent");
ds.setTargetName("NetsightServer");
ds.setTargetSubName("Server");
ds.setTimeStamp(System.currentTimeMillis());
stub.addDataSample(document);
```



Method: addDataSamples

Add multiple data samples to the reporting table.

Parameters

Name	Type	Description
ds	DataSample	The raw statistic which contains the target name, statistic name, value, and timestamp

Returns

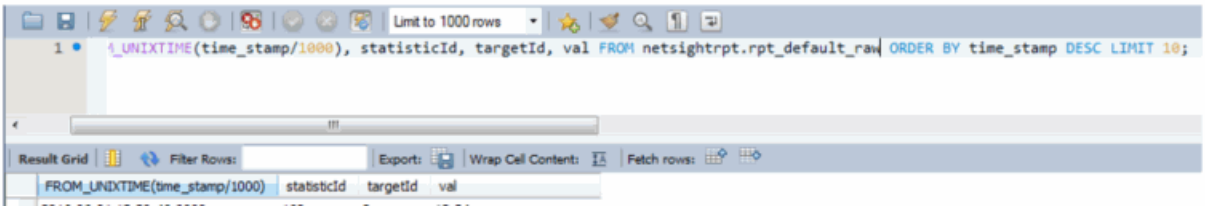
Returns a RptResult with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
numFailures	int	Number of operation failures
partialFailure	boolean	**True** if the operation did not complete
returnCode	int	Web service error code, **0** if the operation is successful
success	boolean	Displays **True** if the operation occurred successfully

Example

This example sets the NsServerDiskUsedPercent statistic on the NetsightServer to 12.34.


```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddDataSamplesDocument document = AddDataSamplesDocument.Factory.newInstance();
AddDataSamples data = document.addNewAddDataSamples();
DataSample ds = data.addNewDs();
ds.setDomainName("Default");
ds.setSingleValue(BigDecimal.valueOf(12.34));
ds.setStatName("NsServerDiskUsedPercent");
ds.setTargetName("NetsightServer");
ds.setTargetSubName("Server");
ds.setTimeStamp(System.currentTimeMillis());
stub.addDataSamples(document);
```



Method: addOrModifyCollectorConfigObjs

Add or update a collector configuration.

Parameters

Name	Type	Description
ccs	CollectorConfig	Collector configuration

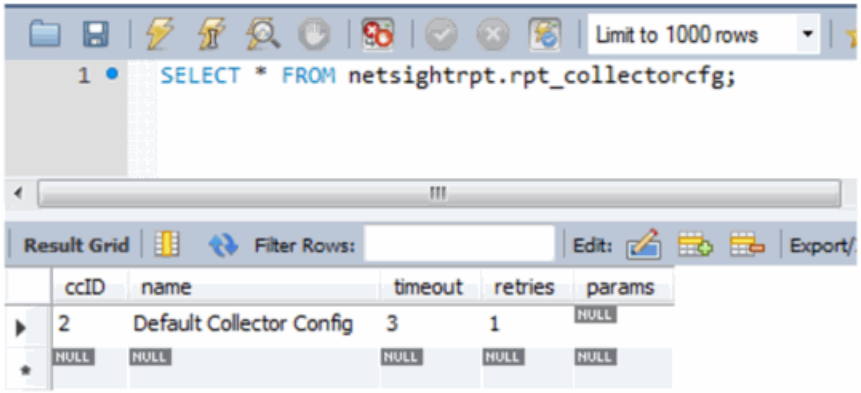
Returns

Returns a RptResultCollectorCfg with a structure defined by the following table.

Name	Type	Description
configs	CollectorConfig	Collector configuration
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, **0** if the operation is successful
success	boolean	Displays **True** if the operation occurred successfully

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddOrModifyCollectorConfigObjsDocument document = AddOrModifyCollectorConfigObjsDocument.Factory.newInstance();
AddOrModifyCollectorConfigObjs objs = document.addNewAddOrModifyCollectorConfigObjs();
CollectorConfig cfg = objs.addNewCcs();
cfg.setName("Default Collector Config");
cfg.setRetries(1);
cfg.setTimeout(3);
stub.addOrModifyCollectorConfigObjs(document);
```



Method: addOrModifyCollectorConfigs

Add or update a collector configuration.

Parameters

Name	Type	Description
ccs	CollectorConfig	Collector configuration

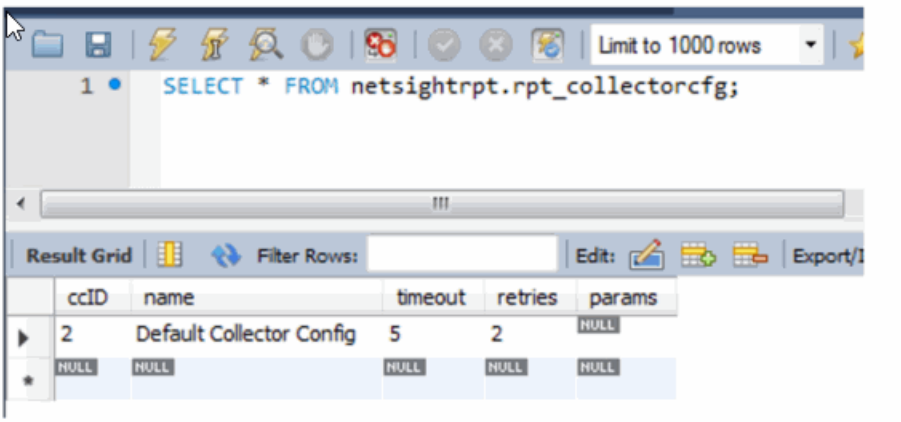
Returns

Returns a MultiObjRptResult with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
numFailures	int	Number of operation failures
partialFailure	boolean	**True** indicates the operation did not complete
returnCode	int	Web service error code, **0** if the operation is successful
success	boolean	Displays **True** if the operation occurred successfully

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddOrModifyCollectorConfigsDocument document = AddOrModifyCollectorConfigsDocument.Factory.newInstance();
AddOrModifyCollectorConfigs objs = document.addNewAddOrModifyCollectorConfigs();
CollectorConfig cfg = objs.addNewCcs();
cfg.setName("Default Collector Config");
cfg.setRetries(2);
cfg.setTimeout(5);
stub.addOrModifyCollectorConfigs(document);
```



Method: addOrModifyStatistic

Add or update a statistic.

Parameters

Name	Type	Description
name	string	Statistic name
dt	DataType	Statistic data type

Returns

Returns a RptResultStat with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, **0** if the operation is successful
stat	Statistic	Updated Statistic
success	boolean	Displays **True** if the operation occurred successfully

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddOrModifyStatisticDocument document = AddOrModifyStatisticDocument.Factory.newInstance();
AddOrModifyStatistic statistic = document.addNewAddOrModifyStatistic();
statistic.setName("ExtremeControlAuthenticatedUserCount");
DataType data = statistic.addNewDt();
data.setVal("Counter");
stub.addOrModifyStatistic(document);
```

Method: addOrModifyStatisticObj

Add or update a statistic.

Parameters

Name	Type	Description
stat	Statistic	Statistic to update

Returns

Returns a RptResultStat with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
stat	Statistic	Updated Statistic

Name	Type	Description
success	boolean	Displays **True** if the operation occurred successfully

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddOrModifyStatisticObjDocument document = AddOrModifyStatisticObjDocument.Factory.newInstance();
AddOrModifyStatisticObj obj = document.addNewAddOrModifyStatisticObj();
Statistic statistic = obj.addNewStat();
statistic.setDataTypeString("Counter");
statistic.setDescription("Example Statistic");
statistic.setDisplayName("This is an example");
statistic.setName("ExtremeControlAuthenticatedUserCount");
statistic.setObjectType("NAC");
statistic.setStatisticID(205);
stub.addOrModifyStatisticObj(document);
```

Method: addOrModifyStatisticObjs

Add or update multiple statistics.

Parameters

Name	Type	Description
stats	Statistic	Statistics to update

Returns

Returns a RptResultStat with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
stat	Statistic	Updated Statistic
success	boolean	Displays True if the operation occurred successfully

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddOrModifyStatisticObjsDocument document = AddOrModifyStatisticObjsDocument.Factory.newInstance();
AddOrModifyStatisticObjs objs = document.addNewAddOrModifyStatisticObjs();
Statistic statistic = objs.addNewStats();
statistic.setDataTypeString("Counter");
statistic.setDescription("Updated example statistic");
statistic.setDisplayName("This is another example");
statistic.setName("ExtremeControlAuthenticatedUserCount");
statistic.setObjectType("NAC");
statistic.setStatisticID(205);
stub.addOrModifyStatisticObjs(document);
```

Method: addOrModifyTarget

Add or update a target.

Parameters

Name	Type	Description
objectID	string	Target object ID

Name	Type	Description
objectSubID	string	Target object sub ID
description	string	Description of target
tags	string	Optional field for collector specific values

Returns

Returns a RptResultTarget with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, **0** if the operation is successful
success	boolean	Displays **True** if the operation occurred successfully
target	Target	Updated target

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddOrModifyTargetDocument document = AddOrModifyTargetDocument.Factory.newInstance();
AddOrModifyTarget data = document.addNewAddOrModifyTarget();
data.setDescription("Example Target");
data.setObjectID("SSID");
data.setObjectSubID("SSID");
stub.addOrModifyTarget(document);
```

Method: addOrModifyTargetObj

Add or update a target.

Parameters

Name	Type	Description
targ	Target	Target to update

Returns

Returns a RptResultTarget with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, **0** if the operation is successful
success	boolean	Displays **True** if the operation occurred successfully
target	Target	Updated target

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddOrModifyTargetObjDocument document = AddOrModifyTargetObjDocument.Factory.newInstance();
AddOrModifyTargetObj data = document.addNewAddOrModifyTargetObj();
Target target = data.addNewTarg();
target.setDescription("Updated example description");
target.setDisplayName("SSID Example");
target.setObjectID("SSID");
target.setObjectSubID("SSID");
target.setTargetID(34);
stub.addOrModifyTargetObj(document);
```

Method: addOrModifyTargetObjs

Add or update multiple targets.

Parameters

Name	Type	Description
targ	Target	Target to update

Returns

A return element having the structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
success	boolean	Displays True if the operation occurred successfully
target	Target	Updated target

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
AddOrModifyTargetObjsDocument document = AddOrModifyTargetObjsDocument.Factory.newInstance();
AddOrModifyTargetObjs data = document.addNewAddOrModifyTargetObjs();
Target target = data.addNewTarg();
target.setDescription("Updated Example Description");
target.setDisplayName("Updated SSID Example");
target.setObjectID("SSID");
target.setObjectSubID("SSID");
target.setTargetID(34);
stub.addOrModifyTargetObjs(document);
```

Method: deleteCollectorConfig

Delete a collector configuration.

Parameters

Name	Type	Description
cc	CollectorConfig	Collector configuration to delete

Returns

Returns a RptResult with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
success	boolean	Displays True if the operation occurred successfully

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
DeleteCollectorConfigDocument document = DeleteCollectorConfigDocument.Factory.newInstance();
DeleteCollectorConfig config = document.addNewDeleteCollectorConfig();
CollectorConfig cc = config.addNewCc();
cc.setName("Default Collector Config");
stub.deleteCollectorConfig(document);
```

Method: deleteCollectorConfigs

Delete multiple collector configurations.

Parameters

Name	Type	Description
ccs	CollectorConfig	Collector configurations to delete

Returns

Returns a RptResultCollecotrCfg with a structure defined by the following table.

Name	Type	Description
configs	CollectorConfig	Deleted collector configurations
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
success	boolean	Displays True if the operation occurred successfully

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
DeleteCollectorConfigsDocument document = DeleteCollectorConfigsDocument.Factory.newInstance();
DeleteCollectorConfigs config = document.addNewDeleteCollectorConfigs();
CollectorConfig cc = config.addNewCcs();
cc.setName("Default Collector Config");
stub.deleteCollectorConfigs(document);
```

Method: deleteDomain

Delete a domain.

Parameters

Name	Type	Description
domain	string	Domain to delete

Returns

Returns a RptResult with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
success	boolean	Displays True if the operation occurred successfully

Method: deleteStatistic

Delete a statistic.

Parameters

Name	Type	Description
name	string	Statistic name

Returns

Returns a RptResultStat with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
stat	Statistic	Updated statistic
success	boolean	Displays True if the operation occurred successfully

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
DeleteStatisticDocument document = DeleteStatisticDocument.Factory.newInstance();
DeleteStatistic statistic = document.addNewDeleteStatistic();
statistic.setName("ExtremeControlAuthenticatedUserCount");
stub.deleteStatistic(document);
```

Method: deleteTarget

Delete a target.

Parameters

Name	Type	Description
objectID	string	Target object ID

Name	Type	Description
objectSubID	string	Target object sub ID

Returns

Returns a RptResultTarget with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
success	boolean	Displays True if the operation occurred successfully
target	Target	Updated target

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
DeleteTargetDocument document = DeleteTargetDocument.Factory.newInstance();
DeleteTarget target = document.addNewDeleteTarget();
target.setObjectID("SSID");
target.setObjectSubID("SSID");
stub.deleteTarget(document);
```

Method: deleteTargetObjs

Delete multiple targets.

Parameters

Name	Type	Description
targs	Target	Targets to delete

Returns

Returns a RptResultTarget with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
success	boolean	Displays True if the operation occurred successfully
target	Target	Updated target

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
DeleteTargetObjsDocument document = DeleteTargetObjsDocument.Factory.newInstance();
DeleteTargetObjs objs = document.addNewDeleteTargetObjs();
Target target = objs.addNewTargs();
target.setObjectID("SSID");
target.setObjectSubID("Example");
stub.deleteTargetObjs(document);
```

Method: getAllCollectorConfigs

Retrieve collector configurations.

Returns

Returns a list of collector configurations.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/getAllCollectorConfigs

Method: getAllStatistics

Retrieve all statistics.

Returns

Returns a list of statistics.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/getAllStatistics

Method: getAllTargets

Retrieve all targets.

Returns

Returns a list of all the targets.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/getAllTargets

Method: getAllTargetsForObjectID

Retrieve all targets with a matching object ID.

Parameters

Name	Type	Description
objectID	string	Object ID name

Returns

Returns a list of matching targets.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/getAllTargetsForObjectID?objectID=NAC

Method: getAllTargetsForObjectType

Retrieve all targets with a matching object type.

Parameters

Name	Type	Description
objectType	string	Object type name

Returns

Returns a list of matching targets.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/getAllTargetsForObjectType?objectType=ESPROFILE

Method: getCollectorConfigForName

Retrieve collector configuration.

Parameters

Name	Type	Description
name	string	Collector configuration name

Returns

Returns a RptResultCollecotrCfg with a structure defined by the following table.

Name	Type	Description
configs	CollectorConfig	Collector configuration data
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, **0** if the operation is successful
success	boolean	Displays **True** if the operation occurred successfully

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/getCollectorConfigForName?name=Default Collector Config

Method: getGoogleChartApiUrl

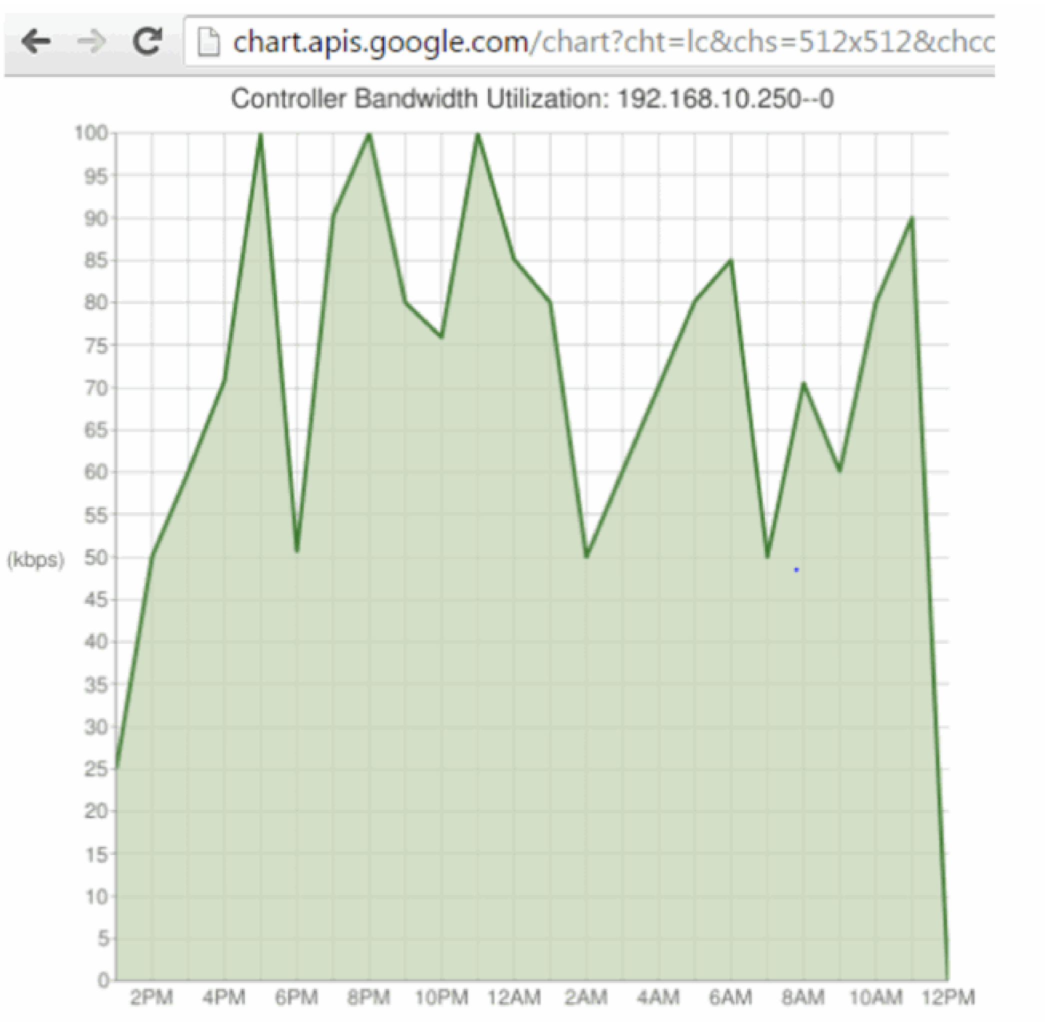
Generate an online chart using Google's chart API. Collections must be enabled for the AP and/or wireless controller for this operation to work correctly.

Parameters

Name	Type	Description
type	string	Type of statistic, available options are: APBwUtil – AP bandwidth ControllerBwUtil – wireless controller bandwidth
params	string	Chart parameters in key=value format, available parameters are: target – AP serial number for APBwUtil or wireless controller IP address for ControllerBwUtil width – chart width height – chart height

Returns

The values from the URL were modified in the example below.



Method: getPerformanceSummary

Retrieve the Extreme Management Center reporting engine performance summary.

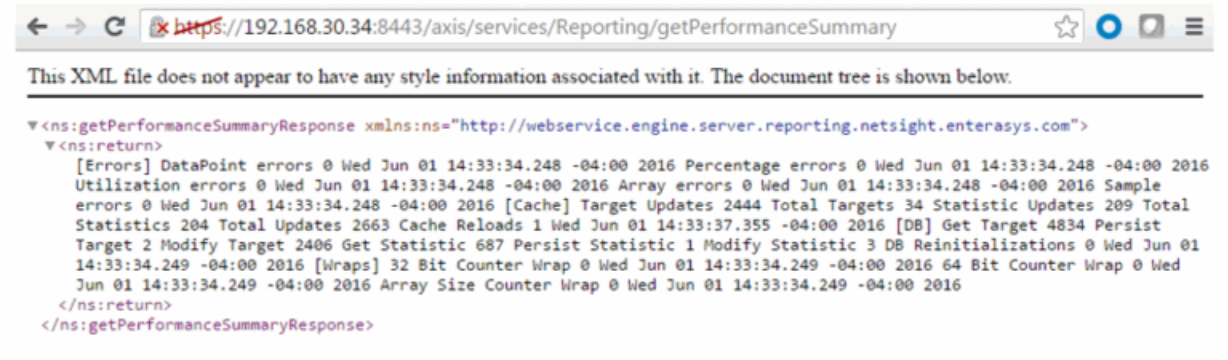
Returns

Returns a summary of the Extreme Management Center reporting engine.

Example

Execute the following web service with a browser: >

https://192.168.30.34:8443/axis/services/Reporting/getPerformanceSummary



Method: getProperties

Retrieve a list of properties from a target.

Parameters

Name	Type	Description
target	Target	Target to retrieve properties from

Returns

Returns a list of properties.

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
GetAllTargetsForObjectIDDocument document0 = GetAllTargetsForObjectIDDocument.Factory.newInstance();
GetAllTargetsForObjectID objectId = document0.addNewGetAllTargetsForObjectID();
objectId.setObjectID("12171238235W0000");
GetAllTargetsForObjectIDResponseDocument response = stub.getAllTargetsForObjectID(document0);
Target target = response.getGetAllTargetsForObjectIDResponse().getReturnArray(0);
GetPropertiesDocument document1 = GetPropertiesDocument.Factory.newInstance();
GetProperties properties = document1.addNewGetProperties();
properties.setTarget(target);
System.out.println(stub.getProperties(document1));
```

```
<ns:getPropertiesResponse xmlns:ax21="http://model.common.reporting.netsight.ente
  <ns:return type="com.enterasys.netsight.reporting.common.webservice.Property">
    <ax23:name>apIsStandalone</ax23:name>
    <ax23:value>true</ax23:value>
  </ns:return>
  <ns:return type="com.enterasys.netsight.reporting.common.webservice.Property">
    <ax23:name>C1.controllerIp</ax23:name>
    <ax23:value>192.168.10.250</ax23:value>
  </ns:return>
  <ns:return type="com.enterasys.netsight.reporting.common.webservice.Property">
    <ax23:name>C1.apState</ax23:name>
    <ax23:value>1</ax23:value>
  </ns:return>
  <ns:return type="com.enterasys.netsight.reporting.common.webservice.Property">
    <ax23:name>C1.apStatus</ax23:name>
    <ax23:value>1</ax23:value>
  </ns:return>
  <ns:return type="com.enterasys.netsight.reporting.common.webservice.Property">
    <ax23:name>C1.RADIOIDX</ax23:name>
    <ax23:value/>
  </ns:return>
```

Method: getProperty

Retrieve a property from a target.

Parameters

Name	Type	Description
target	Target	Target to retrieve property from
key	string	Property key to retrieve

Returns

Returns property key and value.

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
GetAllTargetsForObjectIDDocument document0 = GetAllTargetsForObjectIDDocument.Factory.newInstance();
GetAllTargetsForObjectID objectId = document0.addNewGetAllTargetsForObjectID();
objectId.setObjectID("12171238235W0000");
GetAllTargetsForObjectIDResponseDocument response = stub.getAllTargetsForObjectID(document0);
Target target = response.getGetAllTargetsForObjectIDResponse().getReturnArray(0);
GetPropertyDocument document1 = GetPropertyDocument.Factory.newInstance();
GetProperty property = document1.addNewGetProperty();
property.setTarget(target);
property.setKey("C1.controllerIp");
System.out.println(stub.getProperty(document1));
```

```
<ns:getPropertyResponse xmlns:ns="http://web
  <ns:return type="com.enterasys.netsight.re
    <ax23:name>C1.controllerIp</ax23:name>
    <ax23:value>192.168.10.250</ax23:value>
  </ns:return>
</ns:getPropertyResponse>
```

Method: getPropertyAsLong

Retrieve a property from a target.

Parameters

Name	Type	Description
target	Target	Target to retrieve property from
key	string	Property key to retrieve
defaultVal	long	Default value

Returns

Returns property key and value.

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
GetAllTargetsForObjectIDDocument document0 = GetAllTargetsForObjectIDDocument.Factory.newInstance();
GetAllTargetsForObjectID objectId = document0.addNewGetAllTargetsForObjectID();
objectId.setObjectID("12171238235W0000");
GetAllTargetsForObjectIDResponseDocument response = stub.getAllTargetsForObjectID(document0);
Target target = response.getGetAllTargetsForObjectIDResponse().getReturnArray(0);
GetPropertyAsLongDocument document1 = GetPropertyAsLongDocument.Factory.newInstance();
GetPropertyAsLong property = document1.addNewGetPropertyAsLong();
property.setTarget(target);
property.setKey("updateTime");
property.setDefaultVal(0);
System.out.println(stub.getPropertyAsLong(document1));
```

```
<ns:getPropertyAsLongResponse xmlns:ns="http://webs
  <ns:return>1464892909437</ns:return>
</ns:getPropertyAsLongResponse>
```

Method: getServerStatus

Retrieve the Extreme Management Center server status.

Returns

Returns a status.

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/getServerStatus

Method: getTargetByNameAndType

Return target based on the object ID name and type.

Parameters

Name	Type	Description
objectIDName	string	Object ID name
objectType	string	Object type

Returns

Returns a RptResultTarget with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
success	boolean	Displays True if the operation occurred successfully
target	Target	Updated target

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/getTargetByNameAndType?objectIDName=192.168.10.250&objectType=HWC

Method: modifyTarget

Update existing target with new object ID and object sub ID.

Parameters

Name	Type	Description
targetID	long	Target ID to modify
newObjectID	string	New object ID
newObjectSubID	string	New object sub ID

Returns

Returns a RptResultTarget with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful

Name	Type	Description
success	boolean	Displays **True** if the operation occurred successfully
target	Target	Updated target

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/modifyTarget?targetID=33&newObjectID=ExampleID&newObjectSubID=ExampleSubID

Method: setProperty

Set target property.

Parameters

Name	Type	Description
target	Target	Target to update
prop	Property	Property to update

Returns

Returns a RptResultTarget with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, 0 if the operation is successful
success	boolean	Displays True if the operation occurred successfully
target	Target	Updated target

Example

```
ReportingStub stub = new ReportingStub("https://192.168.30.34:8443/axis/services/Reporting?wsdl");
HttpTransportProperties.Authenticator basicAuth = new HttpTransportProperties.Authenticator();
basicAuth.setUsername("root");
basicAuth.setPassword("password");
basicAuth.setPreemptiveAuthentication(true);
stub._getServiceClient().getOptions().setProperty(HTTPConstants.AUTHENTICATE, basicAuth);
SetPropertyDocument document = SetPropertyDocument.Factory.newInstance();
SetProperty property = document.addNewSetProperty();
Target t = property.addNewTarget();
t.setObjectID("ExampleID");
t.setObjectSubID("ExampleSubID");
t.setTargetID(33);
Property p = property.addNewProp();
p.setName("MyKey");
p.setValue("MyValue");
System.out.println(stub.setProperty(document));
```

```
<ns:setPropertyResponse xmlns:ns="http://webservice.engine.server.reporting.netsight.enterasys.com" xmlns:soapenv="http:
  <ns:return type="com.enterasys.netsight.reporting.common.webservice.retval.RptResultTarget" xmlns:ax22="http://status.
    <ax26:errorMessage xsi:nil="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
    <ax26:returnCode>0</ax26:returnCode>
    <ax26:success>true</ax26:success>
    <ax26:target type="com.enterasys.netsight.reporting.common.model.Target">
      <ax21:activeLastDay>Active</ax21:activeLastDay>
      <ax21:activeLastMonth>Active</ax21:activeLastMonth>
      <ax21:activeLastWeek>Active</ax21:activeLastWeek>
      <ax21:createTime>1464896964676</ax21:createTime>
      <ax21:description xsi:nil="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
      <ax21:displayName xsi:nil="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
      <ax21:encodedProperties>MyKey=MyValue,updateTime=1464896964676,createTime=1464896964676</ax21:encodedProperties>
      <ax21:nickName xsi:nil="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
      <ax21:objectID>ExampleID</ax21:objectID>
      <ax21:objectIDName xsi:nil="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
      <ax21:objectSubID>ExampleSubID</ax21:objectSubID>
      <ax21:objectSubIDName xsi:nil="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
      <ax21:params xsi:nil="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
      <ax21:tags xsi:nil="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
      <ax21:targetID>33</ax21:targetID>
      <ax21:type xsi:nil="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
      <ax21:updateTime>1464896964676</ax21:updateTime>
    </ax26:target>
  </ns:return>
</ns:setPropertyResponse>
```

Method: statExists

Check if statistic exists.

Parameters

Name	Type	Description
name	string	Statistic Name

Returns

Returns a RptResultStat with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, **0** if the operation is successful
stat	Statistic	Statistic information
success	boolean	Displays **True** if the operation occurred successfully

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/statExists?name=ifInOctets

Method: targetExists

Check if target exists.

Parameters

Name	Type	Description
objectID	string	Target object ID
objectSubID	string	Target object sub ID

Returns

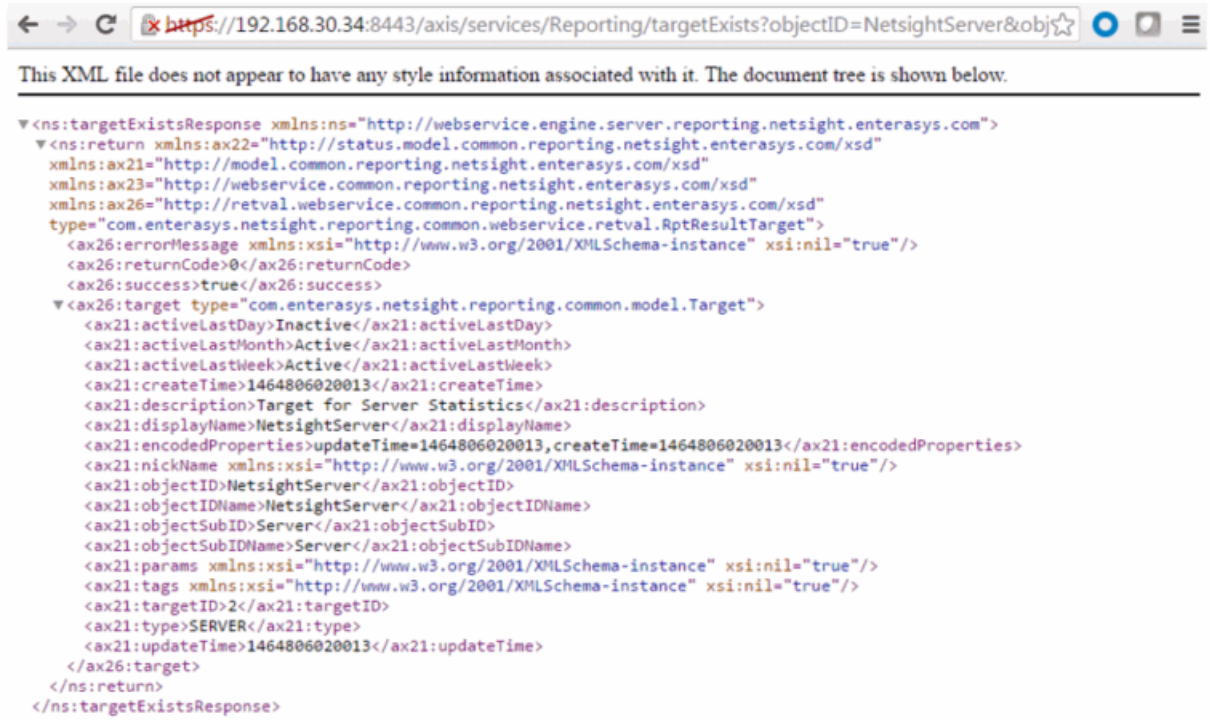
Returns a RptResultTarget with a structure defined by the following table.

Name	Type	Description
errorMessage	string	Error message in readable text
returnCode	int	Web service error code, **0** if the operation is successful
success	boolean	Displays **True** if the operation occurred successfully
target	Target	Updated target

Example

Execute the following web service with a browser:

https://192.168.30.34:8443/axis/services/Reporting/targetExists?objectID=NetsightServer&objectSubID=Server



Data Center/Cloud Integration

The various integrations for Data Center/Cloud focus on the automation of provisioning highly mobile end-systems like virtual machines or providing user information for virtual desktops. Depending on the capabilities of the 3rd party product, the automation can include the creation of virtual networks and VLAN configuration within the respective product.

- Citrix XenServer
- Citrix XenDesktop
- Microsoft Intune
- Google G Suite
- Microsoft System Center Virtual Machine Manager (SCVMM)

- Microsoft Hyper-V
- VMware vSphere
- VMware View

Citrix XenServer

The XenServer integration offers provisioning of virtual machines in the network as well as automating the creation of virtual networks based on end-system access groups. In addition, data within Extreme Management Center is enriched for each end-system and conversely made available within XenCenter (=management tool for XenServer environments).

Module Configuration

Service Configuration	Description
Username	Username used to connect to the XenServer's web service. Read/Write/Execute permissions required.
Password	Password used to connect to the XenServer's web service.
XenCenter Webservice URL	Web service url of the XenSever
XenCenter Server IP	IP address of the XenServer.

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the XenServer.
Module log level	Verbosity of the module. Logs are stored in Extreme Management Center's server.log file.
Module enabled	Whether or not the module is enabled.
Push update to remote service	If this is set to "true", data from other modules will be pushed to the service.
Update local data from remote service	If this is set to "true", data from the remote service will be used to update the internal end-system table.
Default end-system group:	The default end-system group name to use if it is not set dynamically.
Enable Data Persistence	Enabling this option will force the module to store end-system, end-system group and VLAN data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use	The custom field within Extreme Control to update the information for end-systems retrieved from XEN (valid values: 1-4).
Outgoing data format	The format of the Extreme Control data (like last seen time, switch IP, switch port, etc.) that is written to the description fields of the VMs within XEN. You can customize the appearance and what information you want to include/exclude from there.
Format of the incoming data	The format of the data that is received from XEN and written to the custom field.

Service Specific Configuration	
Use global end-system groups	This feature allows for the module to use the global end-system groups of the Extreme Connect. This will enable the XEN module to use the end-system groups retrieved from the Extreme Control module and assign XEN VMs to these end-system groups.
Network deletion	If this option is enabled, networks created by end-system groups will be deleted if the end-system group does not exist anymore or sync is disabled. Any connected VM will be rerouted to the Deletion Group below.
Deletion Group	If the "Network Deletion" feature is enabled, this setting will define the catchall network for VMs that have been connected to a XEN network after it has been deleted in Extreme Management Center. For example: If you have a XEN network "VM Test" that is managed by Extreme Connect and you delete the corresponding end-system group in Extreme Management Center, this feature will make sure that all VMs that are connected to "VM Test" will be disconnected from it and automatically reconnected to the XEN network defined with this setting. This feature is meant to provide a fallback network for all VMs that have been connected to Extreme Connect managed XEN networks.
Destroy NIC Bonds	If enabled, Extreme Connect will automatically destroy (remove) a bonding of 2 or more NICs on the Citrix XenServer in case the last network that used this bond has been removed using the Extreme Management Center group configuration. Example: Let's assume you have created a new end-system group using multiple NICs with "nic=eth0:eth1", Extreme Connect will create - A bond over eth0 + eth1 with a default naming schema and - A new external network connected to that bond named as your end-system group. Now you create a second end-system group also using the same NIC definition "nic=eth0:eth1". This will only create a new external network connected to the already existing bond and called according to your end-system group. If you now delete (or set "sync=false") one of these end-system groups, only the external Xen network will be removed, not the bond since it is in use by the other network. If you then also delete the other end-system group, the corresponding external network will be deleted and the bond between eth0 and eth1 will be destroyed.

Verification

1. Click on a virtual machine.
2. Click the "General" tab on the right side of the screen.
3. At the top of the "General" tab there is a description field that will contain the corresponding data from Extreme Management Center. If this data is correct, then the integration is verified.

Citrix XenDesktop

The integration with XenDesktop is a one-way integration: information on virtual desktops is retrieved from XenDesktop and used within NAC but no data nor configuration is written from NAC towards XenDesktop.

Module Configuration

The table below describes the configuration options available for the XendDesktop OFConnect module (config file: XenDesktopHandler.xml)

Service Configuration	Description
Adapter IP	The IP address on which the Extreme XenDesktop adapter is running (this is configurable within the adapter's config file). It should be running on the same IP as your XenDesktop server.
Adapter Port	The TCP port on which the Extreme XenDesktop adapter is running (this is configurable within the adapter's config file).
Pre-Shared Key	The key used to encrypt traffic from and to the adapter running on the XenDesktop server. This must match the configured pre-shared key from the adapter's config file.

General Module Configuration	
Poll interval in seconds	The wait time between two polls. The module will contact the XenDesktop adapter and request the latest data on the VDI infrastructure, then wait for this interval to pass and then poll the adapter again.
Module log level	Verbosity of the module. Logs are stored in Extreme Management Center's server.log file.
Module enabled	Whether or not the module is enabled.
Update local data from remote service	If this is set to "true", data from the remote service will be used to update the internal end-system table.
Default end-system group	The default end-system group name to use if it is not set dynamically.
Enable Data Persistence	Enabling this option will force the module to store end-system and end-system group data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use	The custom field within Extreme Management Center to update the information for end-systems retrieved from the adapter running on the XenDesktop server (valid values: 1-4).
Format of the incoming data	The format of the data that is received from the adapter running on the XenDesktop server and written to the custom field.

Adapter Installation

OFConnect retrieves data from the XenDesktop server using an adapter. This adapter needs to be installed and configured prior to enabling the corresponding module within OFConnect. The adapter consists of a Java executable file (.jar) and a configuration file. To install the adapter:

1. Install Windows .NET Framework 3.5 SP1 or above, Windows Powershell 2.0 and the latest Java Runtime Environment on the XenDesktop server.
2. Locate the file "Datacenter Manager XenDesktop Adapter.zip" on the Extreme Control server in the directory../jboss/server/default/deploy/fusion_ jboss.war/XenPlugin/ (it can also be downloaded via browser at https://Extreme Control-IP:8443/fusion_jboss/XenPlugin/ Datacenter%20Manager%20XenDesktop%20Adapter.zip).
3. Copy the executable jar file (DCM_XENDESKTOP_ADAPTER_<version>.jar) and the configuration file (DCM_XENDESKTOP_ADAPTER.config) into a separate directory, created under "Program Files/Extreme Networks/XenDesktop Adapter" directly on the XenDesktop server.
4. Edit the configuration file according to your environment. The configuration file contains an explanation of all settings. You can also find them listed below.
5. Save and close the configuration file.
6. Start the adapter manually by opening a cmd shell or Powershell,
7. Navigate into the installation directory and use the following command: java –jar DCM_XENDESKTOP_ADAPTER_<version>.jar.
8. Check the log file to validate proper functionality.
9. Check the end-system list within OneView or NAC Manager to see data for the XenDesktop virtual machines coming into the custom column you've configured within the XenDesktopHandler.xml config file.
10. After successfully verifying the integration, you will need to ensure that the DCM_ XENDESKTOP_ADAPTER_1.00.jar file is getting started on Windows server startup automatically. Stop the adapter currently running within the cmd/Powershell window.
11. Configure the auto-start for the .jar file (this depends on your Windows Server version) and restart your XenDesktop server, when appropriate, in order to test the auto-start of the .jar file (you should see a java process running in the process tree).

Adapter Configuration

The table below lists the configuration options for the XenDesktop agent.

Configuration Option	Description
NETSIGHT_IP	The IP address of the Extreme Management Center server.
NETSIGHT_ USERNAME	The username to authenticate against the Extreme Management Center server.
NETSIGHT_ PASSWORD	The password to authenticate against the Extreme Management Center server.
LOG_LEVEL	Set the log level of the adapter to one of the following values: ERROR, WARN or DEBUG. If not set, the default will be WARN.
IP	IP address for the web service (=agent) to listen on.
PORT	TCP Port for the web service to listen on - must NOT be used by any other application on this server!
XENDESKTOP_ SERVER	The host/DNS name of the XenDekstop Deliver Controller to connect to. So far this has only been tested with this adapter and the XD Deliver Controller running on the same server although remote connections might work as well. Example: XenDesktop5 or with FQDN: XenDesktop5.test.local.
PRE_SHARED_ KEY	The pre-shared key used for the communication between the adapter and OFConnect. This must match the key entered when installing the OFConnect XenDesktop module.
IS_PRE_ SHARED_KEY_ ENCRYPTED	If set to 'false' the adapter assumes that the 'PRE_SHARED_KEY' configured above is not encrypted - on the first start the adapter will automatically encrypt the key and set this value to “true”. If you want to change this key at a later stage, change the key above, set this value back to 'false' and restart the adapter service.
ENABLE_ PUSH_USER_ TO_NETSIGHT	If set to "true" the adapter will use web service calls to Extreme Management Center to push the user name for each virtual desktop session to the corresponding end-system in Extreme Management Center/NAC. If configured properly in NAC, this will cause a re-authentication of the user on this virtual desktop and assign a user-based policy.
ENABLE_ PUSH_DATA_ TO_NETSIGHT	If set to "true" the adapter will push end-system data back to the corresponding module within OFConnect/Extreme Management Center. This will enable you to retrieve data on the virtual desktop within Extreme Management Center/OFConnect and display it within the end-system table inside of NAC manager

Verification

To verify proper functionality, validate the data within the custom field configured to use for the XenDesktop integration in your end-system list (in NAC Manager or OneView).

You will only see the username being set accordingly if you enable the following option within the adapter’s config file: ENABLE_PUSH_USER_TO_ NETSIGHT=true

You will only see the additional information (within the custom column that you’ve specified in your OFConnect XenDesktopHandler config file) if you’ve enabled the following option within the adapter’s config file:

ENABLE_PUSH_DATA_TO_NETSIGHT=true

Be aware that the username from XenDesktop can also be used to automatically assign a policy to each user as you could do with any 802.1X or Kerberos username. So make sure you've configured your rule set in NAC correctly before enabling this feature.

Microsoft Intune

The Intune integration requires registering a Microsoft Azure application. The Azure application will act as a proxy to execute REST API calls on behalf of Connect. This information is used in the Intune module tab.

Module Configuration

The table below lists the configuration options for the MS Intune agent.

Configuration Option	Description
Client ID:	Application client ID
Password:	Application client secret
Tenant:	Tenant ID to retrieve specific customer devices

Service Configuration

The table below lists the configuration options for the MS Intune server.

Configuration Option	Description
Poll interval:	Time period between queries to the Intune NAC web service
End system group for managed business mobile devices:	Mobile IAM end-system group that corporate-owned devices will be part of
End system group for managed personal mobile devices:	Mobile IAM end system group that personal devices will be part of
Default end system group for managed mobile devices:	Mobile IAM end-system group that unknown devices will be part of
Update Kerberos username:	Enable/disable option to update end-system username
Update device type:	Enable/disable option to update end-system device type
Notify user when quarantined:	Enable/disable option to notify user when end-system is quarantined based on assessment scoring
Enable assessment:	Enable/disable option to use Mobile IAM assessment agent

Register Azure Application

An Azure application is required to access Microsoft's Intune NAC API. The application will need permission from an administrator to access device

information from Intune.

1. Login the Azure portal https://portal.azure.com.
2. Select “More services >” at the bottom of the page and select “App registrations."
3. Create a new application.
4. Enter the application name, type, and sign-on URL. In this example, the application name is Connect. The application type must be set to “Web app / API.” The sign-on URL is used as a redirection page once the permissions have been accepted. In this example, the web page will be redirected to the ExtremeManagement server.
5. Once the information is entered, the client ID will be made available. The client ID in the example below is 344763b9-8615-439b-b9dd-0f4c5eeafb9c. This is the ID used in the service configuration.
6. The Azure application will use the Microsoft Intune API and permissions must be enabled to access mobile device information.
7. Select the Azure application permissions, in this example all available permissions are enabled.
8. Select the Keys menu to generate the client secret.

   In this example, the description is set to Secret and the duration is set to expire in 2299. It is recommended to set the duration to a lower value. The generated secret is XZeGGzca8e1saCVgNtdbMIFvlpzSuYG17Esqo8tW5+c=. This is the secret used in the service configuration.

Verification

1. Enroll new device with Microsoft Intune.
2. Connect to test SSID, wait for re-synchronization poll to occur, and verify end system in ExtremeControl has device information from Intune.

Policy Configuration

To support the previous workflow, the device in unregistered state must be able to communicate via HTTPS with the Intune server and via the Apple push service with Apple.

Some configurations require downloading an agent to be registered by Intune so Google Play and Apple appStore access must be provided as well in this

state. If this is the case, policies must be adapted to provide connectivity to the Agent.

The following policies (or more generic ones) are needed to allow Intune registration:

1. Allow HTTPS to Microsoft Intune network.
2. Allow TCP 5223 to 17.0.0.0/8:TCP:5223, Apple Push service.
3. Allow TCP/UDP 5228 to 173.194.0.0/16, Google Play login.
4. Allow HTTPS to 74.125.0.0/16, Google Play Downloads.

Google G Suite

Combining Extreme Networks Access Control (EAC) solution with Google's G Suite allows network and security administrators to ensure that only registered Chrome OS devices are able to use the network and its resources. The solution also pulls extensive device data from G Suite and updates the end-systems in EAC to provide network administrators with a unique view of Chrome OS data within a single management interface.

The solution currently only support Chrome OS devices.

Module Configuration

The table below lists the configuration options for the Google GSuite agent.

Configuration Option	Description
Service Account ID:	Email address of the service account to use for authentication. You can find your service account ID within your Google API Manager project (https://console.developers.google.com/projectselector/apis/credentials?pli=1) where you configured/created your service account when you go into the account details. Example: gsuiteserviceaccount2@extreme-gsuite-test.iam.gserviceaccount.com
Service Account User:	Email address of a user account from your G Suite account / domain. This is used for Connect to know to which domain to connect to. Example: kurt@extremetest.net

Service Configuration

The table below lists the configuration options for the Google GSuite server.

Configuration Option	Description
Poll interval:	The time (in seconds) the module will wait after each run. For example, if you want to run the synchronization once per hour you can configure '3600' here.

Configuration Option	Description
Default end-system group for all devices from G Suite:	The default end-system group name where we assign all G Suite devices to in NAC. If you don't want end-systems from G Suite to be assigned to this default group, configure a group name which doesn't exist in NAC or disable the group assignment feature on the “Extreme Control” module. Default: Chrome Devices
Format of the incoming data for devices from G Suite:	Format of the data that gets stored in the custom data field. You can choose and combine any of the available variables: nwAdapterType, mac, annotatedAssetId, annotatedLocation, annotatedUser, recentUsers, currentUser, deviceId, etag, firmwareVersion, kind, lastEnrollmentTime, lastSync, model, notes, orderNumber, orgUnitPath, osVersion, platformVersion, serialNumber, status, supportEndDate, willAutoRenew. But be aware that G Suite might update the “lastSync” and “lastEnrollmentTime” values for each device very regularly and Connect is calling XMC's API to refresh that value in all end-systems custom fields. Depeding on your poll interval this might put a lot of stress onto the XMC server and it is thus recommended to _NOT_ use these variables in large environments. It should only be used if the poll interval is very low (like a few times per day) and the number of end-systems isn't too high (below 1000). Default: user=#currentUser#, recentUsers=#recentUsers#, annotatedUser=#annotatedUser#, adapterType=#nwAdapterType#; OS=#osVersion#, firmware=#firmwareVersion#
End-system group for decommissioned devices:	The default end-system group for devices which existed in G Suite but have been deleted. If you want to explicitly identify those devices and even authorize them differently (since they are no longer managed by G Suite anymore and that could pose a threat) you can configure the group they should automatically be moved to here and enable the corresponding feature below. Make sure you manually create this end-system group in NAC.
Remove device from other groups on decommission:	Enable this to move devices which have been deleted from G Suite to the NAC end-system group configured by the corresponding option above. If disabled, devices won't be automatically move to this group but rather stay with their existing group membership(s). Default: false
Delete custom data in XMC for decommissioned devices:	If a device is deleted in G Suite the end-system's custom data field in XMC will be cleared as well. On the one hand this will keep your data clean in NAC but on the other hand it might often be helpful to still see the (old) G Suite data for those end-systems which have once been managed by G Suite. Default: false
Overwrite the existing username with the one acquired from G Suite:	If set to "true" the username for devices retrieved from G Suite will overwrite the username which is already in NAC. If no username could be retrieved from G Suite for a given end-system, then no change is performed in NAC. Be aware that this might mess up existing NAC processes if you are already retrieving and using the username through some other mechanism like 802.1X or Kerberos snooping --> this will be overwritten! Default: false

Google APIs

You will need to create a “service account” within the Google APIs management site: https://console.developers.google.com

That service account provides Connect with a credentials that enables it to authenticate and authorize against the Google Admin SDK that is used to pull data from your G Suite domain.

1. Access the API Console Credentials page: https://console.developers.google.com/project/_/apis/credentials
2. Select your project (or create a new one) from the drop-down menu.
3. On the Credentials page, select the Create credentials drop-down, then select Service account key.

4. From the Service account drop-down, select an existing service account or create a new one.
5. For Key type, select the P12 key option, then select Create. The file automatically downloads to your computer.
6. Rename the downloaded credentials file to “gSuiteCredentials.p12“ and copy it to your XMC server (using WinSCP for example) to this location /usr/local/Extreme_Networks/NetSight/wildfly/standalone/configuration/connect/gSuiteCredentials.p12
7. Go into the details on your newly created Credentials and note down the “Client-ID” (number) [Symbol] this will be needed later on to authorize these credentials on your G Suite domain

Google Admin

If not already done, create a Google G Suite account and connect it with your domain. For test accounts, use: https://gsuite.google.com/signup/basic/welcome.

You will need to authorize the Extreme Connect application to provide it with access to your domain and two scopes. The basic process is described at https://developers.google.com/identity/protocols/OAuth2ServiceAccount?#delegatingauthority

To delegate domain-wide authority to a service account, first enable domain-wide delegation for an existing service account in the Service accounts page (https://console.developers.google.com/permissions /serviceaccounts) or create a new service account (https://developers.google.com/identity/protocols/OAuth2ServiceAccount?#creatinganaccount) with domain-wide delegation enabled.

Then, an administrator of the G Suite domain must complete the following steps:

1. Access the G Suite domain’s Admin console.
2. Select Security from the list of controls. If you don't see Security listed, select More controls from the gray bar at the bottom of the page, then select Security from the list of controls. If you can't see the controls, make sure you're signed in as an administrator for the domain.
3. Select Show more and then Advanced settings from the list of options.
4. Select Manage API client access in the Authentication section.

5. In the Client Name field, enter the service account's Client ID. You can find your service account's client ID in the Service accounts page.
6. In the One or More API Scopes field, enter the list of scopes that your application should be granted access.
7. Enter these two scopes for the API client that you authorize for Connect: https://www.googleapis.com/auth/admin.directory.device.chromeos, https://www.googleapis.com/auth/admin.directory.user.readonly

   The first one allows Connect to view and manage your Chrome OS devices' metadata, and the second one allows Connect to view users on your domain.
8. Click Authorize.
9. Remember to enable “domain-wide authority delegation” as described in the link above.

User Privileges

Ensure that the configured user is configured to have at least the prvileges to manage Chrome OS devices as shown below. This privilege is needed to retrieve data on Chrome OS devices.

Verification

You should verify that data from all devices managed by G Suite is imported to NAC. Navigate to the end-system table under the “Connect” tab and display the custom data field which you have configured for the G Suite module. You might need to make the corresponding column visible first. If you enabled the corresponding features you should also see the username retrieved from G Suite.

You can also verify whether all devices managed by G Suite have been assigned to configured end-system group in NAC (if you created such a group and configured it within the “G Suite” module).

Deleting G Suite Devices

To test this workflow, simply “deprovision” a device from G Suite and wait for the next Connect synchronization. Then verify that

1. This device’s custom field has been emptied (if this feature has been enabled in the config file).

2. This device is now member of the NAC end-system group for decommissioned devices (if this feature has been enabled).
3. This device does not appear in the end-system list that is displayed at the bottom of the Connect management web site (tab: G Suite). This means that the device has been deleted in the internal list as well.

Microsoft System Center Virtual Machine Manager (SCVMM)

The SCVMM integration offers provisioning of virtual machines into NAC end-system groups based on the virtual interfaces to which each VM is connected. Data within Extreme Management Center is enriched for each end-system and conversely made available within SCVMM. The VMM is a central Microsoft server that enables management of multiple Hyper-V servers from one console.

Note: The SCVMM server requires an adapter agent to be installed and configured prior to enabling the corresponding module within Extreme Connect. The adapter file is provided by Extreme Networks.

Module Configuration

The table below describes the configuration options available for the SCVMM OFConnect module (config file: SCVMMHandler.xml)

Service Configuration	Description
ADapter IP	IP Address of the Virtual Machine Manager adapter.
Adapter Port	Port where the Virtual Machine Manager adapter is listening on.
Pre-Shared Key	The pre-shared key used to communicate with the SCVMM adapter.

General Module Configuration	
Poll interval in seconds	Number of seconds between connections to the adapter running on the SCVMM server.
Module loglevel	Verbosity of the module. Logs are stored in Extreme Management Center's server.log file.
Module enabled	Whether or not the module is enabled.
Push update to remote service	If this is set to “true”, data from other modules will be pushed to the service.
Update local data from remote service	If this is set to “true”, data from the remote service will be used to update the internal end-system table.

General Module Configuration	
Default end-system group	The default end-system group name to use if it is not set dynamically.
Enable Data Persistence	Enabling this option will force the module to store end-system, end-system group and VLAN data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use	The custom field within Extreme Management Center to update the information for end-systems retrieved from the adapter running on the SCVMM server (valid values: 1-4).
Outgoing data format	The format of the Extreme Management Center data (like last seen time, switch IP, switch port, etc.) that is written to the description fields of the VMs within the SCVMM management console. You can customize the appearance and what information you want to include/exclude from there.
Format of the incoming data	The format of the data that is received from the adapter running on the SCVMM server and written to the custom field.
Use network name as end-system group	If this is set to true, the name of the portgroup /network will be used as the name for the end-system group (Note: Only data before the first _ will be used).

Adapter Installation

OFConnect is retrieving and setting datato/from a Virtual Machine Manager (VMM) server using an adapter. This adapter needs to be installed and configured prior to enabling the corresponding module within OFConnect. The adapter consists of a Java executable file (.jar) and a configuration file. To install the adapter:

1. Install the latest Java Runtime Environment, .NET framework and Windows Powershell 2.0 on the SCVMM server.
2. Acquire the file “Datacenter Manager SCVMM Adapter.zip” from GTAC or by contacting your local Extreme representative.
3. Copy the executable jar file (DCM_SCVMM_ADAPTER_<version>.jar) and the configuration file (DCM_SCVMM_ADAPTER.config) into a separate directory created under “Program Files/Extreme Networks/SCVMM Adapter” directly on the SCVMM server.
4. Edit the configuration file according to your environment. The configuration file contains an explanation of all settings and you can also find them listed below.
5. Save and close the configuration file.

6. Start the adapter manually first by opening a cmd shell or Powershell, navigate into the installation directory and use the following command: java –jar DCM_SCVMM_ ADAPTER_<version>.jar.
7. Check the log file to validate proper functionality.
8. Check the end-system list within OneView or NAC Manager to see data for the SCVMM virtual machines coming into the custom column you've configured within the SCVMMHandler.xml config file.
9. After you have successfully verified the integration, ensure that the DCM_ SCVMM _ ADAPTER_<version>.jar file is getting started on Windows server startup automatically. Stop the adapter currently running within the cmd/Powershell window, configure the auto-start for the .jar file (this depends on your Windows Server version) and restart your SCVMM server when appropriate in order to test the auto-start of the .jar file (you should see a java process running in the process tree).

Adapter Configuration

The table below lists the configuration options for the SCVMM agent.

Configuration Option	Description
LOG_LEVEL	Set the log level of the adapter to one of the following values: ERROR, WARN or DEBUG. If not set, the default will be WARN.
IP	IP address for the web service (=agent) to listen on
PORT	TCP Port for the web service to listen on - must NOT be used by any other application on this server!
SCVMM_DLL	Location (path + file name) of Microsoft.SystemCenter.VirtualMachineManager.dll Example: C:\Program Files\Microsoft System Center Virtual Machine Manager 2008 R2\bin\Microsoft.SystemCenter.VirtualMachineManager.dll
PRE_SHARED_KEY	The pre-shared key used for the communication between the adapter and OFConnect. This must match the key entered when installing the OFConnect SCVMM module.
IS_PRE_SHARED_KEY_ENCRYPTED	If set to "false" the adapter assumes that the 'PRE_SHARED_KEY' configured above is not encrypted - on the first start the adapter will automatically encrypt the key and set this value to "true". To change this key at a later stage, change the key above, set this value back to "false" and restart the adapter service
SCVMM_SERVER	The DNS name of the Virtual Machine Manager server to connect to. So far this has only been tested with this adapter and the VMM server running on the same server although remote connections might work as well.

Verification

Within the SCVMM management console, add the description field/column to the overview list of all VMs. You should see network related information retrieved from Extreme Management Center/NAC within this column as well as additional data from SCVMM within the end-system list in OneView or NAC Manager.

Microsoft Hyper-V

The Hyper-V integration offers provisioning of virtual machines into NAC end-system groups based on the virtual interfaces to which each VM is connected. Data within Access Control engine is enriched for each end-system and conversely made available within Hyper-V. When integrating with multiple Hyper-V servers you can either add each of those servers as a new entry within this module's config (list of services/agents to connect to) or use the integration with System Center Virtual Machine Manager.

Note: The Hyper-V server requires an adapter agent to be installed and configured prior to enabling the corresponding module within Extreme Connect. The adapter file is provided by Extreme Networks.

Module Configuration

The table below describes the configuration options available for the Hyper-V OFConnect module (config file: HyperVHandler.xml)

Service Configuration	Description
Adapter IP	IP Address of the Hyper-V adapter.
Adapter Port	Port where the Hyper-V adapter is listening on.
Pre-Shared Key	The pre-shared key used to communicate with the Hyper-V adapter.

General Module Configuration	
Poll Interval in seconds	Number of seconds between connections to the adapter running on the Hyper-V server.
Module loglevel	Verbosity of the module. Logs are stored in Access Control engine's server.log file.
Module Enabled	Whether or not the module is enabled.
Push update to remote service	If this is set to "true", data from other modules will be pushed to the service.
Update local data from remote service	If this is set to "true", data from the remote service will be used to update the internal end-system table.
Default end-system group	The default end-system group name to use if it is not set dynamically.
Enable Data Persistence	Enabling this option will force the module to store end-system, end-system group and VLAN data to a file after each cycle. If this option is disabled, the module will forget all data after a service restart, but in order to clean already existing data, the corresponding .dat files have to be deleted.

Service Specific Configuration	
Custom field to use	The custom field within Access Control engine to update the information for end-systems retrieved from the adapter running on the Hyper-V server (valid values: 1-4).
Outgoing data format	The format of the Access Control engine data (like last seen time, switch IP, switch port, etc.) that is written to the description fields of the VMs within the Hyper-V management console. You can customize the appearance and what information you want to include/exclude from there.
Format of the incoming data	The format of the data that is received from the adapter running on the Hyper-V server and written to the custom field.
Use network name as end-system group	If this is set to "true", the name of the portgroup /network will be used as the name for the end-system group (Note: Only data before the first _ will be used).

Adapter Installation

Extreme Management CenterConnect retrieves and sets data from and to a Hyper-V server using an adapter. This adapter needs to be installed and configured prior to enabling the corresponding module within Extreme Management Center. The adapter consists of a Java executable file (.jar) and a configuration file and uses a Powershell module as a pre-requisite. To install the adapter manually:

1. The adapter utilizes a Powershell module that needs to be downloaded and installed prior to installing the adapter. Download the module here: http://pshyperv.codeplex.com/releases/view/62842#DownloadId=219013
2. Right click on zip file and UNBLOCK.
3. Copy the zip file to the following location: C:\Windows\System32\WindowsPowerShell\v1.0\Modules
4. Unzip and install the HyperV module using the "install.cmd" file.
5. Bring up Powershell and enter "Set-ExecutionPolicy Unrestricted"
6. Run the command "Import-Module HyperV" and make sure that no errors occur. If this doesn't load the module you can insert the folder "<folderwhereyouunzippedthedownloadedfile>\Hyper-V" into your PATH environment variable so Windows knows from where to load the module.
7. As a final test run "get-command -module HyperV" and check if this prints out the available Hyper-V commands.
8. Install the latest Java Runtime Environment.

9. Create a dedicated folder (example: “C:\Program Files\Extreme Networks\HyperV Adapter”) and copy the two files (DCM_HYPERV_ADAPTER_<version>.jar and DCM_HYPERV_ADAPTER.config) into it
10. Edit the configuration file DCM_HYPERV_ADAPTER.config according to your environment.
11. You are now ready to start the adapter by double-clicking the file DCM_HYPERV_ADAPTER.jar or running it within a shell using “java –jar DCM_HYPERV_ADAPTER.jar”. Verify the log file that should have been created in the same folder where the jar file is located. The adapter is automatically started when the Windows Server starts up.
12. Repeat these steps on all Hyper-V servers that you want to integrate with Extreme Management Center.

Adapter Configuration

The table below lists the configuration options for the Hyper-V agent.

Configuration Option	Description
LOG_LEVEL	Set the log level of the adapter to one of the following values: ERROR, WARN or DEBUG. If not set, the default will be WARN.
IP	IP address for the web service (=agent) to listen on.
PORT	TCP Port for the web service to listen on - must NOT be used by any other application on this server.
PRE_SHARED_KEY	The pre-shared key used for the communication between the adapter and OFConnect. This must match the key entered when installing the OFConnect Hyper-V module.
IS_PRE_SHARED_KEY_ENCRYPTED	If set to 'false' the adapter assumes that the 'PRE_SHARED_KEY' configured above is not encrypted - on the first start the adapter will automatically encrypt the key and set this value to 'true'. If you want to change this key at a later stage, change the key above, set this value back to 'false' and restart the adapter service.

Verification

Within the Hyper-V management console, click on a virtual machine. You should see the corresponding data from Extreme Management Center in the “Notes” field on the bottom of the page.

VMware vSphere

The Vmware vSphere integration offers provisioning of virtual machines in the network as well as automating the creation of virtual networks based on end-

system access groups. In addition, data within Extreme Management Center is enriched for each end-system and conversely made available within vSphere.

Module Configuration

Configuration Option	Description
Username	Username used to connect to the vSphere web service. Read/Write/Execute permissions required.
Password	Password used to connect to the vSphere web service.
VMware Webservice URL	Web service URL of the VMware vSphere server.
Module enabled	Enables and Disables Module.

- Outgoing data format: The format of the Extreme Control data (like last seen time, switch IP, switch port, etc.) that is written to the description fields of the VMs within VMware or XEN. You can customize the appearance and what information you want to include/exclude from there. Hint: For the VMware vSphere client the annotation field is limited in size. The default outgoing format is very close to the maximum string length allowed for this field. If you want to add additional information to this field consider replacing it with some of the existing default value.
- Format of the incoming data: The format of the data that is coming from VMware or XEN and that is written to the custom field.
- Create Private VLAN Entries: If set to false, the Datacenter manager will not automatically create any pVLAN entries on dvSwitches even if you configured any. This feature is disabled per default and needs to be enabled manually if needed.
- Create Portgroups from End-system Groups: If set to true, the Datacenter manager will automatically create new portgroups within VMware based on the Extreme Access Control engine end-system groups and your other configuration.
- Update Portgroup VLAN IDs: Only useful if the setting above is set to true. If you change the “vlan=XXXX” value within an end-system group this setting will automatically also change your portgroup VLAN IDs accordingly.
- Use Global End-system Groups: Only if this is set to true, the VMware module will have access to the global end-system groups that are provided by the Extreme Control module within the main module. This is necessary if you want to automatically create portgroups based on Extreme Control NAC end-system groups.
- Enable NAC Plugin: Using this option, the automatic Extreme Access Control engine Plugin Extension registration may be disabled.
- NAC Plugin URL: The URL of the configuration file for the Extreme Datacenter manager plugin for VMware. This is used by vCenter server to tell any connecting vCenter clients from where to download the Extreme plugin.

- Enable Custom Attributes: En-/Disables the creation and updates of Custom Attributes for vCenter Servers.
- Custom Attributes Data Format: This text field allows the configuration of Custom Attributes for vCenter Servers. Connect will create and update these attributes for each VM and allow for searching and sorting for this data within vCenter. Each attribute has to be configured on a single line and follow the format: NAME=VALUE where NAME is the name of the Custom Attribute and VALUE is a free text that may utilize all variables that are available in the "Outgoing data format" option. If a VM should use more than one network interface, the data for each variable is presented as "NIC1DATA/NIC2DATA/...".
- Deletion Group: Name of the portgroup that a VM will be redirected to if it's current endsystem group is deleted.
- Port Group Import: Enables the automatic creation of endsystemgroups in Extreme Control based on port groups. The port group name will be used for the endsystem group. Be aware that the delimiter also applies here. In the default configuration, the text after the last delimiter will be truncated from the name.
  i.e. MyPortGroup_VLAN1_dvSwitch0 will be imported as MyPortGroup_VLAN1 in Extreme Control. VLAN IDs will be updated if they change.
- Automatic Enforce after import: Enables the automatic enforcement of all appliances and the policy domain (only for extended import) if a portgroup was imported.
- Extended PortGroup Import: Also creates NAC Configuration and policy profiles during PortGroup Import. Requires the options for NAC Configuration, Policy Domain and Forward as Tagged also to be defined. Be aware that the truncated port group name will also be used as the VLAN name and must adhere to naming limitations.
- Enable PortGroup Import Removal: Delete the NAC Configuration and/or End-System Group if the portgroup is deleted.

Stop then start the Extreme Management Center services (refer to Extreme Connect Installation section for instructions).

Verification

Within the vSphere Client, click on a virtual machine and then on the "Summary" tab on the right side. At the bottom of this tab there should be an annotations field that should contain the corresponding data from Extreme Management Center (for example, information on the switch port and switch IP to which this VM is physically connected).

VMware View

The integration of VMware View does not require any special tool or software to integrate. The virtual desktops need to be configured to use 802.1x and users have to use the View Client to access those desktops via PCoIP in order to allow user-based authentication. Any Extreme switch with a reasonable amount of multi-user authentication capacity is suitable to authenticate each virtual desktop individually and apply a policy based on the username.

In addition to that, standard Extreme Connect operation may be used to provision a NAC rule for the connected portgroup of each VM, if user authentication via 802.1x is not available.

Please see the VMware View VDI documentation for further information regarding the setup procedure.

Web Service Error Codes

Error Code	Description
0	Operation was successful
1	The requested object does not exist
2	Object already exists
3	Parameter value is incorrect
4	Error parsing an input
5	Result would be an Invalid configuration

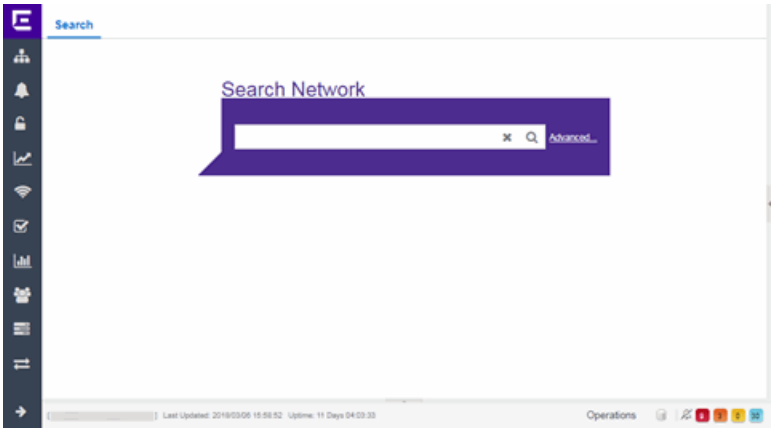
Error Code	Description
6	Remote connection error
7	Unexpected error condition
8	End system group does not exist
9	CSV operation error

Search Network

Extreme Management Center's Search Network 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 Extreme Access Control end-system name, username, and registration custom field attributes. A device must be in the Extreme Management Center 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 Extreme Access Control authenticated client.

In addition, there are two Advanced Search options, accessed from the Advanced link to the right of the Search Network field: searching in Compass and searching in Maps.

To view Extreme Management Center 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. (For more information on authorization capabilities, see the Help topic, "How to Configure User Access to Extreme Management Center Applications," located in Suite-Wide Tools > Authorization Device Access.)



This Help topic provides information on the following topics:

Using Extreme Management Center Search Network

In the Search Network field, enter a MAC address or IP address and press Enter to begin the search. You can copy the IP or MAC address from another source and enter it into the Search Network field. You can also search on AP serial numbers, and by Extreme Access Control end-system hostname, user name, and registration custom field attributes.

Depending on the type of item you searched for, 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 Examples

Following are some examples of different kinds of searches you can perform using the Extreme Management Center 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 Extreme Access Control Authenticated Client IP Address

You can also search on an Extreme Access Control authenticated end-system's IP address. For example, you can copy an end-system's IP address from the Control tab's End-Systems view and paste it into the Search Network field.

Search your Network for a Device IP Address

To perform a search on a device, you can copy a device IP address from the Network tab. The search results show only the single device. Right-click on the device to open additional reports.

Search Options/Limitations

The maximum number of PortView Search results displayed at one time is configured in the Management Center Options (Administration > Options > Management Center > Session Limits). The default maximum number is five. Once 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 Extreme Access Control authenticated environment (six devices may be returned if the client is also connected via wire). The number of devices returned becomes smaller as you search for one of the five devices. For example, if you search for an AP instead of a client, four devices are returned. If you search for a Wireless Controller, Extreme Access Control Gateway, or switch, one device is returned.

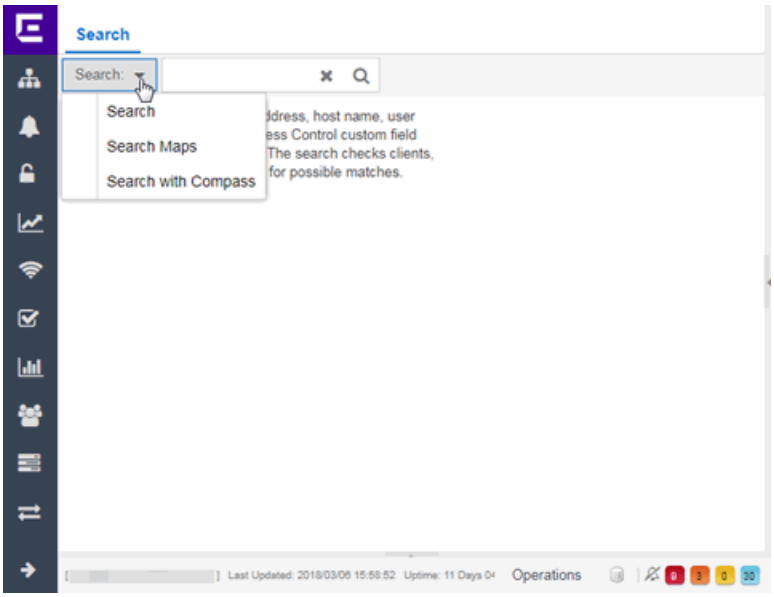
Advanced Search Options

The Advanced Search, accessed from the Advanced link to the right of the Search Network field, provides two additional search options available from the Search drop-down menu at the top-left of the Search page.

- Search in Maps — Allows you to search your existing maps to find a wired or wireless client or device. If the search item is found, the map opens on a separate

tab. For more information, see Maps Overview.

- Search with Compass — Provides additional fields, allowing you to refine your search. For more information, see Search with Compass.



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.

You can access the Search with Compass option from the Search drop-down menu at the top-left of the Search page. To perform a search, specify the following information:

- Device Group (Search Scope) — Use the drop-down menu to select a device group to search. The menu is populated with the system and user-defined device groups in Console. If you do a search on a user-defined device group that contains interfaces, the whole device on which the interface is located is searched.
- Search Type — There are multiple search types available from the drop-down menu. 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:

- Click on 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 Extreme Management Center 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.

Related Information

For information on related tabs:

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

Extreme Management Center 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.

How to Discover Devices

Extreme Management Center allows you to discover the devices of your network and add them to the Extreme Management Center 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 Extreme Management Center, see Extreme Management Center Initial Configuration Checklist.

You can discover new devices based on the following criteria:

- Seed addresses for CDP, LLDP, or EDP-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 Extreme Management Center database, where they are displayed in the left-panel tree on the Network > Devices tab.

To discover devices, begin by using the Site tab to configure the default settings that apply to devices you add to Extreme Management Center and then configure individual devices and add them to the Extreme Management Center 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 Extreme Management Center.

Discovering Devices

1. Open the Network > Devices tab.
2. Select Sites from the left-panel drop-down menu.
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. Click 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 menu.
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, or EDP-compliant devices.
    - **Address Range** — Enter the **Start Address** and **End Address** for the IP addresses in the same address range.

    NOTE: Extreme Management Center only allows a subnet search of a 16-bit mask or higher when discovering devices.
9. Click the **Add** button in the Profiles section of the window to open the Add Profile window. Select **New** in the drop-down menu to create SNMP and CLI credentials for the profile and click the **Save** button.

    Profiles allow you to configure different sets of SNMP and CLI credentials for read access, write access, and maximum access. Once 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 and any other appropriate actions for your devices in the Device Actions section of the window.

12. Repeat the process for all devices added to this site.
    For additional information about sites, see Site tab.
13. Click **Save**.
14. Click **Discover**.
15. Open the Operations table at the bottom of the Extreme Management Center window by clicking the **Operations** button in the Bottom menu to monitor the progress of the device discovery.
16. Open the **Network** > **Discovered** tab when the device discovery is complete.
    The **Discovered** tab displays.

Adding Devices

1. Open the **Network** > **Discovered** tab in Extreme Management Center.
   For more information about the **Discovered** tab, see Discovered tab.
2. Select the devices you want to add to the Extreme Management Center database and click 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. Click the **Add** button.
   The devices are added to the Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center database. For additional information on discovering and adding devices, see How to Discover Devices in Extreme Management Center.

For a list of instructions outlining the initial setup of your network in Extreme Management Center, see Extreme Management Center Initial Configuration Checklist.

When you first log into Extreme Management Center 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 Extreme Management Center, which is accomplished by performing the following steps:

1. Create Authorization Groups
2. Add Users to Authorization Groups
3. Select the Authentication Method

IMPORTANT: Extreme Management Center 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 Extreme Management Center users.

1. Access the **Administration** > Users tab.
2. Click 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 allows you to make changes to the authorization groups and authorized users.

3. Click the **Add** button in the Authorization Groups section at the bottom of the tab.
4. Enter the appropriate information for each authorization group using Extreme Management Center.
   The Capability section of the window allows 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. Click 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 Extreme Management Center and add them to an authorization group depending on the level of access they require.

1. Click 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. Click the **Save** button to save the new user.
4. Repeat the process to add all Extreme Management Center users for each authorization group.

Select the Authentication Method

Finally, use **Administration** > **Users** tab to select the method by which users authenticate when accessing Extreme Management Center.

Extreme Management Center 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 menu 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. Click the **Release Lock** button to allow 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 Extreme Management Center 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 Configuration/Firmware > Compare Last Configurations.

From the Reports tab:

Use the Reports tab to compare two configuration files selected from all archived files for the device.

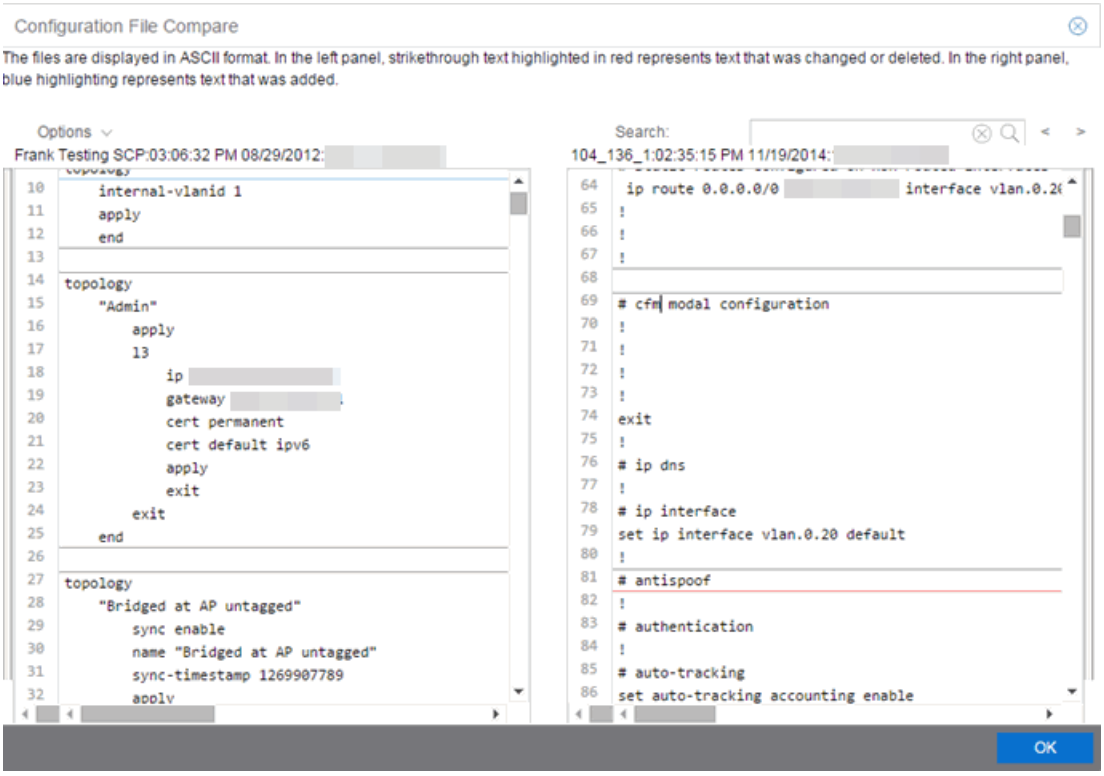
Select the Device > Device Archives report. Click on the Archive Details tab in the right panel and then click on the Archives by Device sub-tab.

The tab displays all the Extreme Management Center archives by device IP address. Select two files to compare and click 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

DeviceView

DeviceView is an Extreme Management Center component that provides a wide range of analysis and troubleshooting information for your network wired and wireless devices, including a device summary, FlexViews, and Extreme Management Center reports.

The primary launch point for DeviceView is from the Network tab. DeviceView can also be launched from other locations in Extreme Management Center and Console.

This Help topic provides the following DeviceView information:

- Requirements
  - Access Requirements
  - Data Collection Requirements
- DeviceView Reports
  - Left-Panel Device Summary
- Launching DeviceView

Requirements

Access Requirements

Access to DeviceView reports is determined by the user's membership in an Extreme Management Center authorization group and the group's assigned capabilities. The following list shows the capabilities required for full access to all the DeviceView 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

For more information on how to configure capabilities and authorization group membership, see the Help topic How to Configure User Access to Extreme Management Center Applications located in Extreme Management Center Suite-Wide Tools > Authorization Device Access.

Data Collection Requirements

DeviceView 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 Extreme Management Center User Guide.

DeviceView Reports

The DeviceView is comprised of a left-panel device summary, and a selection of tabbed panels that display FlexViews and reports based on the device family.

The following table shows the reports available for EOS devices, ExtremeXOS devices, and wireless controllers. The reports displayed in a DeviceView vary according to the selected device.

EOS Devices*	ExtremeXOS devices**	Wireless Controllers
Ports***	Ports***	Ports***
User Sessions	User Sessions	User Sessions
Switch Resources	Device and Module Information	Controller History

EOS Devices*	ExtremeXOS devices**	Wireless Controllers
Power and Fan Status	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
Alarms and Events	VPLS	Archives
Archives	Port Utilization	
	Alarms and Events	
	Archives	

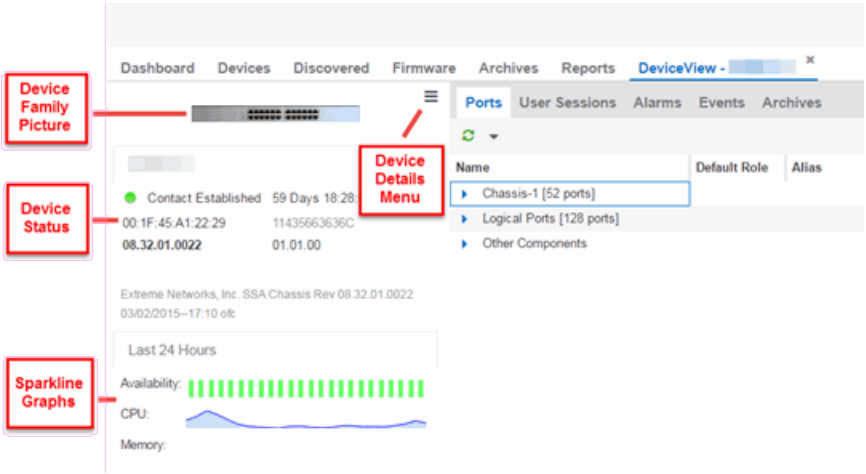
*Includes N-Series, S-Series, and K-Series devices.
**Includes BlackDiamond, E4G, and Summit Series devices.
***Right-clicking ports and selecting Add to Device Group opens the Add to Device Group window, which allows you to select a device group to which to add the selected ports. Additionally, right-click a port and select the **Application Telemetry** menu to view the Interface Top Applications Treemap or Top Clients by Interface report for the port.

NOTE: 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.

Left-Panel Device Summary

The left-panel device summary view (shown below) is displayed in each DeviceView 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 Extreme Management Center User Guide.
- 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 — Click the Menu icon (☰) in the upper right corner to access additional device reports.

Launching DeviceView

DeviceView can be launched from a variety of locations in Extreme Management Center.

Network Tab

The primary launch point for DeviceView is from the Network tab.

1. Open the Network > Devices tab.
2. Hover your mouse over the first column and click on the DeviceView icon .
3. The DeviceView opens as a separate tab.

NOTE: You can also launch a DeviceView from any Device Details menu throughout Extreme Management Center.

Control Tab

Use the following steps to launch DeviceView from the Control tab.

1. Open the **Control** > Dashboard tab.
2. Click on the System view.
3. In the Engine Information report, click on an engine IP address to open a DeviceView for the engine.

Extreme Management Center Maps

Use the following steps to launch DeviceView from a map.

1. Open Extreme Management Center Maps and click on a map.
2. In the map, right-click on a device icon and select DeviceView.

Search

Use the following steps to launch DeviceView from the **Search** tab.

1. Open Search and search for a device.
2. In the Overview, right-click on the device icon and select DeviceView.

Related Information

For information on related topics:

- Network Tab

How to Check for Extreme Management Center Updates

Extreme Management Center provides an easy way to access the Extreme Networks website to obtain information about the latest Extreme Networks firmware releases available for download.

Before using the Check for Updates feature, it is important to configure your Update Credentials in the ExtremeNetworks.com Updates options (Administration > Options > ExtremeNetworks.com Updates). These credentials are used to access the website to obtain the update information. First, create an account at ExtremeNetworks.com and define a user name and password for the account credentials. Then you can configure those credentials in the options.

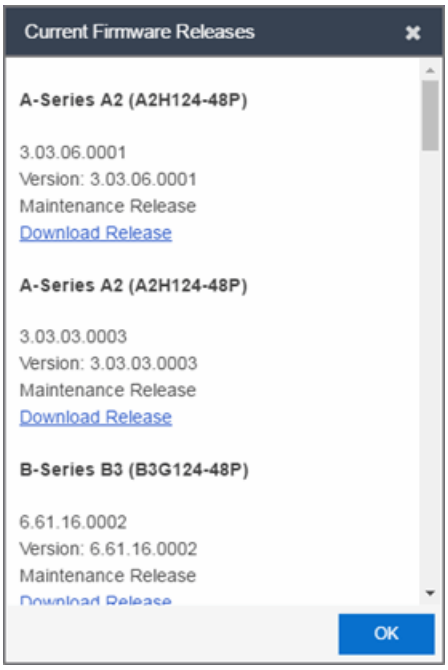
In addition, if your network is behind a firewall, you must also specify in the options the HTTP Proxy server being used, prior to performing an update. Check with your network administrator for the proxy server information.

After you have configured the options, use the following steps to check for firmware updates:

1. Access the Network > Devices tab.
2. Use the left-panel drop-down menu to select All Devices, Maps, or Sites, depending on the devices for which you are updating the firmware. You can also use the drop-down menu 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. Click the Menu icon (≡) or right-click in the Devices list.
5. Select Configuration/Firmware > Check For Updates.

NOTE: You can also right-click a device in the left-panel and select Configuration/Firmware > Check For Updates.

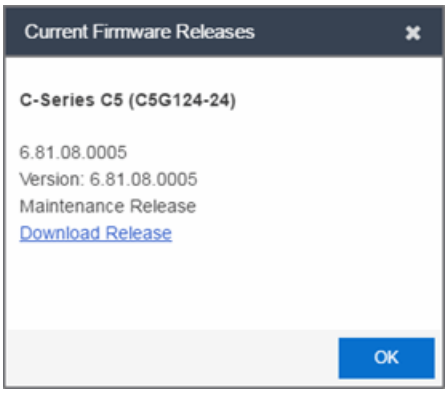
Extreme Management Center checks ExtremeNetworks.com for the latest firmware versions available for Extreme Networks devices and displays the information in the Current Firmware Releases window.



6. Click **OK**.

   The **Firmware** icon ( ) in the **Updates** column of the **Devices** tab indicates a firmware update is available for the device.

7. Select a device on which you want to update the firmware and click the **Menu** icon ( ) or right-click the device in the Devices list.
8. Select **Configuration/Firmware** > **View Available Releases**.
9. The **Current Firmware Releases** window displays, which allows you to see the firmware available for that device and download the firmware.



10. Click on the **Download Release** link to access the website and navigate to the product Firmware download page.

11. Enter your credentials to access the website (use the same credentials configured in the ExtremeNetworks.com Updates options (Administration > Options > ExtremeNetworks.com Updates).

Once you download a firmware version, you can upgrade the firmware on the device.

Related Information

For information on related topics:

- How to Upgrade Firmware
- ExtremeNetworks.com Updates Options

How to Upgrade Firmware in Extreme Management Center

Extreme Management Center allows you 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 two ways:

- For a particular device on your network
- For all devices of a device type

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.

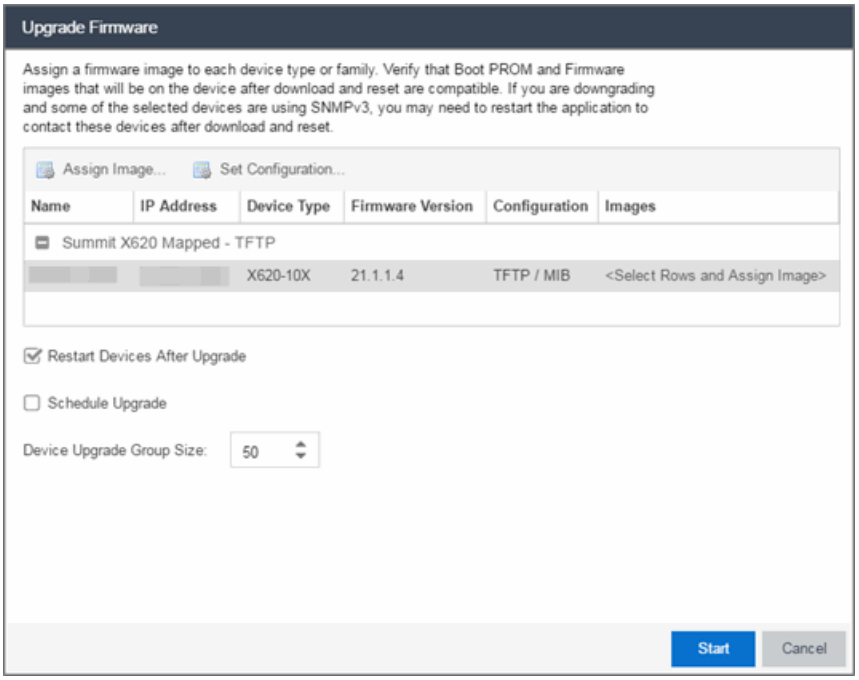
Upgrading for a Device

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 menu, 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. Click the **Menu** icon (≡) or right-click in the Devices list.
7. Select **Configuration/Firmware** > **Upgrade Firmware**.

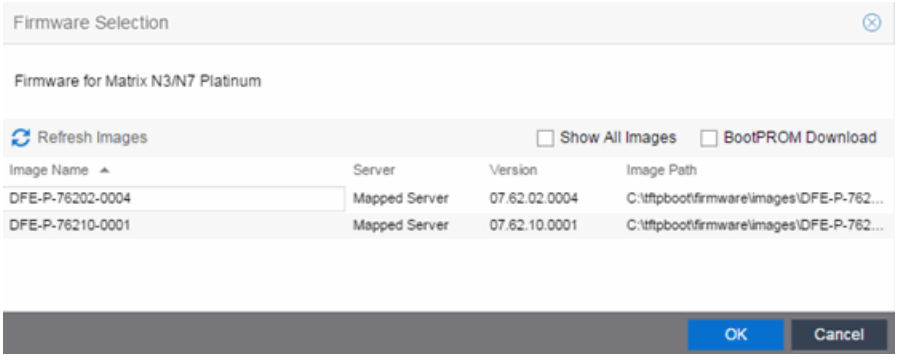
NOTE: You can also right-click a single device in the left-panel and select **Configuration/Firmware** > **Upgrade Firmware**.

The Upgrade Firmware window opens, displaying the devices you selected grouped by device family.



8. Select one or more devices and click **Assign Image**.

   The Firmware Selection window opens, displaying the firmware versions compatible with the device type.



9. Click 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** check box in the Firmware Selection window. This clears any images already assigned and only displays boot PROM images for selection.

12. Click **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).

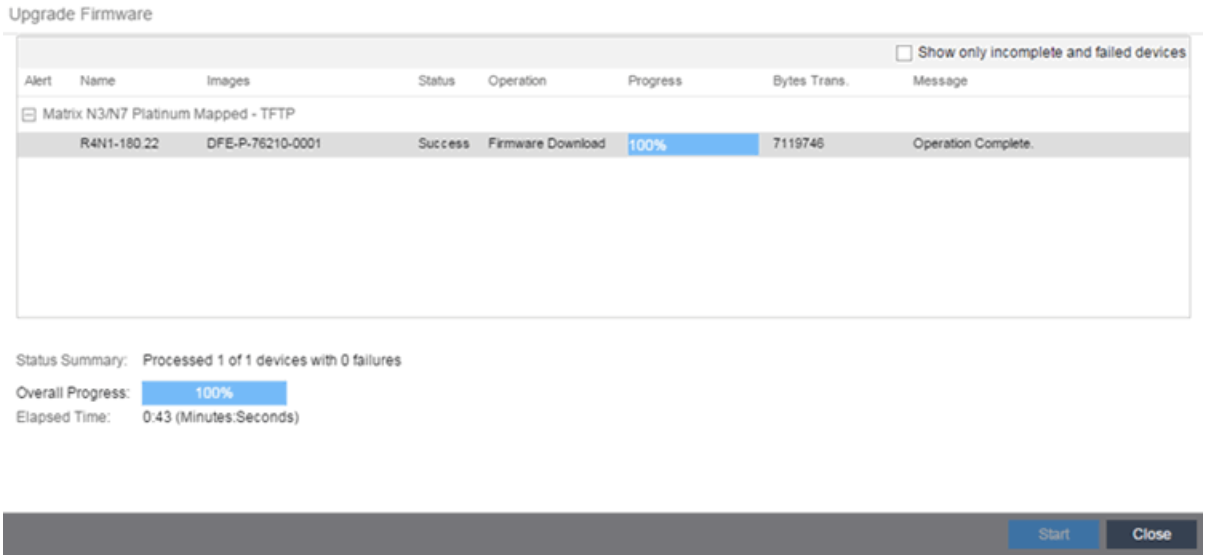
14. Click the **Restart Devices After Upgrade** checkbox to automatically restart devices that support restarting immediately after upgrading the firmware image.

NOTES: Clicking 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.
If the **Restart Devices After Upgrade** checkbox is selected, the **Schedule Upgrade** checkbox is unavailable.
You can also restart a device manually in the Restart Devices window, accessible from the **Network** tab in Extreme Management Center by right-clicking the device and selecting **Configuration/Firmware** > **Restart Device** option.

15. Click the **Schedule Upgrade** checkbox to run the firmware image upgrade at a future date. Clicking 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 click 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 click the drop-down arrow to select the time from a drop-down menu.
    - **Abort on Failure** — Clicking this checkbox causes the upgrade to terminate in the event it is not successful.

NOTE: If the **Schedule Upgrade** checkbox is selected, the **Restart Devices After Upgrade** checkbox is unavailable.

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. Click **Start** if you are upgrading the firmware immediately or **Schedule** if the upgrade is scheduled for a future date.
18. If upgrading the firmware image immediately, a progress column appears on the **Upgrade Firmware** window. Once the upgrade is complete, a Status section appears, displaying whether the upgrade occurred successfully.

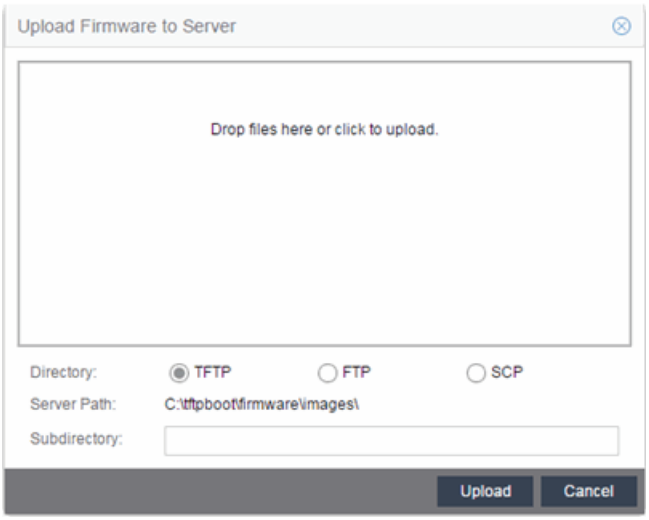


19. Click **Close**.

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. Click the **Upload** button to open the Upload Firmware to Server window from which you can save image files to the Extreme Management Center server.



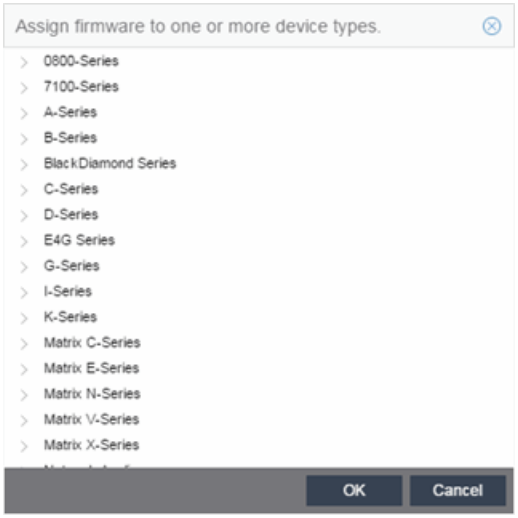
b. Drag the file or files into the box in the main part of the window or click the box to open a window from which you can navigate to the appropriate directory.

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. Click the **Upload** button.
A status bar displays over the file icon and a checkmark indicates when the upload is complete. Anyone with access to Extreme Management Center 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. Click **OK**.

If you did not select **Restart Devices After Upgrade**, restart your devices.

Related Information

For information on related windows:

- Network Tab
- Devices Tab
- Firmware 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 menu to select All Devices, Maps, or Sites, depending on the devices you are restarting. You can also use the drop-down menu 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. Click the Menu icon (≡) or right-click in the Devices list.
6. Select Configuration/Firmware > Restart Device.

   NOTE: You can also right-click a single device in the left-panel and select Configuration/Firmware > Restart Device.

   The Restart Devices window displays.
7. Select the devices you want to restart by clicking 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. Click 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. Click Finish to close the window.

Related Information

For information on related topics:

- How to Upgrade Firmware
- Restart Device Window

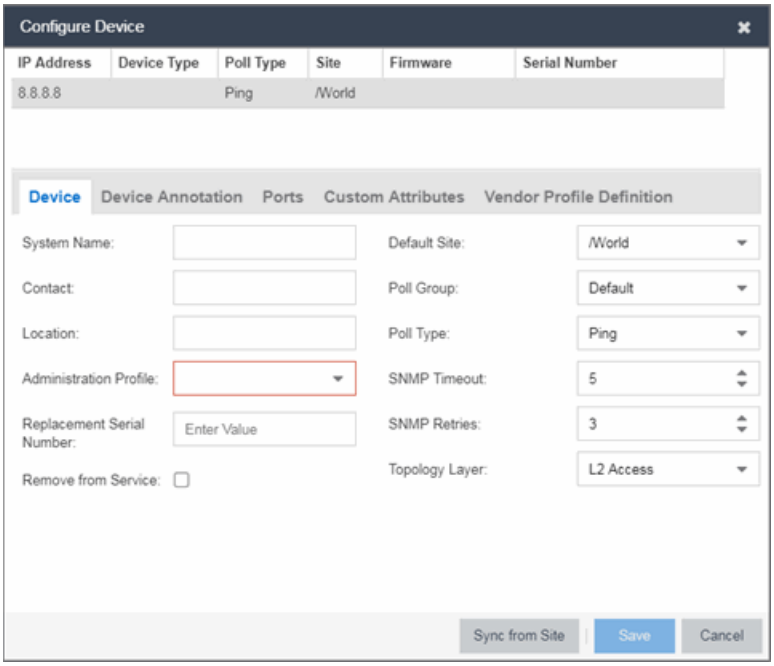
How to Create and Edit a VLAN in Extreme Management Center

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

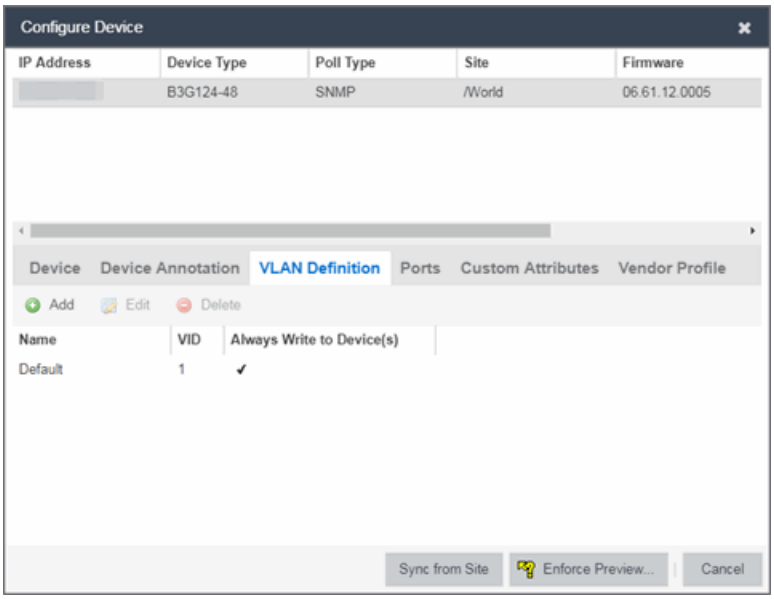
- Create a new VLAN
- Edit the ports of an existing VLAN
- Edit the name of an existing VLAN
- Remove devices from an existing VLAN

To create a new VLAN:

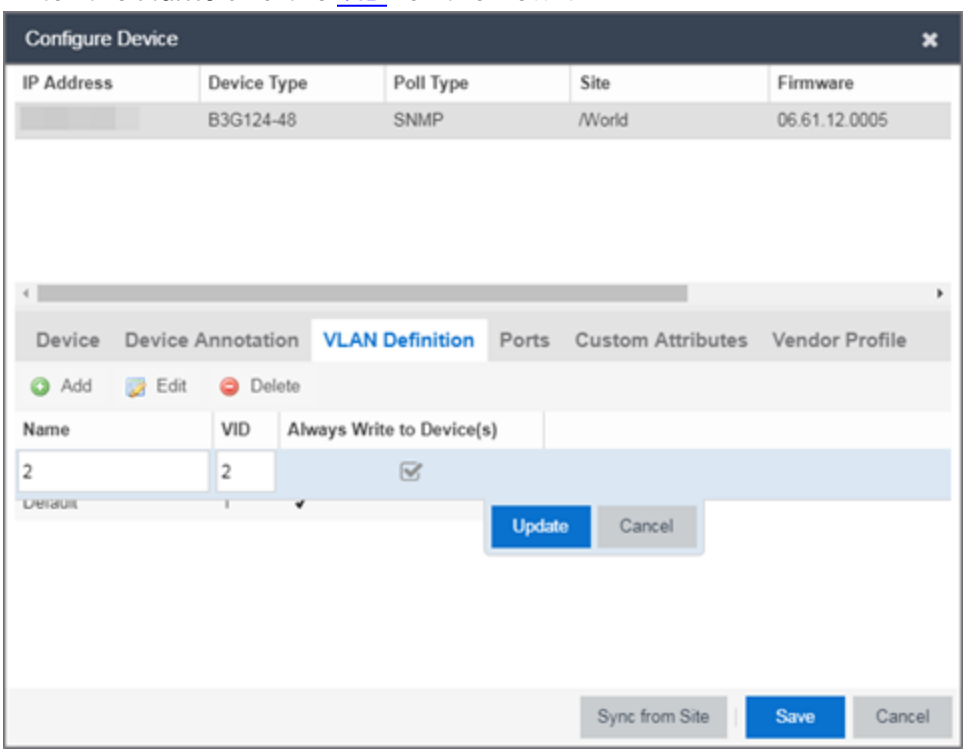
1. Launch Extreme Management Center.
2. Open the **Network > Devices** tab.
3. Select the device from the devices list. Right-click the device and select **Device > Configure Device**.
   The Configure Device window opens.



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

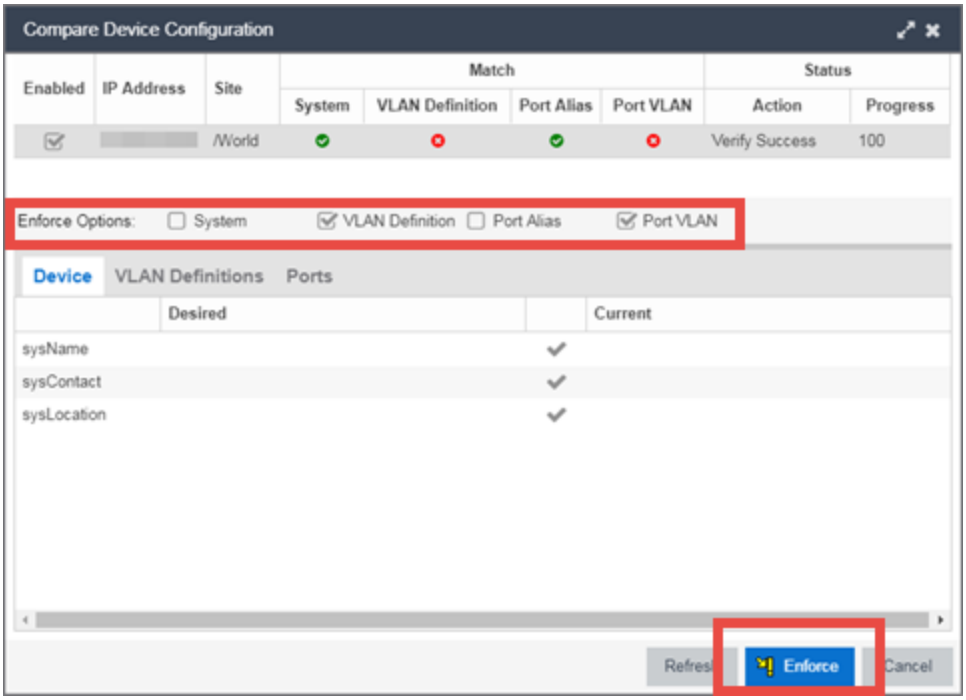


5. Click the **Add** button.
6. Enter the **Name** and the VID for the new VLAN.



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 Extreme Management Center to select the checkboxes by default, open the `NSJBoss.properties` file and change **false** to **true** in the following lines:

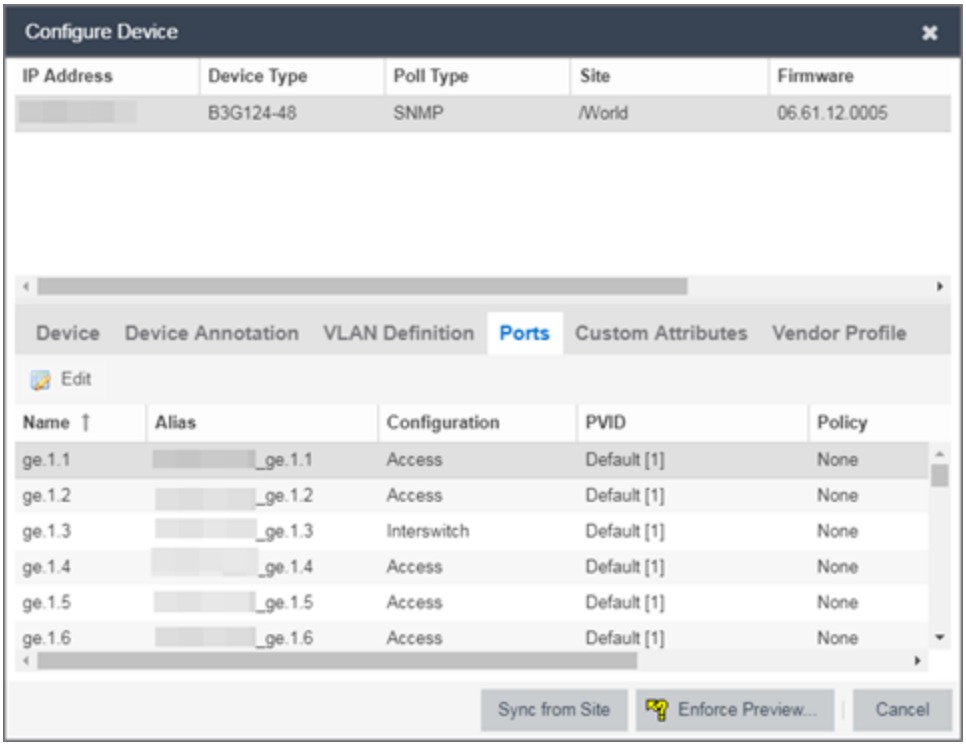
- `site.enforceOption.autoEnable.system=false`
- `site.enforceOption.autoEnable.vlanDefinition=false`
- `site.enforceOption.autoEnable.portAlias=false`
- `site.enforceOption.autoEnable.portVlan=false`

The VLAN is now created and assigned to the device.

To configure the VLAN(s) on the ports

1. Launch Extreme Management Center.
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. Click **Enforce Preview**.
10. Under the Enforce Options, select the **Port VLAN** checkbox and select **Enforce**.

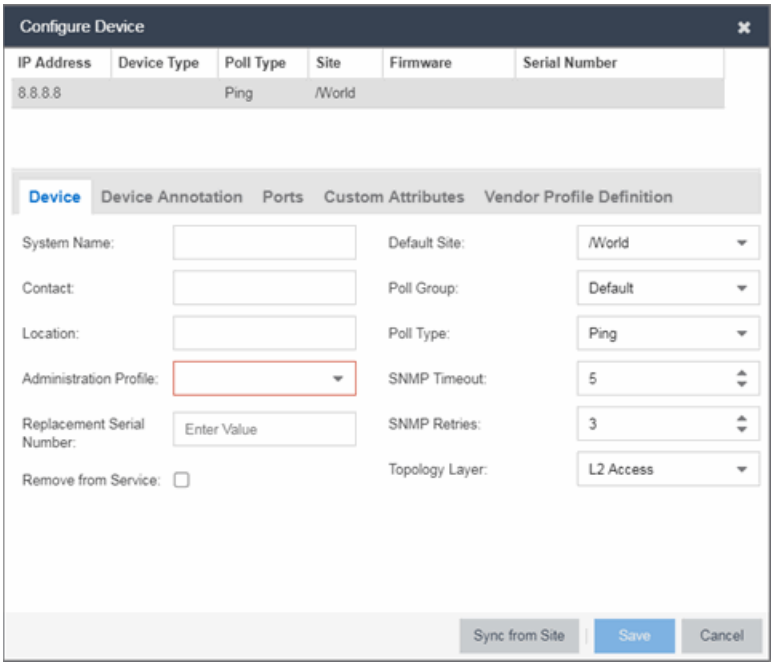
NOTE: By default, the checkboxes in the Enforce Options section of the window are not selected. To configure Extreme Management Center to select the checkboxes by default, open the `NSJBoss.properties` file and change **false** to **true** in the following lines:

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

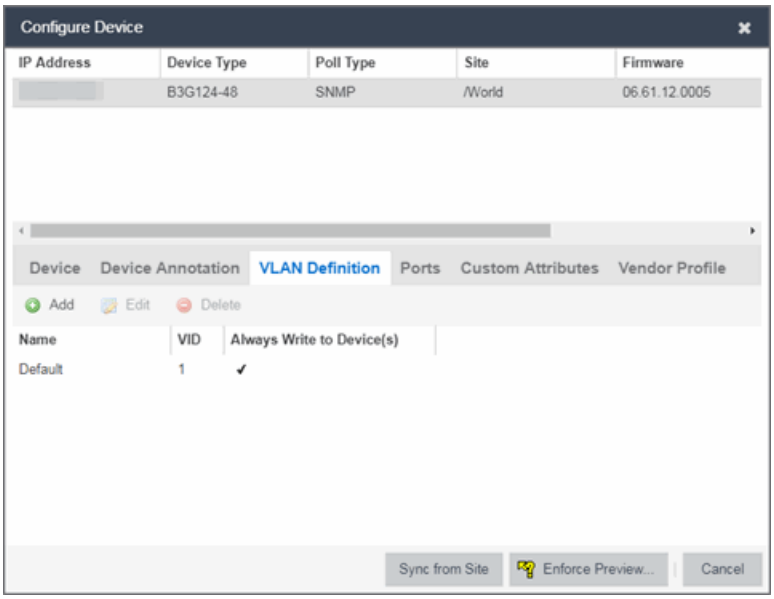
The VLAN is now configured to the Ports.

To edit the name of a VLAN:

1. Launch Extreme Management Center.
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. Click the **VLAN Definition** tab.

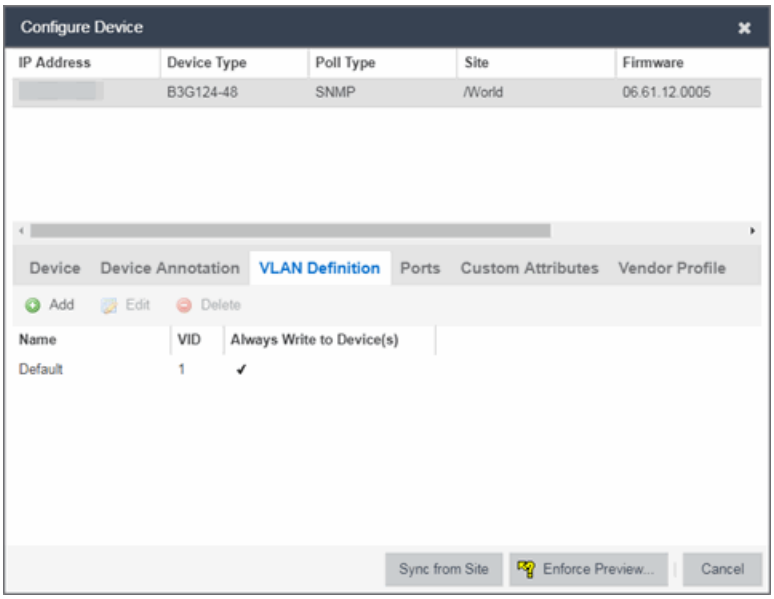


6. Select the VLAN to edit and then select the **Edit** button.
7. Enter the new name for the VLAN.
8. Click **Update**.
   The Edit pane closes.
9. Click **Save** to exit the VLAN Definition window. The VLAN is updated.

To remove devices from a VLAN:

1. Launch Extreme Management Center.
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. Click the **VLAN Definition** tab.
   The VLAN Definition pane opens.



5. Select the VLAN and click **Delete**.

Related Information

For information on related topics:

- Maps
- Devices tab

How to Add a New Regime in Extreme Management Center

The Governance 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 **Governance** > Audit Tests tab.
2. Click 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 governance audit.

   NOTE: Because of the number of wireless events potentially stored by Extreme Management Center, wireless events are not included in a governance audit the first time it is run. Once the governance audit is run the first time, older wireless events are moved, so older events are not included in the results.

6. Click **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 menu.
   d. Select the device type to which the audit test applies in the **Device Type** drop-down menu.
   e. Click **Copy**.
8. Create your own audit tests.
   a. Click 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. Click **Save**.

Your custom regime is now available on the Governance tab.

Related Information

For information on related tabs:

- Governance Overview
- Diagnostics

How to Obtain and Apply a Governance License in Extreme Management Center

To use the Governance tab in Extreme Management Center, an additional license is required.

To obtain and apply the license in Extreme Management Center:

1. Contact your sales representative to purchase an IGE (Information Governance Engine) 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 click **Create An Account**.

      An email is sent to you with instructions to activate your account.
   c. Click 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. Click **Activate**.
3. Access the Extreme Networks Support Portal at https://extremeportal.force.com/ExtrLicenseLanding.
4. Enter your **Email** and **Password** and click **Log In**.
5. Click **Generate License**.

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

   A window displays with your software license key.
8. Copy the license key from the window.

9. Open Extreme Management Center.
10. Access the **Administration** > Diagnostics tab.
11. Select **Server** > **Server Licenses** in the left-panel.

    The **Server Licenses** panel displays.
12. Click **Add**.

    The **Add License** window displays.
13. Paste the license key you copied in Step 9 and click **OK**.
14. Restart Extreme Management Center.
15. The Governance tab is now available in the menu, allowing you to use governance audit functionality.

Related Information

For information on related tabs:

- Governance Overview
- Diagnostics

ZTP+ Device Configuration

Using Extreme Networks' ZTP+ (Zero Touch Provisioning Plus) functionality, you can quickly add new devices to your network and configure them in Extreme Management Center.

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: Accessing the device via the local console during ZTP+ device configuration using a console cable causes the process to fail. To complete the process after a failure, either configure the device manually or type `unconfigure switch all` and restart the ZTP+ configuration process outlined in this topic.

Stacked systems do not currently support ZTP+ configuration.

In Extreme Management Center, new devices are automatically discovered on the network the moment they are connected. ZTP+ enabled devices send information to Extreme Management Center automatically, including the serial number, the number and speed of the ports, and the firmware version. Once a ZTP+ device is connected, you can add it to Extreme Management Center 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.

Pre-Configuration

Before connecting your devices, you need to pre-configure the following:

- Select the Reference Firmware Image Location
- Download XMODs
- Default Device Configuration in Extreme Management Center
- Switch/Engine Settings

Select the Reference Firmware Image Location

You can configure Extreme Management Center 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 Extreme Management Center. Once the firmware image is saved on the Extreme Management Center server, it is available in Extreme Management Center and can be downloaded to the device.

NOTE: Application Analytics and Extreme Access Control engines do not support firmware image downgrades via ZTP+.

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 Extreme Management Center.

To configure the file transfer directory:

1. Access the **Administration** > **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.

   NOTE: ExtremeXOS devices must be running version 21.1 or later.

Once you download the firmware image from ExtremeNetworks.com and save it on the Extreme Management Center server, use the **Firmware** tab in Extreme Management Center to download the image from the Extreme Management Center 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**.

   NOTE: Firmware for an ExtremeXOS device contains a filename extension of .XOS and firmware for an Application Analytics engine contains a filename extension of .BIN.

   Your device automatically updates with this firmware image when it restarts and is

logged in the Event log with a **Category** of **Inventory**.

Download XMODs

XMODs are files that work in conjunction with firmware image upgrades to enhance ZTP+ functionality 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.

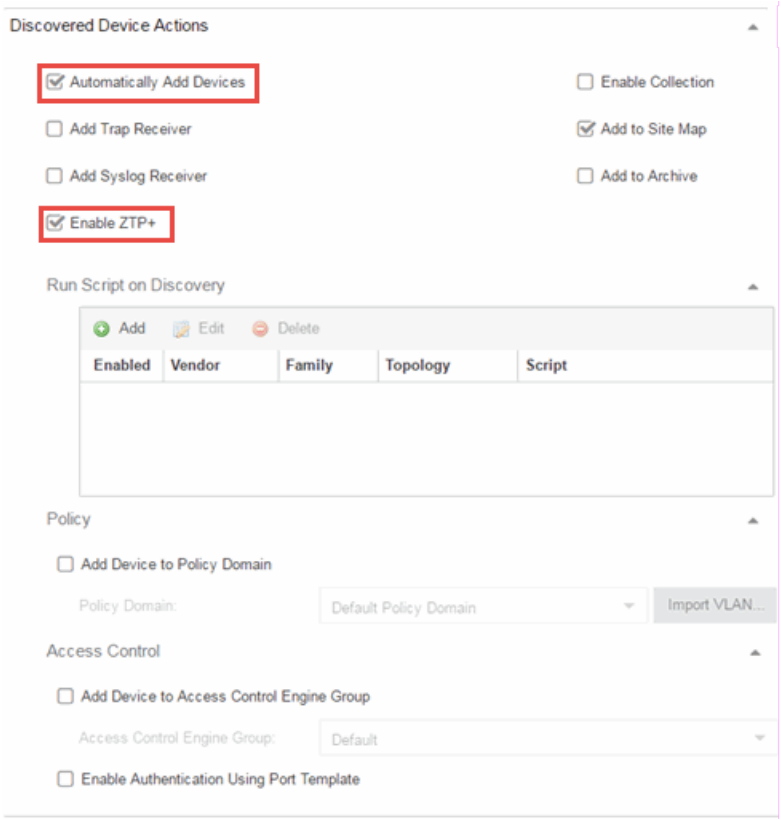
IMPORTANT: ExtremeXOS devices on which version 21.1.1.4 is running require an update to the CloudConnector XMOD for ZTP+ functionality to work properly. Saving the most recent XMOD in the directory specified above updates the device and allows ZTP+ to function as intended.

If multiple CloudConnector XMOD files exist in the same directory on the Extreme Management Center server as the reference image, Extreme Management Center downloads the XMOD file with the higher version number on the device.

Default Device Configuration in Extreme Management Center

Before connecting your devices, you can configure the default settings that Extreme Management Center applies to all devices you add to the network. This is accomplished using the Site tab.

1. Access the **Network** > **Devices** tab in Extreme Management Center.
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 **Enable ZTP+** and **Automatically Add Devices** checkboxes in the Discovered Device Actions section and any other actions you want to occur on your devices discovered in Extreme Management Center.



5. Use the Run Script on Discovery section to automatically run a script on devices being added to the site, if necessary.
6. Select **Add Device to Policy Domain** or **Add Device to Extreme Access Control Engine Group** to automatically add devices being added to the site to a Policy Domain or Extreme Access Control engine group.
7. Enter the **Gateway Address**, **Domain Name**, and **DNS Server** address in the ZTP+ Device Defaults section. Additionally, you can configure the NTP Server address and select the protocols to enable on your devices, if necessary.
8. Add the VLANs that are used on your devices in the ZTP+ VLAN Definition section of the tab by clicking the **Add** button and entering the **Name** and **VID**.
9. Click **Save**.

   The default configuration for this site is complete and any devices you discover with this site selected use this criteria.

Switch/Engine Settings

In order for the switch or engine to communicate to the Extreme Management Center 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 Extreme Management Center server.

Once the Extreme Management Center and ZTP+ device are pre-configured, you can add the site definition to the Extreme Management Center database.

Adding the Device to the Extreme Management Center Database

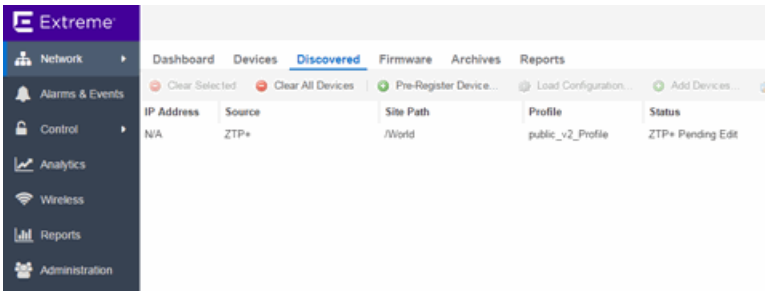
Now that you have set the default criteria for devices added to the World Site and set up the DHCP and DNS servers allowing the device to communicate with the Extreme Management Center database, you can connect the device and add it to Extreme Management Center.

1. Connect the device to your network.

   ZTP+ enabled devices communicate with Extreme Management Center securely via an HTTPS connection and transmits information to Extreme Management Center, including the serial number, firmware version, MAC address, operating system, and port information. Extreme Management Center determines the status of devices and if new updates are available in the Firmware tab and set as Reference images, they are automatically installed.

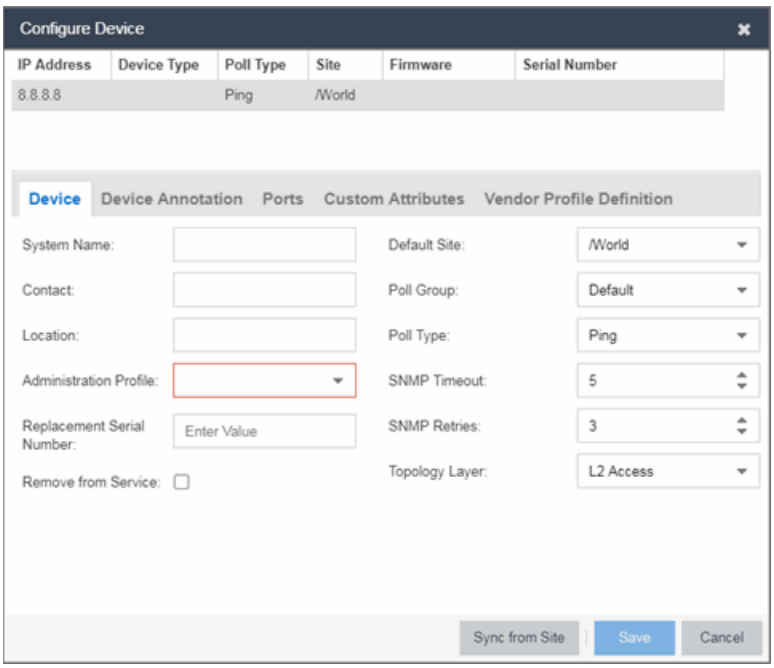
2. Open the **Network** > Discovered tab in Extreme Management Center.

   The device is listed with a **Status** of **ZTP+ Pending Edit**, indicating the device configuration needs to be edited before adding it to the Extreme Management Center server.



3. Select the device and click the **Configure Devices** button.

   The Configure Device window opens.

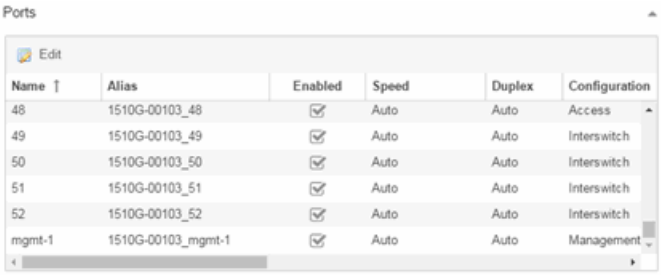


4. Select the **Default Site** for the device.
5. Select the **Poll Group** for the device, which indicates the frequency with which Extreme Management Center checks for new configurations or updates.
6. Select **ZTP Plus** for the **Poll Type**.
7. Open the ZTP+ Device settings section by clicking the heading.
8. Enter an IP address and subnet in the **IP Address/Subnet** field.

NOTE: Extreme Management Center allows you to enter the IP address in either IPv4 of IPv6 format.

9. Change the **Gateway Address**, if necessary.
10. Open the Ports section of the window by clicking the section heading.

    The Ports section opens, displaying the ports transmitted by the device to Extreme Management Center when connected to the network.

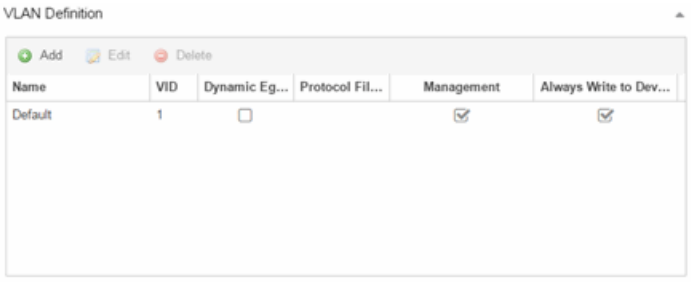


11. Select a port in the list to configure the port Name, Alias, Configuration, or port VLAN ID.

    You can also add and delete ports by clicking 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 Extreme Management Center.
    c. Enter a VLAN ID for the port in the **PVID** field.
    d. Configure the port **Speed** and **Duplex**.
12. Open the ZTP+ VLAN Definition section of the window by clicking the section heading.

    The ZTP+ VLAN definition section opens, containing any VLANs you configured on the **Site** tab.



13. Add any device-specific VLANs to those already included in the list by clicking the **Add** button.
14. Change any incorrect fields in the Device, Device Annotation, or Discovered Device Actions sections.
15. Click **Save** at the bottom of the window.

    The device is added to the Extreme Management Center database and moves from the **Network** > **Discovered** tab to the **Network** > **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, click the **Add Devices** button (the Add Device window appears), and click the **Add** button to add the device to the Extreme Management Center 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 Extreme Management Center will push the configuration to the device the next time the device contacts Extreme Management Center.

When Extreme Management Center pushes the configuration to the device, the device **Status** is **ZTP+ Complete**. Extreme Management Center 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

ZTP+ Device Configuration

Using Extreme Networks' ZTP+ (Zero Touch Provisioning Plus) functionality, you can quickly add new devices to your network and configure them in Extreme Management Center.

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: Accessing the device via the local console during ZTP+ device configuration using a console cable causes the process to fail. To complete the process after a failure, either configure the device manually or type `unconfigure switch all` and restart the ZTP+ configuration process outlined in this topic.

Stacked systems do not currently support ZTP+ configuration.

In Extreme Management Center, new devices are automatically discovered on the network the moment they are connected. ZTP+ enabled devices send information to Extreme Management Center automatically, including the serial number, the number and speed of the ports, and the firmware version. Once a ZTP+ device is connected, you can add it to Extreme Management Center 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.

Pre-Configuration

Before connecting your devices, you need to pre-configure the following:

- Select the Default Firmware Image Location
- Download XMODs

- Default Device Configuration in Extreme Management Center
- Switch/Engine Settings

Select the Reference Firmware Image Location

You can configure Extreme Management Center 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 Extreme Management Center. Once the firmware image is saved on the Extreme Management Center server, it is available in Extreme Management Center and can be downloaded to the device.

NOTE: Application Analytics and Extreme Access Control engines do not support firmware image downgrades via ZTP+.

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 Extreme Management Center.

To configure the file transfer directory:

1. Access the **Administration** > **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.

   NOTE: ExtremeXOS devices must be running version 21.1 or later.

Once you download the firmware image from ExtremeNetworks.com and save it on the Extreme Management Center server, use the **Firmware** tab in Extreme Management Center to download the image from the Extreme Management Center 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**.

   NOTE: Firmware for an ExtremeXOS device contains a filename extension of .XOS and firmware for an Application Analytics engine contains a filename extension of .BIN.

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

Download XMODs

XMODs are files that work in conjunction with firmware image upgrades to enhance ZTP+ functionality 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 21.1.1.4 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.

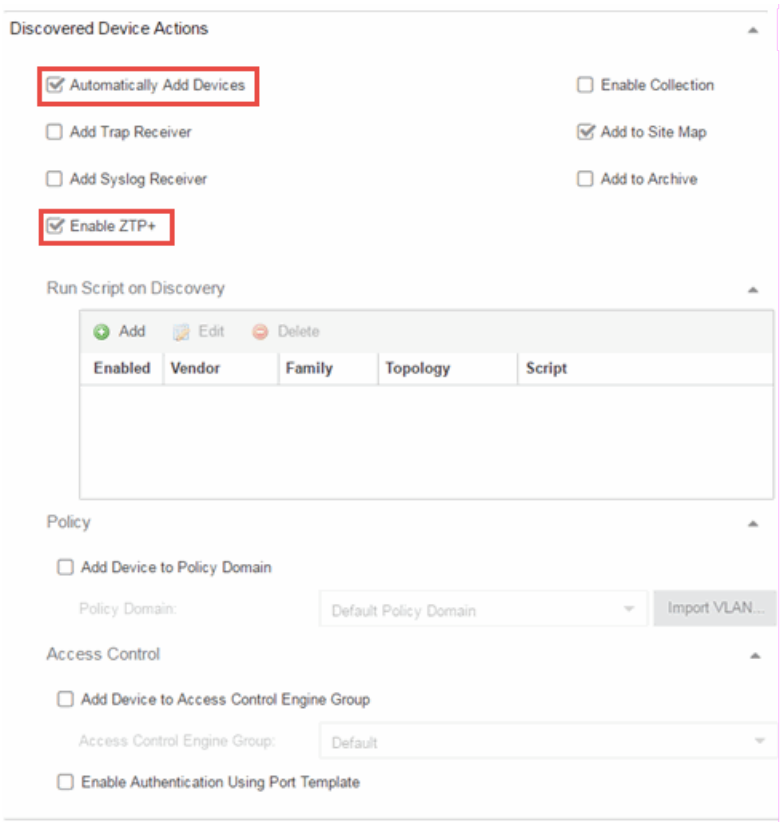
If multiple CloudConnector XMOD files exist in the same directory on the Extreme Management Center server as the reference image, Extreme Management Center downloads the XMOD file with the higher version number on the device.

Default Device Configuration in Extreme Management Center

Before connecting your devices, you can configure the default settings that Extreme Management Center applies to all devices you add to the network. This is accomplished using the Site tab.

1. Access the **Network** > **Devices** tab in Extreme Management Center.
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 **Enable ZTP+** and **Automatically Add Devices** checkboxes in the Discovered Device Actions section and any other actions you want to occur on your devices discovered in Extreme Management Center.



5. Use the Run Script on Discovery section to automatically run a script on devices being added to the site, if necessary.
6. Select **Add Device to Policy Domain** or **Add Device to Extreme Access Control Engine Group** to automatically add devices being added to the site to a Policy Domain or Extreme Access Control engine group.
7. Enter the **Gateway Address**, **Domain Name**, and **DNS Server** address in the ZTP+ Device Defaults section. Additionally, you can configure the NTP Server address and select the protocols to enable on your devices, if necessary.
8. Add the VLANs that are used on your devices in the ZTP+ VLAN Definition section of the tab by clicking the **Add** button and entering the **Name** and **VID**.
9. Click **Save**.

   The default configuration for this site is complete and any devices you discover with this site selected use this criteria.

Switch/Engine Settings

In order for the switch or engine to communicate to the Extreme Management Center 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 Extreme Management Center server.

Once the Extreme Management Center and ZTP+ device are pre-configured, you can add the site definition to the Extreme Management Center database.

Adding the Device to the Extreme Management Center Database

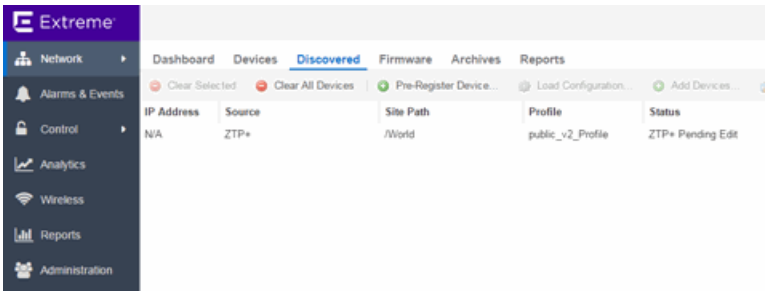
Now that you have set the default criteria for devices added to the World Site and set up the DHCP and DNS servers allowing the device to communicate with the Extreme Management Center database, you can connect the device and add it to Extreme Management Center.

1. Connect the device to your network.

   ZTP+ enabled devices communicate with Extreme Management Center securely via an HTTPS connection and transmits information to Extreme Management Center, including the serial number, firmware version, MAC address, operating system, and port information. Extreme Management Center determines the status of devices and if new updates are available in the Firmware tab and set as Reference images, they are automatically installed.

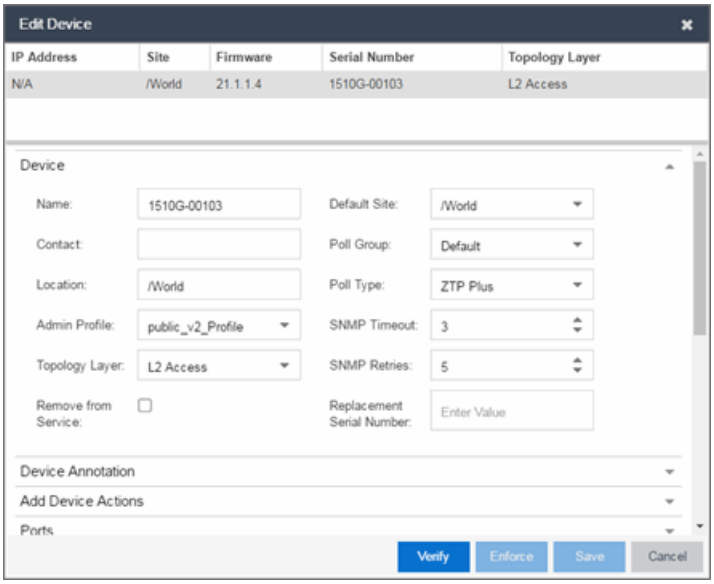
2. Open the **Network** > Discovered tab in Extreme Management Center.

   The device is listed with a **Status** of **ZTP+ Pending Edit**, indicating the device configuration needs to be edited before adding it to the Extreme Management Center server.



3. Select the device and click the **Edit Devices** button.

   The Edit Device window opens.



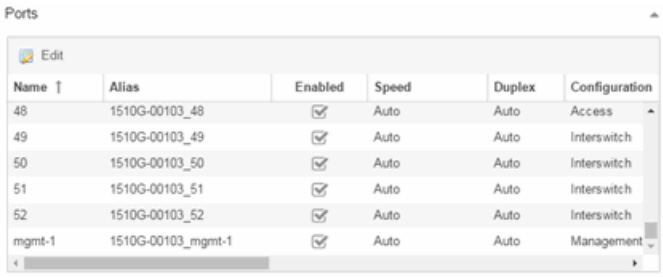
4. Select the **Default Site** for the device.
5. Select the **Poll Group** for the device, which indicates the frequency with which Extreme Management Center checks for new configurations or updates.
6. Select **ZTP Plus** for the **Poll Type**.
7. Open the ZTP+ Device settings section by clicking the heading.
8. Enter an IP address and subnet in the **IP Address/Subnet** field.

   NOTE: Extreme Management Center allows you to enter the IP address in either IPv4 of IPv6 format.

9. Change the **Gateway Address**, if necessary.

10. Open the Ports section of the window by clicking the section heading.

    The Ports section opens, displaying the ports transmitted by the device to Extreme Management Center when connected to the network.



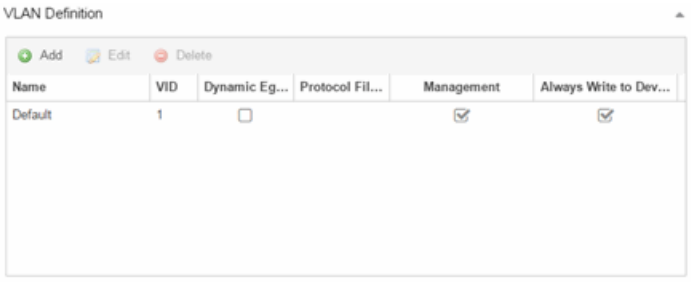
11. Select a port in the list to configure the port Name, Alias, Configuration, or port VLAN ID.

    You can also add and delete ports by clicking 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 Extreme Management Center.
    c. Enter a VLAN ID for the port in the **PVID** field.
    d. Configure the port **Speed** and **Duplex**.

12. Open the ZTP+ VLAN Definition section of the window by clicking the section heading.

    The ZTP+ VLAN definition section opens, containing any VLANs you configured on the **Site** tab.



13. Add any device-specific VLANs to those already included in the list by clicking the **Add** button.
14. Change any incorrect fields in the Device, Device Annotation, or Discovered Device Actions sections.
15. Click **Save** at the bottom of the window.

    The device is added to the Extreme Management Center database and moves from the **Network** > **Discovered** tab to the **Network** > **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, click the **Add Devices** button (the Add Device window appears), and click the **Add** button to add the device to the Extreme Management Center 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 Extreme Management Center will push the configuration to the device the next time the device contacts Extreme Management Center.

When Extreme Management Center pushes the configuration to the device, the device **Status** is **ZTP+ Complete**.

Related Information

For information on related topics:

- Sites
- Profiles

- Add Device
- Edit Device
- Devices

ZTP+ Analytics Engine Configuration

Using Extreme Networks' ZTP+ (Zero Touch Provisioning Plus) functionality, you can quickly add new Application Analytics engines to your network and configure them in Extreme Management Center.

Typically, when adding a new engine to the network, a network administrator connects a console cable to the device to access the local console and manually configure the device.

IMPORTANT: Accessing the device via the local console during ZTP+ device configuration using a console cable causes the process to fail. To complete the process after a failure, either configure the device manually or type `unconfigure switch all` and restart the ZTP+ configuration process outlined in this topic.

Stacked systems do not currently support ZTP+ configuration.

In Extreme Management Center, new devices are automatically discovered on the network the moment they are connected. ZTP+ enabled devices send information to Extreme Management Center automatically, including the serial number, the number and speed of the ports, and the firmware version. Once a ZTP+ device is connected, you can add it to Extreme Management Center 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.

Pre-Configuration

Before connecting your devices, you need to pre-configure the following:

- Select the Default Firmware Image Location
- Download XMODs
- Default Device Configuration in Extreme Management Center
- Switch/Engine Settings

Select the Reference Firmware Image Location

You can configure Extreme Management Center 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 Extreme Management Center. Once the firmware image is saved on the Extreme Management Center server, it is available in Extreme Management Center and can be downloaded to the device.

NOTE: Application Analytics and Extreme Access Control engines do not support firmware image downgrades via ZTP+.

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 Extreme Management Center.

To configure the file transfer directory:

1. Access the **Administration** > **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.

   NOTE: ExtremeXOS devices must be running version 21.1 or later.

Once you download the firmware image from ExtremeNetworks.com and save it on the Extreme Management Center server, use the **Firmware** tab in Extreme Management Center to download the image from the Extreme Management Center 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**.

   NOTE: Firmware for an ExtremeXOS device contains a filename extension of .XOS and firmware for an Application Analytics engine contains a filename extension of .BIN.

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

Download XMODs

XMODs are files that work in conjunction with firmware image upgrades to enhance ZTP+ functionality 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.

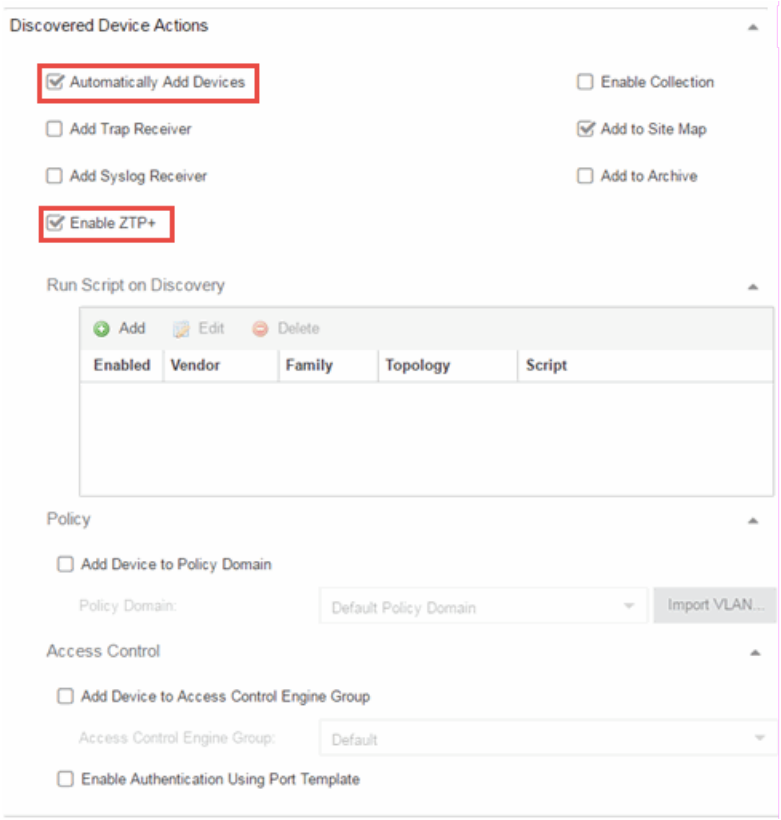
IMPORTANT: ExtremeXOS devices on which version 21.1.1.4 is running require an update to the CloudConnector XMOD for ZTP+ functionality to work properly. Saving the most recent XMOD in the directory specified above updates the device and allows ZTP+ to function as intended.

If multiple CloudConnector XMOD files exist in the same directory on the Extreme Management Center server as the reference image, Extreme Management Center downloads the XMOD file with the higher version number on the device.

Default Device Configuration in Extreme Management Center

Before connecting your devices, you can configure the default settings that Extreme Management Center applies to all devices you add to the network. This is accomplished using the Site tab.

1. Access the **Network** > **Devices** tab in Extreme Management Center.
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 **Enable ZTP+** and **Automatically Add Devices** checkboxes in the Discovered Device Actions section and any other actions you want to occur on your devices discovered in Extreme Management Center.



5. Use the Run Script on Discovery section to automatically run a script on devices being added to the site, if necessary.
6. Select **Add Device to Policy Domain** or **Add Device to Extreme Access Control Engine Group** to automatically add devices being added to the site to a Policy Domain or Extreme Access Control engine group.
7. Enter the **Gateway Address**, **Domain Name**, and **DNS Server** address in the ZTP+ Device Defaults section. Additionally, you can configure the NTP Server address and select the protocols to enable on your devices, if necessary.
8. Add the VLANs that are used on your devices in the ZTP+ VLAN Definition section of the tab by clicking the **Add** button and entering the **Name** and **VID**.
9. Click **Save**.

   The default configuration for this site is complete and any devices you discover with this site selected use this criteria.

Switch/Engine Settings

In order for the switch or engine to communicate to the Extreme Management Center 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 Extreme Management Center server.

Once the Extreme Management Center and ZTP+ device are pre-configured, you can add the site definition to the Extreme Management Center database.

Adding the Device to the Extreme Management Center Database

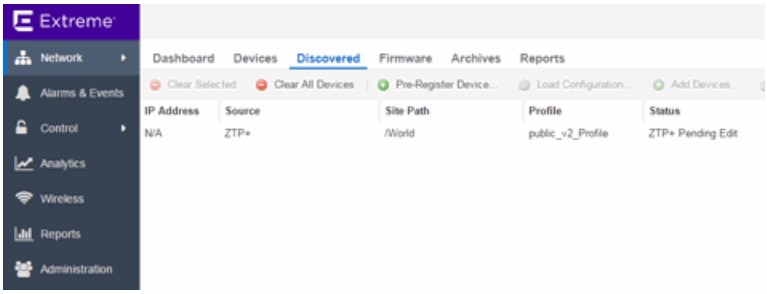
Now that you have set the default criteria for devices added to the World Site and set up the DHCP and DNS servers allowing the device to communicate with the Extreme Management Center database, you can connect the device and add it to Extreme Management Center.

1. Connect the device to your network.

   ZTP+ enabled devices communicate with Extreme Management Center securely via an HTTPS connection and transmits information to Extreme Management Center, including the serial number, firmware version, MAC address, operating system, and port information. Extreme Management Center determines the status of devices and if new updates are available in the Firmware tab and set as Reference images, they are automatically installed.

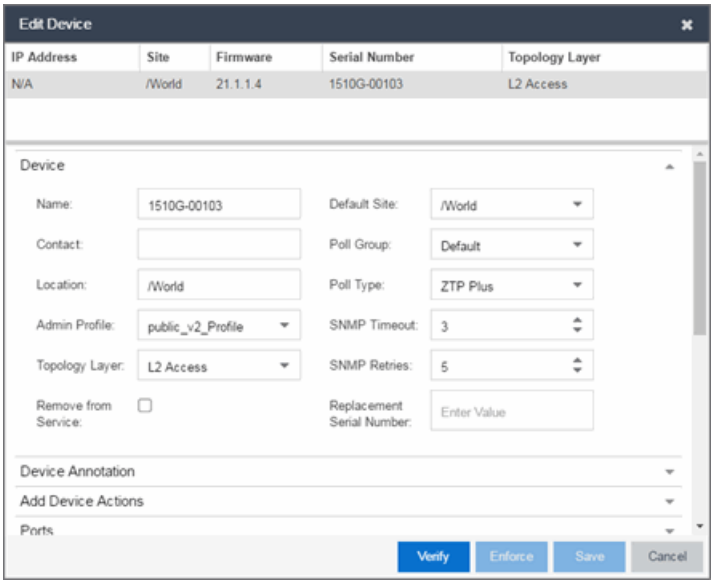
2. Open the **Network** > Discovered tab in Extreme Management Center.

   The device is listed with a **Status** of **ZTP+ Pending Edit**, indicating the device configuration needs to be edited before adding it to the Extreme Management Center server.



3. Select the device and click the **Edit Devices** button.

   The Edit Device window opens.



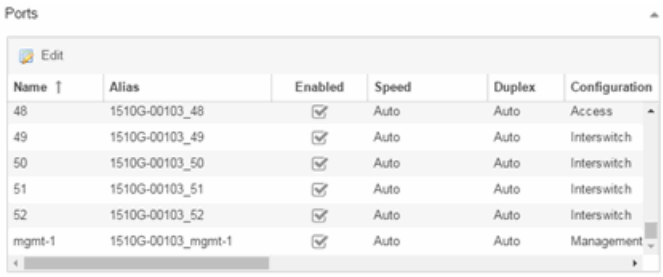
4. Select the **Default Site** for the device.
5. Select the **Poll Group** for the device, which indicates the frequency with which Extreme Management Center checks for new configurations or updates.
6. Select **ZTP Plus** for the **Poll Type**.
7. Open the ZTP+ Device settings section by clicking the heading.
8. Enter an IP address and subnet in the **IP Address/Subnet** field.

   NOTE: Extreme Management Center allows you to enter the IP address in either IPv4 of IPv6 format.

9. Change the **Gateway Address**, if necessary.

10. Open the Ports section of the window by clicking the section heading.

    The Ports section opens, displaying the ports transmitted by the device to Extreme Management Center when connected to the network.



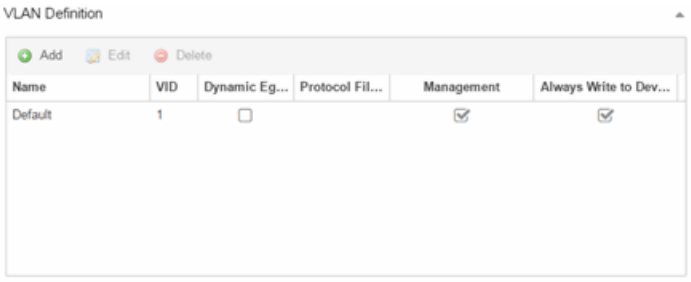
11. Select a port in the list to configure the port Name, Alias, Configuration, or port VLAN ID.

    You can also add and delete ports by clicking 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 Extreme Management Center.
    c. Enter a VLAN ID for the port in the **PVID** field.
    d. Configure the port **Speed** and **Duplex**.

12. Open the ZTP+ VLAN Definition section of the window by clicking the section heading.

    The ZTP+ VLAN definition section opens, containing any VLANs you configured on the **Site** tab.



13. Add any device-specific VLANs to those already included in the list by clicking the **Add** button.
14. Change any incorrect fields in the Device, Device Annotation, or Discovered Device Actions sections.
15. Click **Save** at the bottom of the window.

    The device is added to the Extreme Management Center database and moves from the **Network** > **Discovered** tab to the **Network** > **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, click the **Add Devices** button (the Add Device window appears), and click the **Add** button to add the device to the Extreme Management Center 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 Extreme Management Center will push the configuration to the device the next time the device contacts Extreme Management Center.

When Extreme Management Center pushes the configuration to the device, the device **Status** is **ZTP+ Complete**.

Related Information

For information on related topics:

- Sites
- Profiles

- Add Device
- Edit Device
- Devices

PortView

PortView is an Extreme Management Center component that provides port analysis and troubleshooting information including NetFlow data and Extreme Access Control end-system details, for your network wired and wireless devices.

The primary launch point for PortView is from the Extreme Management Center 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 Extreme Management Center, 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

You must have an Extreme Management Center license (NMS) or Extreme Management Center Advanced license (NMS-ADV) to view PortView reports. (Contact your sales representative for information on obtaining Extreme Management Center licenses.)

In addition, 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. Click an icon to open additional details. End-System — View information about the end-system. End-System Events — View the Extreme Access Control Dashboard end-system events table filtered to display all events for the end-system based on the MAC address. Health Results — Displays risk information for the selected end-system.	Switch must have Extreme Access Control authentication enabled.
Map	Displays the map containing the device to which the end-system is connected.	
Sessions	The tabs within the report contain the following information: Interface History — Historical interface utilization and availability. Client History — Historical statistics for wired or wireless clients. End-System Events — View the Extreme Access Control Dashboard end-system events table filtered to display all events for the end-system based on the MAC address. NetFlow — NetFlow data for the selected port.	Requires active interface statistics collection. Client statistics collection must be enabled. Switch must have Extreme Access Control authentication enabled. The switch must support NetFlow and flow collection must be enabled on the port.

PortView Report	Description	Requirements
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 Extreme Management Center authorization group and the group's assigned capabilities. The following table lists the capabilities required for access to the different PortView reports. For more information on how to configure capabilities and authorization group membership, see the Help topic "How to Configure User Access to Extreme Management Center Applications" located in Extreme Management Center Suite-Wide Tools > Authorization Device Access.

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 > Extreme Access Control > OneView End-Systems Read Access or NetSight OneView > Extreme Access Control > OneView End-Systems Read/Write Access

Launching PortView

You can launch PortView from a variety of locations in Extreme Management Center, as well as the legacy java applications Console and NAC Manager. By default, you can have five active PortView searches displayed in Extreme Management Center at one time. You can change this display limit in the **Maximum PortViews Displayable** field in Management Center Options (Administration > Options > Management Center > 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 Extreme Management Center

Extreme Management Center Search Tab

The primary launch point for PortView is from Extreme Management Center Search. The Search page provides a search field where you can enter a MAC address, IP address, host name, AP serial number, or Extreme Access Control custom field information to begin searching. Depending on the type of item for which you are searching, the search results return one or more PortView tabs, with information pertaining to your search item. You can right-click on the different devices in the topology results to launch additional reports.

1. Open the **Search** tab.
2. Enter a MAC address, IP address, host name, AP serial number, or Identity and Access custom field information, and press **Enter** to begin the search. You can copy the IP or MAC address from another source and enter it into the **Search** field. For example, you can copy an end-system MAC address from the **Control** tab End-Systems view, and then paste the MAC address into the search field and press **Enter**.
3. Depending on the type of item for which you are searching, the secondary navigation bar displays one or more PortView tabs, with information pertaining to your search item, similar to the search results shown below.

Extreme Management Center Interface Summary FlexView

Use the following steps to launch PortView from an Extreme Management Center Interface Summary FlexView.

1. On the **Network** tab, click on the device Name link to open the Interface Summary FlexView.
2. In the Interface Summary, click on 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 Extreme Access Control reports from NAC Manager using either of the following two methods:

- In the **End-Systems** tab, right-click on an end-system in the table and select **PortView** from the menu.
- On the **Control** tab's End-Systems view, right-click the entry with the desired switch port and select **PortView** from the menu.

AP Wireless Real Capture

Real Capture allows real-time collection of Access Point (AP) wireless traffic for troubleshooting and problem resolution. Real Capture collects traces on the AP wireless interface and transmits them to Wireshark running on a local Windows client. It allows Wireshark to capture RF/wireless traffic as if it were running directly on the AP, providing visibility into network connectivity and performance issues. All Wireshark features are supported, including filters and I/O graphs.

NOTE: APs must be running firmware version 8.x or later. The AP2600 series of Access Points does not support the Real Capture feature.

Real Capture can be enabled for each AP individually from PortView in the Extreme Management Center. 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.

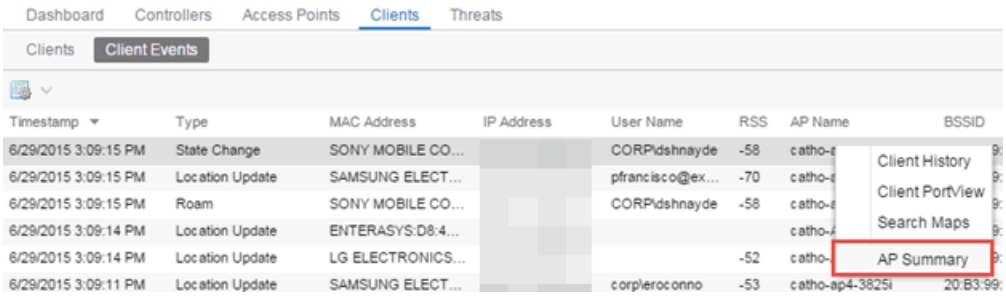
In addition to capturing network traffic for analysis in Wireshark, the AP also collects RF information. The RADIOTAP header format delivers RF information. You must use Wireshark 1.6 or later to read the full RADIOTAP header information. For troubleshooting features like TxBF/STBC, you can enable capturing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

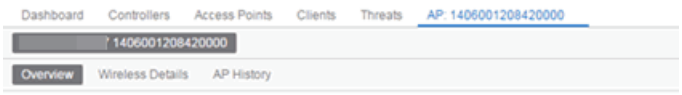
Configure and Use Real Capture

Use the following steps to configure and use the Real Capture feature.

1. Launch Extreme Management Center.
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.

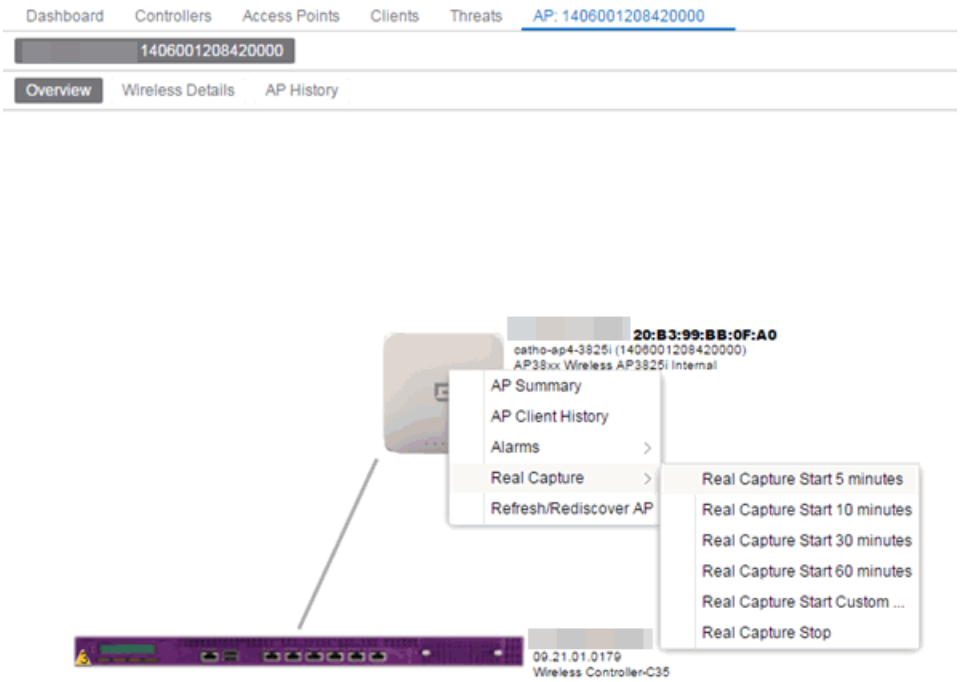


   b. The AP PortView opens.

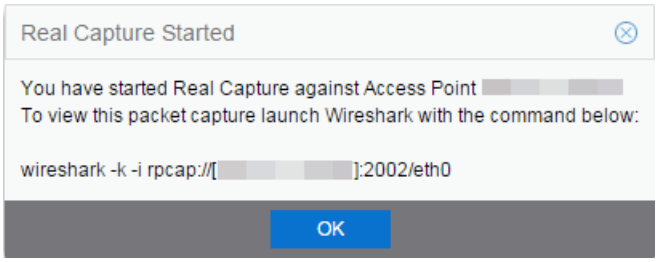


NOTE: You can also launch PortView for the AP using the **Search** tab. Open the **Search** tab, enter the search criteria (MAC, IP, hostname, or AP serial number) and press **Enter** to display the AP PortView.

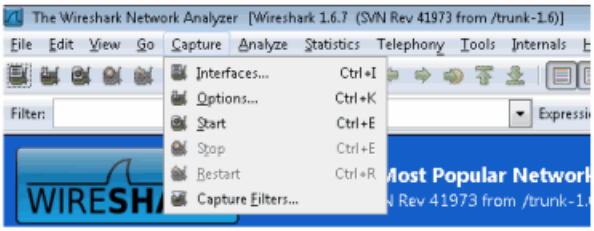
3. Right-click on the AP in the PortView topology display and select **Real Capture** > **Real Capture Start xx minutes**. Select the desired amount of time to run the capture or create a custom capture duration value. If you need to, you can stop the Real Capture by selecting **Real Capture Stop**.



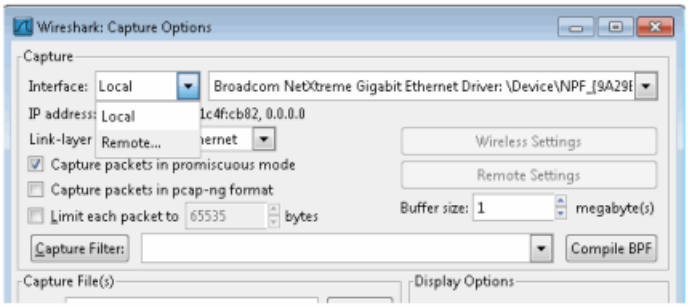
4. A message appears to inform you Real Capture has started, and provides a CLI command you can use on a client on which Wireshark is installed, to launch Wireshark against the AP and view the captured traffic.



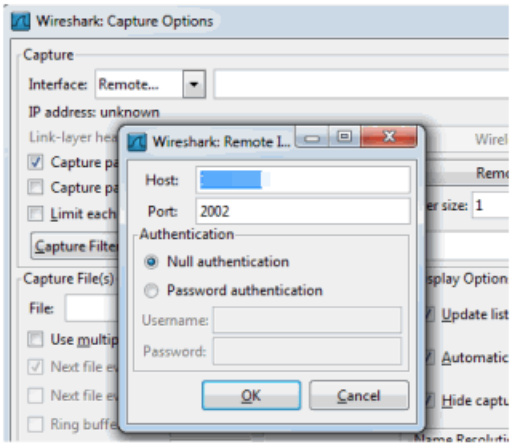
5. You can also access the captured traffic in Wireshark using the following steps:
   a. In Wireshark, select **Capture** > **Options** from the menu bar.



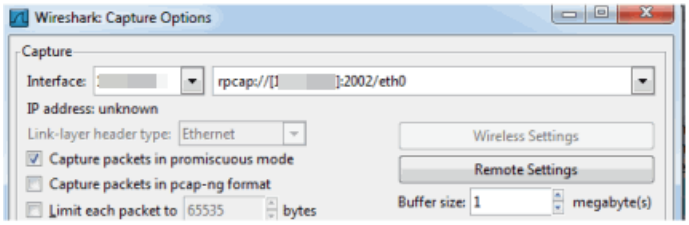
b. In the Capture Options window, set the **Interface** value to **Remote**.



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**. Click **OK**.



d. Wireshark adds the command information to the Capture options.

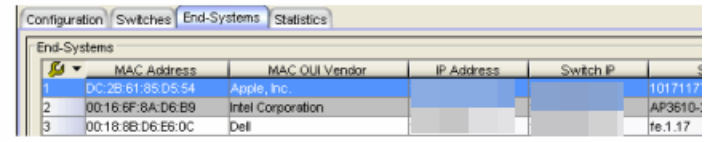


e. Click **OK** in the Capture Options window to begin viewing the captured traffic in Wireshark. When you have the data you need, you can stop the capture and save it to a file for further diagnosis and troubleshooting.

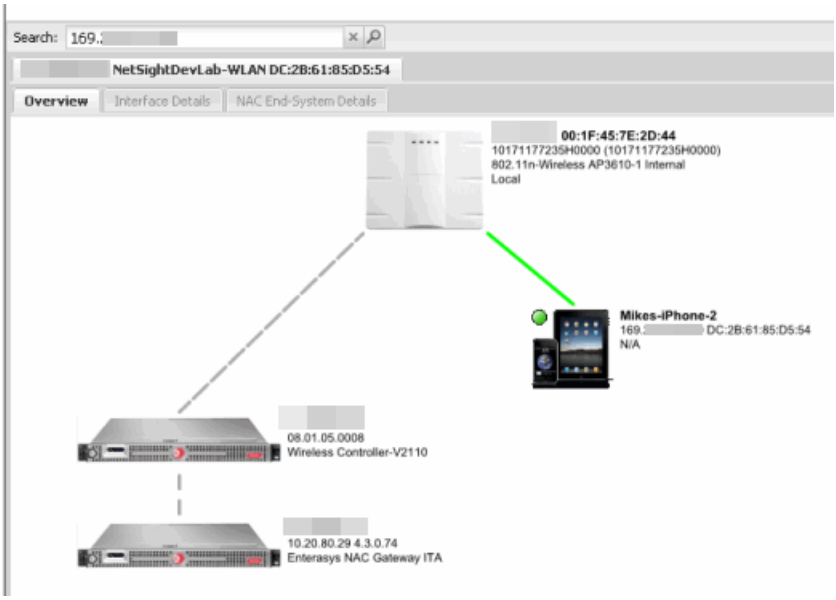
Real Capture Example

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

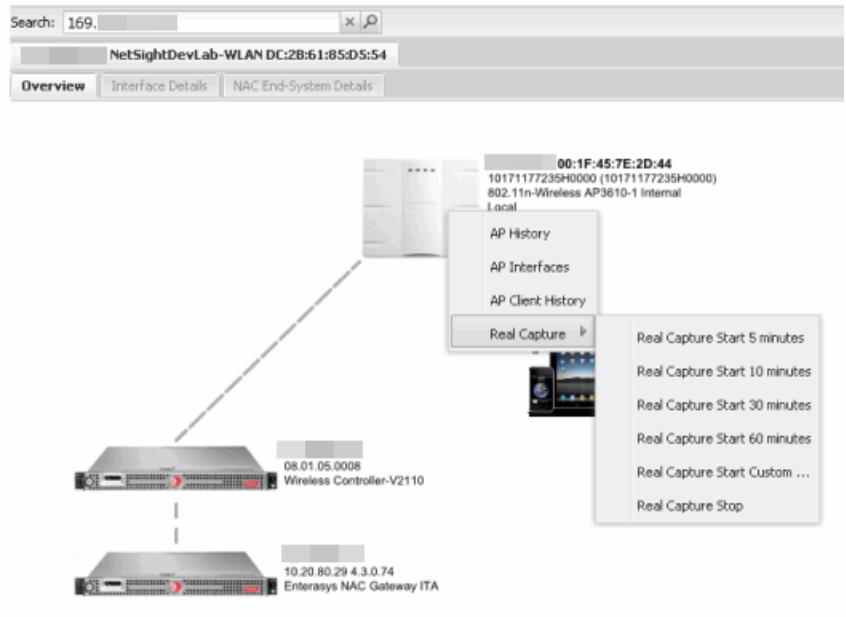
The problem starts when an end-system in NAC Manager is not able to obtain an IP address.



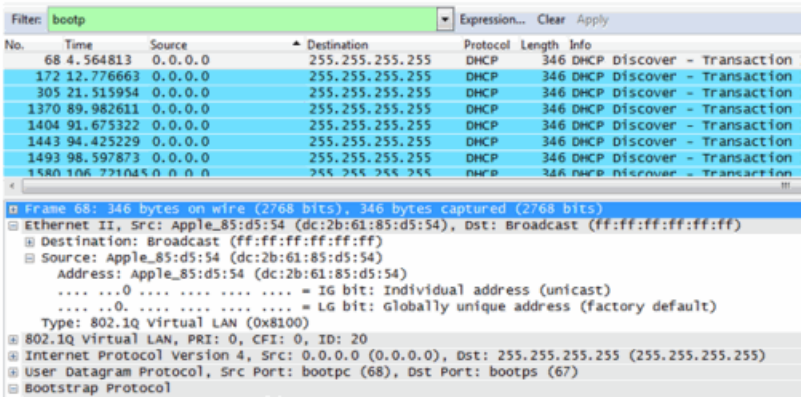
A search is performed on the 169.x.x.x IP address.



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.



How to Use 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. Once 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 Extreme Management Center OneView > Access OneView and NetSight OneView > Access OneView Administration capabilities.

This Help topic provides the following information:

Creating a Report

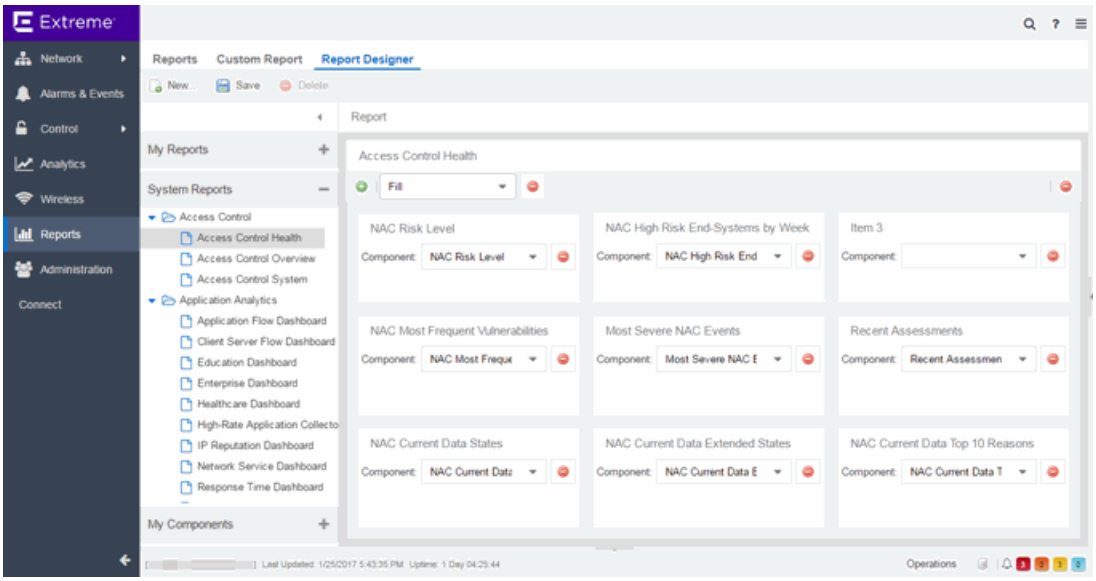
There are two ways to create a report. You can create a report by customizing an existing dashboard report (system report) or by creating a new report based on a selection of individual components.

Customize 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 Extreme Management Center where that report is used.

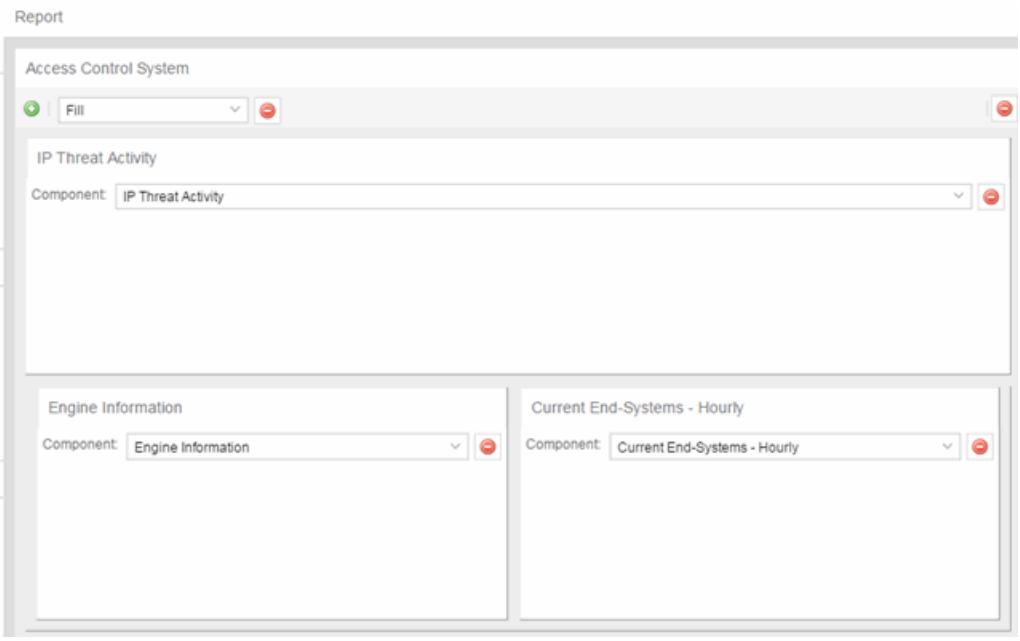
For example, you want to delete some of the dashboard panels and change some of the dashboard components in the Extreme Access Control System report.

1. Select the **Reports** tab in Extreme Management Center and then select the **Report Designer**.
2. Select the system report you want to customize in the System Reports section. In the example below, Extreme Access Control > Extreme Access Control System report is selected. (Use the scroll bar to view the complete list of available reports.) The report becomes available to edit in the right panel.



3. Change the report:
    a. Click the **Delete** button ( ) to delete a panel.
    b. Use the **Component** drop-down menu to select a new component for a panel.
    c. Add a blank panel, if desired.

    In the example below, the Top Switches by End-Systems panel has been deleted, and the Appliance Load panel is being changed to the IP Thread Activity component.



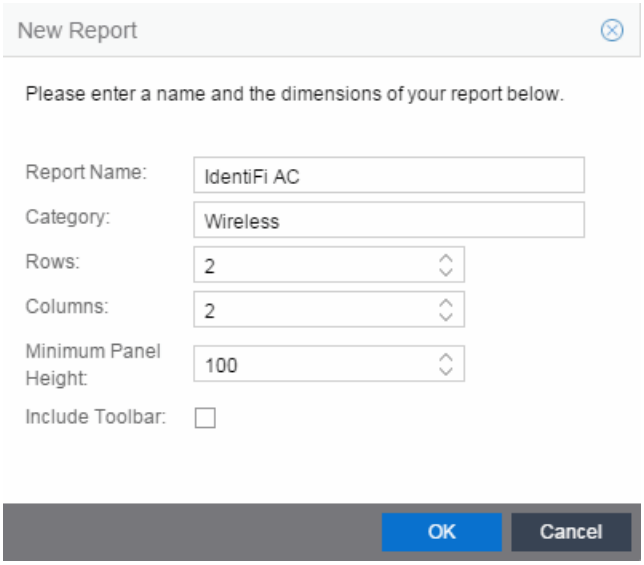
4. Once you have finished making changes to the report, click the **Save** button. The report is populated with data and displayed in a new tab as a way to preview the report. The name of the customized report is added to the My Reports section.

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.

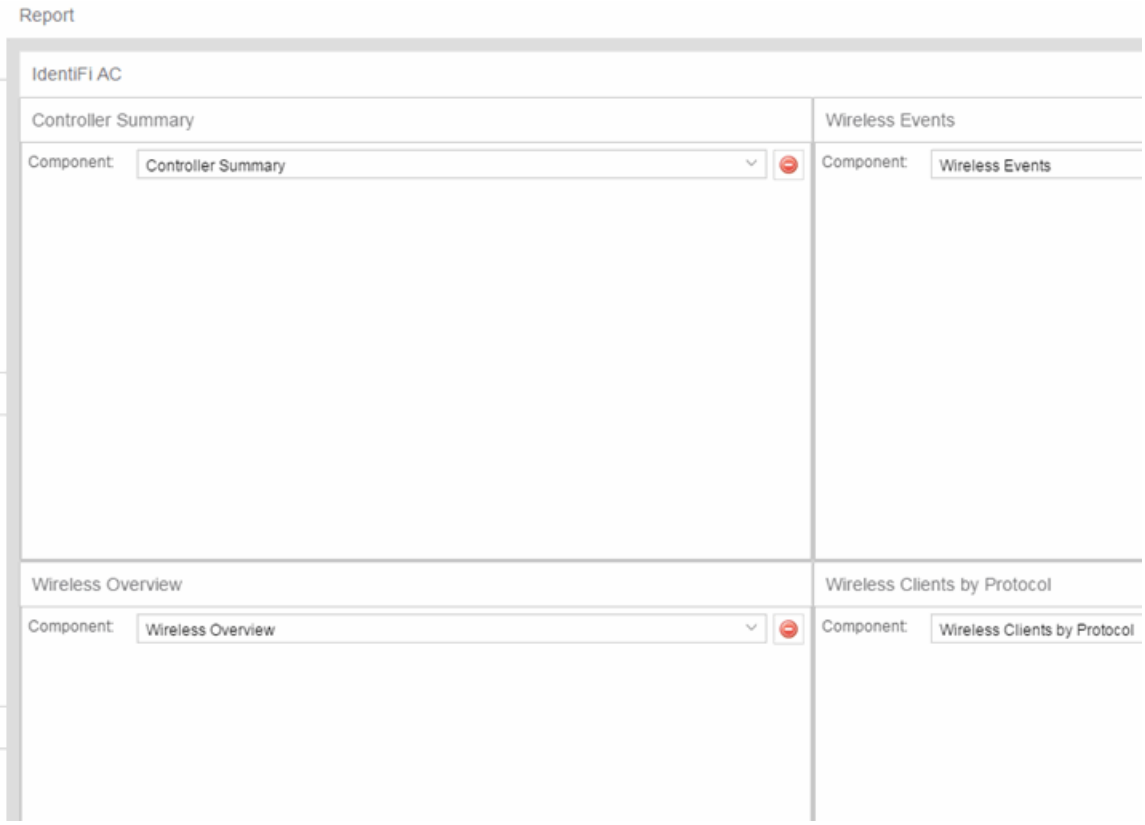
Create a New Report

Use the following steps to create a new report. The new report is added to the **Reports** tab.

1. Select the **Reports** tab and then select the Report Designer.
2. Click on 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. Enter a **Category** for the report. This allows you to group your report within an existing report category (in the **Reports** tab) or create a new category.
5. Select the number of rows (maximum 5) and columns (maximum 3) for your report. This is determined by the number of panels you want to include in your report. For example, if you want six panels, then you can specify two rows with three columns each.
6. Set a minimum panel height (in pixels) for the report. The best panel height depends on the number of rows in your report. For example, if you create a report with five rows (the maximum) and set the minimum panel height to 100, the report panels are small and the data may be difficult to view. But, if you set the minimum panel height to 400, the report panels are larger and a scroll bar is added to make the data easier to view.
7. Click **OK**. The report is created and listed under the appropriate category in the My Reports section, and displayed in the right panel.
8. For each panel, use the drop-down menu to select the component that determines the information displayed in the dashboard.



9. Click the **Save** button. The report populates with data and displays in a new tab as a way to preview the report.

The new report is now listed in the **Reports** tab under the appropriate category.

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.

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 menu to change a component in a panel, or click the **Delete** button to delete a panel.
4. Click 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.

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 Application Analytics 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 menu in the Applications Browser section when you customize a system report or create a new report.

Related Information

For information on related topics:

- Reports

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. Once 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 Extreme Management Center OneView > Access OneView and NetSight OneView > Access OneView Administration capabilities.

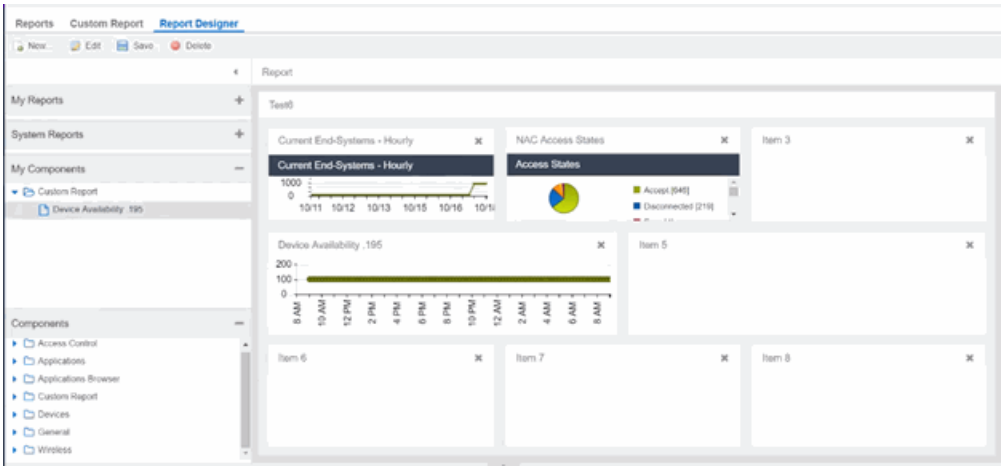
Creating a New Report

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. Click on 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 menu 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 menu.
7. Click the **Include Toolbar** box to add the tool bar to your dashboard.
8. Click 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. Once in place, the components are a live preview of the data.



11. Click **Save**. The new report is now listed in the **Reports** tab under the appropriate category.

Related Information

- ExtremeAnalyticstab

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. Once a report is created, it is available from the report catalog in the **Reports** tab.

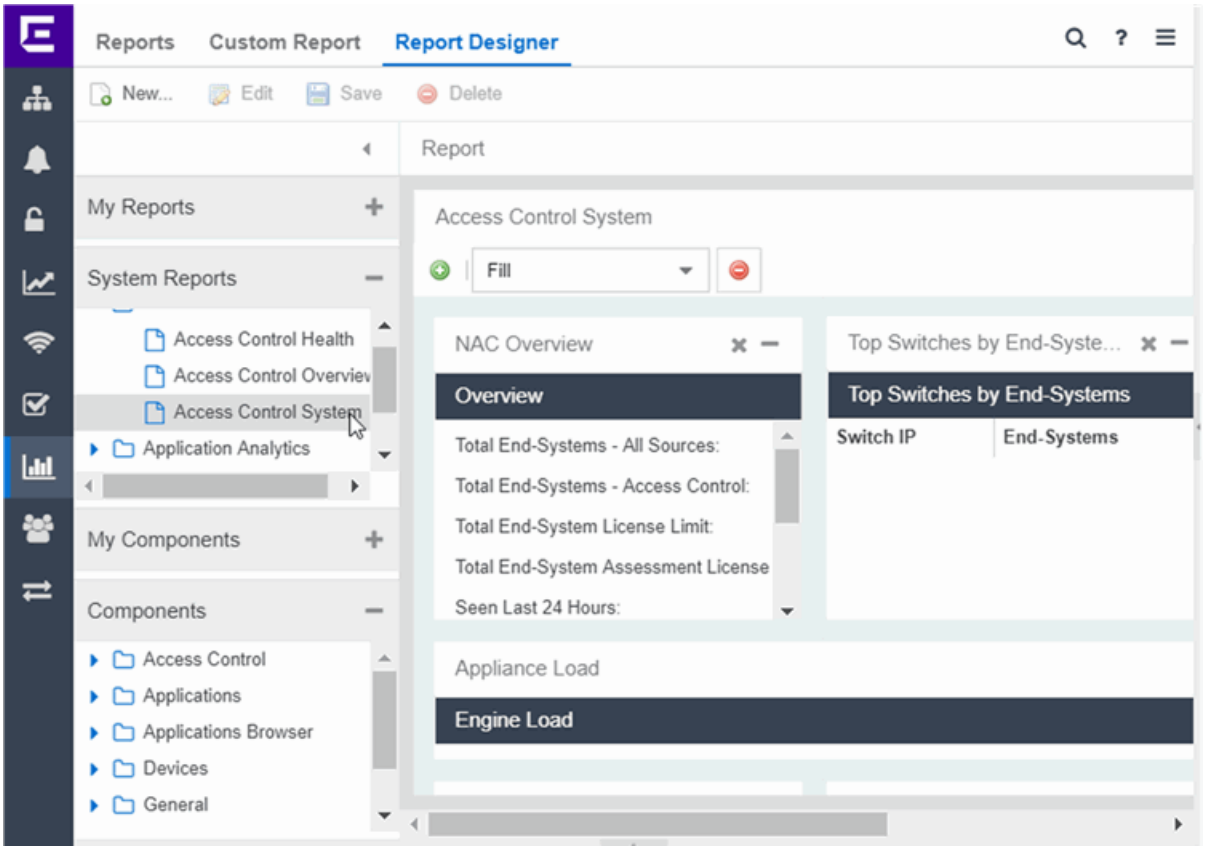
The Report Designer can be accessed from the Reports tab. In order to use the Report Designer, you must be a member of an authorization group that is assigned the Extreme Management Center OneView > Access OneView and NetSight OneView > Access OneView Administration capabilities.

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 Extreme Management Center 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 Extreme Access Control System report.

1. Select the Reports tab in Extreme Management Center and then select the Report Designer.
2. Select the system report you want to customize in the System Reports section. In the example below, Extreme Access Control > Extreme Access Control System report is selected. (Use the scroll bar to view the complete list of available reports.) The report becomes available to edit in the right panel.



3. Change the report:
    a. Drag and drop the components that you want displayed in the dashboard.
    b. Once in place, the components are a live preview of the data.
4. Once you have finished making changes to the report, click 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

Reports Catalog

Extreme Management CenterReports 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 ℹ at the top-right of the Extreme Management Center 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:

- Extreme Access Control — Provides an overview of end-system connection information. You can also see these reports and others on the Control tab.
- Extreme Access Control Health — Provides reports on end-system assessment and state information. In the Risk Level pie chart, click on a pie section to open a filtered end-system grid for more detailed information about end-systems at that risk level.
- Extreme Access Control System — Provides a report of the top ten end-systems by engine.
- Application Analytics — These reports provide visibility into the applications on your network and who's using those applications.
- Console — The NMS Dashboard report provides summary NMS data including top 5 switch, interface, and host statistics as well as important Wireless data. Host data is collected from network devices that support the Host Resource MIB, such as Extreme Management Center engines, Linux systems, and Windows PCs. For more information, click the Info button (ℹ) at the top-right of the Reports tab.
- Data Center Manager — The DCM reports provide an overview of all virtual machines on the network broken down into VM distribution per Identity and Access 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, down devices, inventory summary (including archive distribution, devices backed up, database properties, scheduled events, asset tracking information, and the ability to track the changes made to a specific device), top devices by IPv6 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).
- Interface — These reports present information on your top interfaces by active flows, bandwidth, bandwidth summary, least availability, POE usage, and utilization.
- OpenScape — The OpenScape LIA (Location and Identity Assurance) report provides an overview of all OpenScape phones on the network categorized by phone count, phone type, phone software version, and phone distribution by access switch, as well as a list of phone information by MAC address.
- Policy — Provides a policy rule hit summary report showing top services and roles by rule hits.
- Server — These reports provide data on the Extreme Management Center 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.
- 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. 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

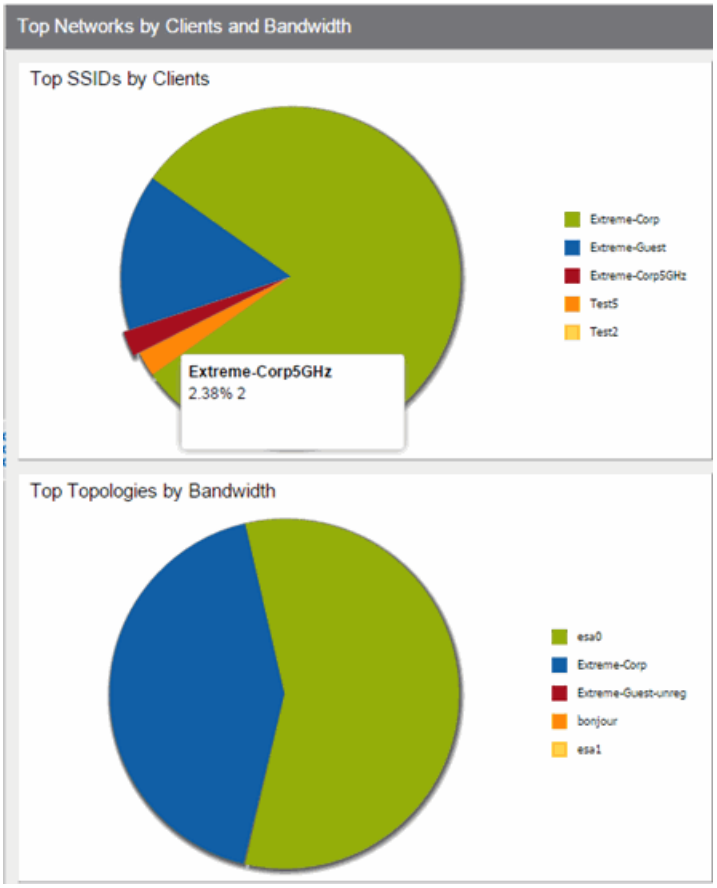
Reports Features

Extreme Management Center Reports provide historical and real-time reporting, offering high-level network summary information as well as detailed reports and drill-downs.

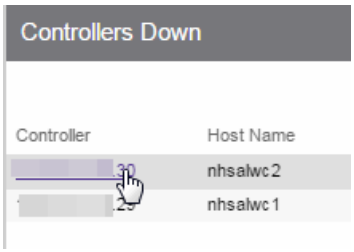
Reports Features

Extreme Management Center reports include the following features (depending on the report selected):

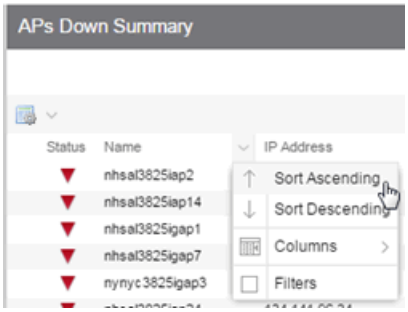
- Hover Over for Info — Hover over a pie section to display the name of the segment, the percentage represented by the segment and the number of elements. for some reports, clicking on a pie section opens a filtered end-systems grid for more detailed information.



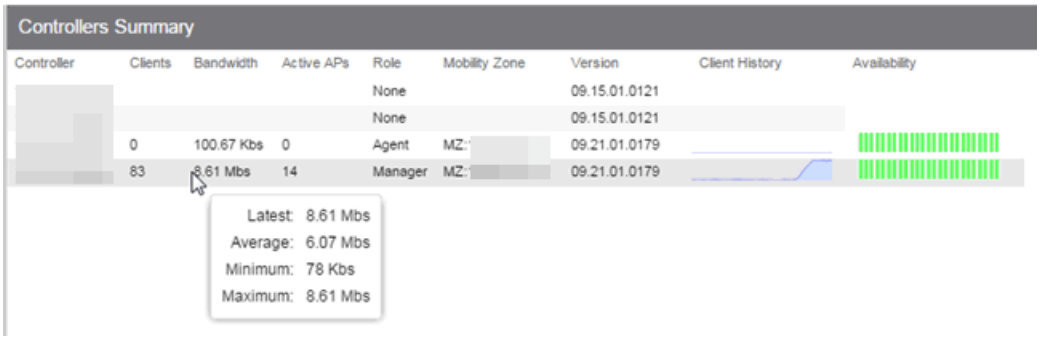
- Drill-down for Details — Link to summary reports containing more detailed information. For example, in the Controller Summary report, clicking on a controller shows a detailed report for that controller over time.



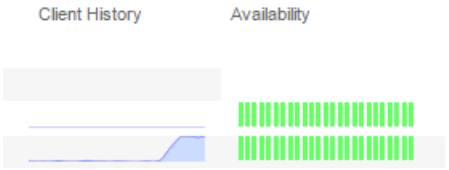
- Interactive Tables — Manipulate table data in several ways to customize the view for your own needs:
  - Click on the column headings to perform an ascending or descending sort on the column data.
  - Hide or display different columns by clicking on a column heading drop-down arrow and selecting the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

Restoring an Extreme Management Center® Database Using the CLI

Use the instructions in this topic to restore an Extreme Management Center 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 Extreme Management Center database backup:

1. Ensure you are running the same version of Extreme Management Center used when creating the database backup on the Extreme Management Center server.
2. Log into the system shell (via the local console or SSH) on the Extreme Management Center server as root on a Linux operating system or open a CMD prompt by selecting Run as administrator on a Windows operating system.
3. Navigate to the scripts directory:
   - On a Windows server, enter `cd "<install directory>"\scripts`.
   - On a Linux server, enter `cd <install directory>/scripts`.
4. Run the mysqlback_restore script:
   - On a Windows server, enter `mysqlbackup_restore.cmd "<full backup directory structure configured on Backup/Restore tab, including path>"`

     (e.g. `mysqlbackup_restore.cmd "C:\Program Files\Extreme Networks\NetSight\backup\netsight_03272017.sql"`).

   - On a Linux server, enter `./mysqlbackup_restore.sh <full backup directory structure configured on Backup/Restore tab, including path>`

     (e.g. `./mysqlbackup_restore.sh /usr/local/Extreme_Networks/NetSight/backup/netsight_03272017.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

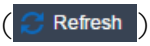
In order to perform the restore configuration operation, you must be a member of an authorization group with the following capabilities.

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. Extreme Management Center uses the default tftpboot\firmware\images directory for storing your firmware.
2. In the left-panel Firmware folder, click the **Refresh** icon (

). Extreme Management Center 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 Extreme Management Center.

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.

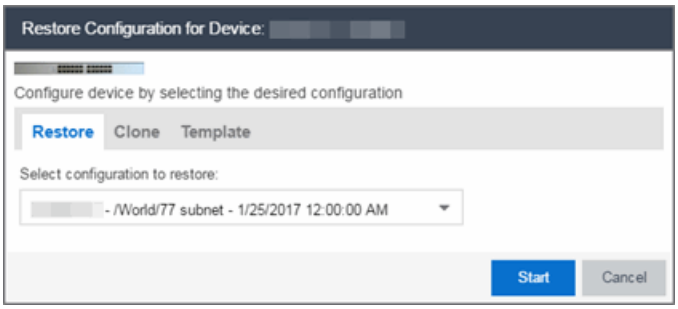
Cloning a device configuration is useful when you want to use the exact same configuration on another device. If you are cloning a device configuration, you must have an existing configuration for that device archived.

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.

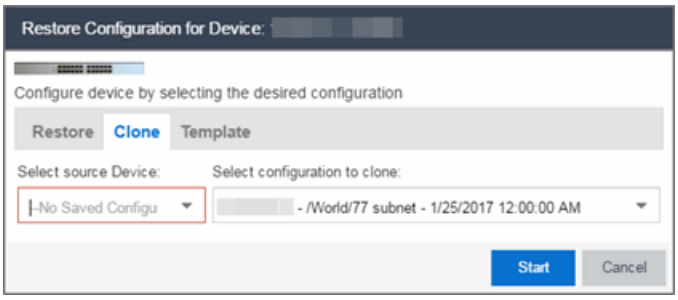
Cloning a Device Configuration

When cloning a device configuration, use an existing configuration of a network device archived in Inventory Manager. 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 Extreme Management Center. On the **Network** > **Devices** tab, right-click on the active device and select **Configuration/Firmware > Restore Configuration**. The Restore Configuration window opens.



2. Select the **Clone** tab.

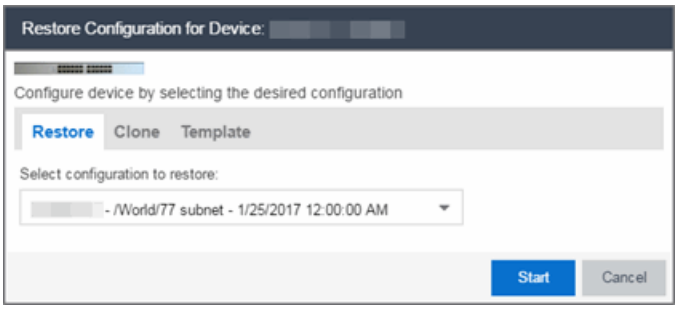


3. If desired, select a new version of firmware to download to the device. (You must add the new firmware version to Inventory Manager. For more information; see "Device Firmware".)
4. Select the Device option as the Configuration Source.
5. Select the source device for the configuration. The selected 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. Click **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 in Inventory Manager as the source configuration for a device.

1. Launch Extreme Management Center. On the **Network** > **Devices** tab, right-click on the active device and select **Configuration/Firmware > Restore Configuration**. The Restore Configuration window opens.



2. If desired, select a new version of firmware to download on the device. (You must add the new firmware version to Inventory Manager, see Device Firmware.)
3. Select the Template option as the Configuration Source.
4. Select the appropriate template from the **Template** drop-down menu and enter the required variables.
5. Select the Profile for the new device.
6. Click **Start**. First, the firmware is updated (if that option is selected), then, the configuration is loaded, the device is restarted, and the new IP address is added to Extreme Management Center.

Related Information

For information on related topics:

- Network Tab
- New Device Configuration in Extreme Management Center

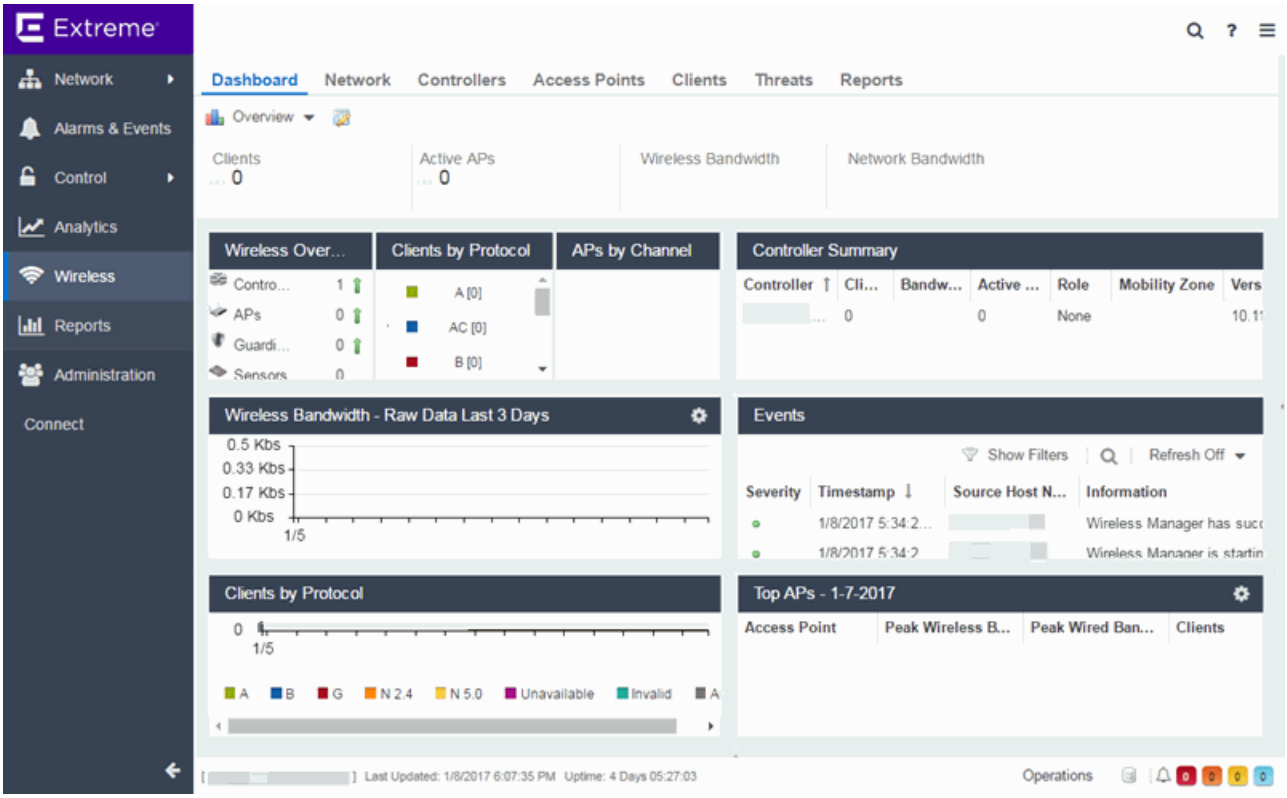
Configuring Enhanced Netflow for Extreme Analytics and Extreme Wireless Controller Version 10.21

When adding a Wireless Controller as a flow source in Extreme Management Center, 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.

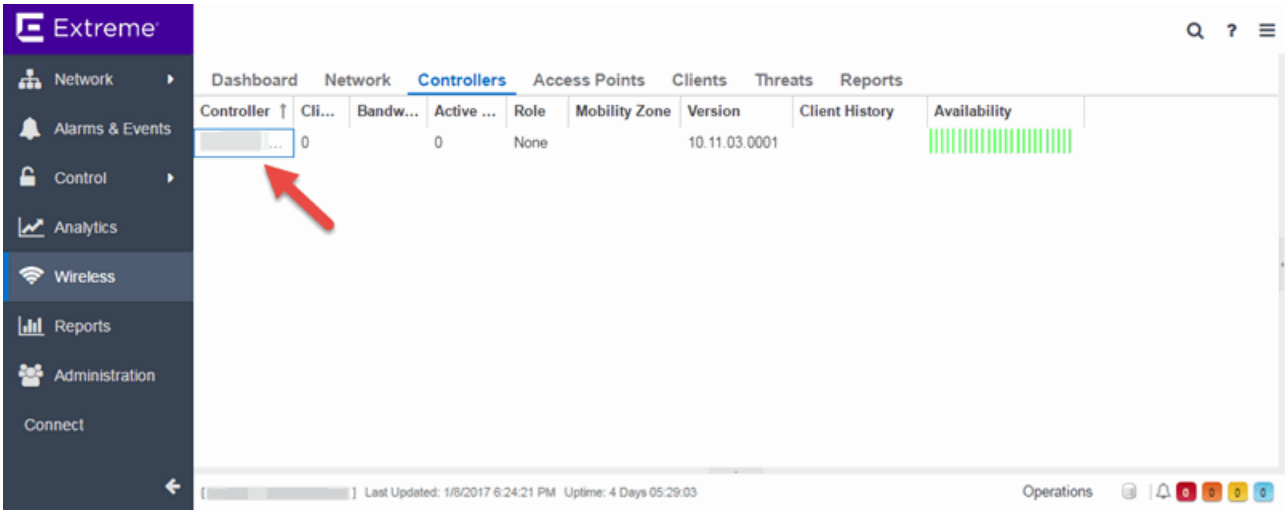
NOTE: Wireless Controllers on which a firmware version lower than 10.21 is installed still require the mirror port be configured.

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

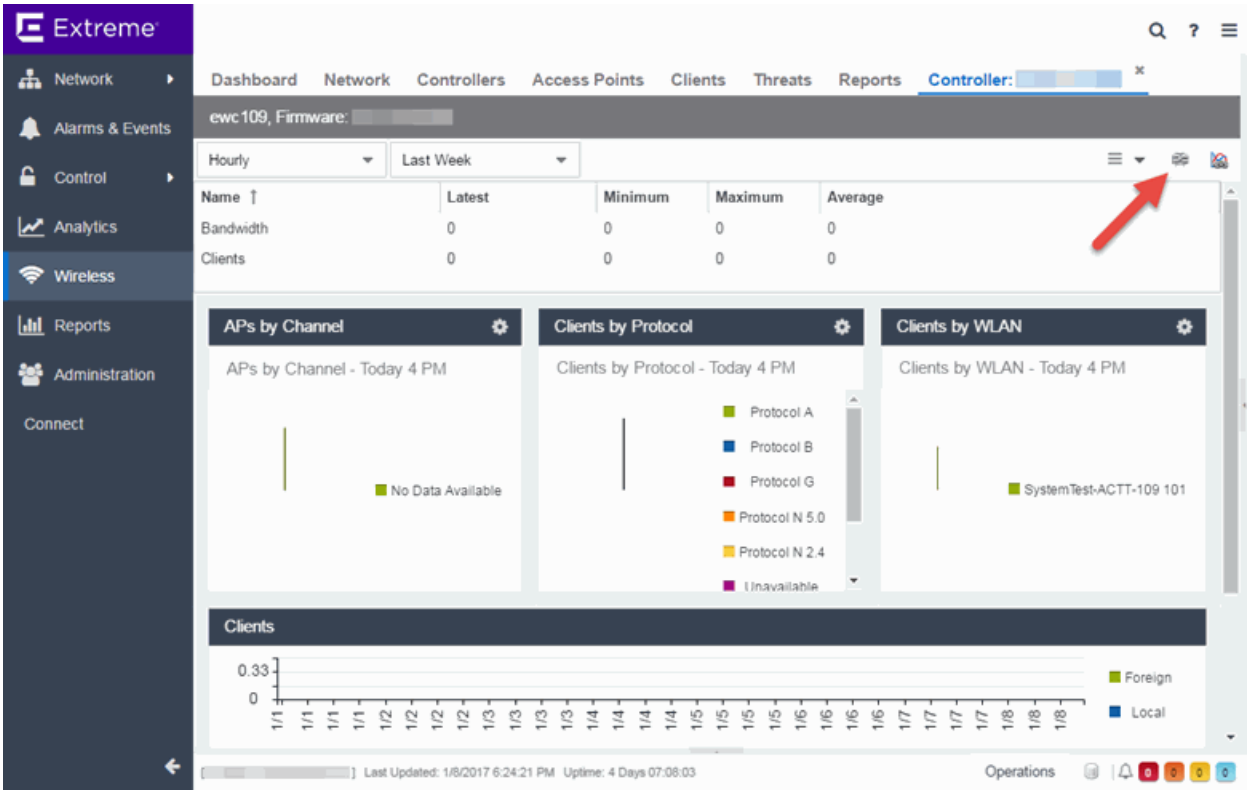
1. Access the **Wireless** tab in Extreme Management Center.
   The Wireless tab opens.



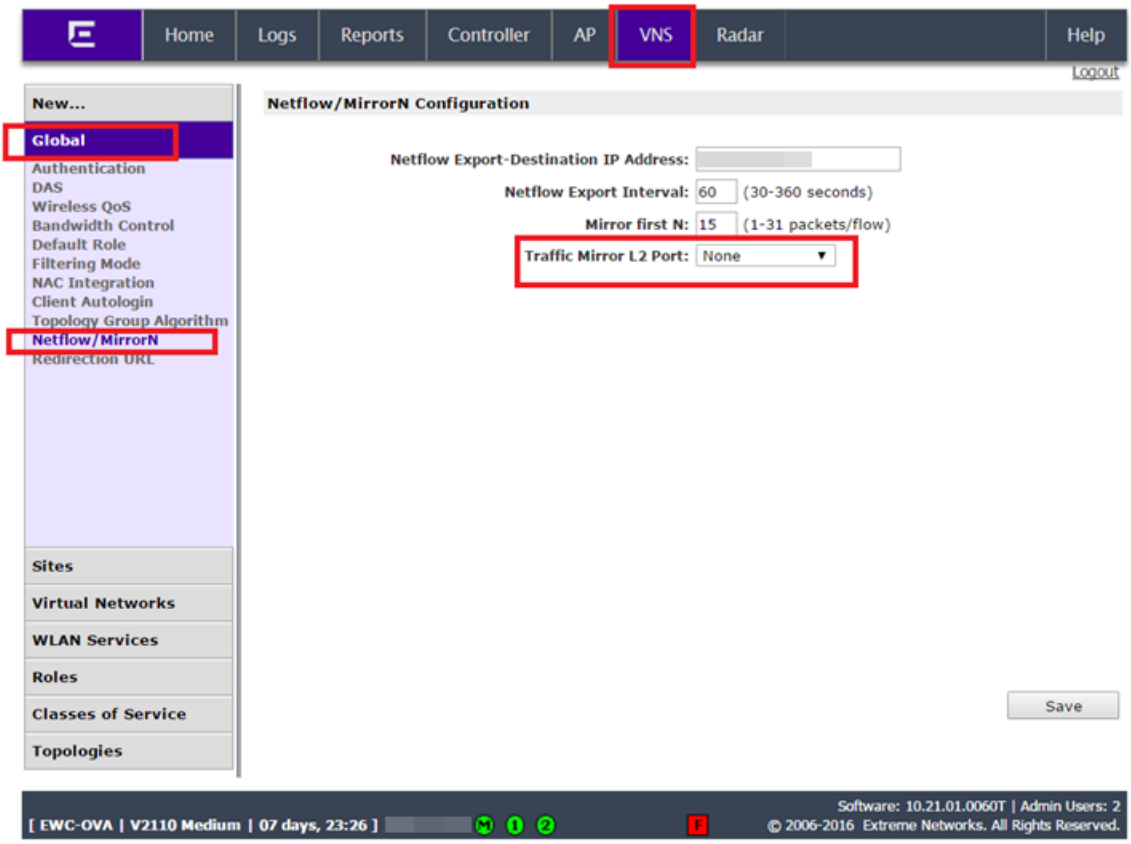
2. Select the **Controllers** tab.
   The Controllers tab opens.



3. Click the **IP address** for the controller, located in the **Controller** column.
   The Wireless Controller Summary page opens.



4. Click the **WebView** icon ( ) at the top right of the Wireless Controller Summary page.
   The WebView opens for the controller.
5. Click the **VNS** tab.
   The **VNS** tab opens.

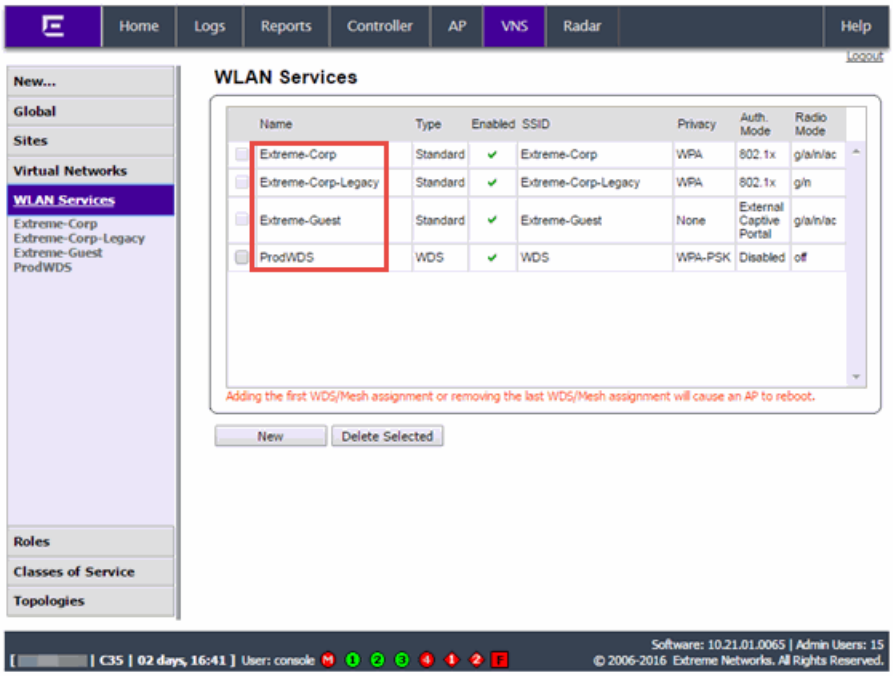


6. Select **Netflow/MirrorN** from the left-panel.
   The Netflow/MirrorN Configuration page opens.
7. Select **None** from the **Traffic Mirror L2 Port** drop-down menu.
8. Click the **Save** button.

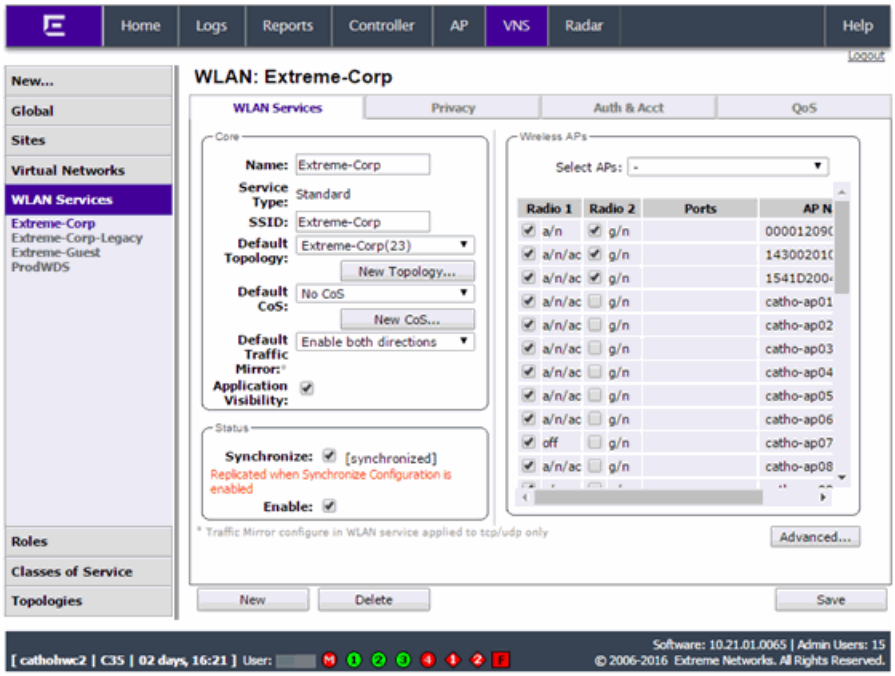
NOTE: The Mirror Port in the Wireless Control Flow Sources section of the **Analytics** > **Configuration** > **Configuration** tab is not available once the **Traffic Mirror L2 Port** is disabled.

---

9. Select **WLAN Services** from the left-panel.
   The WLAN Services page opens.

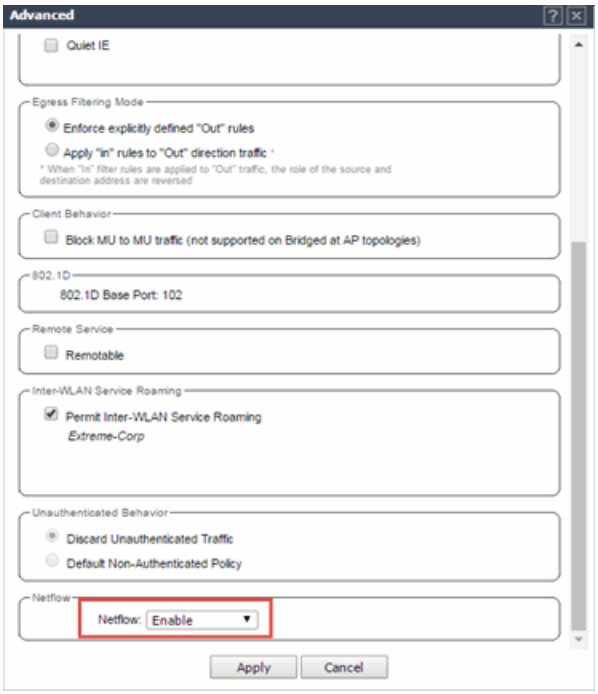


10. Click a wireless LAN in the table.
    The WLAN page opens for the selected wireless LAN.



11. Click the **Advanced** button.
    The **Advanced** window opens.

12. Scroll to the bottom of the window and ensure the **Netflow** drop-down menu is set to **Enable**.



13. Click the **Apply** button.

The wireless controller is now configured.

NOTE: **Rx Packets** and **Rx Bytes** may 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 may 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 Extreme Management Center

This chapter describes how to use the Identity Management — Configuration script on a Summit series or Black Diamond series switch to send events to

Extreme Management Center.

In order to run the Identity Management — Configuration script on a device, you must be a member of an authorization group assigned the Extreme Management Center 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 Extreme Management Center.
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 > Extreme Access Control menu. The Run Script window opens.
4. On the **Device Selection** tab, the selected device is automatically included. Use the arrows to add additional devices or remove devices and to control the order of the selected devices.
5. Click **Next**.
6. On the **Overview** tab of the **Device Settings** tab, set the configuration properties for the script. If desired, click 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 Extreme Management Center server IP.
        - Enter the IP address of the Extreme Access Control engine if using the Extreme Networks ExtremeControl solution.
    - Target Server Type — Selecting netsight monitors the IP, username, and port of the user accessing the device. Users with the Extreme Networks ExtremeControl solution can select nac, which provides you with the ability to run Kerberos authentication (if enabled) on the device.

      NOTE: In order to give elevated access to users when using the Kerberos authentication type on the device, the Target Server Type must be **nac** to allow the Access Control engine to learn the Kerberos traffic.

- Target Server Username — The username of the user to which the web service request is made.
- Target Server Password — The password of the user to which the web service request is made.
- Target Server HTTPs Port — The port that the Extreme Management Center server or Access Control engine uses for HTTPS communication. The default port is 8443, but if the port was changed when configuring the Extreme Management Center 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 "Creating Script Tasks").
   - 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 "Creating Script Tasks").

8. Click **Next**. On the Verify Run Script tab, verify your script selections, and then click **Next**.
9. Click **Next**.
10. On the Results tab, you see the results of the script including any errors.
11. Click **Close**.

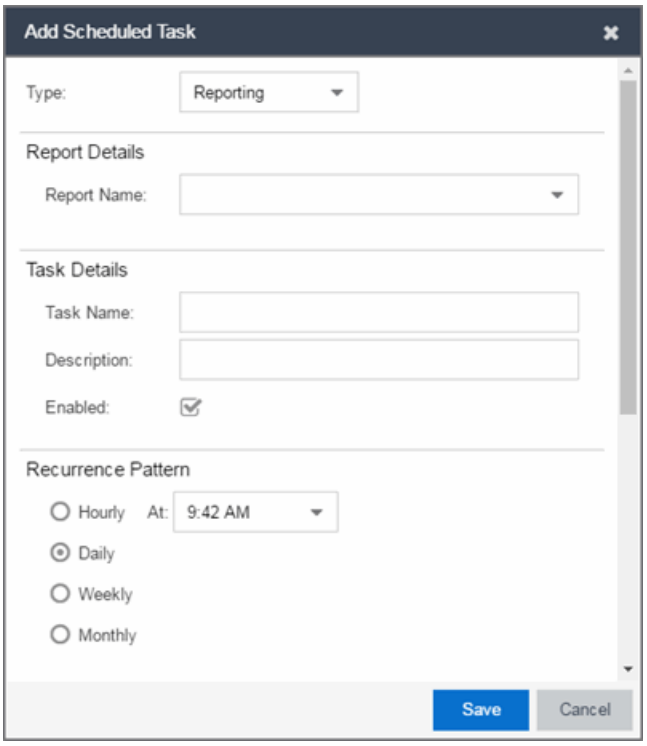
How to Schedule a Task

The **Scheduled Task** tab allows you to configure Extreme Management Center to automatically perform the following tasks:

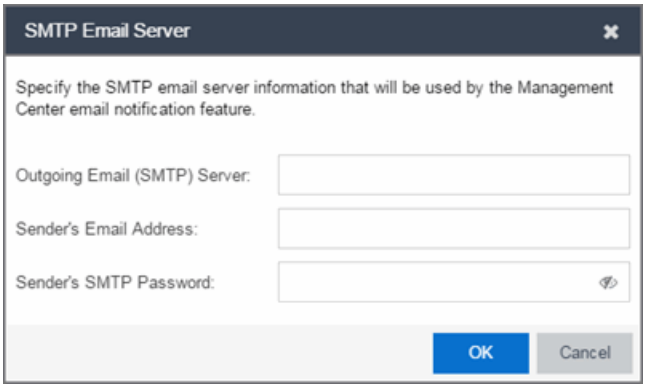
- Generate a subset of available reports in PDF format
- Run a script or workflow
- Email information to Extreme Networks Support
- Discover newly added devices

To create a new task:

1. Launch Extreme Management Center.
2. Select the Tasks tab and select the **Scheduled Tasks** tab.
3. Click 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 click **OK**.
5. Select the type of task from the **Type** drop-down menu in the Add Scheduled Task window:
    - **Reporting** — Emails a report you select (created on the Report Designer tab) on a scheduled basis.

- **Saved Task** — Runs a task saved on the Saved Tasks tab and sends an email 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.
- **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.

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 menu, 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 the email address or list of email addresses (separated by semicolons) where you want the generated PDF reports sent.
12. Enter the subject line and body text for the email, if desired.
13. Click **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. Clicking the **Disable** button causes a task not to run without deleting it from the Scheduled Tasks table.

Click the **Run** button to run the scheduled task immediately, if desired.

Click 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 workflows in a 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 menu 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. Click **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. Click **Update** to save the new variable to the table.
10. Click **Save** to save the new variabe to the site.

Related Information

For information on related topics:

- Sites
- Scripts
- Workflows
- Northbound Interface

How to Create Scripts

This chapter describes the scripting functionality built into Extreme Management Center and describes how to use Extreme Management Center to

create scripts.

Extreme Management Center Scripts Overview

Extreme Management Center scripts are files containing CLI commands, control structures, and data manipulation functions. Extreme Management Center 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.

Extreme Management Center allows you to create Extreme Management Center 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.

Extreme Management Center scripts are similar to ExtremeXOS scripts in that they are collections of ExtremeXOS CLI commands and control structures. Extreme Management Center scripts add some additional commands specific to Extreme Management Center.

In general, Extreme Management Center scripts support syntax and constructs from the following sources:

- ExtremeXOS CLI commands — ExtremeXOS CLI commands in an Extreme Management Center script are sent to the device or port and the response can be used by the script. Abbreviated ExtremeXOS commands do not work unless you prefix the shortened command with CLI.

  For example, to abbreviate `show vlan`, type `CLI sh vlan`.
- ExtremeXOS CLI scripts — Control structures such as IF..ELSE and DO..WHILE can be used in Extreme Management Center scripts. See "CLI Scripting" in the *ExtremeXOS User Guide* for more information on ExtremeXOS script functionality and syntax.
- Python scripting language — Create scripts using the python programming language.
- TCL scripting language version 8.1 — For general information about the TCL scripting language, see www.tcl.tk.

  Syntax and constructs from these sources work seamlessly within Extreme Management Center scripts. For example, the response from a switch to an ExtremeXOS CLI command issued from a script can be processed using TCL functions.

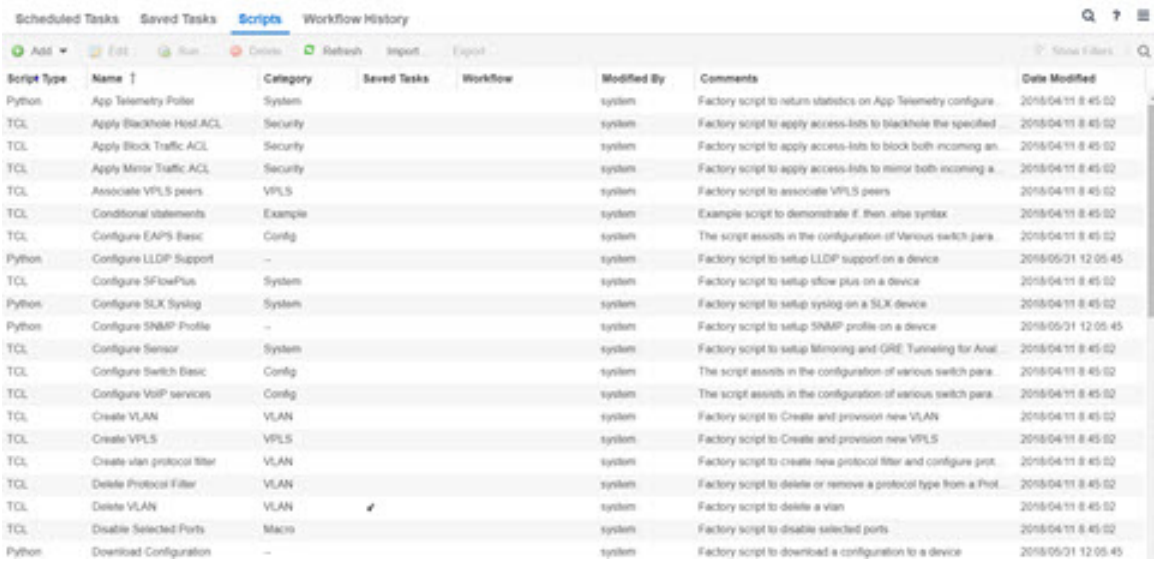
Bundled Extreme Management Center Scripts

Extreme Management Center includes a number of sample scripts you can use as templates for your own Extreme Management Center scripts. These scripts perform such tasks as enable/disable ports, apply ACLs, restart engines, and configure VLANs.

The sample scripts included with Extreme Management Center 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 Extreme Management Center Script Interface

To display the scripts configured in Extreme Management Center, select the **Tasks** tab, then click the **Scripts** tab.

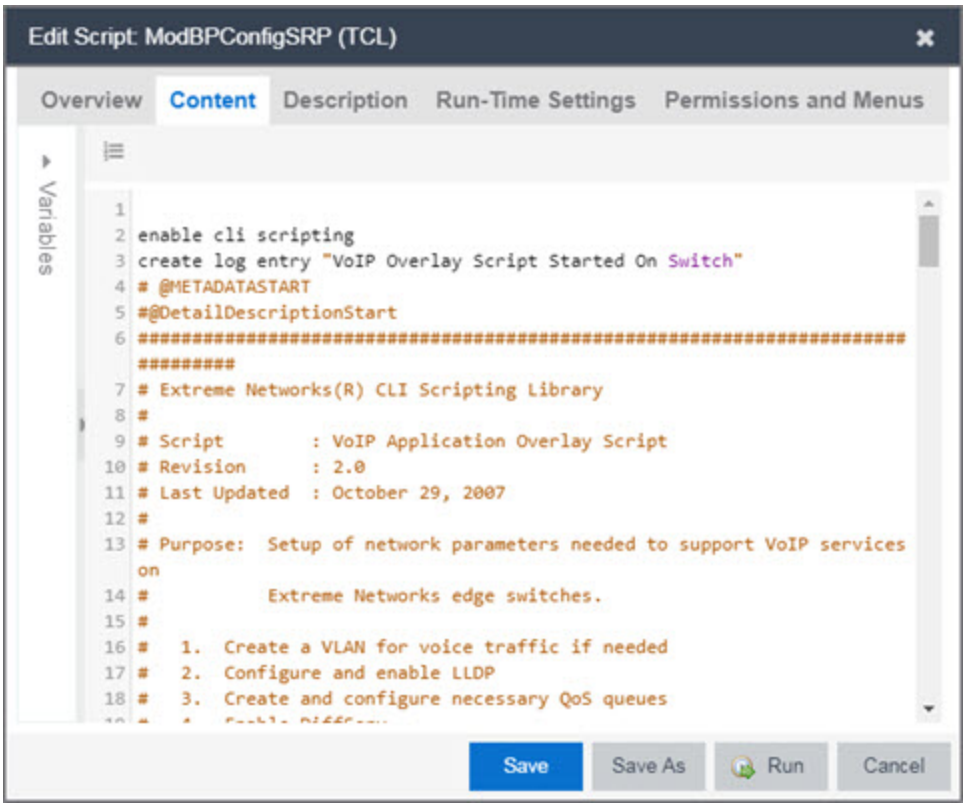


The Scripts tab contains the following information:

- **Script Type** — The language in which the script is written.
- **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.
- **Name** — The name of the script. The script **Name** is defined when adding the script and can not be edited.
- **Workflow** — Indicates if the script is included in a workflow.

- Comments — Comments or a description of the script.
- Modified By — The name of the last user to modify the script.
- Date Modified — The date the script was last modified.

Double-click a script or select a script and click the Edit button to open the Edit Script window.



The Extreme Management Center Edit Script window allows you to add content to a script, set values for parameters, specify run-time settings, and specify the Extreme Management Center users with permission to run the script.

Depending on the type of script you are editing, the following tabs may appear in the Extreme Management Center 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.

- Run-Time Settings — Specifies script settings applied when the script is run.
- Permissions and Menus — Specifies Extreme Management Center user roles with the ability to run the script, and whether or not, and where, the option to run the script appears in the Extreme Management Center interface, such as on a menu or in a shortcut menu.

Managing Extreme Management Center Scripts

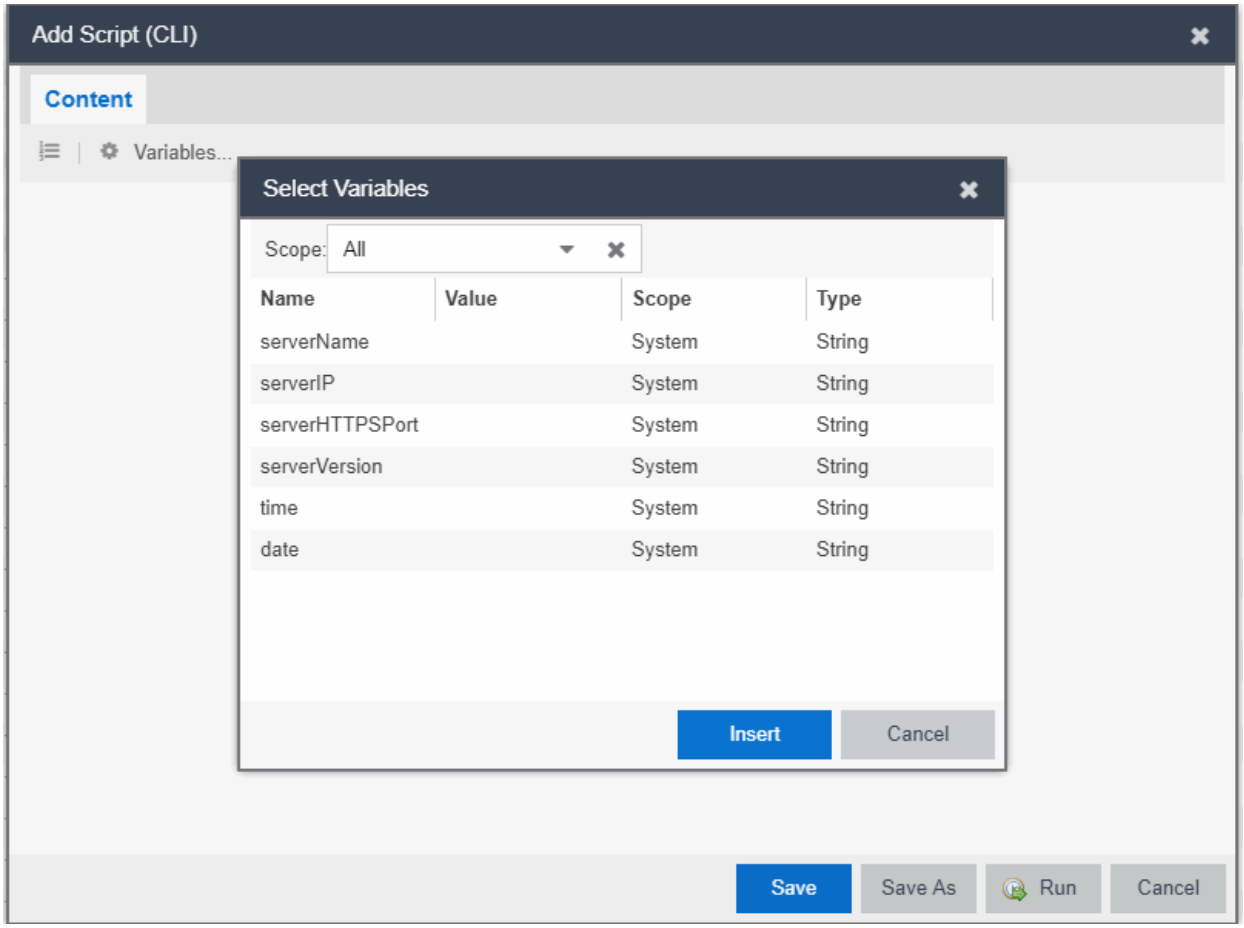
With scripting, you can:

- Create an Extreme Management Center Script
- Specify Run-Time 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 Extreme Management Center
- Export a Script
- Save Script as a Task

Create an Extreme Management Center Script

1. Click Scripts on the Tasks tab.
2. Click the Add button.
3. Select the type of script you are creating:
    - TCL — A Tool Command Language script. 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. Proceed to step 4.

4. When selecting **CLI** from the **Add** drop-down menu, the **Add Script** window opens, where you can enter the CLI commands for the script. Click **Variables** to open the **Select Variables** window, from which you can select variables you define on the Custom Variables tab.



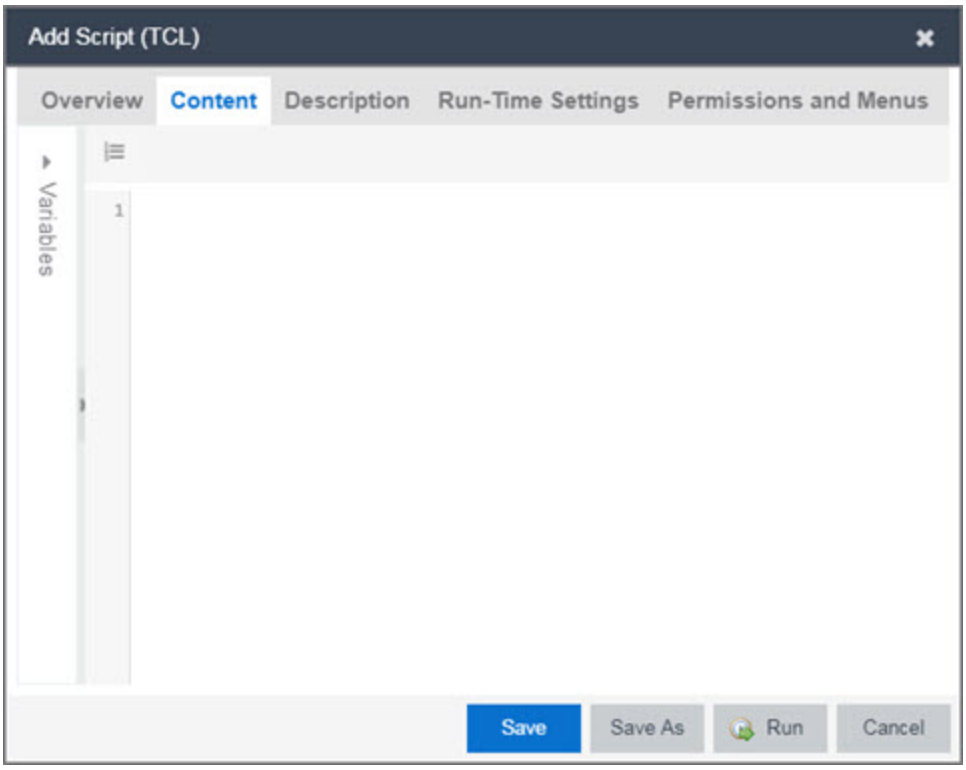
Use the **Scope** drop-down menu to select either **All**, **Global**, or **System** from the drop-down menu, depending on how you configured the variable you are inserting. Click **Insert** to add the variable to your script.

Click **Save** to save the CLI script on the **Scripts** tab or click **Save As** to save the script to the Extreme Management Center server.

Click **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.
- Run-Time Settings — Specify script settings applied when the script is run.
- Permissions and Menus — Specify Extreme Management Center user roles with the ability to run the script, and whether or not, and where, the option to run the script appears in the Extreme Management Center interface, such as on a menu or in a shortcut menu.



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

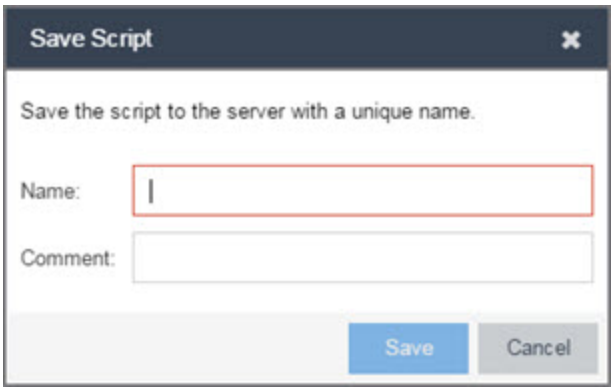
list of system variables appears under Variables. To add a variable to the script, double-click the variable.

8. Enter script commands after the metadata section of the script.

   The following are examples of types of script commands supported in Extreme Management Center:

   - ExtremeXOS 12.1 and later CLI scripting commands
   - TCL commands
   - Constructs

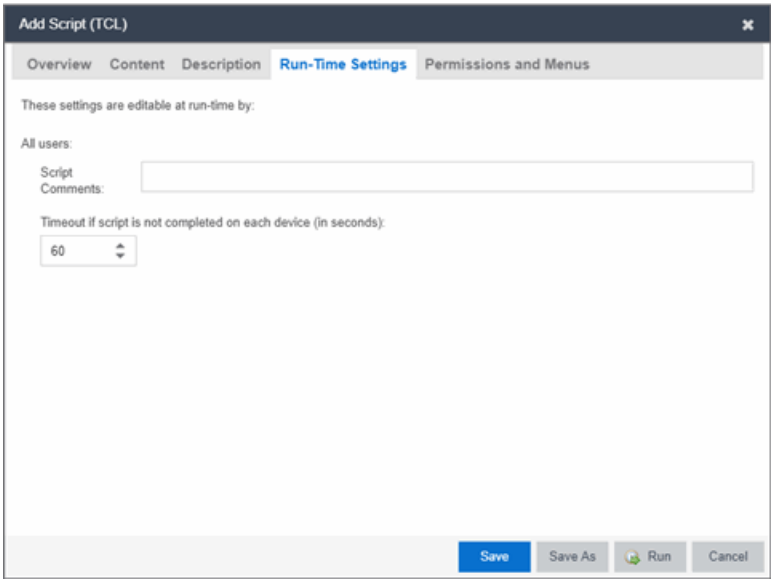
9. Click the **Run-Time Settings** tab to specify run-time settings.
10. Click the **Permissions And Menus** tab to specify which Extreme Management Center user roles have permission to run the script, and whether or not, and where, the script appears in the menu or in a shortcut menu.
11. Click **Save**. The **Save Script** window appears.



12. Type a name for the script file in the **Name** field and a comment about the script in the **Comment** field, if necessary.
13. Click **Save**.
14. Click **Run** to run the script now or **Cancel** to run the script at a later time.

Specify Run-Time Settings for a Script

To specify the run-time settings for a script, click the **Run-Time Settings** tab.



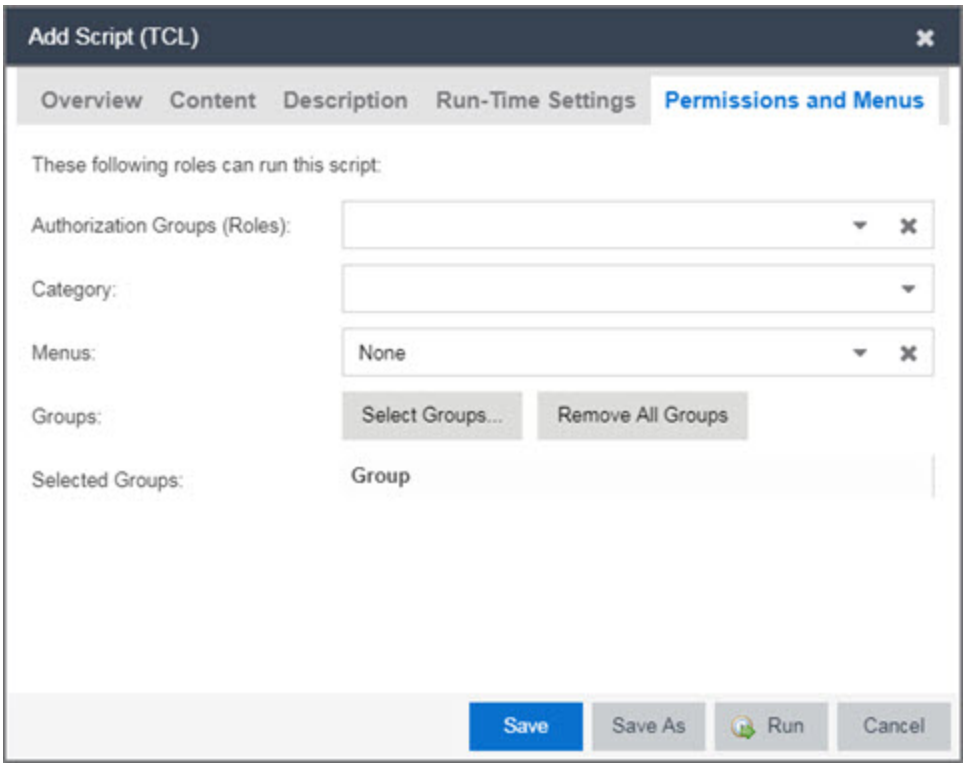
Use this tab to specify the following settings:

- 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 Extreme Management Center 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.

Click 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 menu.

Category

Select the **Category** group from the drop-down menu, which defines the Tasks submenu in which the script is grouped throughout Extreme Management Center.

Menus

Select the Tasks submenus in Extreme Management Center in which you want the script to display from the drop-down menu. Select **Multi-Device** for User Device Group scripts.

Groups

Click the **Select Groups** to select the device groups on which the script displays.

Selected Groups

Displays the Groups in which the script is included.

Run a Script

From the Network 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. Click **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, click the **Description** tab to view the description defined for the script.
6. Click **Next**.

   The **Verify Run Script** tab opens.
7. Verify your script selections, and then click **Run**.
8. On the **Results** tab, you see the results of the script including any errors.
9. Click **Close**.

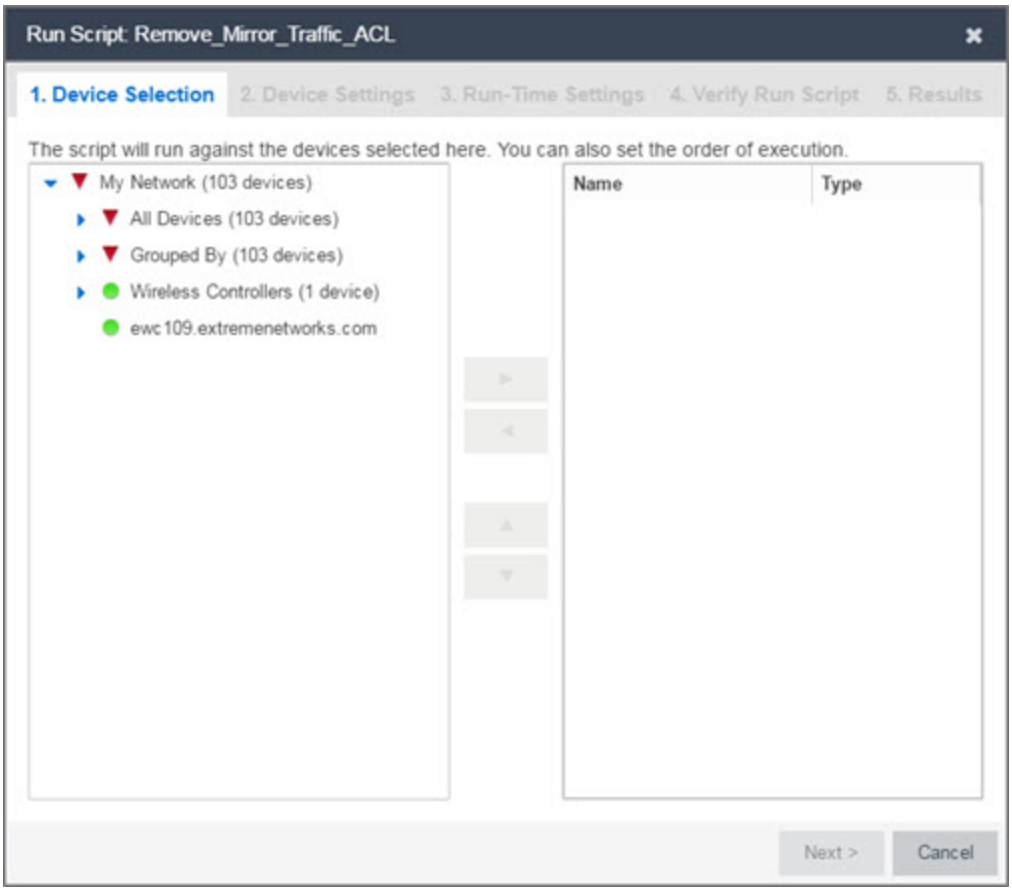
From the Tasks tab

1. Click **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 clicking its row and then click **Run**. The Run Script window opens.

NOTE: Be sure to select only 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. Click **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, click the **Description** tab to view the description defined for the script.
7. Click **Next**.
8. On the **Run-Time Settings** tab, configure the run-time 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. Click **Next**. On the **Verify Run Script** tab, verify your script selections, and then click **Run**.
10. On the **Results** tab, you see the results of the script including any errors.
11. Click **Close**.

View Script Results

Once 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.

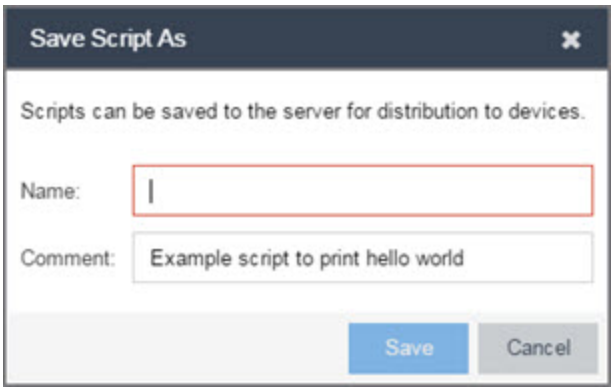
An event is stored in the console.log file in the `<install directory>/appdata/logs` folder each time a script is executed. The event in the log contains the location of the audit file. These audit logs reside in the tmp directory and remain for two weeks (per user), or until the next server restart, whichever comes first. The number of audit files written to the folder is limited to 1,000 files. Once the number of files exceeds 1,000, the oldest 100 are deleted.

Edit a Script

To edit a script:

1. In the **Tasks** tab, click **Scripts**.
2. In the scripts table, select the script you want to edit.
3. Click the **Edit** button. The script opens in the Edit Script window, where you can edit the script.
4. Save the script:
    a. Click the **Save** button to save your changes to the script.
    b. Click **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. Click **Save**.

The script is saved.

Delete a Script

To delete a script:

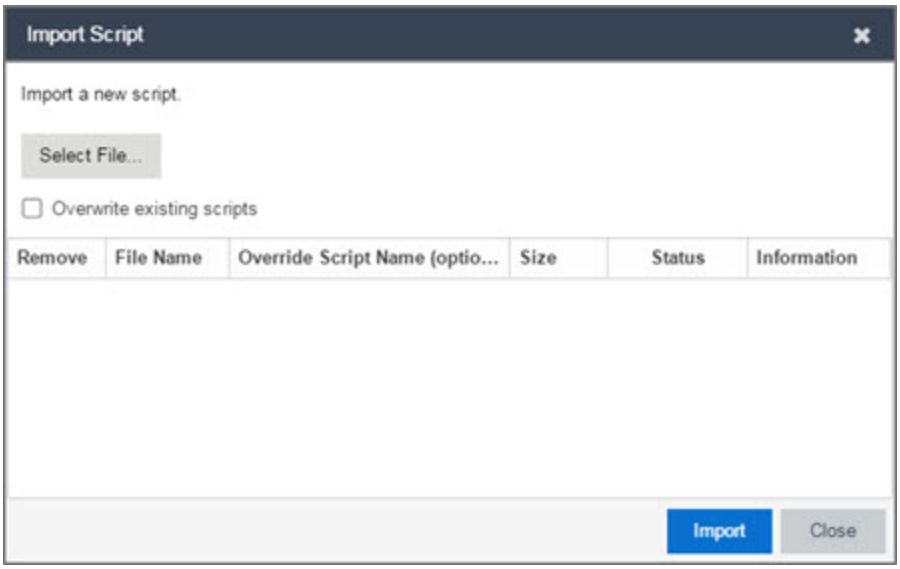
1. In the **Tasks** tab, click **Scripts**.
2. In the scripts table, select one or more scripts you want to delete.
3. Click the **Delete** button.
4. Click **Yes** to confirm the script deletion.

Import Scripts into Extreme Management Center

Import XML-formatted scripts into Extreme Management Center.

To import a script:

1. In the **Tasks** tab, click **Scripts**.
2. Click the **Import** button.



3. Click **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 edit the name of the script.
5. Click **Import**.
6. Verify the script is imported and click **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. Click 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 run-time settings, and then allows you to manually run the script task at a later time or schedule it to run in the future either once, 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 **Run-Time Settings** tab.
3. Enter a new name for the task in the **Task Name** field.

Extreme Management Center saves the script to the **Saved Tasks** tab.

Extreme Management Center Script Reference

This section contains reference information for Extreme Management Center scripts. It contains the following topics:

- Metadata Tags
- Extreme Management Center-Specific Scripting Constructs
- TCL Support in Extreme Management Center Scripts
- Entering Special Characters
- Line Continuation Character
- Case Sensitivity in Extreme Management Center Scripts
- Reserved Words in Extreme Management Center Scripts
- ExtremeXOS CLI Scripting Commands Supported in Extreme Management Center Scripts
- Extreme Management Center-Specific System Variables

An Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center 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.

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 Extreme
Management Center 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. Once 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 menu 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 ""
```

Extreme Management Center-Specific Scripting Constructs

This section describes the scripting constructs specific to Extreme Management Center:

- Specifying the Wait Time Between Commands
- Printing System Variables
- Configuring a Carriage Return Prompt Response
- Synchronizing the Device with Extreme Management Center
- 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 Extreme Management Center

The PerformSync command manually initiates a synchronization for specified Extreme Management Center 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, Extreme Management Center 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 Extreme Management Center Scripts

The following TCL commands are supported in Extreme Management Center scripts:

after	concat	for	info	lrange	puts	set	unset
append	continue	foreach	interp	lreplace	read	split	update
array	eof	format	join	lsearch	regexp	string	uplevel

binary	error	gets	lappend	lsort	regsub	subst	upvar
break	eval	global	lindex	namespace	rename	switch	variable
catch	expr	history	linsert	open	return	tell	vwait
clock	fblocked	if	list	package	scan	time	while
close	flush	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 Extreme Management Center 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 Extreme Management Center script.

Line Continuation Character

The line continuation character is not supported in Extreme Management Center scripts. Place each command statement on a single line.

Case Sensitivity in Extreme Management Center Scripts

The commands and constructs in an Extreme Management Center 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 Extreme Management Center documentation.

Example (Usage of the Extreme Management Center command ECHO)

```
echo hi (valid)

echo [echo hi] (error)

echo [ECHO hi] (valid)
```

Reserved Words in Extreme Management Center Scripts

The following words are reserved by Extreme Management Center and cannot be used as variable names in a script:

- Names of system variables (see Extreme Management Center-Specific System Variables)
- Names of Extreme Management Center command extensions (see Extreme Management Center-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 Extreme Management Center Scripts

Extreme Management Center 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 12.1 and higher support this command.
- Example — `if ($VAREXISTS(foo)) then show var foo endif`

$TCL

- Evaluates a given TCL command. The following constructs support the $TCL command:
  - `set var if`
  - while
- See TCL Support in Extreme Management Center 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 12.1 CLI scripting. Use the $TCL (string toupper <string>) command instead. Example: set var foo $TCL ("foo") .

---

show var

- Prints the current value of a specified variable.
- Switch Compatibility — Devices running ExtremeXOS 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`

Extreme Management Center-Specific System Variables

The following system variables can be set in Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center server.

$serverName
The host name of the Extreme Management Center server.

$serverPort
The port number used by the Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center Devices and do not require the installation of any software (including Extreme Management Center) other than the browser itself.

You can also add your own custom FlexViews in Extreme Management Center.

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. The maximum number of FlexViews you can open at one time is 10.

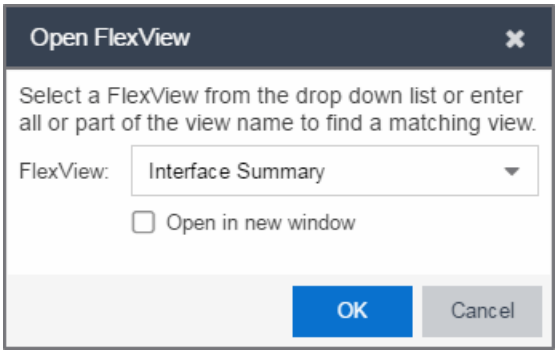
1. Launch Extreme Management Center and click on Network > Devices.
2. Select one or more devices in the Devices list.

   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. Click the Menu icon (≡) and select View > FlexView from the menu. You can also double-click the device in the Devices table to launch a FlexView.

   The Open FlexView window opens.

4. Select a FlexView from the drop-down menu, or enter all or part of the FlexView name to find a matching view. Any FlexView configured is listed for selection, including standard FlexViews and custom FlexViews you create.



   The FlexView opens in a new browser tab.

Using FlexViews

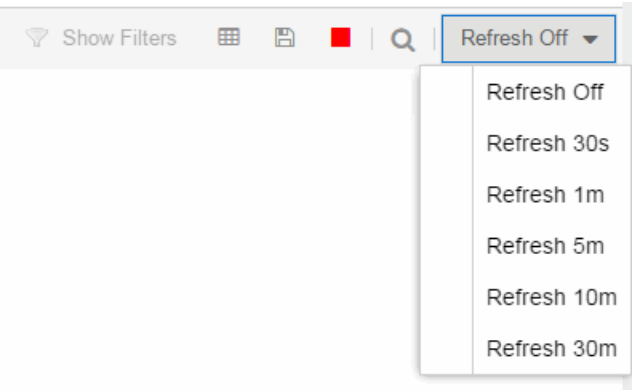
FlexViews let you manipulate the table data in several ways to customize the view for your own needs:

- Click on the column headings to sort column data in ascending or descending order.
- Hide or display different columns by clicking on 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.

NOTE: Row creation and data exports are not currently supported in FlexViews.

Setting the Refresh Interval

Use the Refresh drop-down menu to specify an interval (in seconds) at which the FlexView data is automatically refreshed. To stop auto refresh, select the **Refresh Off** option.

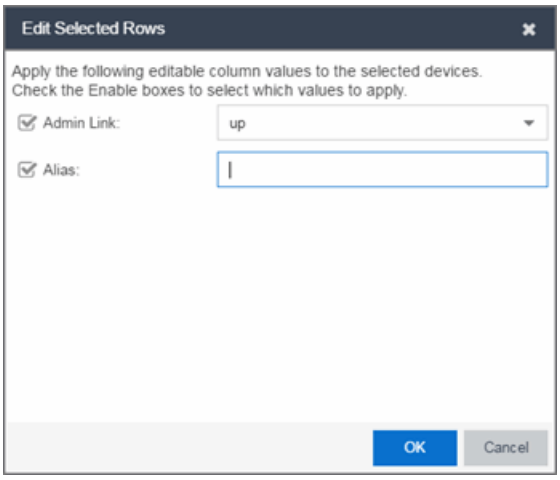


Editing Writable Values

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 Extreme Management Center and the CLI of the switch to display the character string.

3. Click OK to enter your changes into the selected rows. The new values are written directly to the device.

Related Information

For information on related topics:

- Network

Extreme Management Center VLAN Concepts

The following concepts will assist you in configuring VLAN and port template definitions in Extreme Management Center.

Information on:

- Egress Rules (Transmitting Frames)
    - Dynamic Egress
        - GVRP
        - GARP Timers
- Enforcing
- Frame Types
- IGMP
    - Interface Robustness (Robustness Variable)
    - Last Member Query Interval
    - Query Interval
    - Query Response
- Ingress Filtering
- Priority Classification
    - Weighted Priority
- Verifying
- VLAN Identification
    - Port VLAN ID (PVID)
    - VLAN ID (VID)
- VLAN Model
- VLAN Learning

Egress Rules (Transmitting Frames)

A device determines which frames can be transmitted out a port based on the Egress List of the VLAN associated with it. Each VLAN has an Egress List that specifies the ports out of which frames can be forwarded, and specifies whether the frames will be transmitted as tagged or untagged frames. You can add or remove ports to or from a VLAN's Egress List, thereby controlling which VLAN's frames can be forwarded out which ports.

When a frame is transmitted out a port, the device first checks the Egress List. If the port is listed on the Egress List of the VLAN associated with it, the frame is then transmitted according to the priority assigned to the frame. The frame is transmitted as tagged or untagged according to the specification in the Egress List. If the port is not on the Egress List, or if the port is not operational, the frame is discarded.

Dynamic Egress

In Extreme Management Center, 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. In the Port Template Definitions view, 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.)

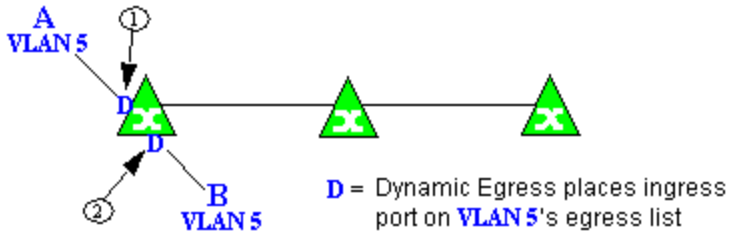
When you disable Dynamic Egress for a VLAN, the VLAN effectively becomes a discard VLAN. Since the destination port is not added to the egress list of the VLAN, the device discards the traffic. If you want a VLAN to act as a discard VLAN, disable Dynamic Egress for that VLAN. (See Example 3, below.)

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.

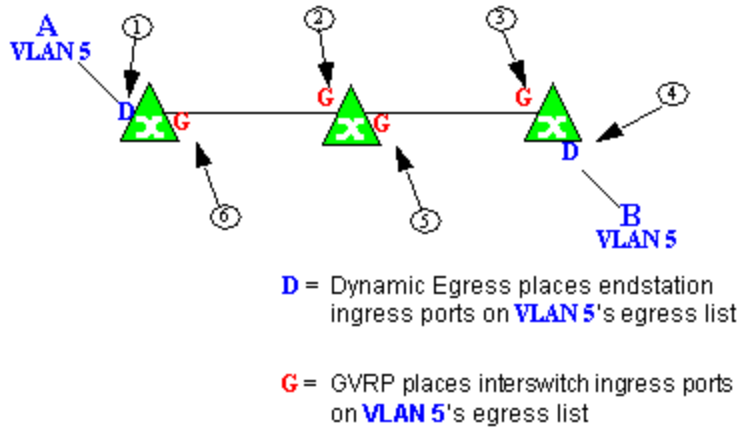
Example 1: Dynamic Egress Enabled

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.



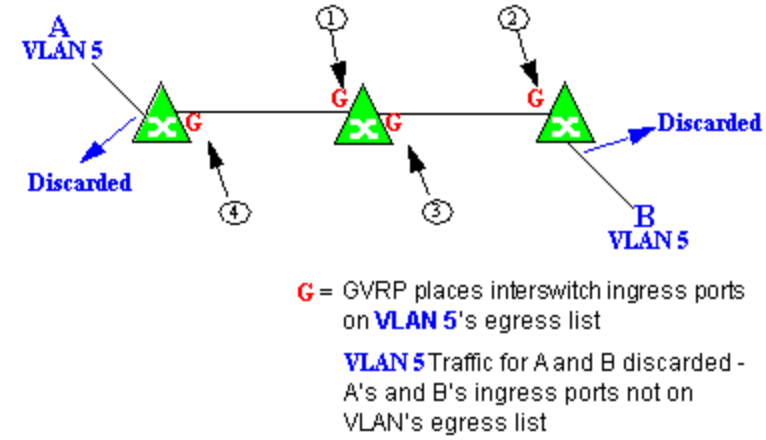
Example 2: Dynamic Egress + GVRP

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. You can enable and disable GVRP in the Port Template Definitions view.

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

In the Port Template Definitions view, you can set GARP timers on the device to control the timing of dynamic VLAN membership updates to connected devices. The timer values must be identical on all connected devices in order for GVRP to operate successfully.

- Join Time - Frequency of messages issued when a new port has been added to the VLAN. Possible values are 1 through 1488800 milliseconds.
- Leave Time - Frequency of messages issued when a single port no longer belongs to the VLAN. This value must be at least three times greater than the Join Time. Possible values are 1 through 1488800 milliseconds.
- Leave All Time - Frequency of messages issued when all ports no longer belong to the VLAN and the VLAN should be deleted. This value must be greater than the value for Leave Time. Possible values are 1 through 1488800 milliseconds.

Enforcing

When working with VLANs in NetSight Console, you can write the definitions in the VLAN model to selected devices or ports by clicking the Enforce button on the Device or Advanced Port view of the right panel VLAN tab in Console's main window. You can also enforce changes to individual ports on the Basic Port view of the VLAN tab in Console's main window. A green exclamation point in a table indicates that the setting will be written to the device when you

enforce. Only those VLANs which have the Write VLAN to Devices box checked on the VLAN Properties tab are enforced. A verification is done automatically after the enforce is complete. A red ✖ appears if the enforcing of a particular setting fails.

NOTE: On the X-Pedition router, enforcing will not overwrite the "System Static" VLAN (SYS_L3_ Interface Name). However, you can update a VLAN model definition with the System Static VLAN definition from the router.

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 on the Port Template Definitions view.

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 on the VLAN Definitions view.

IGMP Intervals

You can control the following IGMP query settings on the VLAN Definitions view:

- Query Interval - Interval (in seconds) between general IGMP queries sent by the device to solicit VLAN membership information from other devices. By setting this interval, you can control the number of IGMP messages on a subnet. Larger values cause queries to be sent less often. The Query Interval must be greater than the Query Response interval. Valid values: 1 through 300 seconds.
- Query Response - Maximum amount of time allowed for responses to general IGMP queries. By setting this value, you can control the burstiness of IGMP messages on a subnet. Larger values result in less bursty traffic, because host responses are spread over a larger interval. This value must be less than the Query Interval. Valid values: 1 through 300.
- Interface Robustness (Robustness Variable) - Indicates the susceptibility of the subnet to lost packets. If a subnet is particularly susceptible to losses, you may wish to increase this value. IGMP is robust to (Robustness Variable-1) packet losses. The

Interface Robustness value is used in the calculation of IGMP message intervals. Valid values are 2 thru 32767.

- Last Member Query Interval - Maximum amount of time (in seconds) between group-specific query messages, including those sent in response to leave-group messages. By setting this value, you can control the "leave latency" of the network. You might lower this interval to reduce the amount of time it takes the device to detect the loss of the last member of a group. Valid values: 10 through 32767 seconds.

Ingress Filtering

Ingress Filtering is a means of filtering out undesired traffic on a port. When Ingress Filtering is enabled, a port determines if a frame can be processed based on whether the port is on the Egress List of the VLAN associated with the frame. For example, if a tagged frame with membership in the Sales VLAN is received on a Port 1, and Ingress Filtering is enabled, the switch will determine if the port is on the Sales VLAN's Egress List. If it is, the frame can be processed. If it is not, the frame is dropped. You can set ingress filtering for a VLAN on the Port Template Definitions view.

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 on the Port Template Definitions view.

Weighted Priority

Weighted priority, available on certain devices, is a way to further refine priority classification. You can control this setting on the Port Template Definitions view.

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 view or Port Template Definitions view. This is done by way of the **Start Verify (Retrieve)** button on the Device or Advanced Port view of the VLAN tab in Console's main window. (In the Basic Port view of the VLAN tab in Console's main window, the button

simply retrieves port VLAN information from the selected devices to populate the table.)

Only those VLANs which have the Write VLAN to Devices box checked on the VLAN Definitions view are compared. Differences are indicated by a red not-equals symbol ≠ in the device or ports table on the VLAN tab in Console's main window. 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 (for VLAN Definitions) or ports (for Port Template Definitions).

For more information, see How to Work with VLAN Models.

VLAN Identification

VLAN identifiers include VLAN ID's and Port VLAN ID's.

VLAN ID (VID)

802.1Q VLANs are defined by VLAN IDs (VIDs) and VLAN names.

VID

A unique number between 1 and 4094 that identifies a particular VLAN. VID 1 is reserved for the Default VLAN.

VLAN Name

An alphanumeric name associated with a VLAN ID, used to make VLANs easier to identify and remember (up to 64 characters).

PVID (Port VLAN ID)

You can change a port's VLAN membership to reflect the specific needs of your network by assigning new VLAN membership to the port. When you assign VLAN membership to a port, that VLAN's ID (VID) becomes the Port VLAN ID (PVID) for the port and the port is added to the VLAN's Egress List.

PVID

The PVID (Port VLAN ID) represents a port's VLAN assignment. Possible values are 1 through 4094.

Egress List

The Egress List specifies which ports can transmit the frames associated with the VLAN.

NOTE: On the X-Pedition Router, you cannot assign a PVID to a port that has an interface assigned to it.

VLAN Model

NetSight Console enables you to 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, which you can define on the VLAN Definitions view and the Port Template Definitions view.

NetSight Console 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:

- Use the Basic Port View of the VLAN tab in Console's main window to enforce the properties of a port template on selected devices. You can also make custom edits for selected ports using this view of the VLAN tab in Console's main window.
- Use the Device or Advanced Port view of the VLAN tab in Console's main window to 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 of the VLAN tab in Console's main window, 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 How to Work with VLAN Models 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.

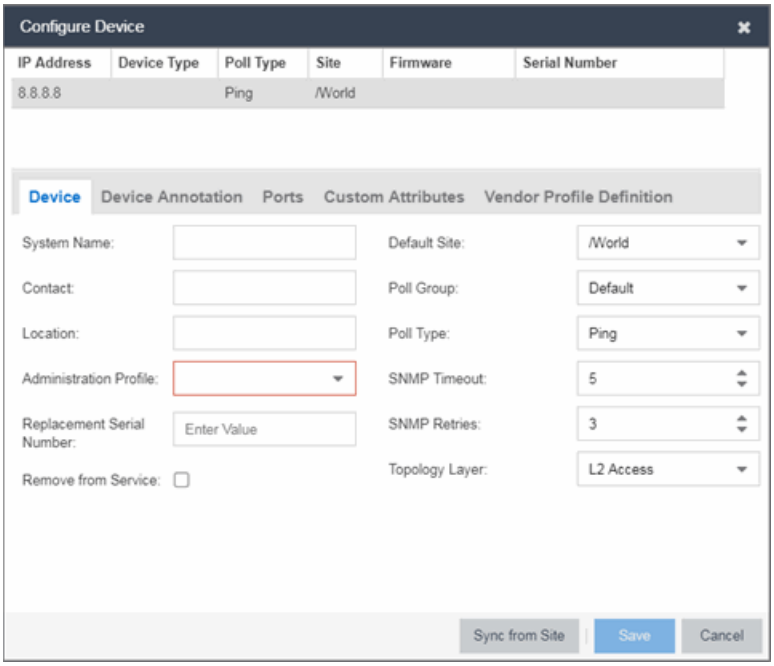
How to Create and Edit a VLAN in Extreme Management Center

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

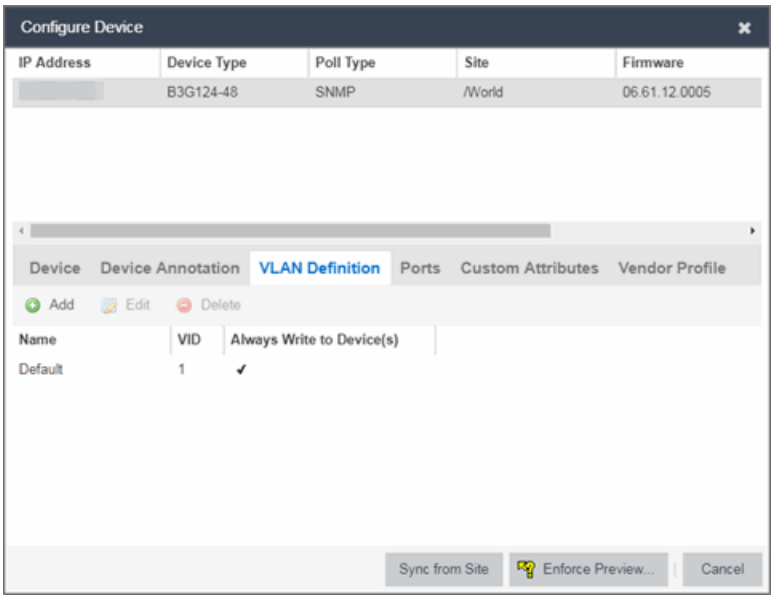
- Create a new VLAN
- Edit the ports of an existing VLAN
- Edit the name of an existing VLAN
- Remove devices from an existing VLAN

To create a new VLAN:

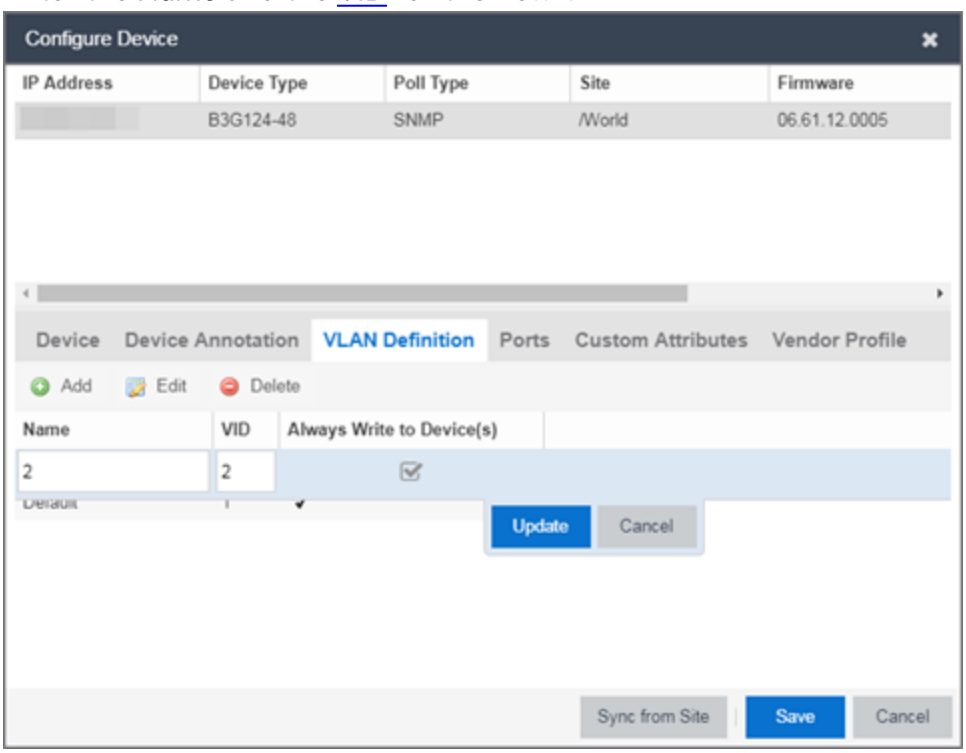
1. Launch Extreme Management Center.
2. Open the **Network > Devices** tab.
3. Select the device from the devices list. Right-click the device and select **Device > Configure Device**.
   The Configure Device window opens.



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

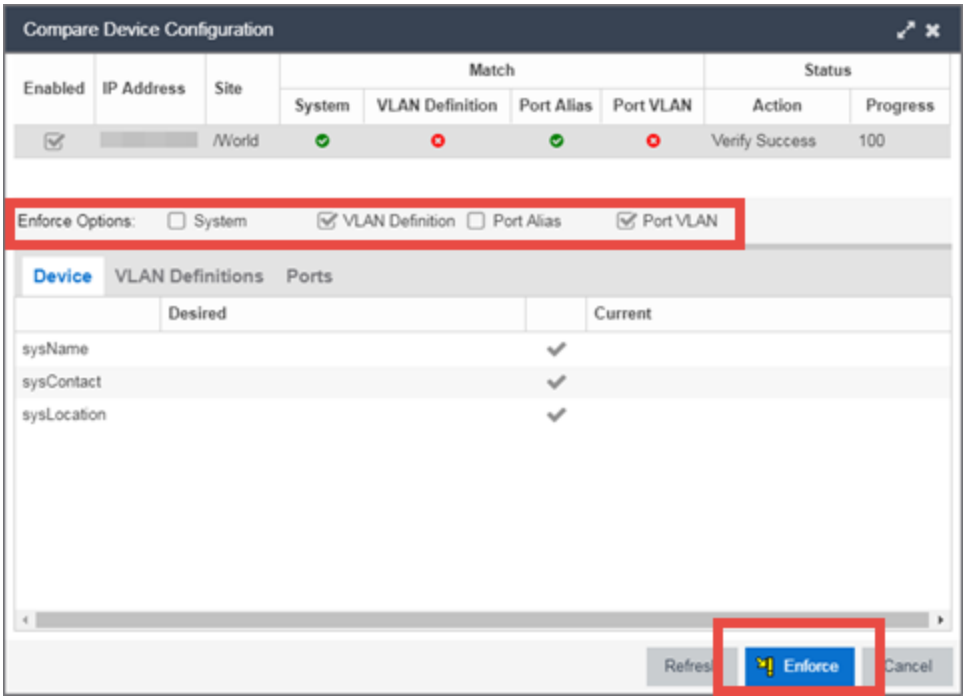


5. Click the **Add** button.
6. Enter the **Name** and the VID for the new VLAN.



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 Extreme Management Center to select the checkboxes by default, open the `NSJBoss.properties` file and change **false** to **true** in the following lines:

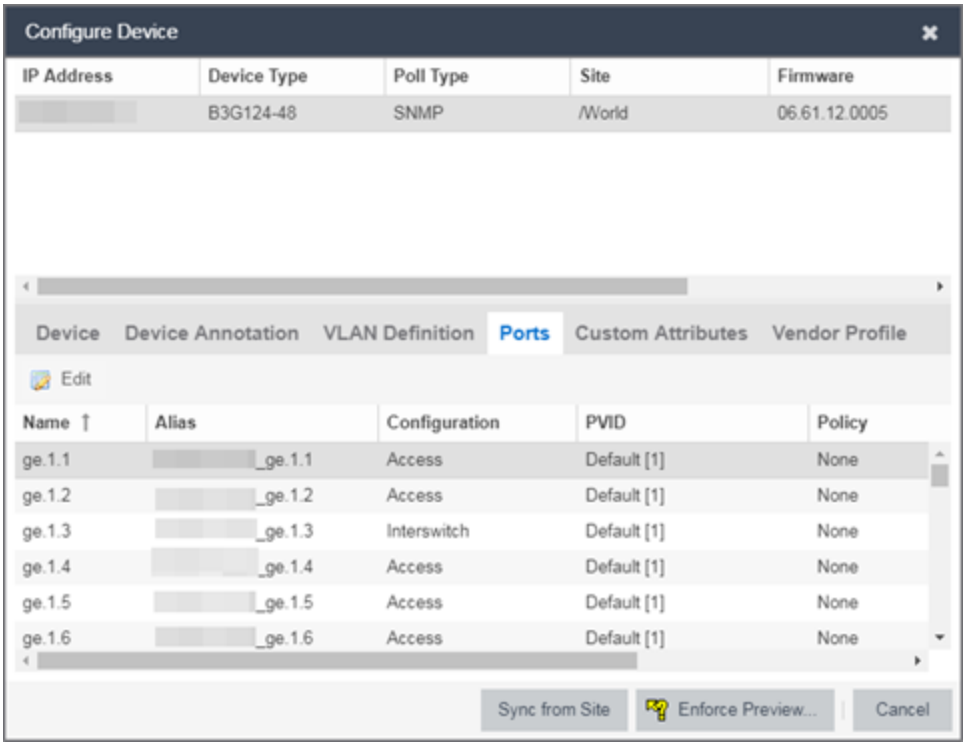
- `site.enforceOption.autoEnable.system=false`
- `site.enforceOption.autoEnable.vlanDefinition=false`
- `site.enforceOption.autoEnable.portAlias=false`
- `site.enforceOption.autoEnable.portVlan=false`

The VLAN is now created and assigned to the device.

To configure the VLAN(s) on the ports

1. Launch Extreme Management Center.
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. Click **Enforce Preview**.
10. Under the Enforce Options, select the **Port VLAN** checkbox and select **Enforce**.

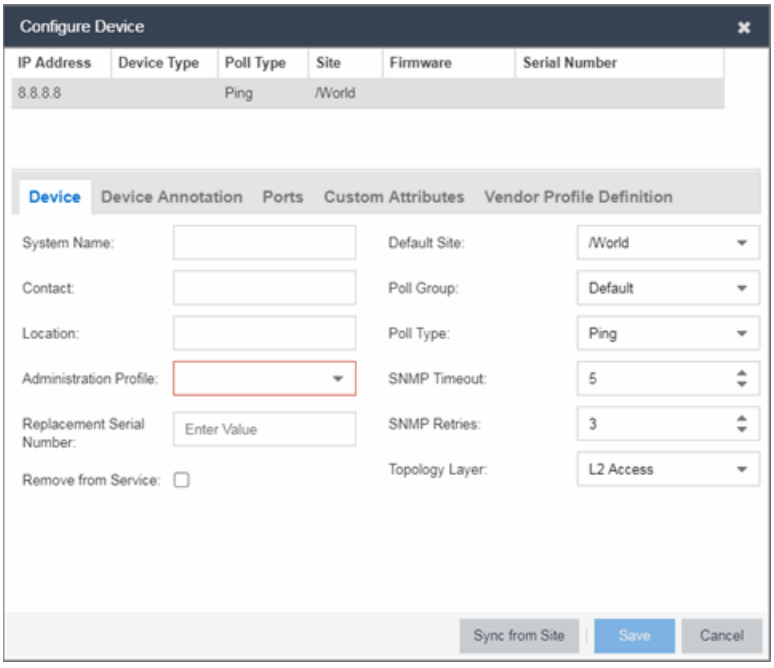
NOTE: By default, the checkboxes in the Enforce Options section of the window are not selected. To configure Extreme Management Center to select the checkboxes by default, open the `NSJBoss.properties` file and change **false** to **true** in the following lines:

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

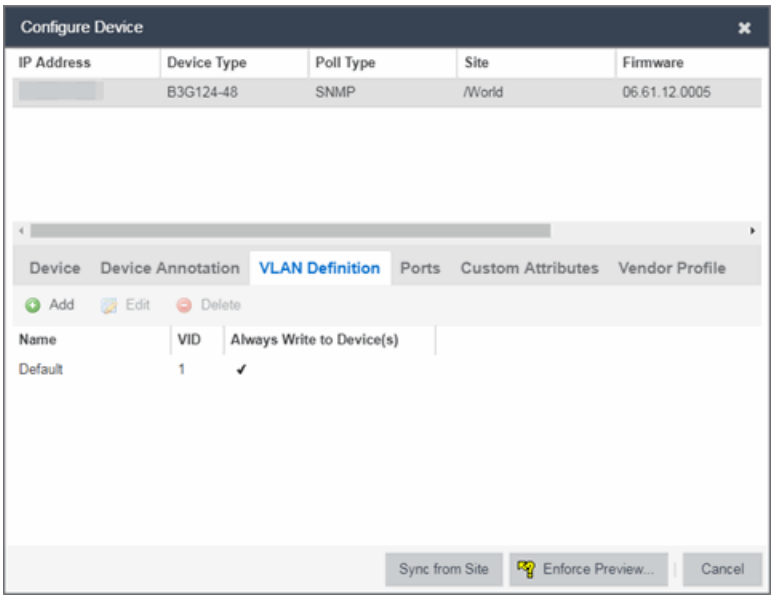
The VLAN is now configured to the Ports.

To edit the name of a VLAN:

1. Launch Extreme Management Center.
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. Click the **VLAN Definition** tab.

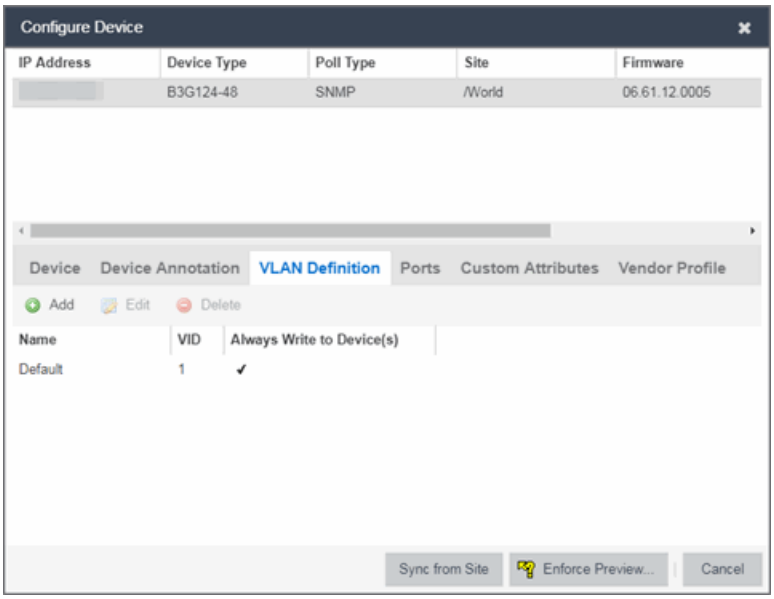


6. Select the VLAN to edit and then select the **Edit** button.
7. Enter the new name for the VLAN.
8. Click **Update**.
   The Edit pane closes.
9. Click **Save** to exit the VLAN Definition window. The VLAN is updated.

To remove devices from a VLAN:

1. Launch Extreme Management Center.
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. Click the **VLAN Definition** tab.
   The VLAN Definition pane opens.



5. Select the VLAN and click **Delete**.

Related Information

For information on related topics:

- Maps
- Devices tab

Adding Custom FlexViews and MIBs in Extreme Management Center

Use the instructions in this topic to add custom FlexViews and MIBs in Extreme Management Center.

To add a new FlexView to Extreme Management Center:

1. Add your custom FlexView files (.TPL) to the `/usr/local/Extreme_Networks/NetSight/appdata/VendorProfiles/Stage/MyVendorProfile/FlexViews` directory on the Extreme Management Center server.
2. 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 Extreme Management Center server.
3. Log into the system shell (via the local console or SSH) on the Extreme Management Center server as root on a Linux operating system or open a CMD prompt by selecting Run as administrator on a Windows operating system.
4. Restart the Extreme Management Center server:
    a. Enter `service nsserver stop`.
    b. Enter `service nsserver start`.

Troubleshooting

This troubleshooting guide provides a list of items to check when Extreme Management Center 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 Extreme Management Center, access **Administration** > **Profiles** tab. b. Select the **CLI Credentials** subtab. c. Select the CLI Credential being used by the controller's Profile, and click **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. Click **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 Extreme Management Center Server and Wireless Controllers to communicate: SSH: 22 SNMP: 161, 162 Langley: 20506