Extreme Networks Extreme Management Center®

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/

Support

For product support, including documentation, visit:
www.extremenetworks.com/support/

Contact

Extreme Networks, Inc.,
145 Rio Robles
San Jose, CA 95134
Tel: +1 408-579-2800

Toll-free: +1 888-257-3000

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 (formerly NetSight) provides access to web-based reporting, network analysis, troubleshooting, and helpdesk tools. 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 Management Center license.

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

Extreme Management Center Features

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 and 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.
- Reports — Historical and real-time reporting offering high-level network summary information as well as detailed reports and drill-downs.
- Administration — Management Center administration tools to monitor and maintain the Management Center application and its components.
- Connect — Provides configuration to allow you to integrate third-party software with 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 Management Center Help documentation.

Date	Revision Number	Description
06-16	7.0 Revision -00	Management Center (formerly NetSight) 7.0 release
07-15	6.3 Revision -00	NetSight 6.3 release
01-15	6.2 Revision -00	NetSight 6.2 release
06-14	6.1 Revision -00	NetSight 6.1 release
02-14	6.0 Revision -00	NetSight 6.0 release

PN: 9034986-01

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 Management Center access requirements, including several different access scenarios. It also provides steps for enabling the statistics and flow collection that provides Management Center reporting data, and information on Management Center scalability.

Requirements

This section provides information on license requirements for the different 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 Management Center features. Contact your sales representative for information on obtaining the appropriate 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 Management Center application and its features is determined by the user's membership in a Management Center authorization group and the group's assigned capabilities. The following table lists the different Management Center access options and features, and their corresponding capabilities. For more information on how to configure capabilities and authorization group membership, see the Management Center Help topic "How to Configure User Access to Extreme Management Center Applications," located in the

Management Center Suite-Wide Tools user guide in the "Authorization Device Access" section.

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

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

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

Here are several scenarios that show how different 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 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 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 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 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 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, Management Center is best viewed on a system with a minimum screen resolution of 1280x1024.

Enable Report Data Collection

To view 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 not available with the NMS-BASE license.

Enable Device Statistics Collection

To view Management Center device reports, you must enable statistics collection for your network devices from either 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 statistics are saved to the database and aggregated over time, and are then used in Management Center reports. The device statistics are also used for active threshold alarms configured in the Console Alarms Manager.

- 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 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 a Extreme Access Control engine, Application Detection engine, or ExtremeWireless Controller, read through the following notes:

- Access Control Engine
  When collecting statistics on a Access Control engine, the engine must be added to Management Center to collect all engine statistics. In addition, Monitor mode is not supported on Access Control engines.
- Application Detection Engine
  When collecting statistics on an Application Detection engine, the engine must be added to the Analytics > Configuration > Application Analytics Engines table in order for 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. See below for information on enabling wireless controller statistics collection.

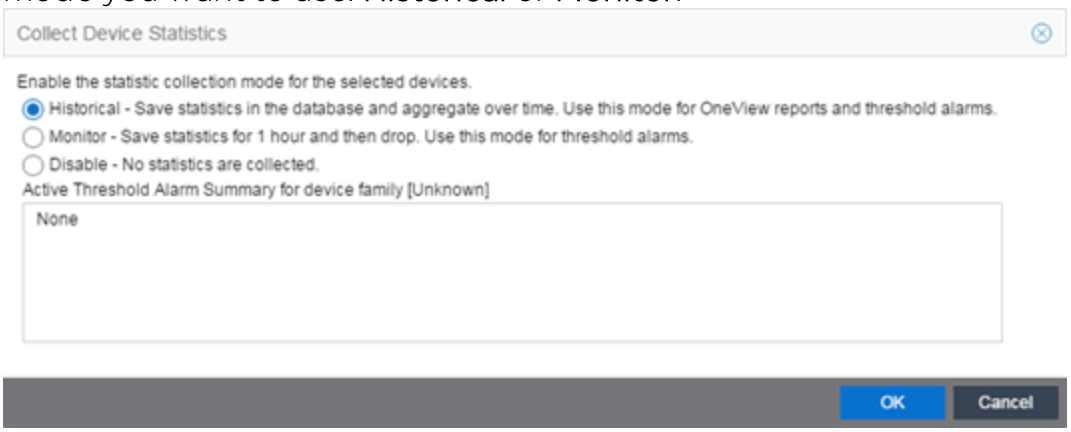
Steps for Enabling Collection

Use the following steps to enable device statistics collection.

1. You can enable statistics collection from either 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 gear menu  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 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. Management Center begins collecting statistics for the selected devices.

Enable Interface Statistics Collection

To view Management Center interface reports, you must enable statistics collection for your device interfaces from either the 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.

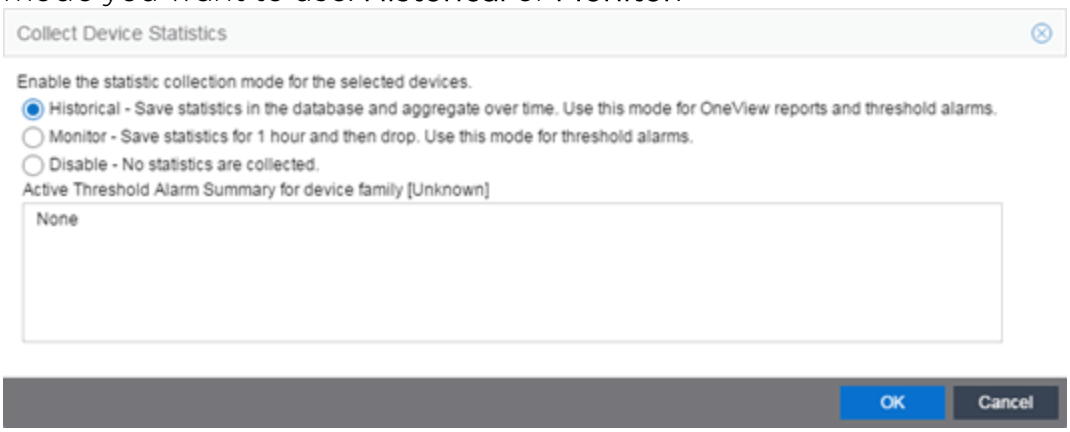
- Historical Mode — Interface statistics are saved to the database and aggregated over time, used in Management Center reports. The interface statistics are also used for active threshold alarms configured in the Alarms and Events tab.

- 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 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 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 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. Management Center begins collecting statistics for the selected interfaces.

Enable Wireless Controller Statistics Collection

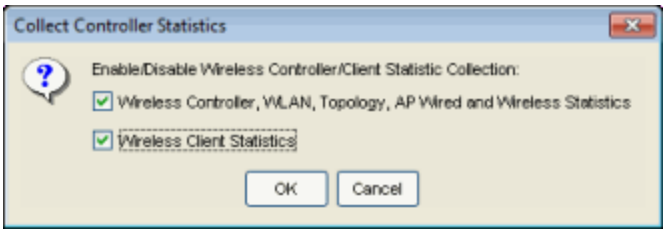
Wireless Controller statistics collection is configured separately from other devices. When you enable Wireless Controller statistics collection, it includes Wireless Controller, WLAN, Topology, and AP wired and wireless statistics, and you also have the option to collect wireless client statistics.

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 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 gear menu 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. Management Center begins collecting statistics for the selected controllers.

Enable Flow Collection

To view Management Center Flow and Application reports, you must enable NetFlow on the device and enable flow collection for the device interfaces. N-Series, S-Series, and K-Series devices support NetFlow flow collection. You must be a member of an authorization group assigned the NetSight OneView > NetFlow Read/Write Access capability to view NetFlow data and enable flow collection in Management Center. Flow collection is not available with the NMS-BASE license.

Enable NetFlow on a Device

In Console, open the Flow Sensor Configuration window (Tools > NetFlow Sensor Configuration). This window lists all the devices that support NetFlow. Select a device and use Enable NetFlow to add the NetSight server as a flow collector for that device.

Enable Flow Collection on an Interface

In PortView, you can enable flow collection from the Configure Collection State section of the Interface Details tab. See Launching PortView for instructions on how to open PortView.

Extreme Management Center Scalability

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

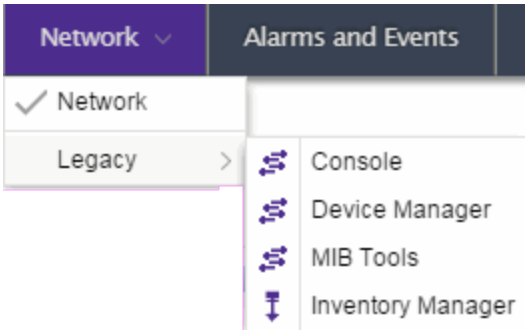
Management Center automatically times out after a specified amount of time, specified in the HTTP Session Timeout section of the Web Server view in the Administration > Options tab. A dialog box appears to warn you when you are two minutes from timing out of an Management Center web page. For additional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

Network

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

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

- Console
- Device Manager
- MIB Tools
- Inventory Manager



Navigating the Network Tab

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

- Dashboard — Displays summary Management Center data including switch 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, and allows you to organize devices into groups and geographically in maps.
- 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.
- Reports — Provides a variety of system reports that give information about your devices, ports, and network traffic.

The Menu at the top of the screen provides links to additional information about your version of Management Center. The Network tab consists of the Device Groups left-hand panel and the Device/Map right-hand panel.

Dashboard

Select the Dashboard sub-tab to view graphical data about devices on your network. Click Info 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 two options, the Overview and the Inventory dashboard.

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

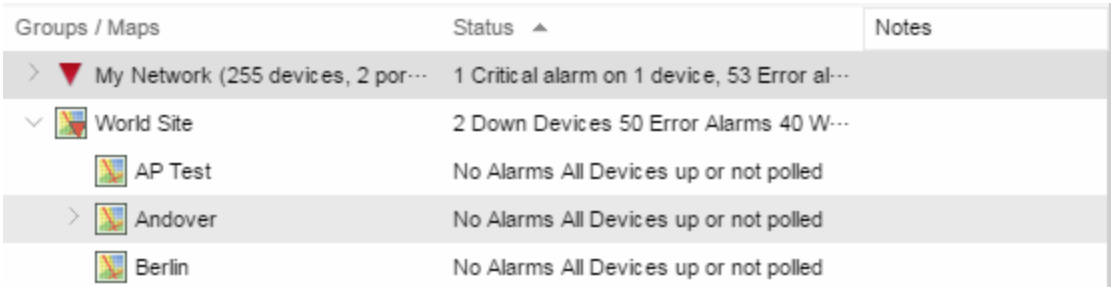
  - Summary — displays the percentage of archived devices, number of devices backed up, a listing of database properties, and upcoming scheduled events.
  - Asset Tracking — provides a list of devices based on their asset tag. An asset tag is a unique asset number assigned to a device for inventory tracking purposes.
  - Device Tracking — allows you to view a history of device attributes and monitor changes made to devices.

Devices

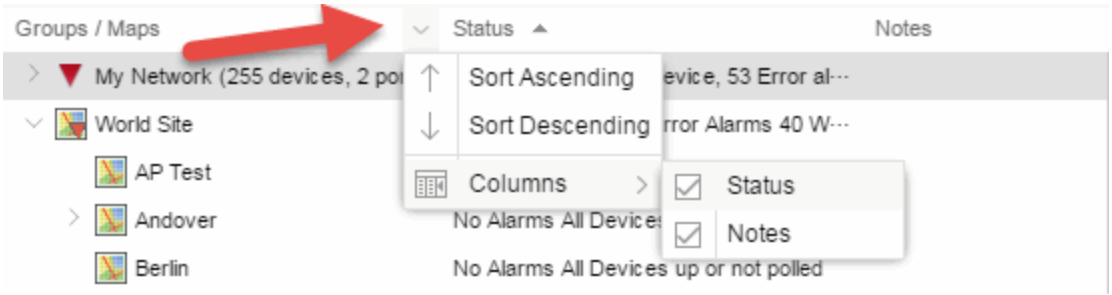
The Devices tab displays information about devices in your network and maps in which they are added. When a device is selected in the My Network navigation tree, the Devices panel displays a summary of the device. Selecting the My

Network navigation tree or a device group in the left-hand panel displays a list of the devices in the selected group. When you select a map from the World map navigation tree in the left-hand panel, the map appears in the right-hand panel as well as any devices included in the map.

The My Network navigation tree organizes your devices into groups. Expanding the All Devices list displays all devices on your network. Expanding the Grouped By list displays device groups using different criteria, including by device type, geographic location, chassis, IP address, and the contact associated with the device. Additional information about the devices in each group is displayed in the other columns.



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.



Right-clicking a device in the My Network navigation tree allows you to add or remove a device from a device group, create a map for the selected device or add the device to an existing map, run a script on a device, add a new device or delete a device. For additional information about creating a device group, see Create Device Group. For additional information about adding devices to a device group, see Add Devices to Group.

The World map navigation tree contains all of the maps you create. These map types can be geographic, topology, device, and floor plans. Right-clicking a map in the World map navigation tree allows you to create a new map, edit the selected map, delete the selected map, or import a new map. For additional

information about creating new maps or editing existing maps, see Create and Edit Maps. For additional information about adding devices to maps, see Add Devices to Maps.

For additional information about the tasks you can perform using the **Device** tab, see Device Operations.

Discovered

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

The **Discovered** tab allows you to quickly configure a new device using a configuration template created in Inventory Manager or a cloned configuration from an existing network device. For additional information about the **Discovered** tab, see Discovered.

For additional information about configuring new devices, see New Device Configuration in Extreme Management Center.

NOTE: You can also add a new device to a specific site using the **Site** tab. For additional information, see the **Site** tab help topic.

Firmware

The **Firmware** tab in the **Network** tab allows you 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. Via the Details section of the tab, the firmware or boot prom image details display and you can save the image to the device.

For additional information about the **Firmware** tab, see Firmware.

Archives

Archives presents a list of archives grouped by device type in the left-hand panel and provides information about archive operations performed on the selected device or device group. Additionally, you can create new archives for your devices on the **Archives** tab.

For additional information about the **Archives** tab, see Archive.

Reports

The **Reports** tab allows you 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** ( ) 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

Device Operations

This Help topic provides information on the following operations available from the **Network** > **Devices** tab:

- Add Device
- Delete Device
- Set Profile

- Create Device Group
- Add Devices to Group
- Backup, Restore, and Compare Device Configurations
- View Port Tree
- View Interface Summary
- View FlexViews
- View User Sessions
- Launch WebView
- View Network Details
- Collect Device Statistics
- Update Firmware
- Register Trap Receiver
- View Device Details
- Create and Edit Maps
- Add Devices to Maps
- View and Set Policy
- Manage Device Serial Numbers
- Run Scripts on Devices, Ports, and Groups
- Working in the Devices Table
    - Set Device Values
    - Table Column Definitions
- Filtering
- Buttons, Search Field, and Paging Toolbar
- Discovered Tab — Configure New Devices

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. For additional information about authorization capabilities, see How to Configure User Access to Extreme Management Center Applications.

Add Device

To add a new device to the Devices list:

1. Click the gear menu 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 Management Center.

Edit Device

To edit device information for an existing device:

1. Click the gear menu or right-click in the Devices list.
2. Select **Device** > **Edit Device**.

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

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 gear menu in the upper left corner of the **Network** tab or right-click and select **Device** > **Delete Device**.

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

Set 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 gear menu in the upper left corner of the **Network** tab or right-click and select **Device** > **Set Profile**.

   The Set Profile window appears.

3. Select a profile from the drop-down menu to change the profile for the selected device or devices.
4. Click Set Profile.

   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 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 gear menu  in the upper left corner of the Network tab or right-click and 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.
3. 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 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 gear menu in the upper left corner of the Network tab or right-click the device to select Configuration/Firmware > Backup Configuration.

   This performs a single configuration archive for the device. You can refer to the Management Center Inventory Event Log to view the archive progress.
3. 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 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 gear menu in the upper left corner of the Network tab or the right-click the device to 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 gear menu in the upper left corner of the **Network** tab or right-click the device and select **Configuration/Firmware** > **Compare Last Configurations**.

   For additional information about comparing device configurations, see Compare Device Configurations 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 gear menu in the upper left corner of the **Network** tab or right-click the device to select **View** > **Port Tree**.

   The Port Tree opens in a new tab.
4. Expand the components to see the device's interfaces. Right-click on an interface to:
   - access PortView for that interface
   - view interface history including interface utilization, availability, and bandwidth/packets/flows statistics
   - run scripts on the selected port
   - enable interface statistic collection
   - create policy profiles, called roles, that are assigned to the ports in your network.

In the Port Tree table, the Stats column displays whether statistics collection is enabled or disabled on the port. A black check indicates that historical collection is enabled, 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 and either click the gear menu in the upper left corner of the Network tab or right-click the device and 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. For additional information about authorization capabilities, see How to Configure User Access to Extreme Management Center Applications.

To launch a FlexView, select a device in the Device list and either click the gear menu in the upper left corner of the Network tab or right-click the device to 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. The FlexView opens in a new tab.

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. For additional information about authorization capabilities, see How to Configure User Access to Extreme Management Center Applications.

To open a user session for a device, select a device in the Device list and either click the gear menu in the upper left corner of the Network tab or right-click the device 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.

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 table and either click the gear menu in the upper left corner of the Network tab or right-click the device 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 gear menu in the upper left corner of the Network tab.
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 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 (multiple devices must belong to the same device family).
2. Click the gear menu in the upper left corner of the Network tab or right-click the device and 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 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.

- 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 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.

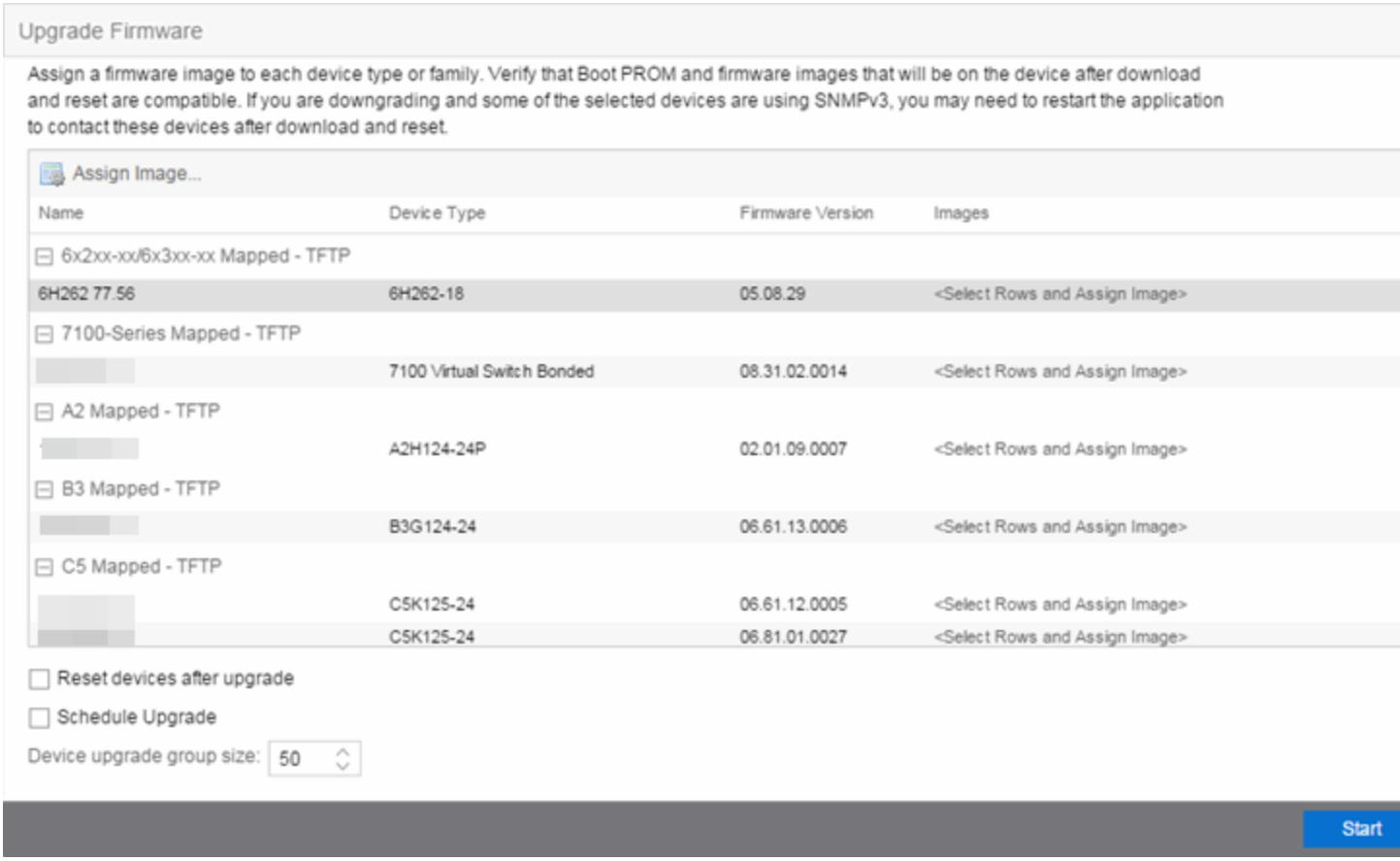
3. If you are enabling statistics collection on an Access Control engine, Application Analytics engine, or ExtremeWireless Controller, read through the following notes:
   - Extreme Access Control Engine — When collecting statistics on a Access Control engine, the active engine must be added to Management Center to collect all appliance statistics. In addition, Monitor mode is not supported on 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 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.

Update Firmware

To update devices in the Management Center database with the latest firmware releases, click the gear menu in the upper left corner of the Network tab or

right-click a device and select **Configuration/Firmware** > **Update 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. Reset devices once the firmware is upgraded via the Reset Devices window by selecting **Configuration/Firmware** > **Reset Device**.



Register Trap Receiver

To receive trap information from the devices on your network, click the gear menu in the upper left corner of the **Network** tab or right-click on a device and select **Device** > **Register Trap Receiver** from the menu.

View Device Details

Select a device in the list, click the gear menu in the upper left corner of the **Network** tab or right-click the device 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 are connected.

You can create a new map by either clicking the gear menu  in the upper left corner of the **Network** tab or right-click 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.

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 gear menu  in the upper left corner of the **Network** tab or right-click the device and 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 gear menu in the upper left corner of the **Network** tab or right-click the device and 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 gear menu in the upper left corner of the **Network** tab or right-click and use 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 gear menu in the upper left corner of the **Network** tab or right-click and select **View** > **Port Tree**.
2. Select one or more ports.
3. 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 gear menu in the upper left corner of the Network tab or right-click and select Configuration/Firmware > Register/Export Serial Numbers.
3. 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 Scripts on Devices, Ports, and Groups

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

To run a script, right-click a device, port, or group in the Device Groups left-hand panel and select a script from the Scripts menu. Additionally, you can select a device in the Devices table, click the gear menu in the upper left corner of the Network tab, and select an option from the Scripts menu. For additional information, see How to Create Scripts.

NOTE: The Scripts 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 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.
- 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.
- 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 gear menu  in the upper left corner of the Network tab 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 gear menu  in the upper left corner 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.
- Chassis ID — The ID of the chassis containing 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.

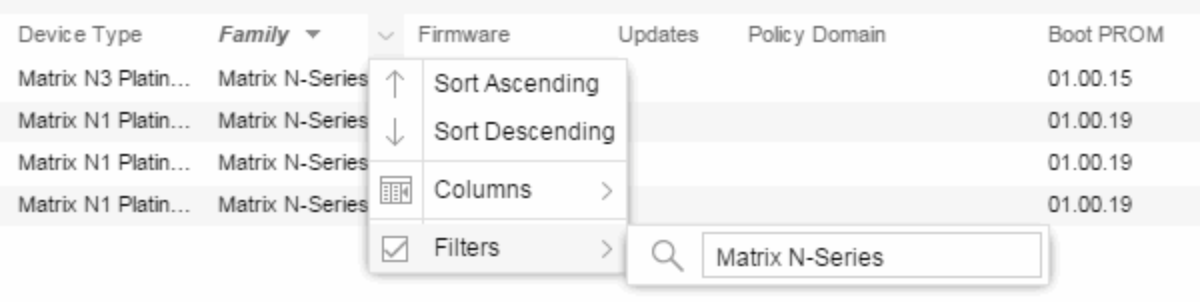
Filtering

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.

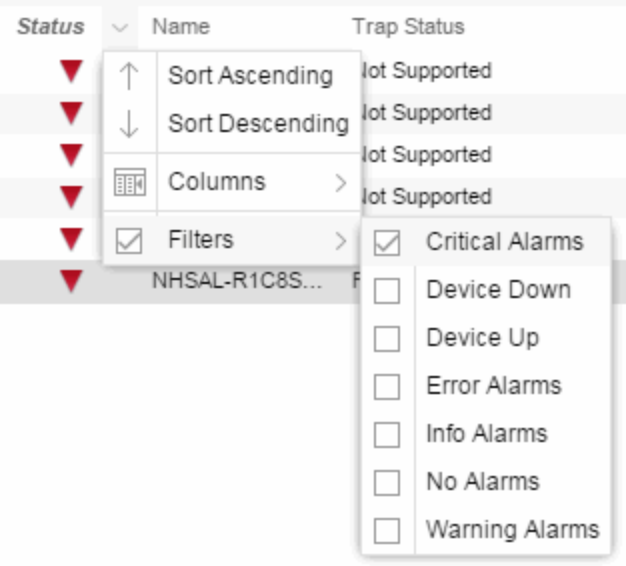
Sample Filter by Family



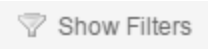
Filter by List Choices

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



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

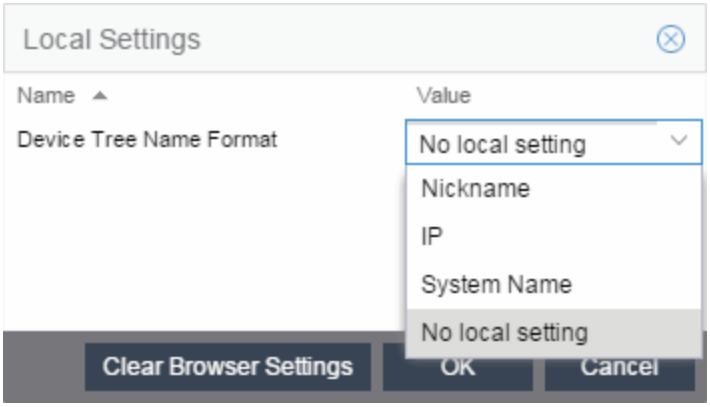
Clears the search field and search results, clears all filters, and refreshes the table.

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 Management Center settings back to the system default.

Related Information

For information on related topics:

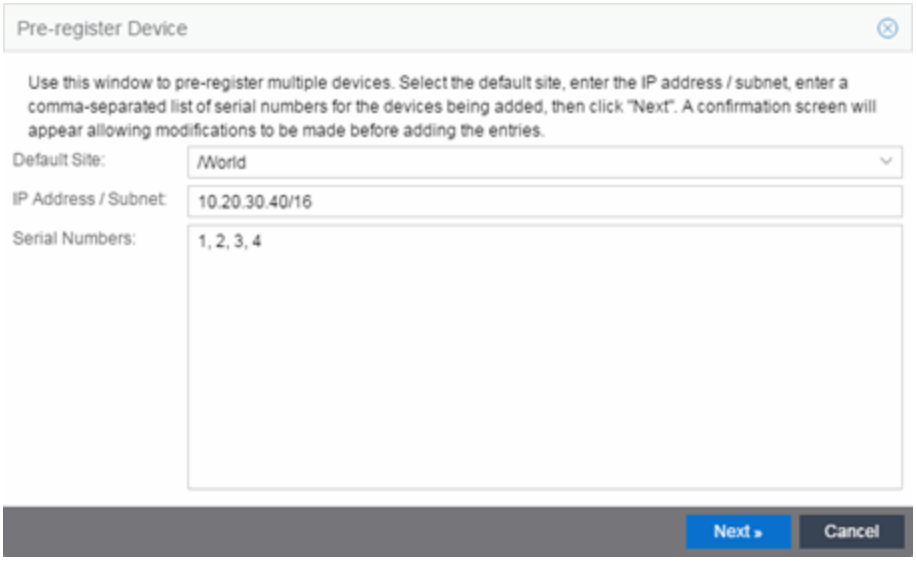
- Network Tab
- How to Upgrade Firmware
- Create and Edit Maps
- How to Create Scripts
- Compare Device Configurations in Extreme Management Center

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.

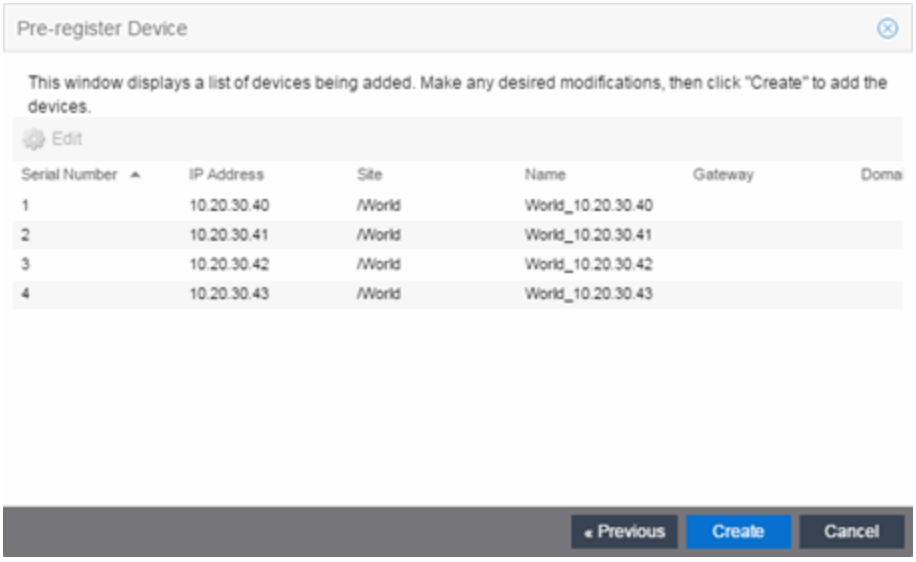
Serial Number
: Enter the manufacturer-assigned serial numbers of the devices being added, separated by commas.

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 Management Center.



Edit
: Select a device and click the **Edit** 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 Edit 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 Management Center database.

Related Information

For information on related windows:

- Discovered

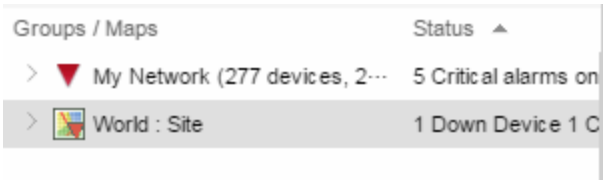
Extreme Management Center Maps Overview

The Extreme Management Center Maps feature in the **Network** 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. (For more information on authorization capabilities, see the Help topic How to Configure User Access to Extreme Management Center Applications located in Management Center Suite-Wide Tools > Authorization Device Access.)

Accessing Maps

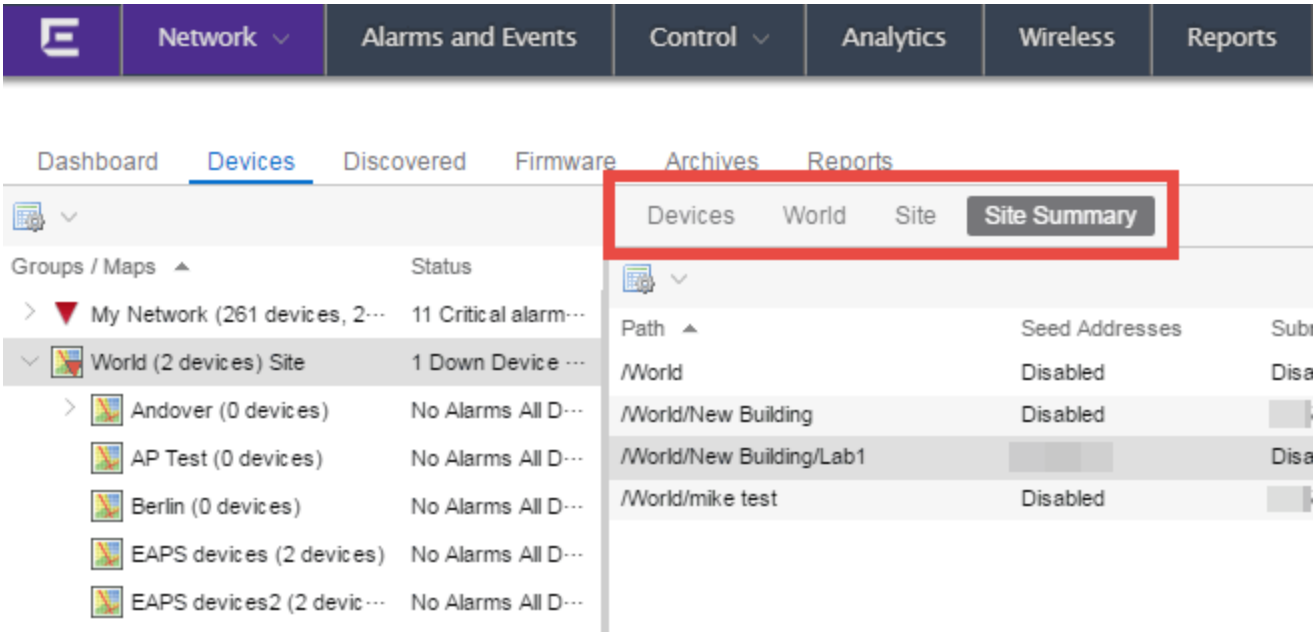
When you first open the **Network** tab, the World map navigation tree is collapsed, as shown below.



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

The Maps page contains four tabs at the top of the window:



Devices

This tab displays a table of the devices contained within the map. This table is identical to the Devices list in the My Network navigation tree above the Map Navigation tree in the left-hand panel 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 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 Maps 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
: The Site tab allows you to configure default settings for devices, discover newly added devices, and automatically add them to the current Site map. For additional information about operations available in this tab, see the Site tab.

  NOTE: When creating a new site, you must first create the map to which it belongs. This is accomplished via the **Network** > **Map** tab.

Site Summary
: The Site Summary tab contains a table of the site paths.

Related Information

For information on related topics:

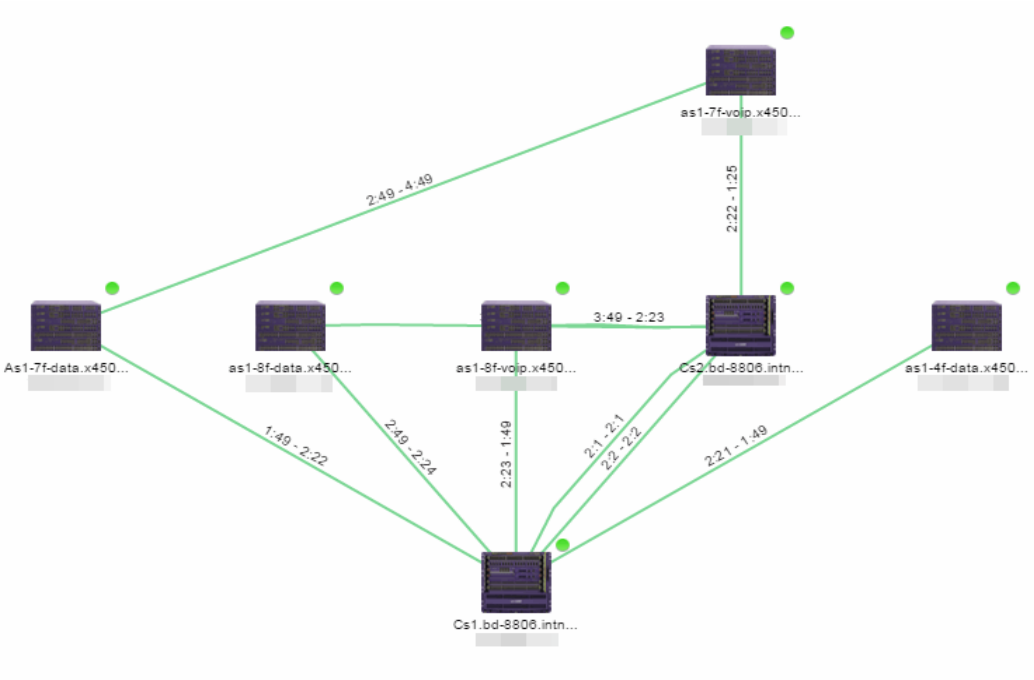
- Devices
- Maps
- Site
- How to Create and Edit Maps
- Advanced Map Features

Maps

The Map tab on the Network tab displays 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.

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.



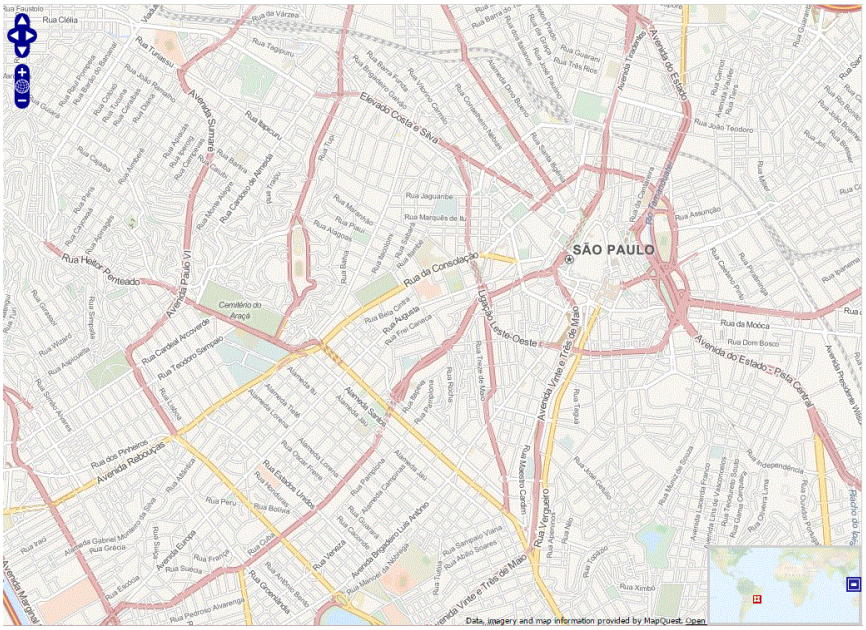
For additional information about devices and links in a Topology map, see the Viewing Alarm and Device Status and Link Information sections.

- 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 MapQuest 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 the **Map** tab.

- 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.

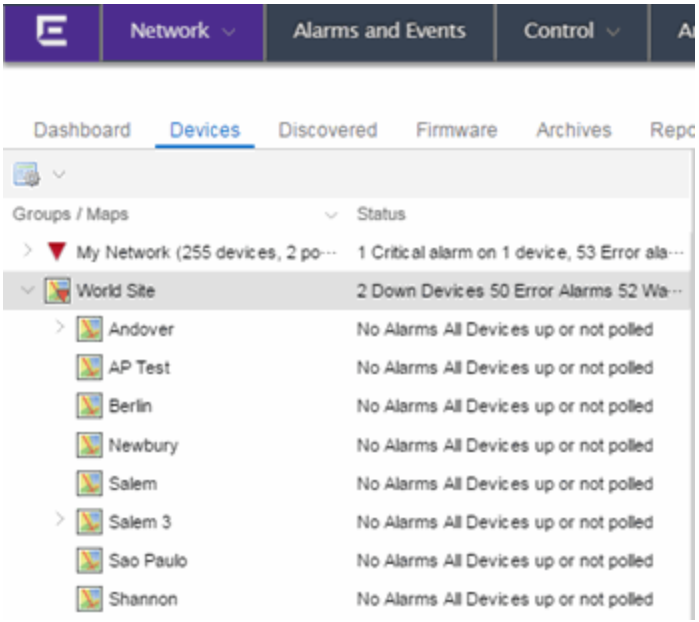
For information on advanced location (triangulation) and wireless coverage maps (available with the NMS-ADV license), see Advanced Map Features.

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. (For more information on authorization capabilities, see the Management Center Help topic How to Configure User Access to Extreme Management Center Applications located in Management Center Suite-Wide Tools > Authorization Device Access.)

Navigating the Map Tab

World Map Navigation Tree

As you create your maps, they appear in the map navigation tree, where you can select them for viewing and editing.



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 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. For additional information, see How to Create and Edit Maps.

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. For additional information, see How to Create and Edit Maps.

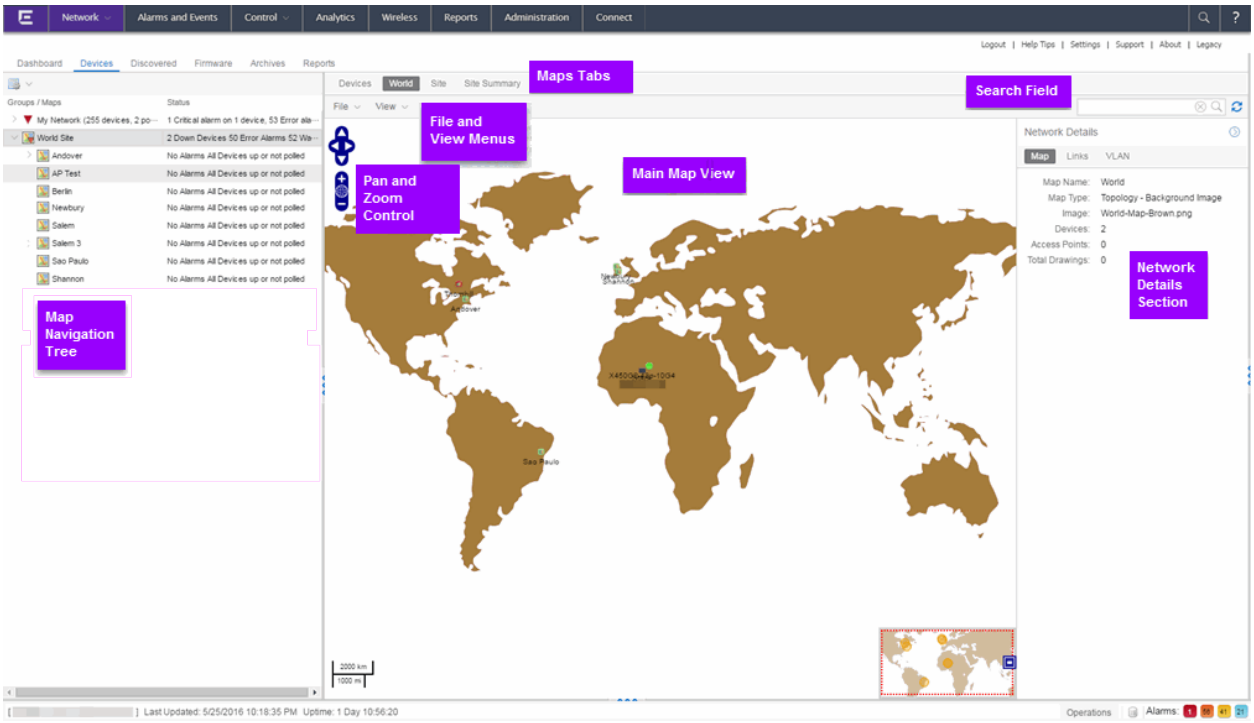
Import Map

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. For additional information, see the Import Map window help topic.

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:

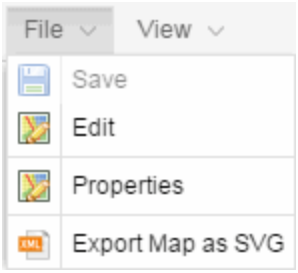
- File, View, and Tool Menus
- Pan and Zoom Control
- Search Field



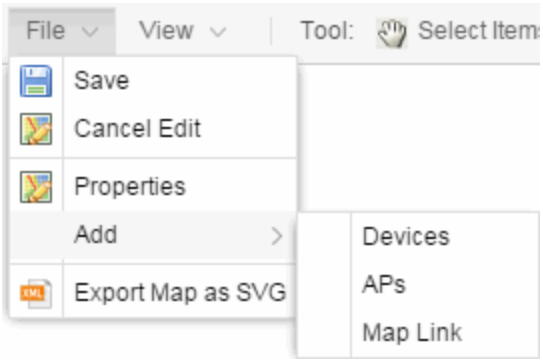
File, View, and Tool Menus

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 Management Center.



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**.

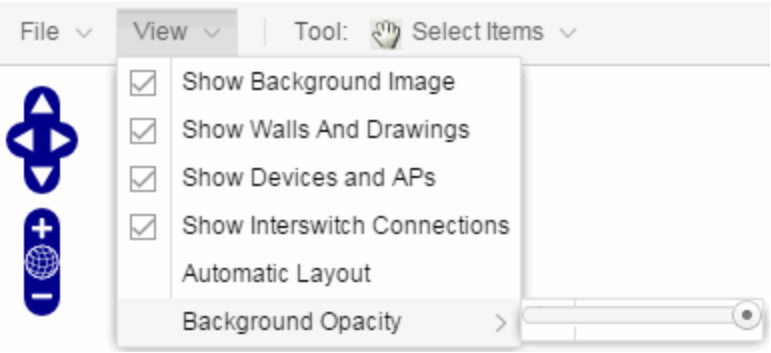
NOTE: For additional information regarding displaying VLANs in a map, see the VLAN tab section.

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 Management Center.

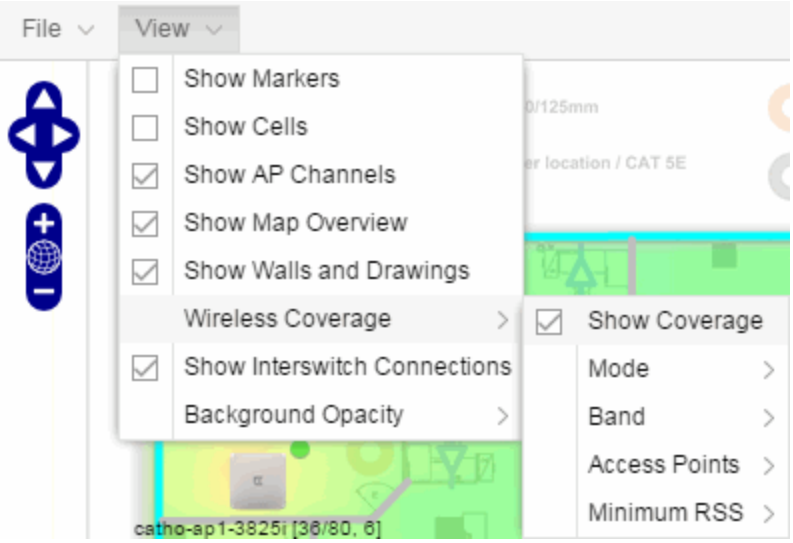
Additionally, by clicking **Edit** in the **File** menu, the map changes to Edit mode and the **Add** submenu is available, from which you can add devices, APs, and map links to the map. Edit mode also allows you to manipulate the existing devices, APs, and map links currently displayed on the map. Click **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.
	**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.

Drawing Tool	Definition
	**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 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.

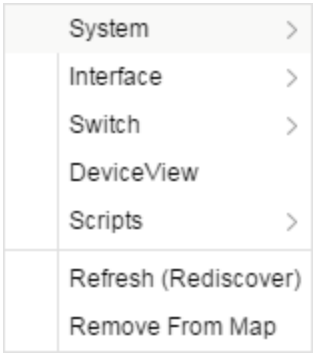
Hover over a device or AP to view a pop-up that displays the IP address for a device or channels for an AP. Additionally, click the **more** link in the pop-up to access the DeviceView or additional information about the AP for a device or AP, respectively.

Accessing Device Information

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

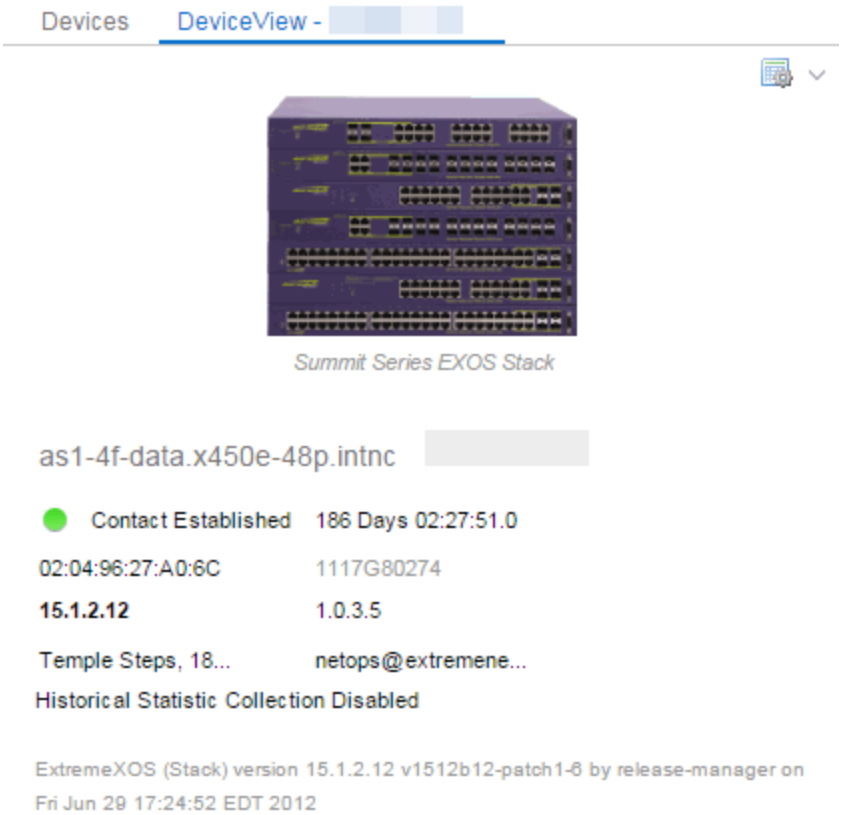
Device Reports

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.

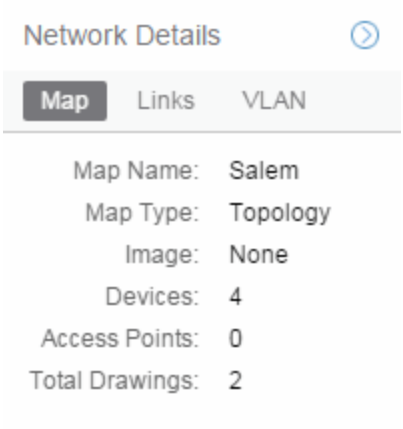
Network Details Section

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

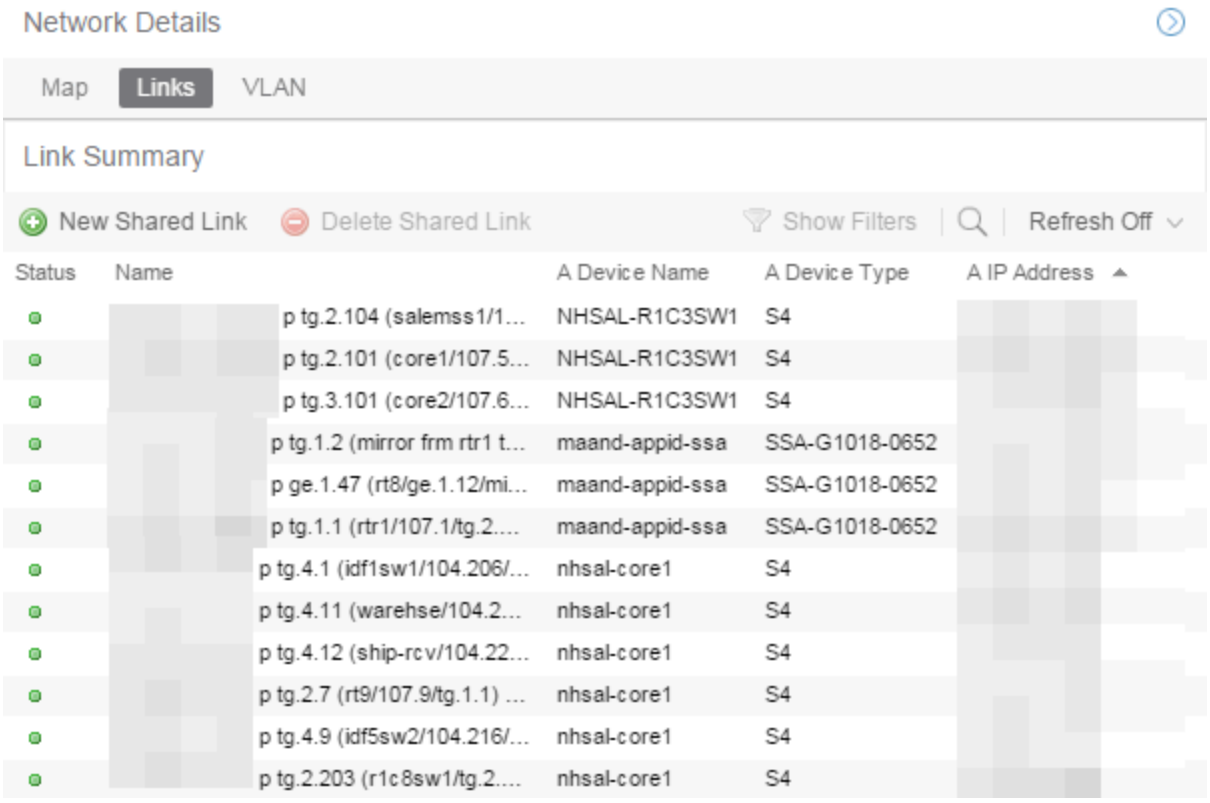
Map tab

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.

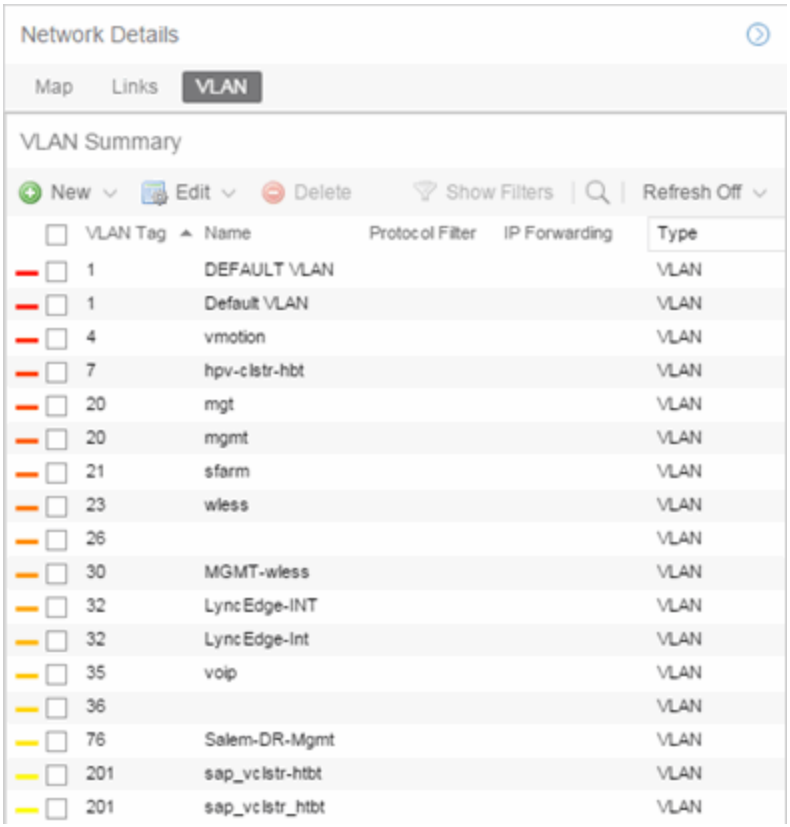
Double-clicking a link opens the Link Details window, where additional information is available about the devices the link connects.

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.

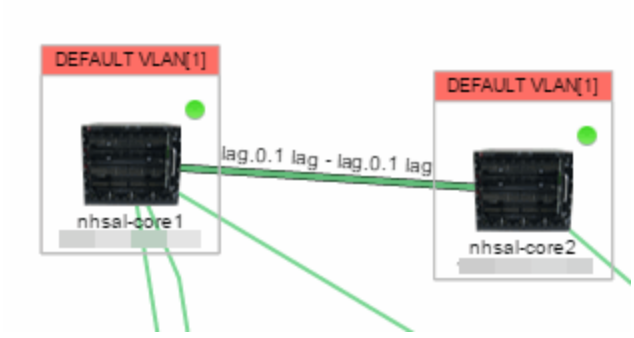
VLAN tab

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

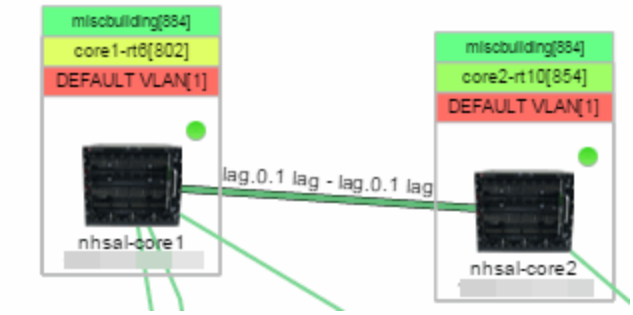
which the VLAN is configured, and whether or not IP forwarding is enabled for the VLAN.



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.



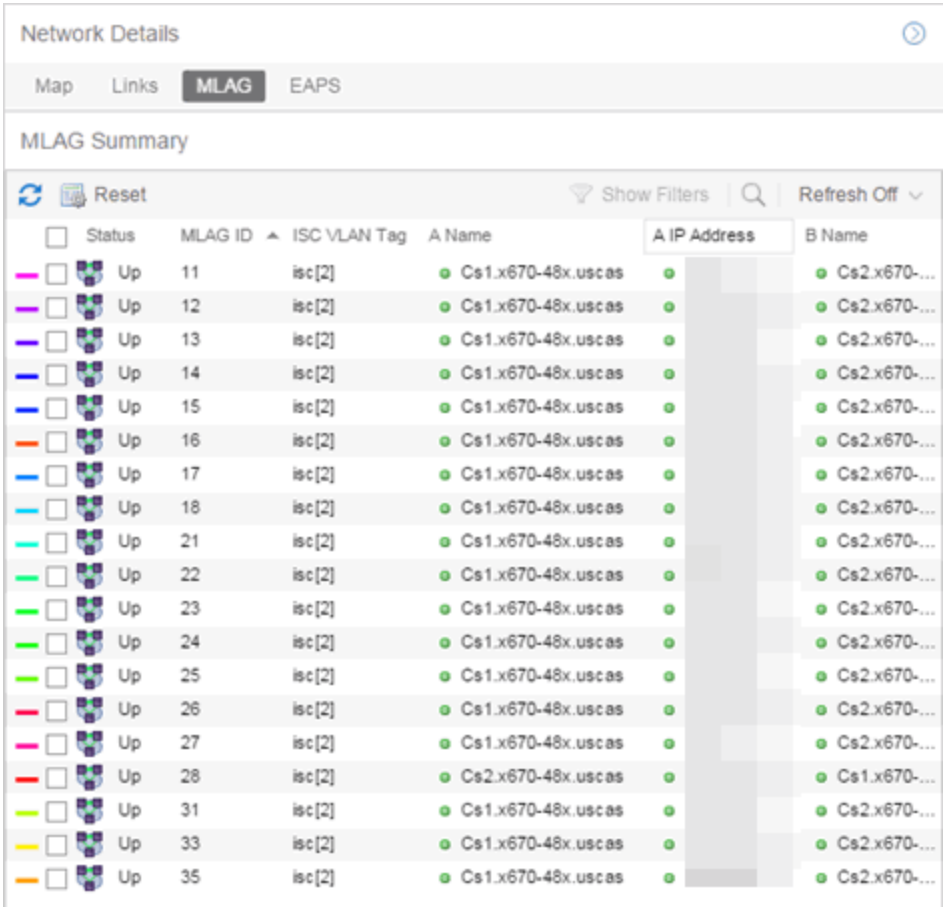
Selecting multiple VLANs assigned to the same device adds a new title bar to the box that displays the VLAN name and associated color.



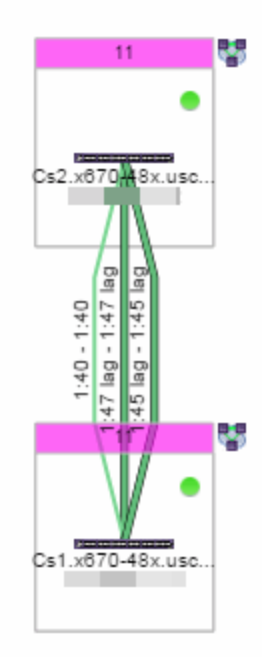
Additionally, from the **VLAN** tab, you can create a new VLAN and create a VLAN protected by an EAPS domain via the New drop-down menu or edit the ports, name, and devices associated with an existing VLAN via the **Edit** drop-down menu. For more information, see How to Create and Edit VLANs.

MLAG tab

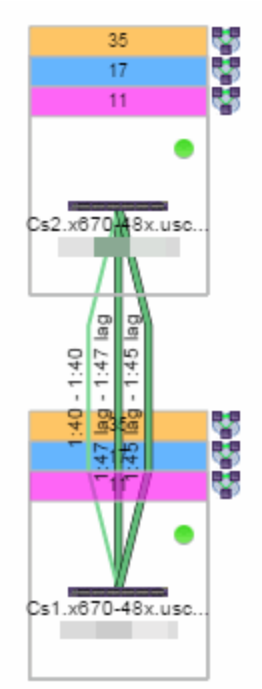
The **MLAG** tab provides a list of the MLAGs (ports combined as a common logical connection on devices) included in the map. The list provides the MLAG's status, ID, ISC VLAN tag, the names and addresses of the devices configured as part of the MLAG, and the ports on those devices assigned as part of 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.

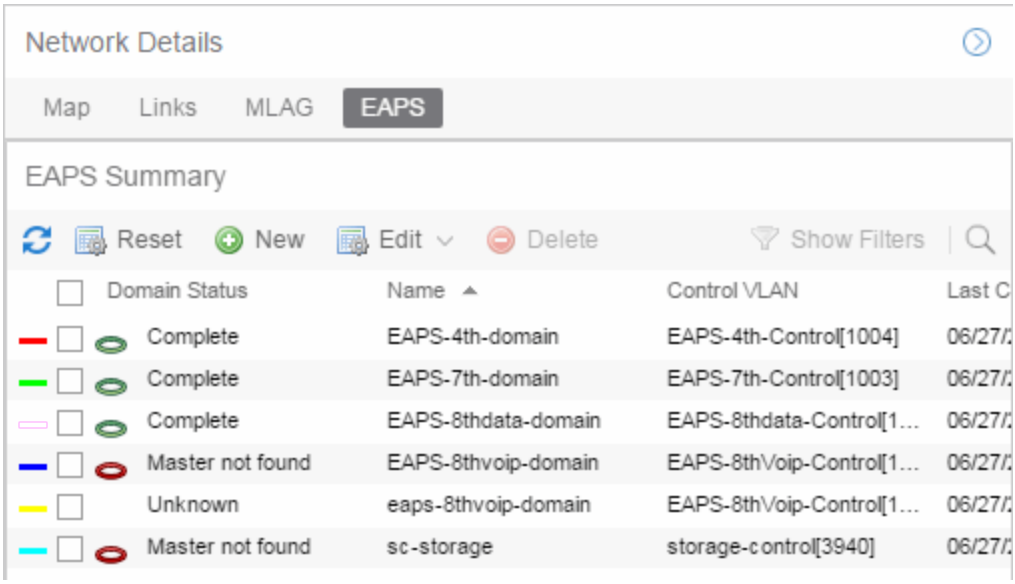


Selecting multiple MLAGs assigned to the same device adds a new title bar to the box containing the VLAN name and associated color.

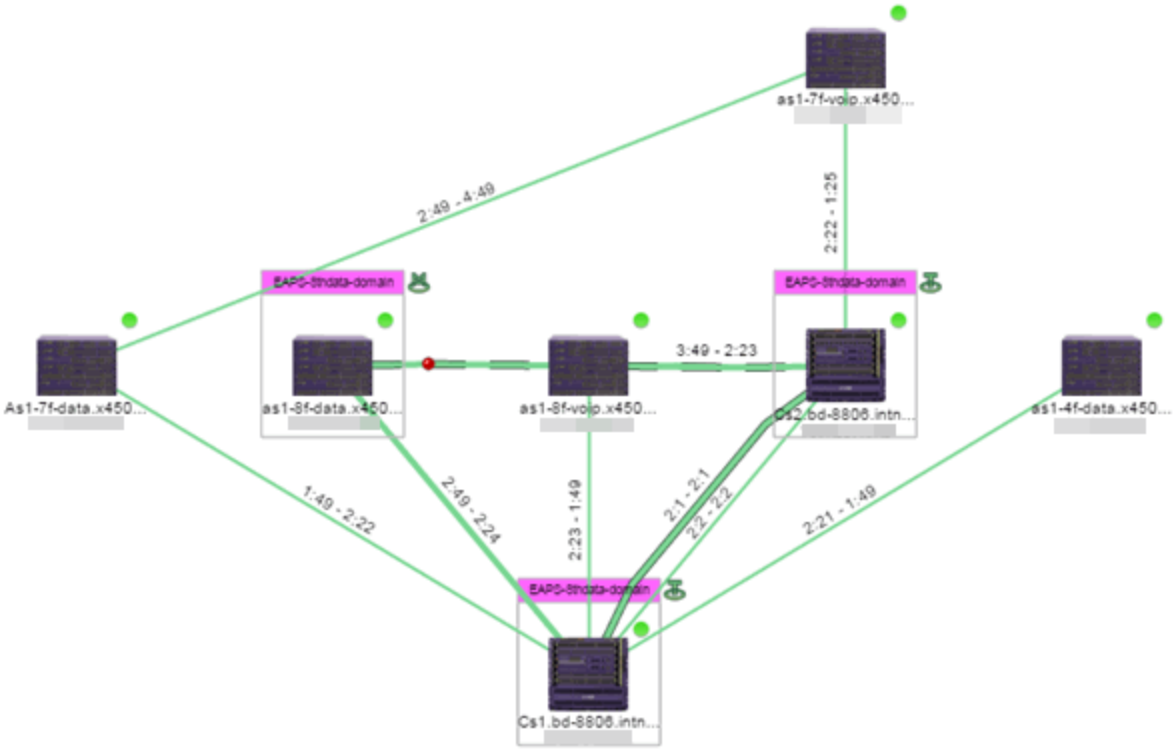


EAPS tab

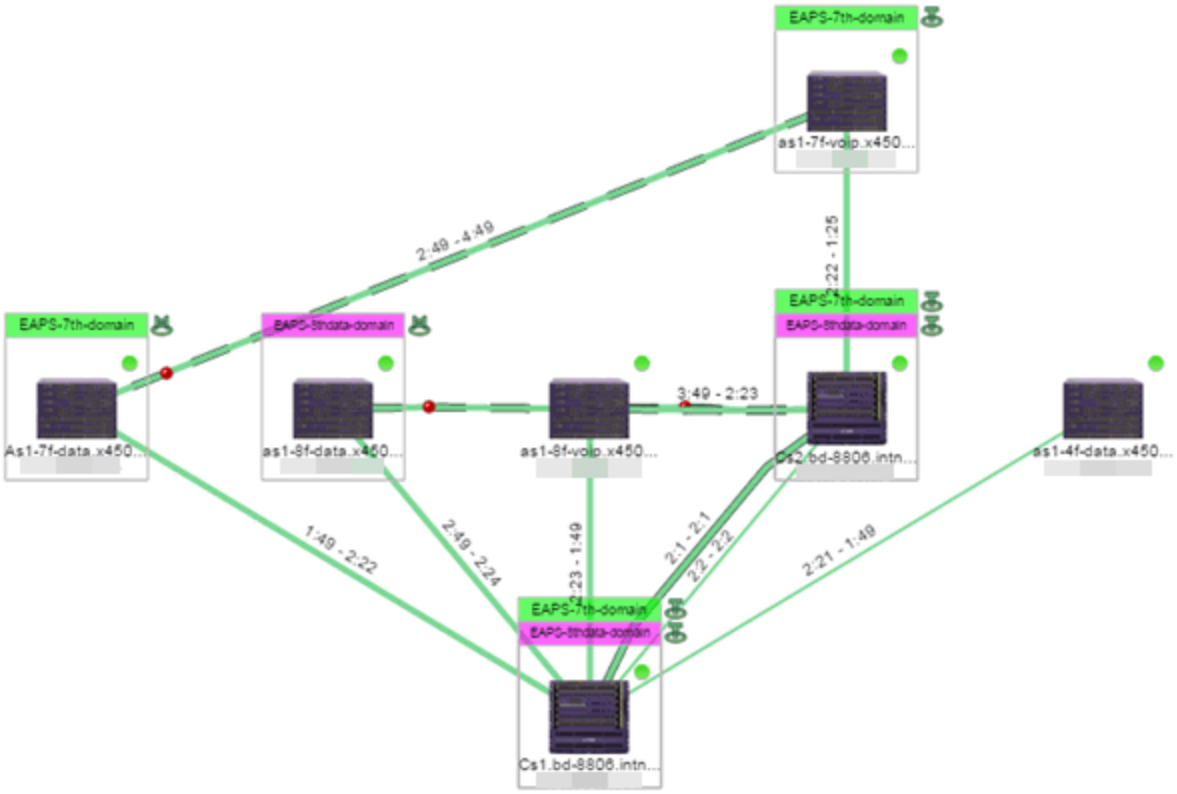
The **EAPS** tab displays a list of the EAPS domains, including their status, name, the control VLAN name, and the IP addresses of the devices utilizing the EAPS domain.



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.



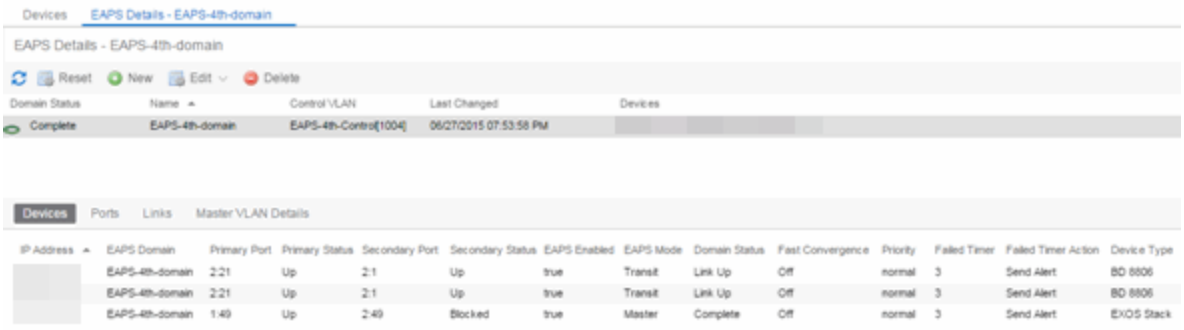
An icon next to the title bar indicates if the node is a master node, indicated by an "M" icon , or if the node is a transit node, indicated by a "T" icon .

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

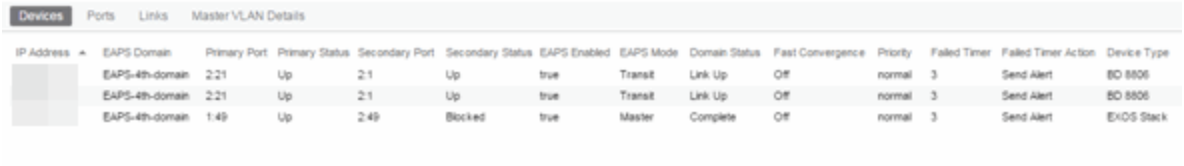
When selecting an EAPS domain, link information is also displayed. A single green line means a link that is not shared, while a dashed line between devices means the link is shared. A red dot icon on a shared link indicates the secondary link is blocked.

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.

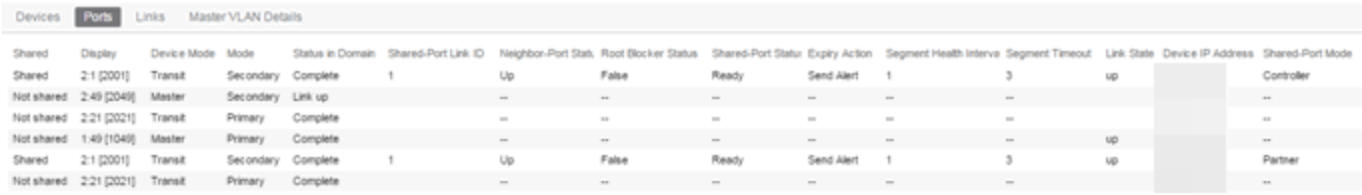


The top of the EAPS Details view displays a summary of the EAPS domain, identical to the information displayed in the **EAPS** tab. At the bottom of the window are three sub-tabs, which display additional information:

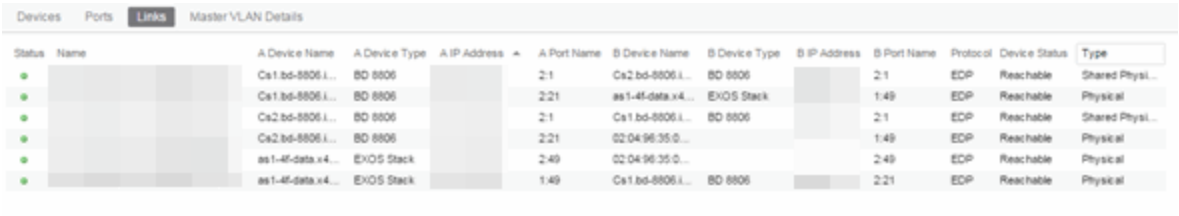
- **Devices** — Displays information about the devices using the EAPS domain.



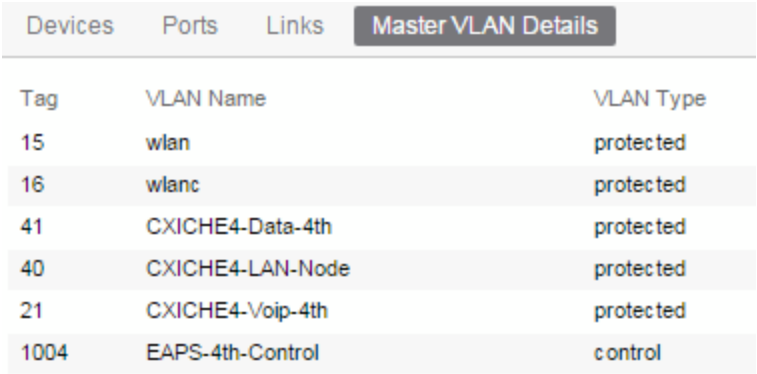
- **Ports** — Displays information about the shared ports associated with the EAPS domain.



- 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 Management Center, outlined below.

Finding a Wireless Client

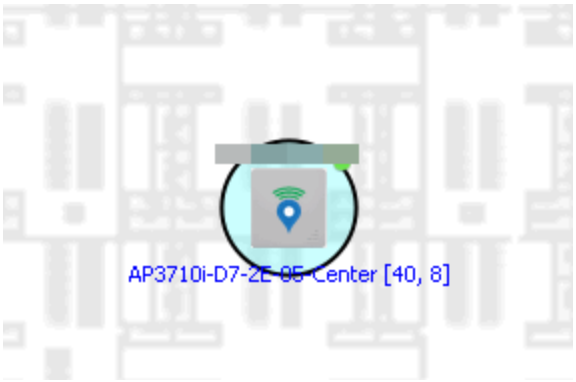
From the Search Field on the Network Tab

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

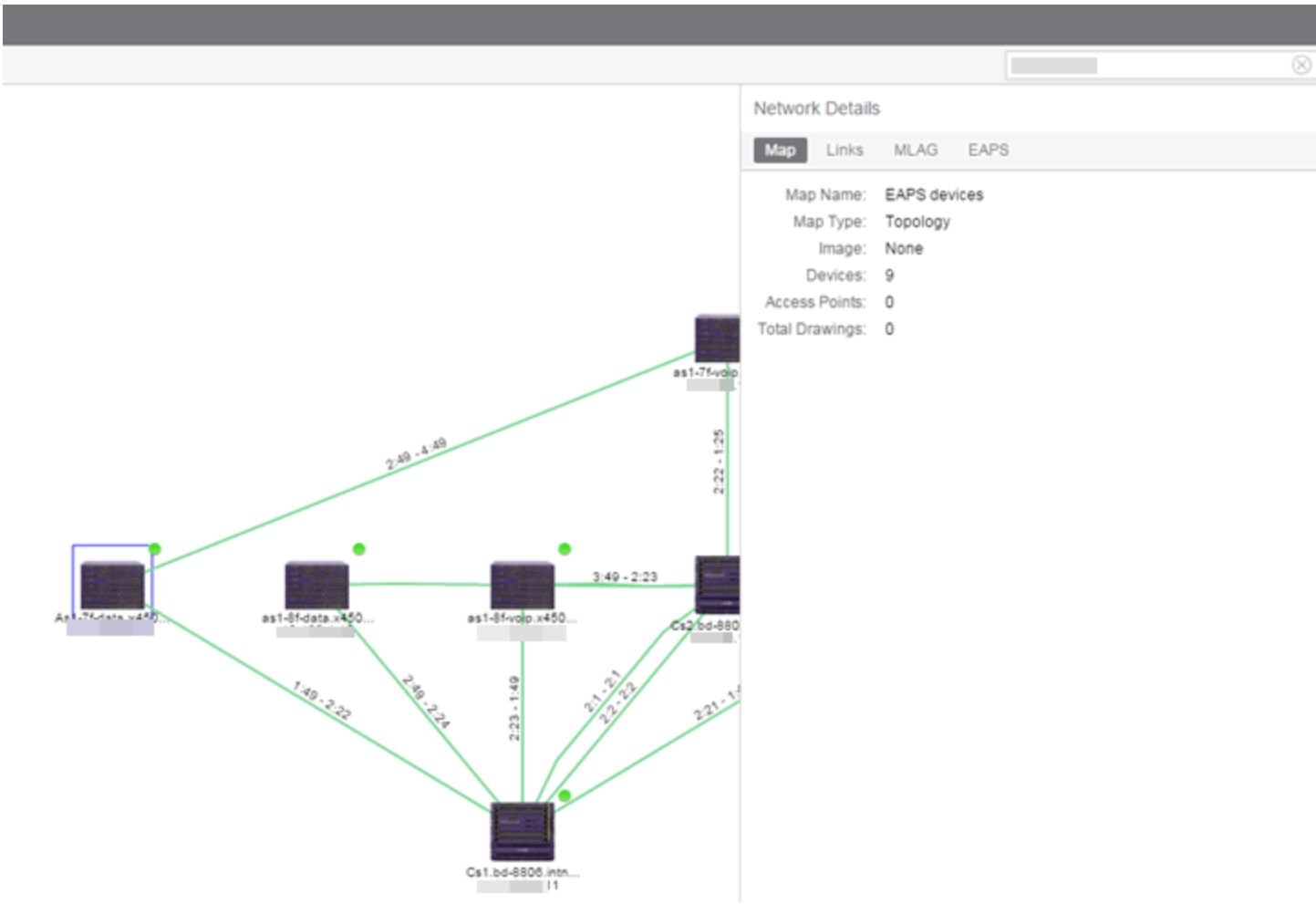
You can locate an AP from the Wireless > APs Summary report on the **Reports** tab. Select an AP in the table, right-click and select **Search Maps**. If a map contains the AP, the map opens with the AP centered on the map.

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 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 a Access Control authenticated wired client from the **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.

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.

You must be in Edit mode to add a link to a map. For more information, see How to Create and Edit Maps.

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

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 Management Center, see Extreme Management Center Maps.

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

- Creating a New Map
- Importing a Map
- Adding Devices/APs from Extreme Management Center Devices and Wireless
    - Add to a Specific Map
    - Add to New Maps Based on Location
- Adding Map Links
- Setting the Map Scale

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. (For more information on authorization capabilities, see the Help topic How to Configure User Access to Extreme Management Center Applications located in Management Center Suite-Wide Tools > Authorization Device Access.)

Creating a New Map

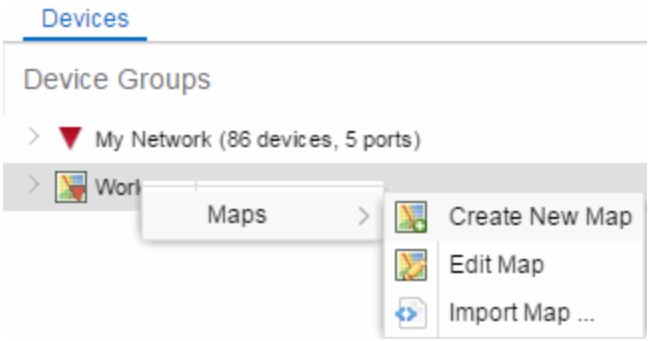
The instructions in this section describe how to create a new Device map.

1. Launch Management Center and click on the **Network** tab.
   For a description of the different sections on the **Network** tab, see the

Network tab help topic.

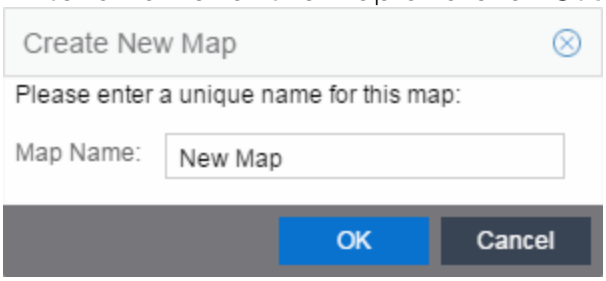
2. Open the **Devices** tab.
3. In the left-panel Groups/Maps navigation tree, right-click on the World Site (or any other map in the tree) and select **Maps** > **Create New Map**.

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



The Create New Map window, shown below, opens.

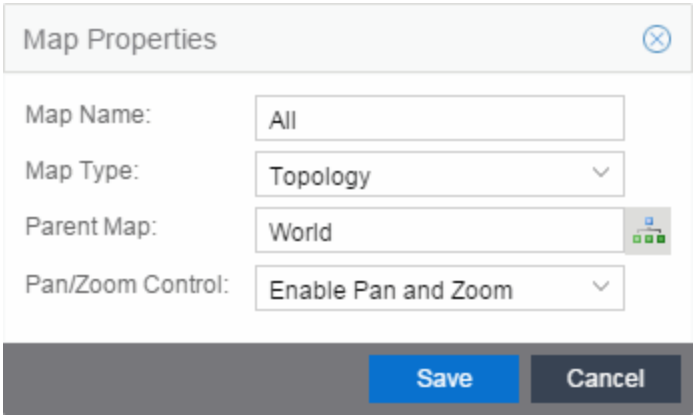
4. Enter a name for the map and click **OK**.



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 gear menu or right-clicking the device or AP and selecting **Maps** > **Create New Map**. To begin adding devices, APs and links to the map, proceed to Step 5. Proceed to Step 4 to edit the map properties.

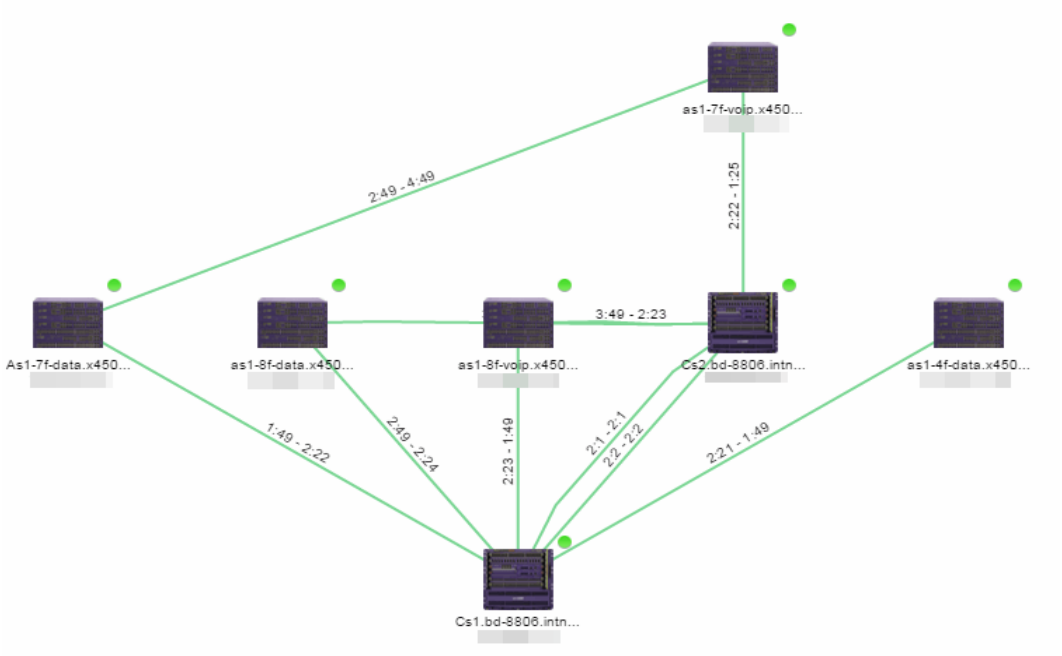
5. Click **File** > **Properties** to open the Map Properties window from which you can edit the map criteria.



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 Image — 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 890 x 670 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 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.

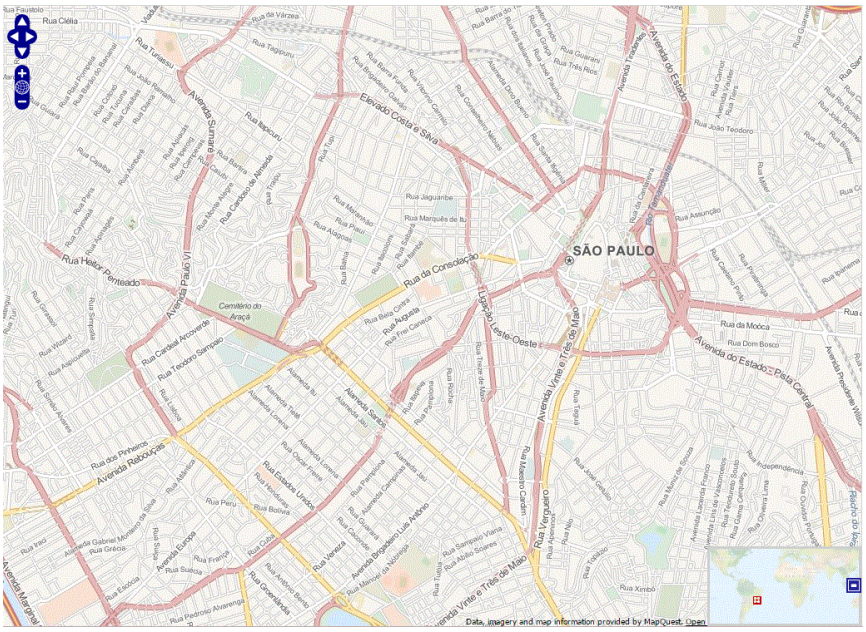
An additional Floor Plan option is available for users with the Management Center NMS-ADV license. For information on creating a custom floor plan design, see Designing a Floor Plan.

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 the **Add** ( ) button to open a window where you can select a local image and upload it to the Management Center server.

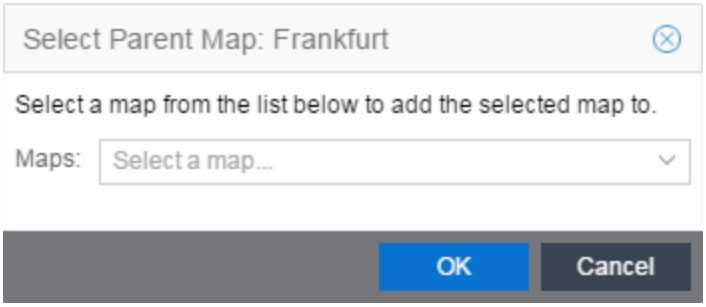
NOTE: If you upload a map image and an image with the same name already exists, the existing image is replaced.

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

NOTE: The geographic map type is hosted by MapQuest 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.



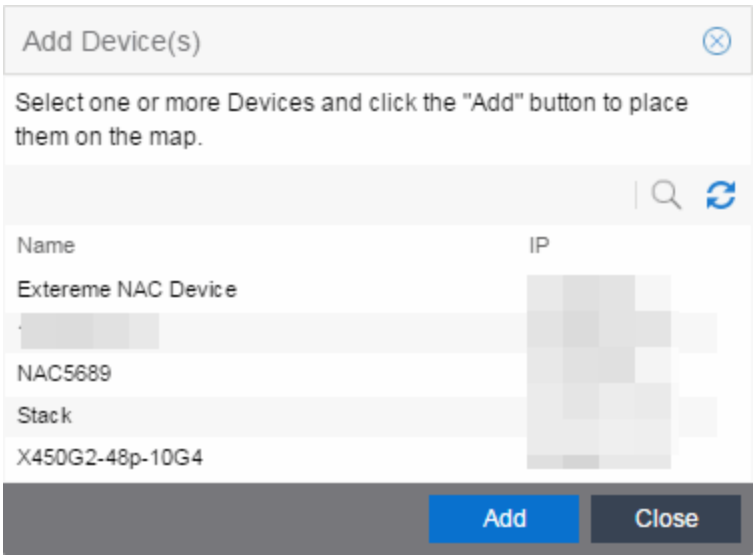
d. Click **Save**.

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.

6. 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 field 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.

7. 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.
8. Click File > Save button to save the map.

NOTE: Map devices and APs do not show their current status until you save the map.

9. 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 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

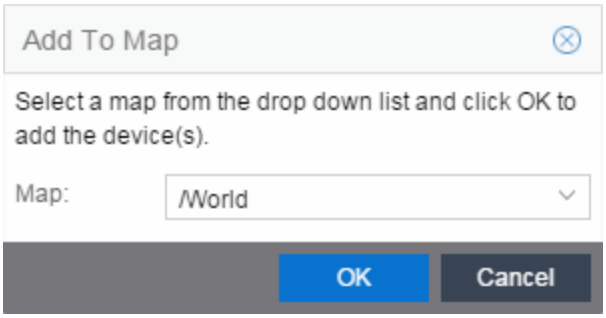
You can quickly add devices and APs to your maps directly from the My Network navigation tree on the Management Center **Network** and **Wireless** tabs. You can add them to a specific map, or create new maps based on device or AP system location.

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** tab, 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**.

2. 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.



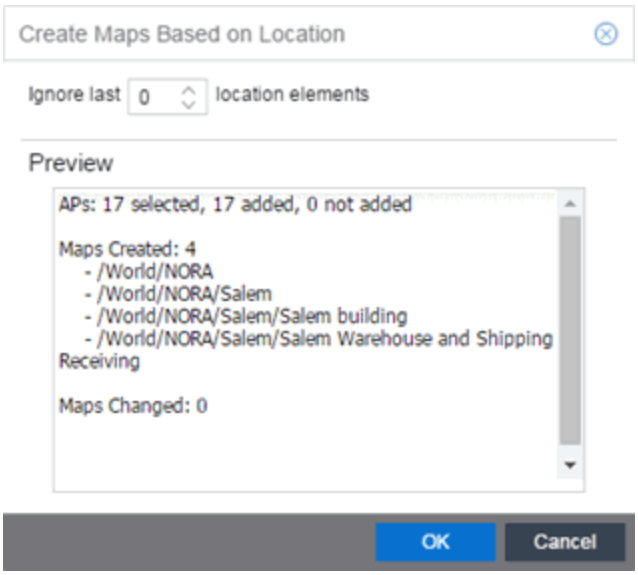
3. Open the Maps page and select the map to which you added the devices. Right-click on the map and select **Edit Map**. You can now position the devices as desired.
4. Click the **Save** button to save the device to the map.

Add to New Maps Based on Location

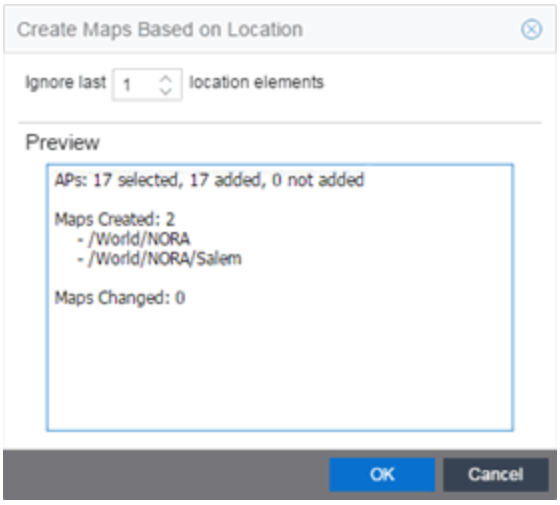
Use these steps to add devices or APs to new maps based on well-named system locations that reflect the desired map structure. For example, if your devices are assigned system locations according to the following structure: US/Boston/Third Floor/Closet One/Rack One/Shelf One, typically, a map would be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

Adding Map Links

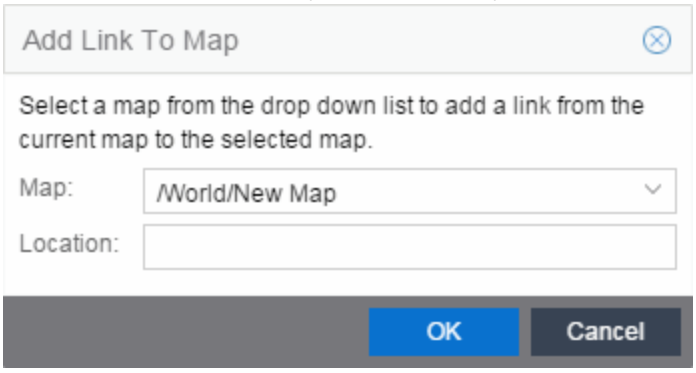
You can use map links to jump from one map to another. Map links display the name of the map and an aggregated alarm/device status for the linked map. Double-click on the link to go to the linked map.

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 drop-down menu, select the map to which you want to link and click **OK**.
5. The map link is added to the map and can be repositioned, if desired.
6. Click the **Save** button to save the map and close the properties panel.

Importing Maps

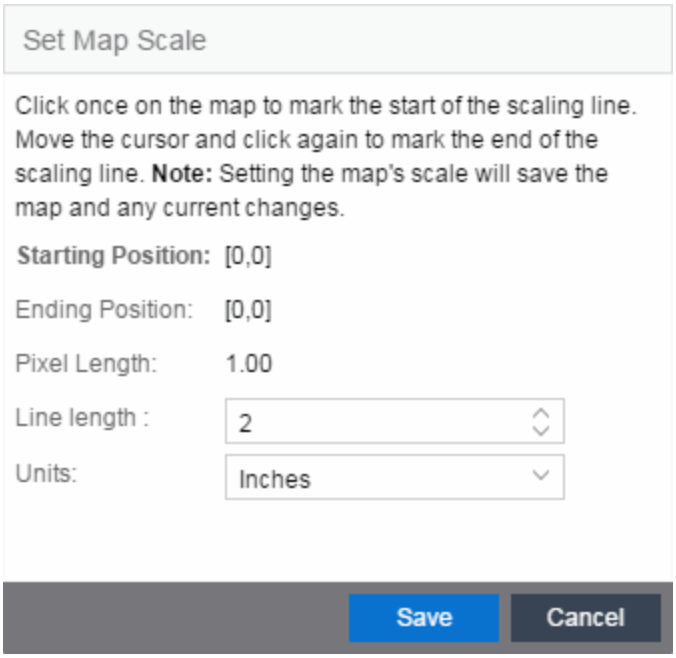
You

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 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

Advanced Map Features

The Network 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.

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 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 Management Center advanced Map features:

- To access the advanced Map features, the Management Center server must be running version 6.2 with a 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. (For more information on authorization capabilities, see the Management Center Help topic How to Configure User Access to Extreme Management Center Applications located in Management Center Suite-Wide Tools > Authorization Device Access.)

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 Floor Plan

You can design and enhance floor plans 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 floor plans 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 floor plan.

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

NOTE: To prevent the automatic synchronization between 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 floor plan 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.

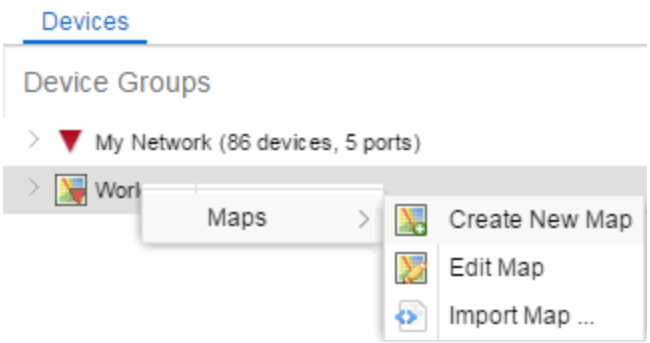
The wall information from the floor plan is used to help determine the degradation of signal strength that occurs as a wireless radio signal passes through the walls, and helps define the probable distance of a client from a given access point. Management Center uses the wall information to provide accuracy in determining wireless device signal strength.

A floor plan 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 floor plan 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 floor plan.

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

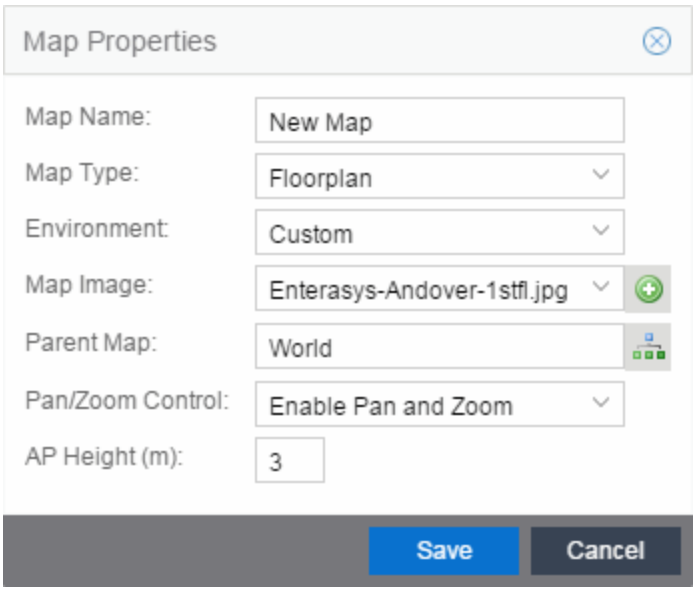
The following steps provide a workflow for creating a floor plan showing the exterior and interior walls of a building. By drawing the walls over an existing floor plan image, you can add information that provide greater accuracy in wireless calculations.

1. Create and configure a new map.
    a. Launch Management Center and click on the Network tab.
    b. In the left-panel 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**, and upload the floor plan image you want to use. 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. (You can also create a floor plan without a background image by setting the Base Map option to Empty.)

f. Set the **Environment** option to **Custom**. This allows you to draw walls over the existing image.

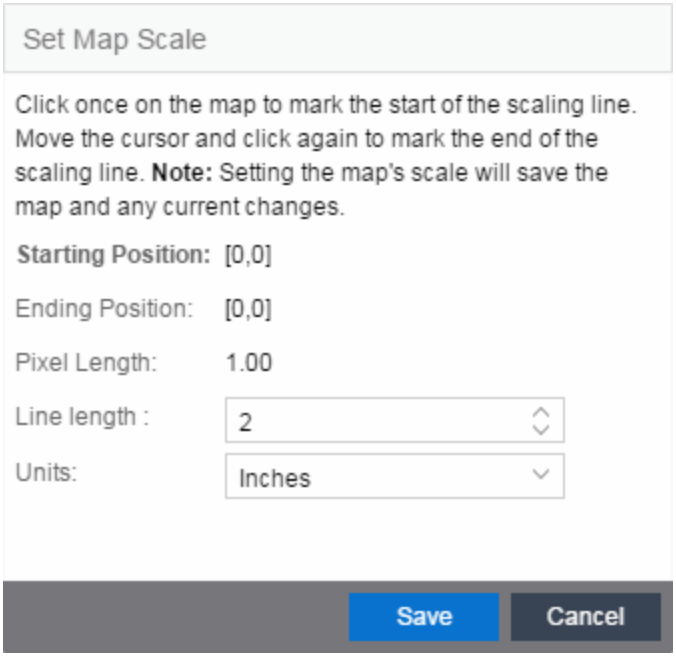
g. Set the **AP Height** property. This value is the distance from the floor to the AP position on the wall or ceiling in meters. This is a single value used for all access points. Setting a reasonable value helps with the accuracy of the location feature. The default for this value is three meters,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

h. 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 floor plan 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.

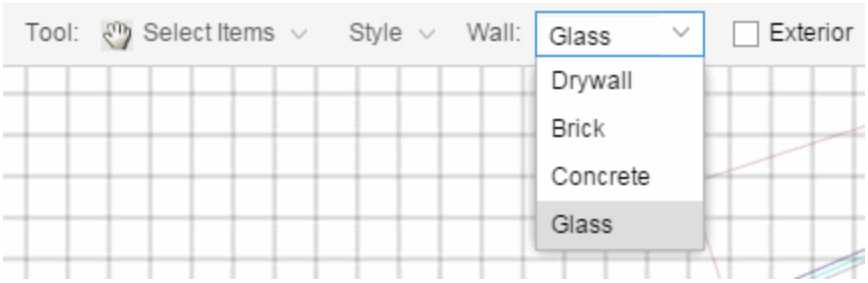
   ii. Enter the line length and units.

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

3. **Draw floor plan 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 floor plan 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 floor plan area included in wireless client location and wireless coverage maps, and should be drawn around the entire perimeter of the floor plan 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 floor plan. Be sure to deselect the **Exterior** checkbox for the other walls.

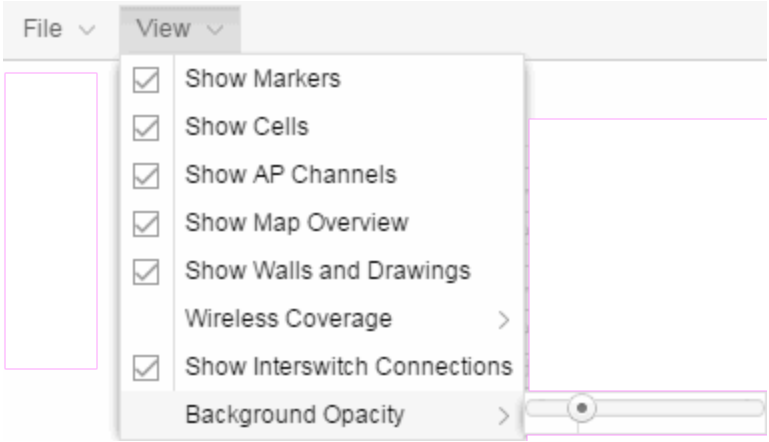
   You can trace over existing walls on the floor plan or add new walls, if necessary. Focus on high attenuation walls like concrete or large sections of glass. It is not necessary to incorporate walls and structures that do not fully divide the space, such as half-walls or cubicles.

   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, floor plan walls and drawings, devices and APs, and interswitch connections. You can also select an automatic layout and set the background image opacity.

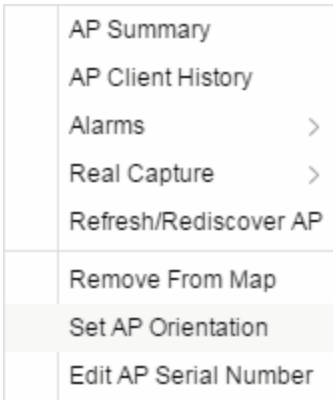


4. **Add your APs to the map.** In Edit mode, a panel that lists equipment available to add to the map is visible beneath the properties panel. The display is filtered on either the currently discovered devices or the APs

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.

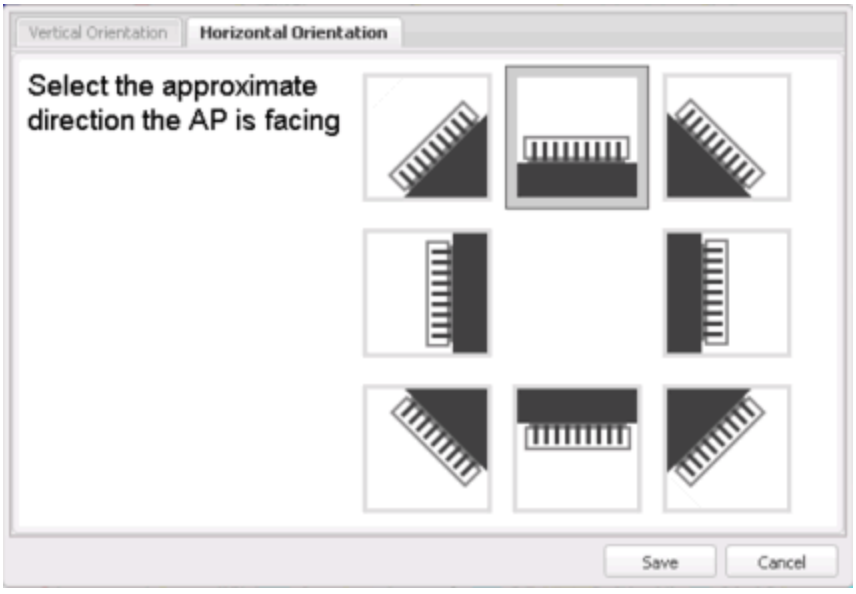
Drag the desired devices and APs onto the map area and position them to produce your network map. Be sure the APs are in the correct location, so your location and coverage maps are accurate. The center of the image is roughly the position of the AP. Be sure to place an AP on the correct side of a wall.

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



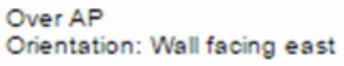
b. Click on the **Vertical Orientation** tab to set whether the AP is on the ceiling or wall.

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.



6. Click Save to save the map. The floor plan 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 floor plans. 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 policy 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. Double-click to release the area line. When you are finished drawing, right-click to release the draw area tool and open the Configure Area window. For additional information, see Configure Area Window.

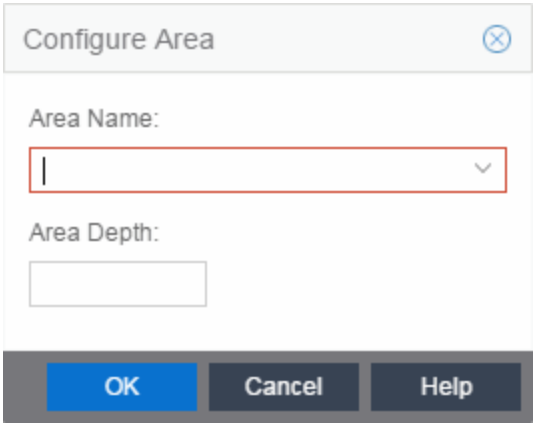
Drawing Tool	Definition
	**Draw Polygon** Position your cursor where you want to start drawing the polygon shape. Click once and draw the first line of the polygon. Click at each corner of the polygon. Double-click to release the polygon line. When you are finished drawing, right-click to release the 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.
	**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 floor plans. Following are definitions of the Style menu options.

Style Option	**Description**
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 floor plan.
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 floor plan and save the map, a copy of the floor plan is sent to each controller. The location engine incorporates information defined in the floor plan 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.

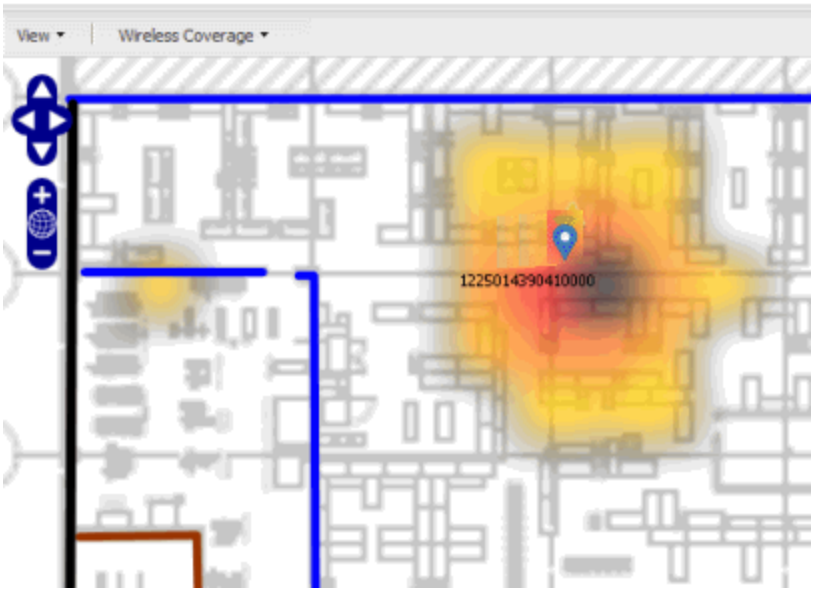
To search for a wireless client, enter a MAC address, IP address, hostname, or user name in the map Search box and press Enter. (The client must be connected to an AP added to a map.)

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.

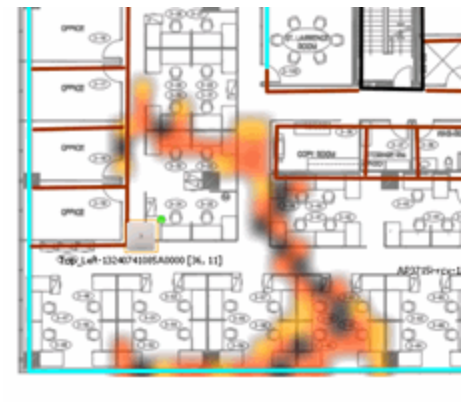
Triangulated Location



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

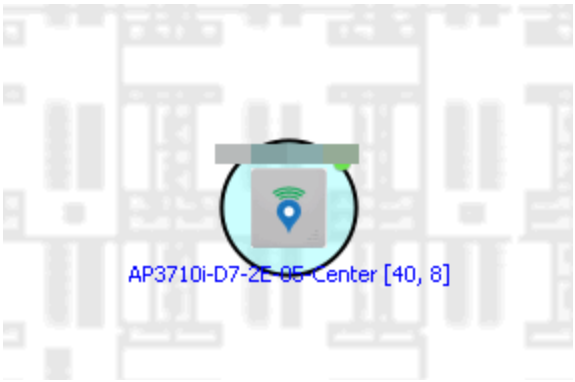
- No client icon is displayed.
- The location confidence distribution area is larger and generally displayed in a circular pattern.
- The associated AP is highlighted.
- The distance is shown beside the confidence legend at the foot of the map.

Location with One AP



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).

Location Based on Client RSS



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 floor plan 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 Management Center floor plan maps. The map export function exports floor plan maps to a ZIP file.

Importing Maps

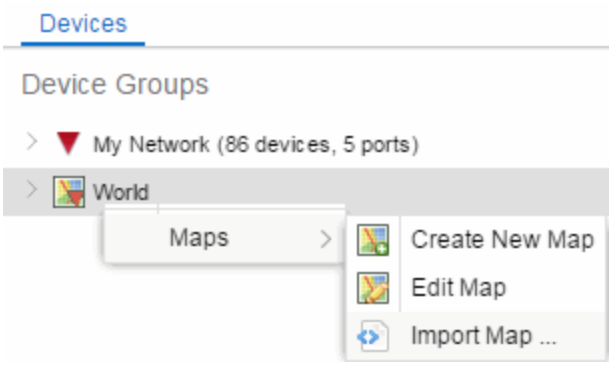
The map import function gives you the ability to import Ekahau maps into Management Center floor plan maps and gives you the ability to import floor plan maps are previously exported from Management Center maps.

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

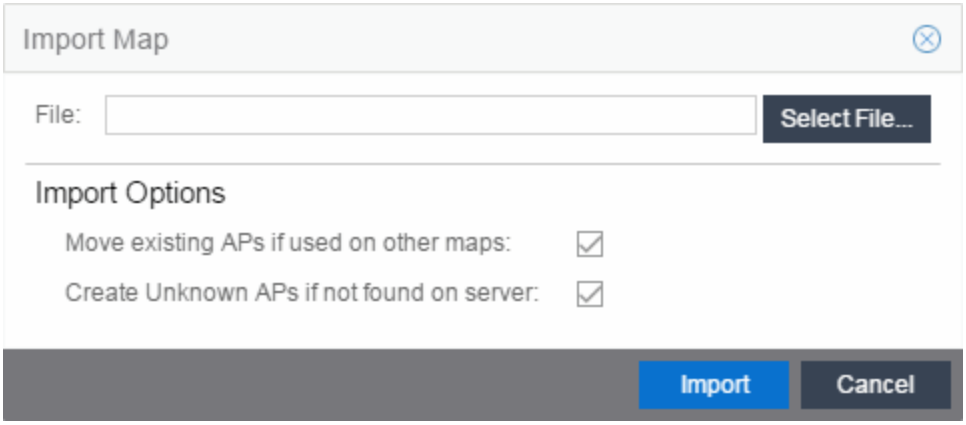
When a map is imported, it is added as a child map of the World map. If the map's name is not unique, a number is appended to the end of the name. After the map is imported it can be moved and renamed, if desired.

To import a map:

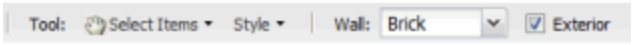
1. Launch Management Center and click on the **Network** tab.
2. In the left-panel Maps navigation tree, right-click on the World map and select **Maps** > **Import Map**.



3. The Import Map window opens. Use the **Select File** button to navigate to the map file to import.



4. 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 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.
5. Click Import.
6. The map is imported and positioned under the World map. It can be moved and renamed, if desired.
7. All the walls in an Ekahau map are imported as internal walls. You need to manually edit the exterior walls after the floor plan 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.



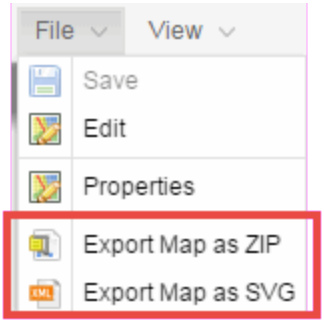
   c. Click Save to save the map.

Exporting Maps

The map export function gives you the ability to export floor plan maps as a ZIP or SVG file.

To export a map:

1. Launch 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.

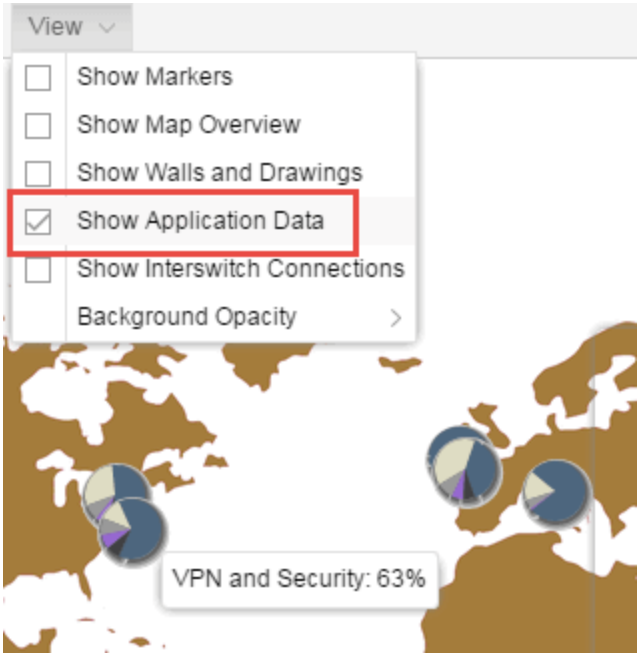
NOTE: The Export Map as ZIP option is only available for Floorplan map types.

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.

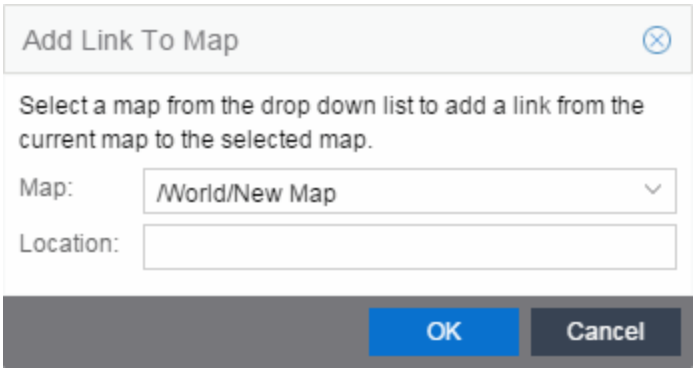
When the **Show Application Data** checkbox in the **View** menu is selected, a pie chart is generated for every map link on the current map. The application data in the pie chart is based on the Location field specified for the link and corresponds to a network location defined in the Application Analytics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

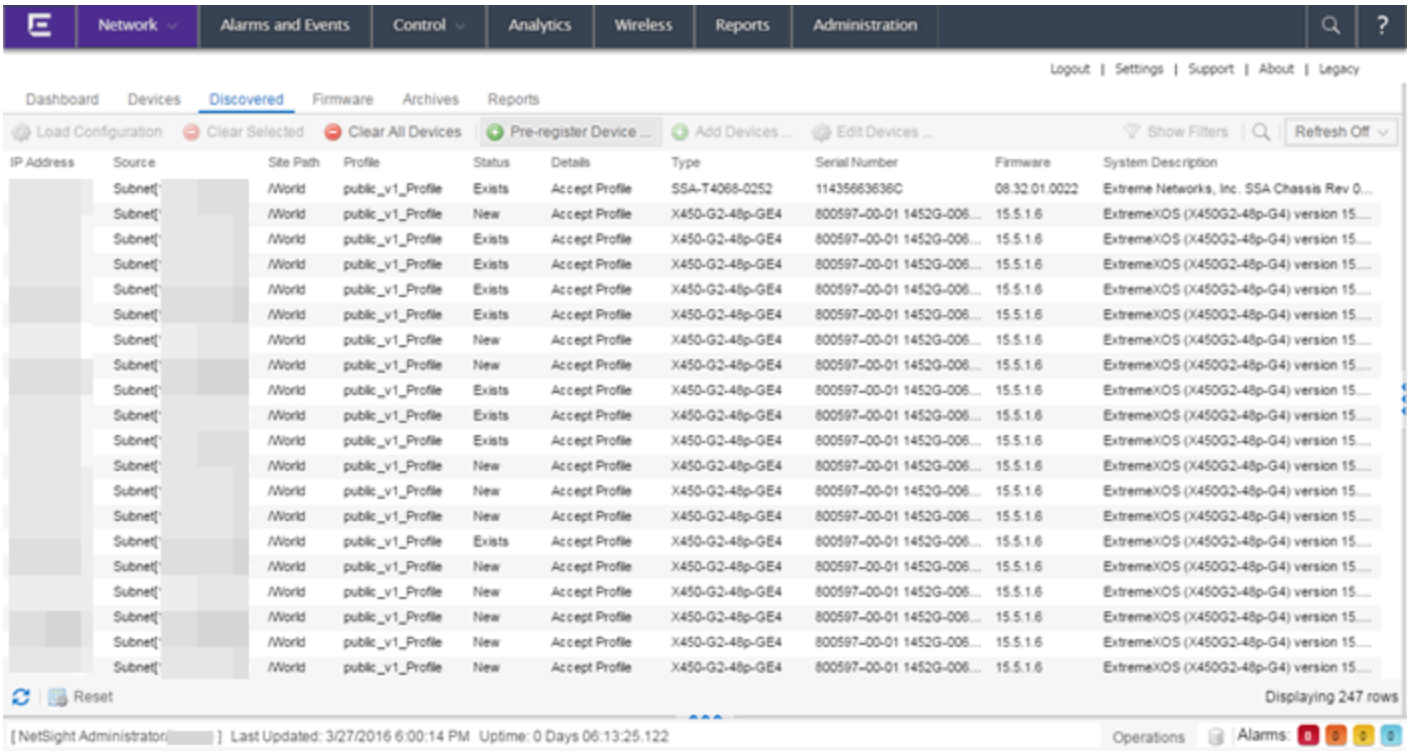
Related Information

- Extreme Management Center Maps Overview
- How to Create and Edit Maps

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.

Columns

The columns on the **Discovered** tab display the details about the devices available to be added to the 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 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. For additional information about sites and maps, see the Maps Overview help topic.

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. For additional information about profiles, see the Profiles help topic.

Status
: The **Status** column indicates whether the device exists in the Management Center database:

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

Management Center. For additional information about profiles, see the Profiles help topic.

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.

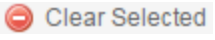
System Description
The System Description provides a complete description of the device.

Toolbar Buttons

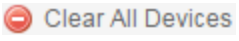
The toolbar at the top of the tab allows you to perform various tasks on the devices on the **Discovered** tab.

Load Configuration 

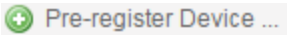
Click to open the Load a configuration on a Discovered Device window, which allows you to use a saved configuration for an existing device on a ZTP (zero touch provisioning) enabled device.

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 Management Center database.

Edit Devices 

Opens the Edit 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 Upgrade Firmware

Load Configuration on a Discovered Device

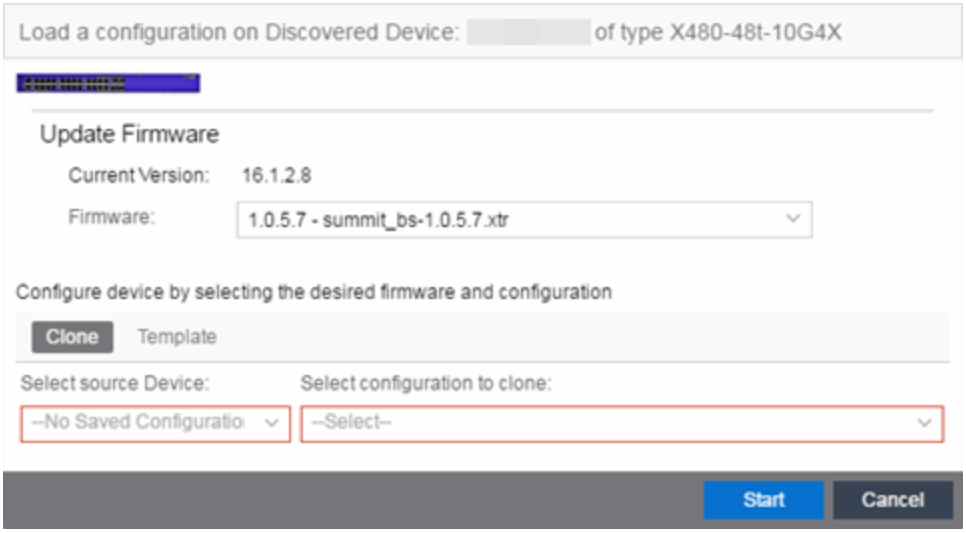
Use this window to use a saved device configuration on a device you are adding to Extreme Management Center. Devices to which you load a saved configuration must have ZTP (Zero Touch Provisioning) enabled.

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 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.

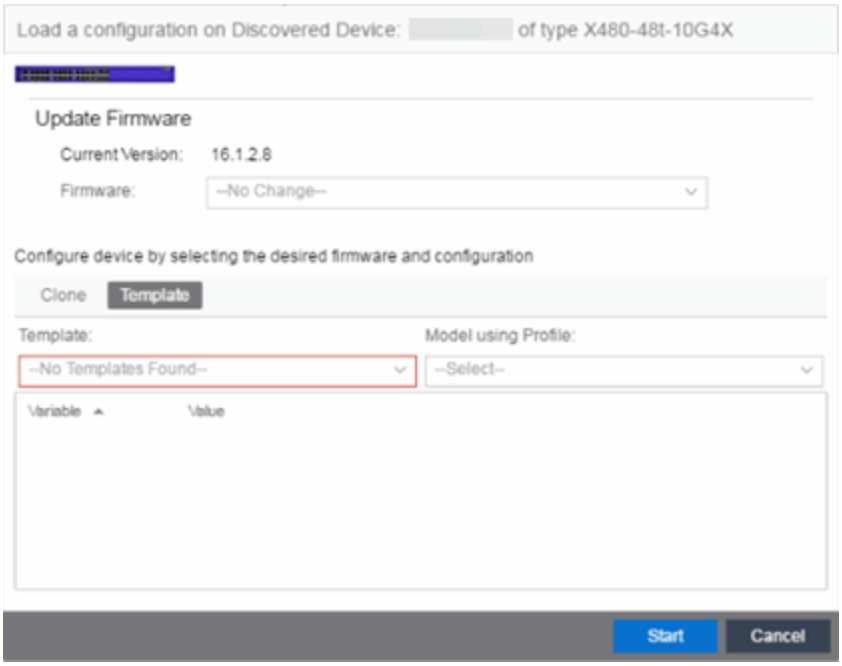
Select source Device
: Use the drop-down menu to select a device currently added to Management Center from which to copy the device configuration.

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 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:

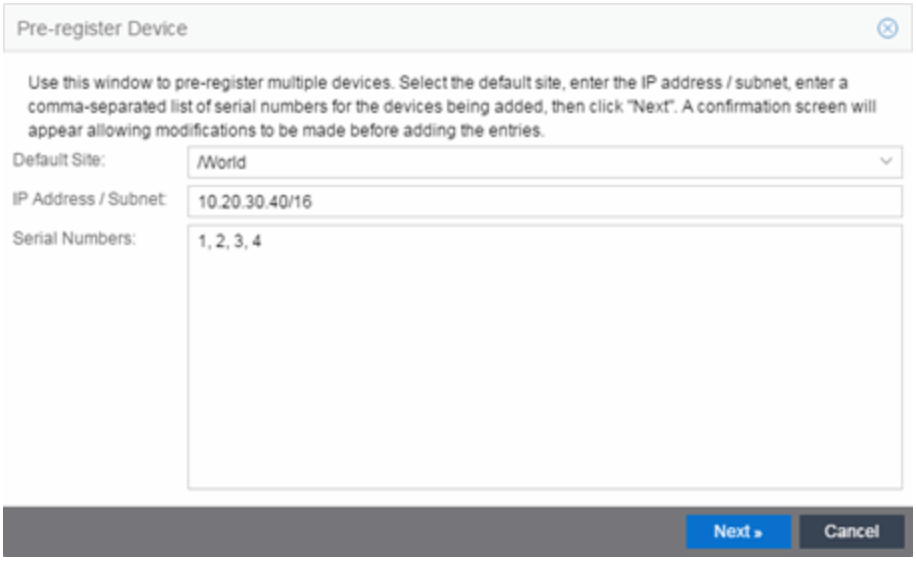
- Discovered

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.

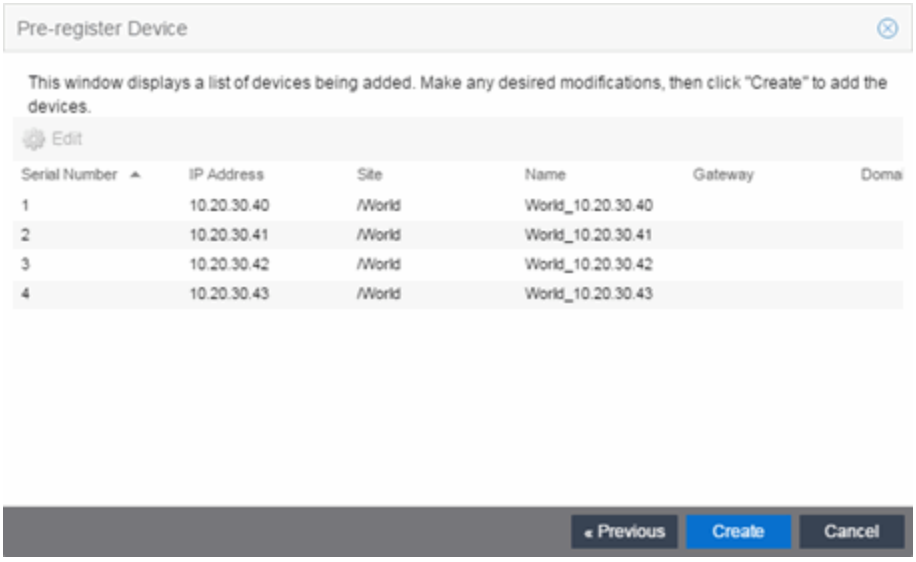
Serial Number
: Enter the manufacturer-assigned serial numbers of the devices being added, separated by commas.

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 Management Center.



Edit
: Select a device and click the **Edit** 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 Edit 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 Management Center database.

Related Information

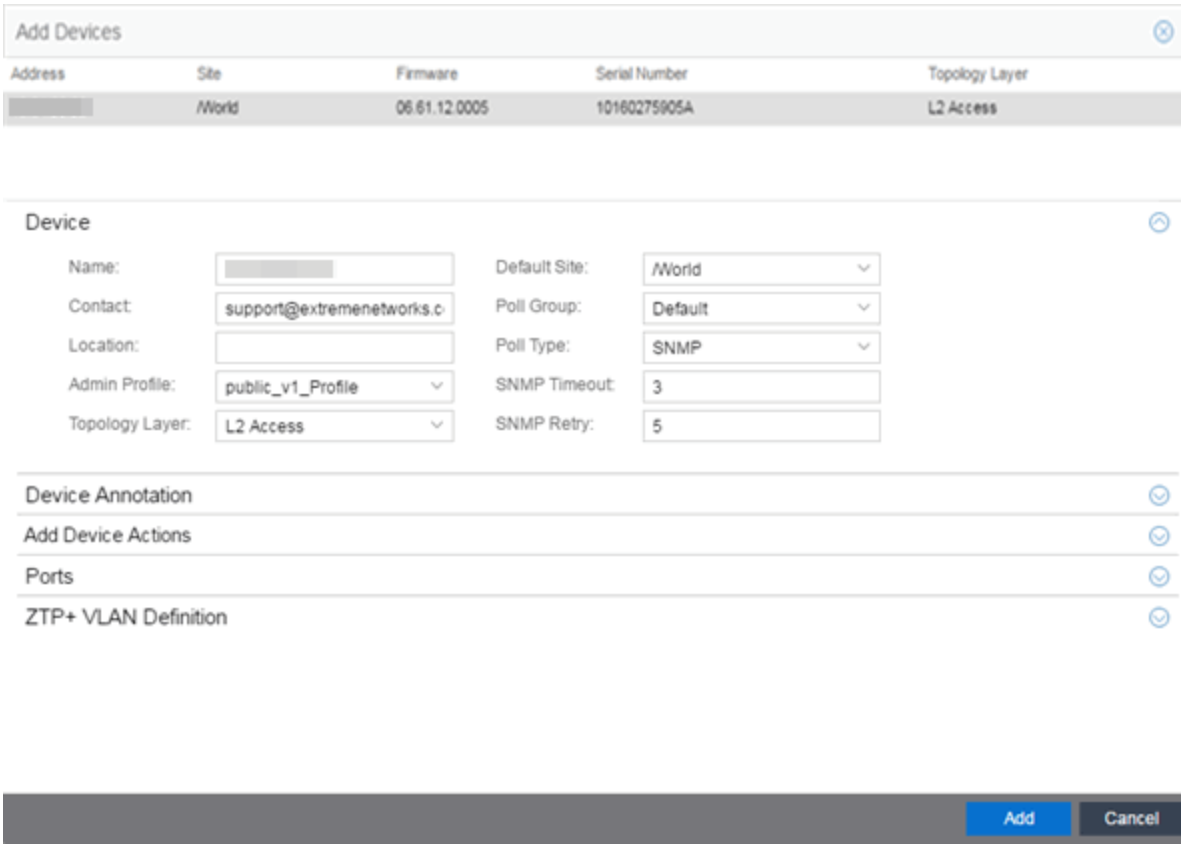
For information on related windows:

- 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.



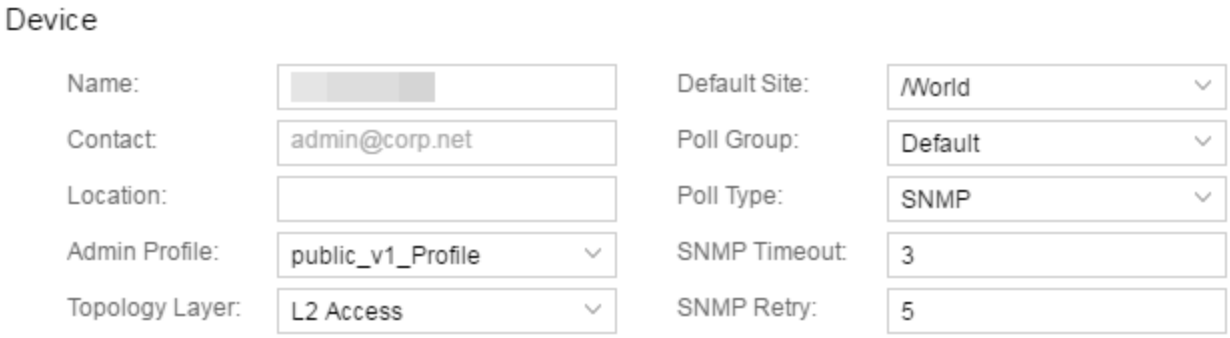
If you selected multiple devices to add, they are listed at the top of the window by IP address.

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

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. 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 (defined 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: 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 Management Center as a user with Administrative privileges.

SNMP Timeout

The amount of time (in seconds) that 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.

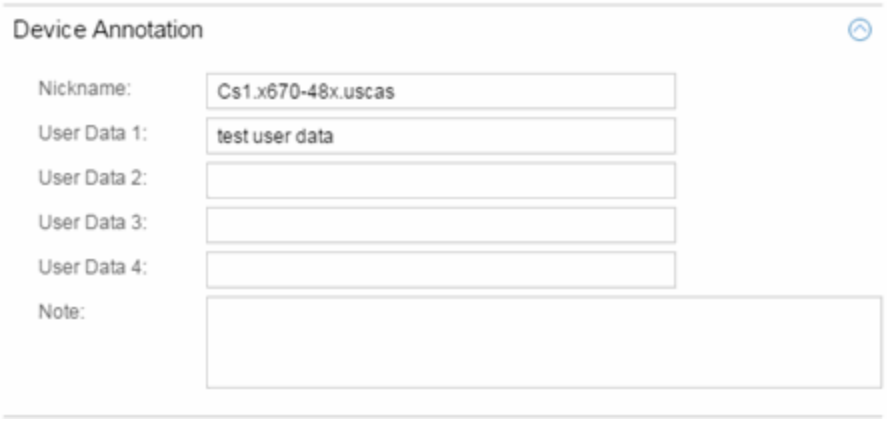
SNMP Retry

The number of attempts 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.



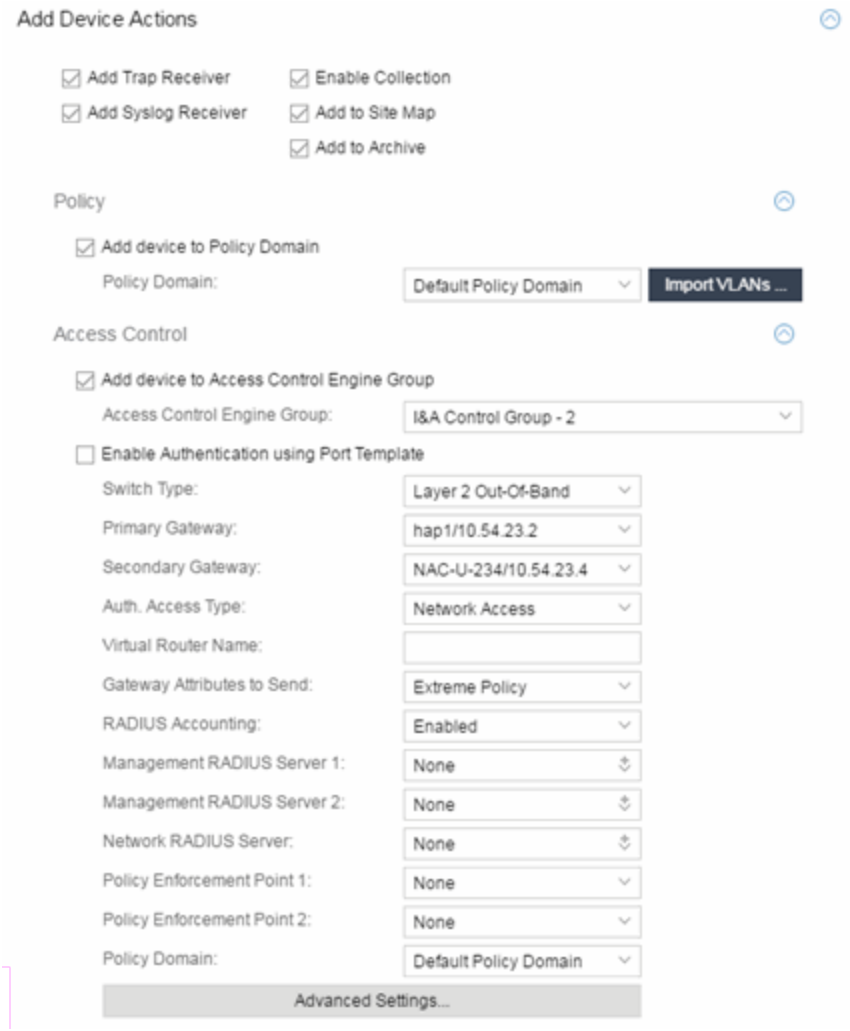
Nickname
: The user-defined nickname for the selected device. This is the name for this device that appears in the device tree in the left panel when **nickname** is selected in the **How to Display Devices in Tree** menu option in the OneView options menu in the **Administration** > **Options** tab.

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 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 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 Control > 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.

Access Control

Add device to Access ControlEngine Group
: Select this checkbox to add the device to an Access ControlEngine Group you create on the Control > 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 Network > Devices > 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 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 Access Control engine, Access Control removes the end-system authentication from their prior port/switch. This allows VMs that quickly move from one server to another and then back again to still have their location updated in Management Center, because only one authenticated session is allowed per end-system in Management Center.
  - **Layer 2 RADIUS Only** — In this mode, 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 a 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 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 Access Control Gateway for the selected switches. If load balancing has been configured for the engine group, the 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 Access Control Gateway for the selected switches. If load balancing has been configured for the engine group, the Management Center server determines the primary and secondary gateways at Enforce, and this field displays Determined by Load Balancer.

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

Auth. Access Type

Use the drop-down 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. 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 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 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 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. Management Center learns about these session via RADIUS accounting. This allows 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 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 - 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 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 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 Access Controlengine, providing real-time connection status in 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 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 Access Controlengine. (This option is only available if a Secondary Gateway is not specified.) Select from the RADIUS servers you have configured in Management Center, or select New or Manage RADIUS Servers to open the Add/Edit RADIUS Server or Manage RADIUS Servers windows.

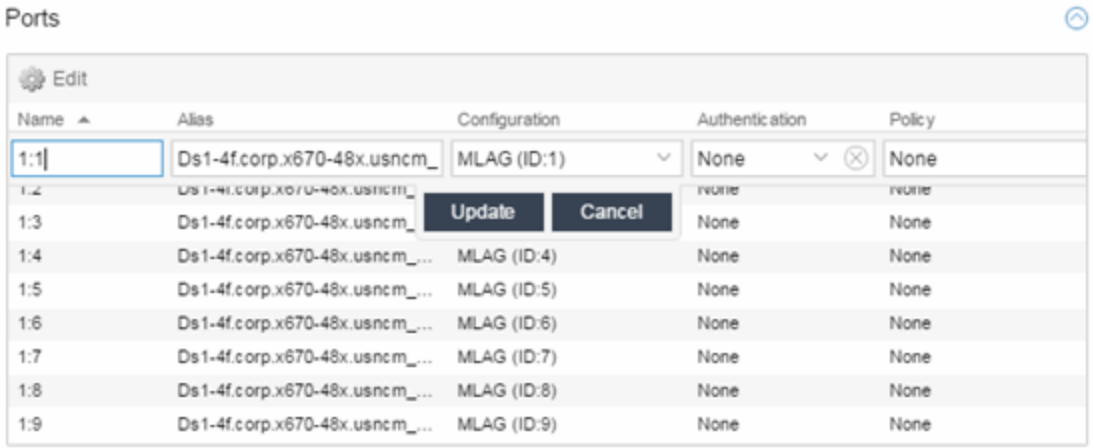
Policy Enforcement Point 1 and 2
: Select the Policy Enforcement Points used to provide authorization for the end-systems connecting to the VPN device you are adding. The list is populated from the N-Series, S-Series, and K-Series devices in your Console device tree. If you do not specify a Policy Enforcement Point, then 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
: 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 Management Center.

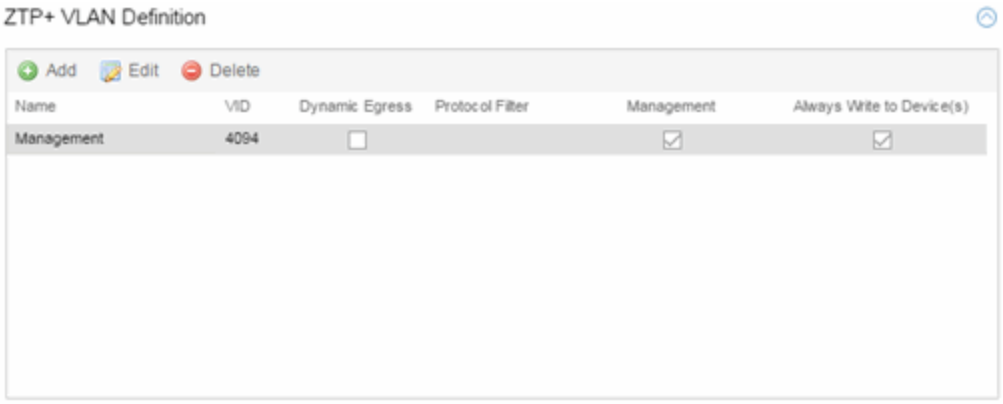
Policy
: The policy assigned to the selected port.

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

Cancel
: Click the Cancel button to close the window without adding the device to the 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:

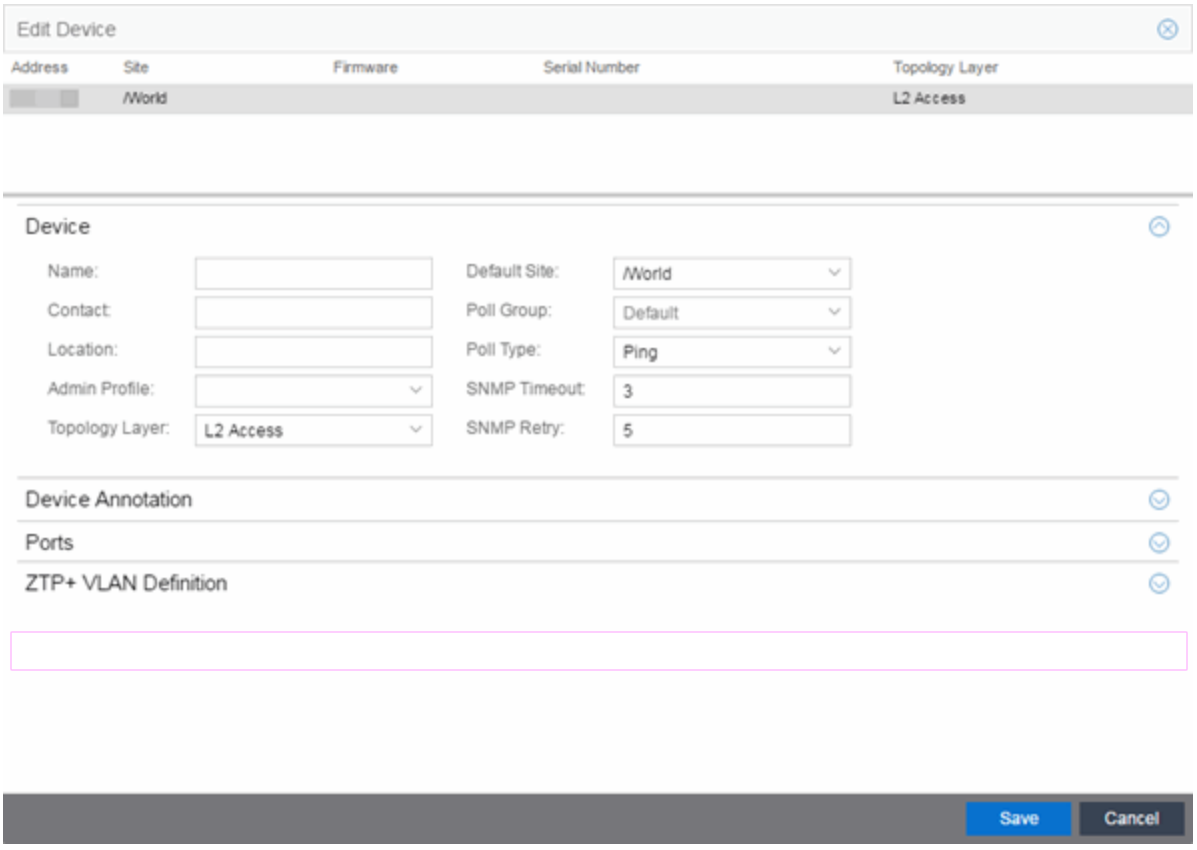
- Discovered

Edit Device

Use this window to edit 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.

Access this window by selecting a device in the Devices table on the **Network** > **Devices** tab, clicking the gear menu or right-clicking on the device and selecting **Device** > **Edit Device**.

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

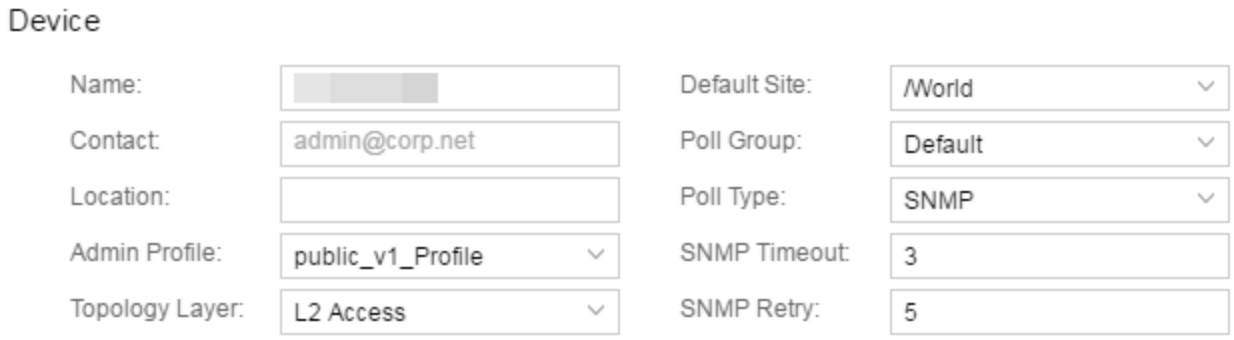


When you first open the window, only the Device section is expanded. Click a section heading to expand that section.

The Edit Device window contains the following sections:

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. 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 (defined 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: 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 Management Center as a user with Administrative privileges.

SNMP Timeout

The amount of time (in seconds) that 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.

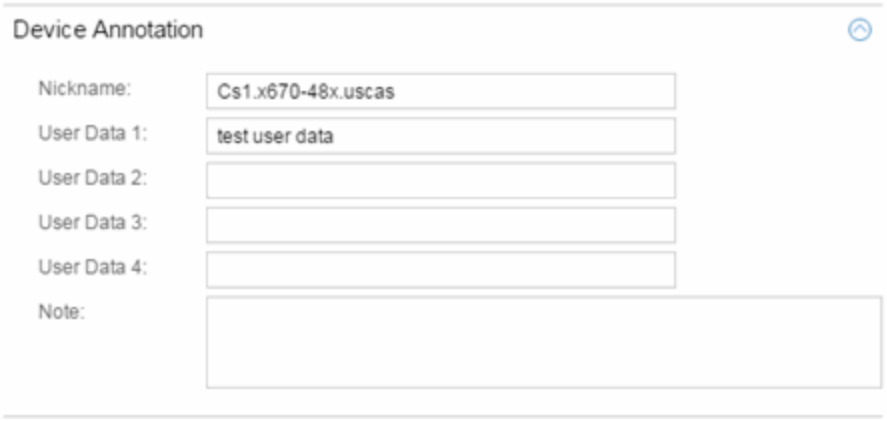
SNMP Retry

The number of attempts 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.



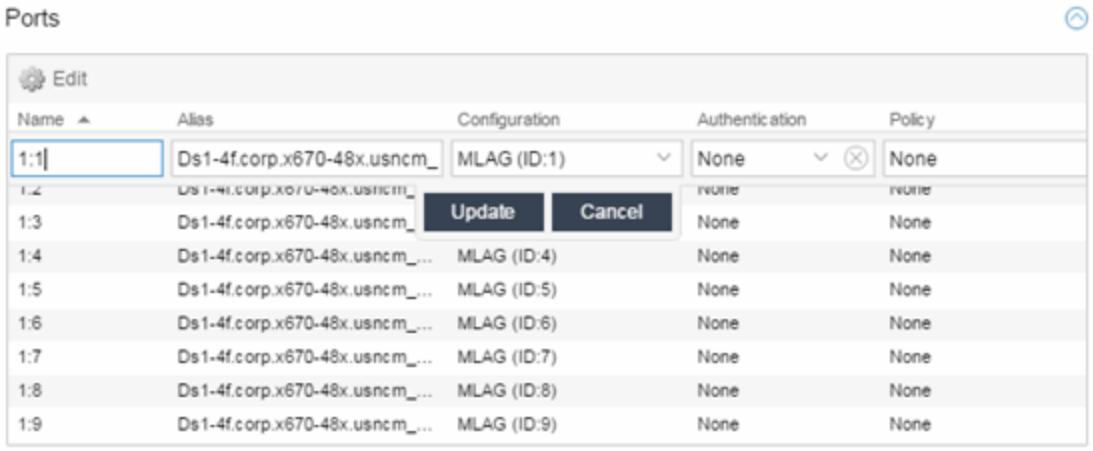
Nickname
: The user-defined nickname for the selected device. This is the name for this device that appears in the device tree in the left panel when **nickname** is selected in the **How to Display Devices in Tree** menu option in the OneView options menu in the **Administration** > **Options** tab.

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.

Ports

The Ports section of the Edit 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
: 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 Management Center.

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.

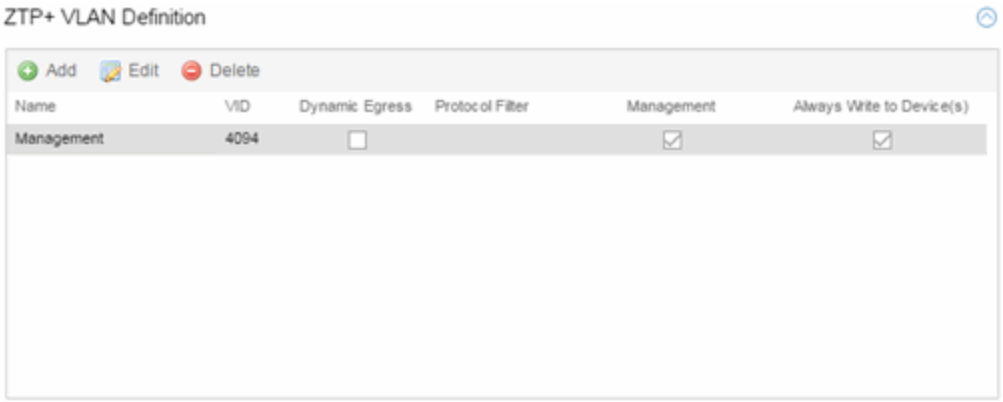
Policy
: The policy assigned to the selected port.

Update
: Click the **Update** button to save any changes made to the device configuration.

Cancel
: Click the **Cancel** button to close the window and discard any changes.

ZTP+ VLAN Definition

The ZTP+ VLAN Definition section 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.

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:

- Edit Policy Mapping Configuration Window

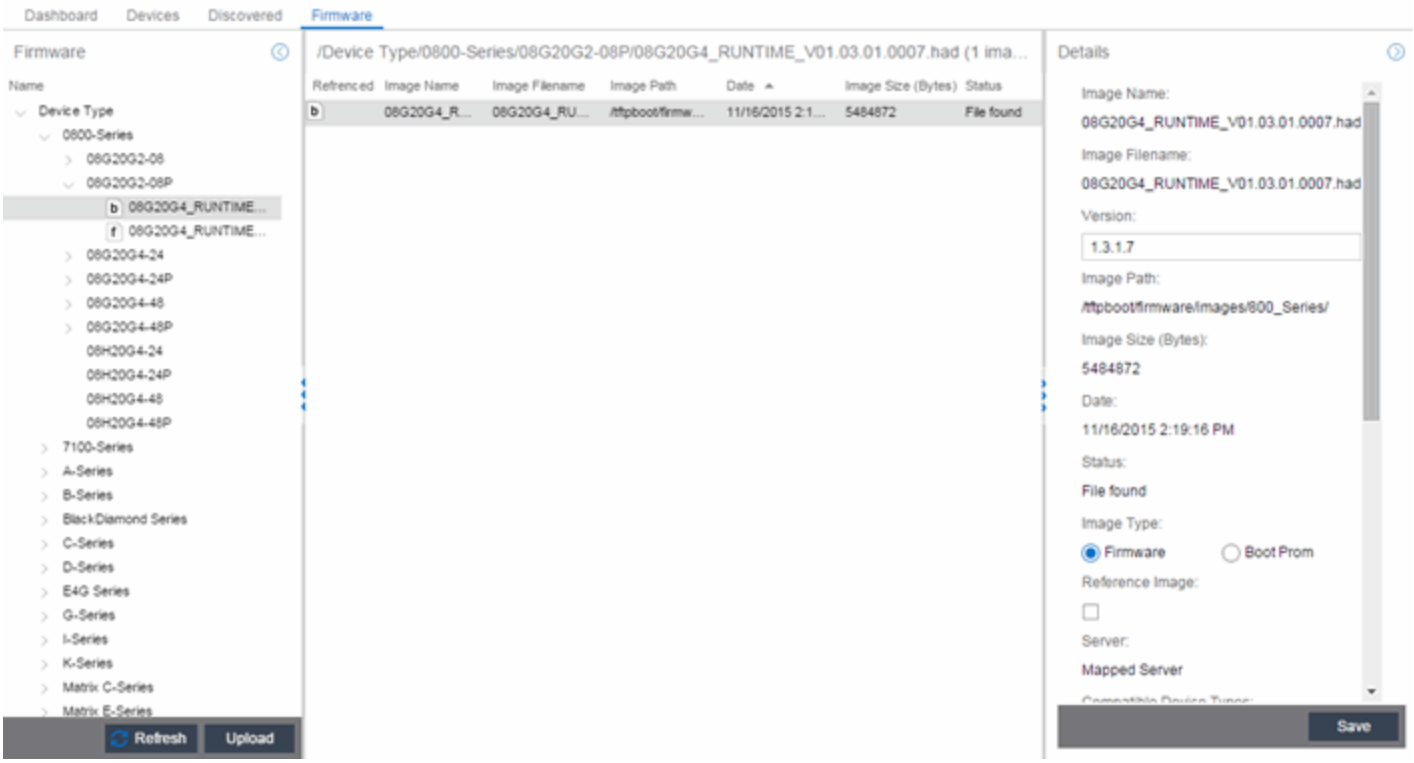
Firmware

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 Management Center could not correlate to a device type.

Name

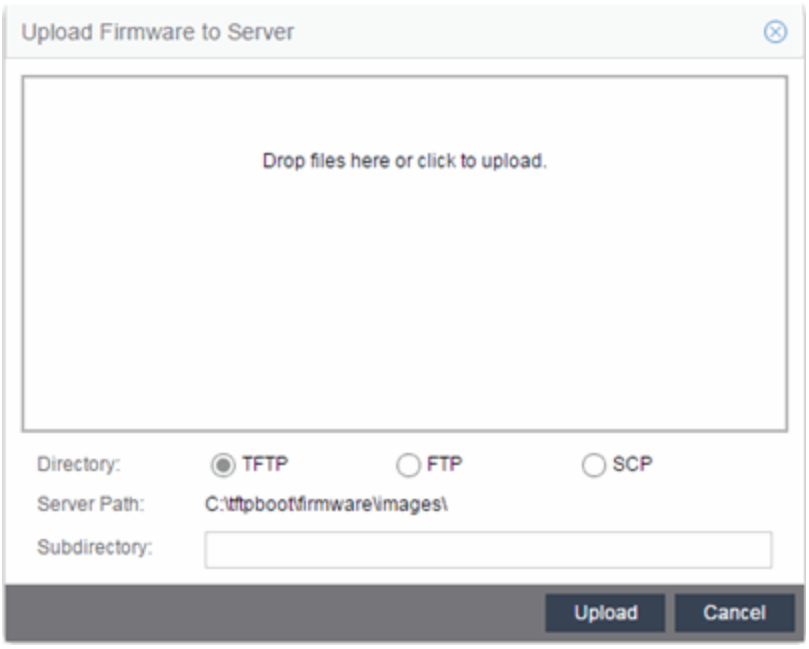
The **Name** navigation tree lists the product families and device types to which you can assign the firmware or boot PROM image.

Refresh Button

Click the **Refresh** button updates the images displayed in the Firmware left-panel to show the recently added firmware and boot PROM images.

Upload

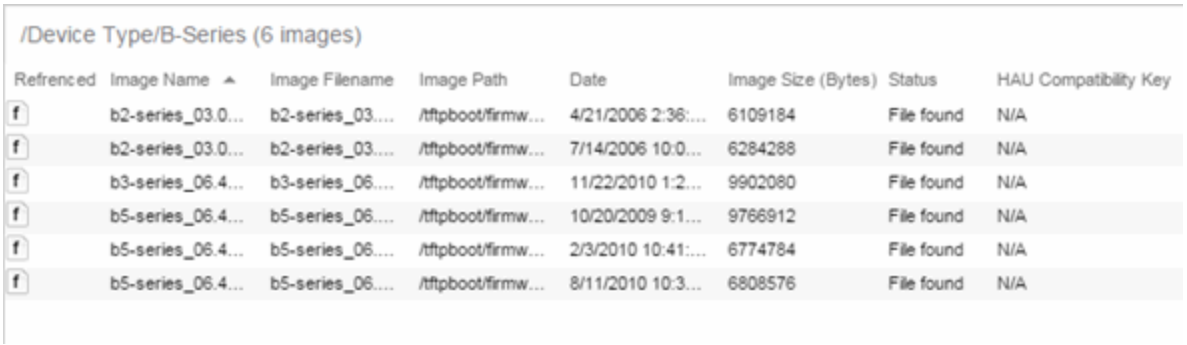
Click the **Upload** button to open the Upload Firmware to Server window from which you can save image files to the Management Center server. This allows anyone with access to Management Center to download the image file to a device.



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

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.).

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
: 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, Management Center performs the upgrade based on this status, and the comparison of the HAU firmware compatibility key on the current firmware with the key on the newly selected firmware.

  During firmware selection, Management Center attempts to determine if the keys are compatible. 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.

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

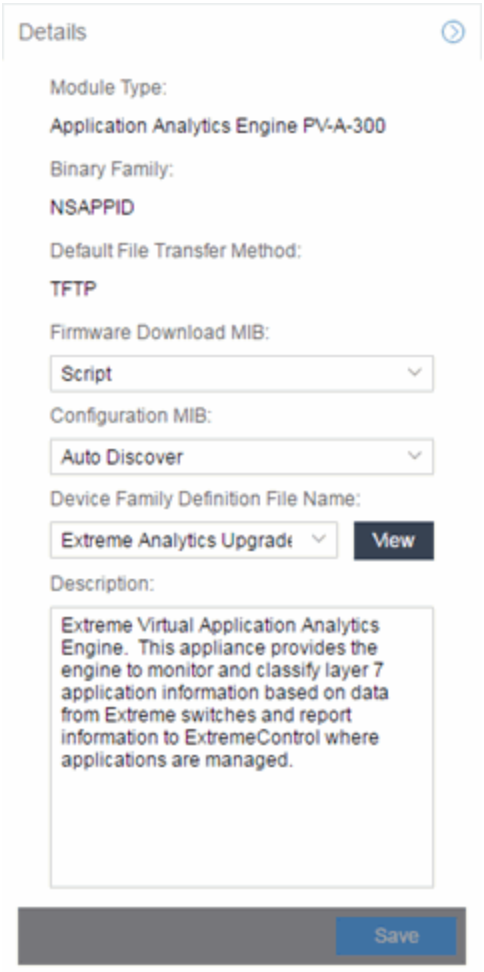
NOTE: Firmware images that were discovered with a version of prior to NetSight version 4.4 need to be removed from and rediscovered in order to populate the compatibility key field.

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 folder in the Firmware Tree left-panel (lowest level folder) and select **Default File Transfer Method**. You can override this default at the device level.

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 — Management Center reads the Firmware Download MIB on the first device of this device type that you add or import, and display it here. 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 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 — Management Center reads the Configuration MIB on the first device of this device type that you add or import, and display it here. 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 Management Center function for specific third-party devices in this file.

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. You can override the MIB specified here on a per-device basis using the MIB and Script Overrides section on the Image Information Tab (Device).

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.

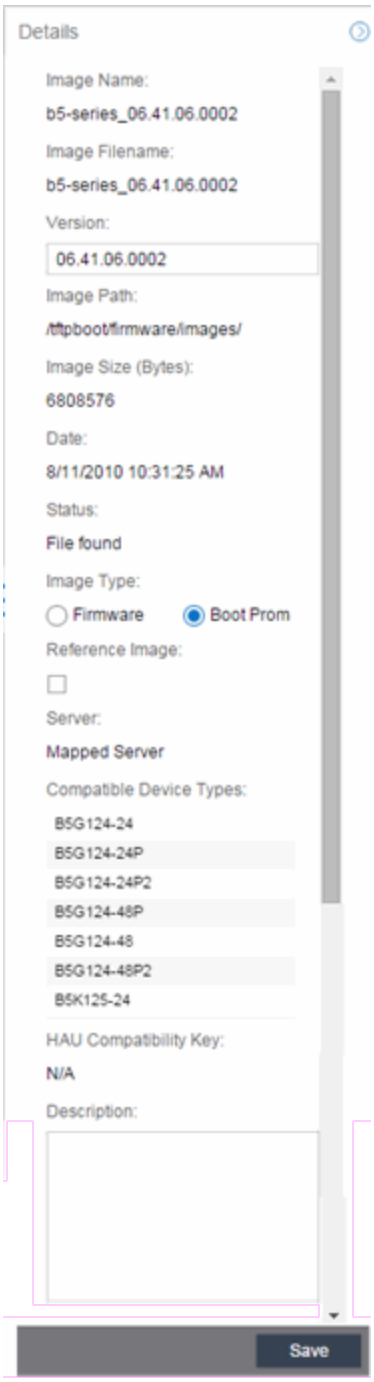


Image Name

The name of the image as it is displayed in the left-panel Firmware Mgmt 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.

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.

Compatible Device Types
: Device types for which the image is valid.

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, 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 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:

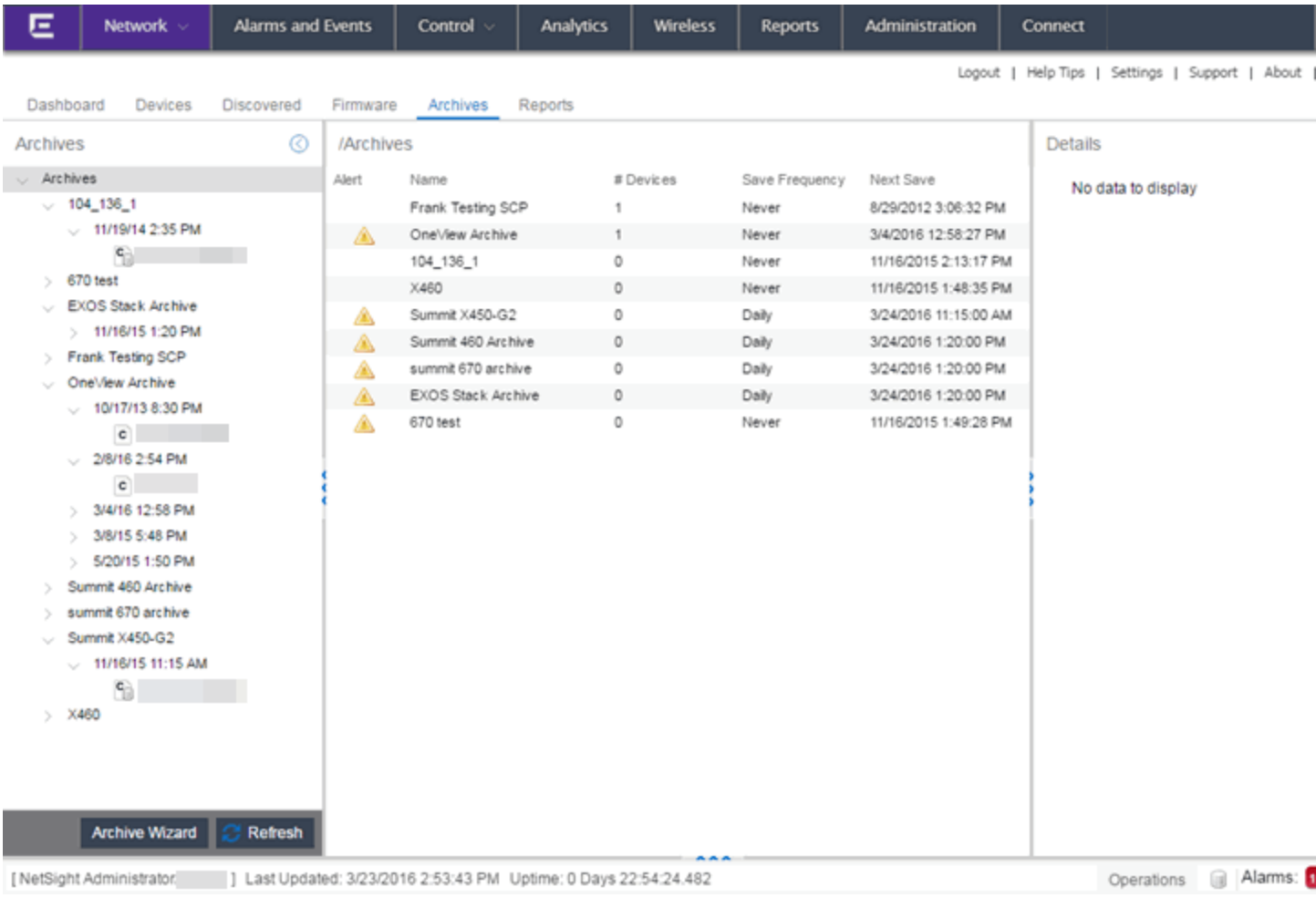
- Network
- Devices

For information on related tasks:

- How to Upgrade Firmware

Archives

The Archives tab allows you to create new archives (saved configurations) via the Archive Wizard. Additionally, the Archive tab allows you to edit an archive's attributes including devices, schedule, process, and setup. On the Archives tab, you can view all of the archives for a particular device family, or see specific details about an individual archive.



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 Folder — 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. For additional information, see the Archive Name Panel help topic.
  - Archive Version Folder — 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. For additional information, see the Archive Version Panel help topic.

    - 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. For additional information, see the Archive File Panel help topic.
- 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 Archive Wizard, which allows you to create new archives for your devices.

Related Information

For information on related tabs:

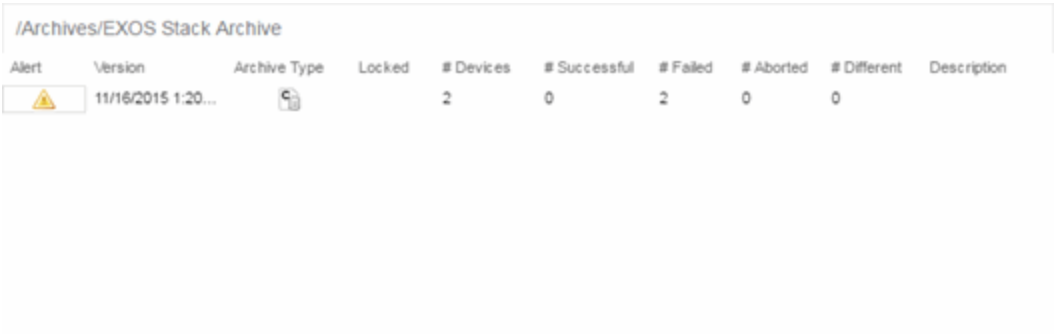
- Archive Name Panel
- Archive Version Panel
- Archive File Panel

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

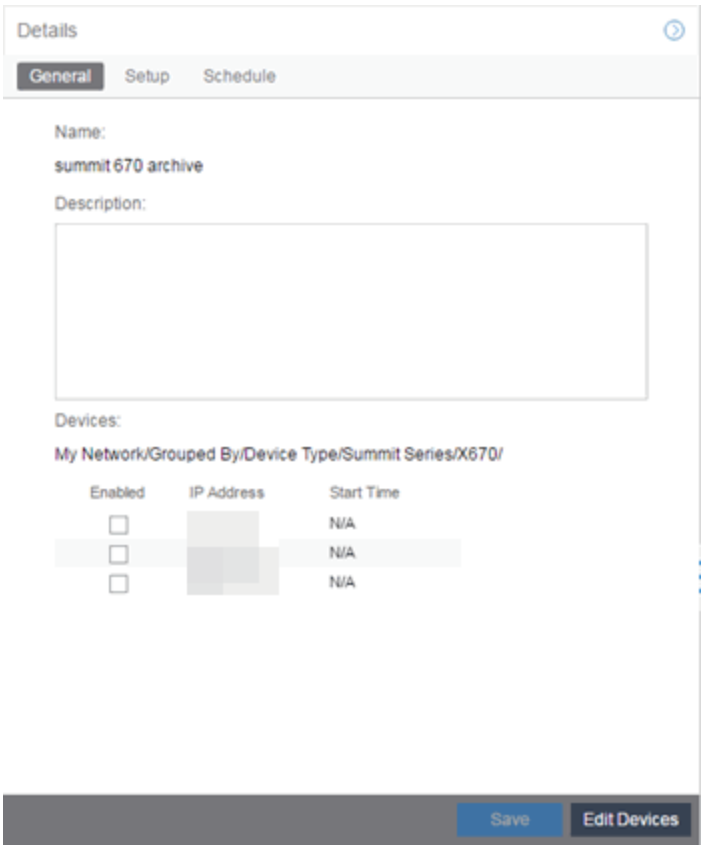
For information on related tasks:

- 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 groups of
: The archive is performed simultaneously on the number of devices specified in the **Process 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.

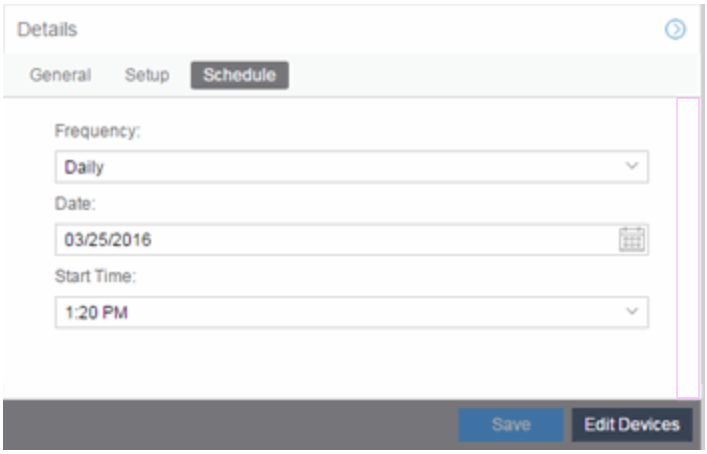
Archive Type
: Select the appropriate checkbox for the type of data you wish to archive:

  - **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.

Save Button
: Saves any changes made to the archive attributes. Selecting a Frequency of **Now** performs the archive immediately.

Edit Devices button
: 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 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.

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:

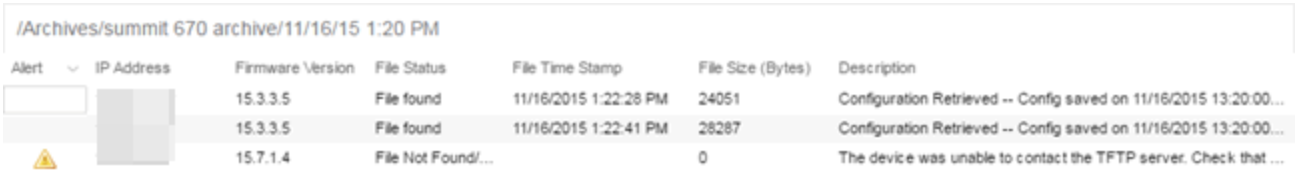
- Archive Name Main Panel

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:

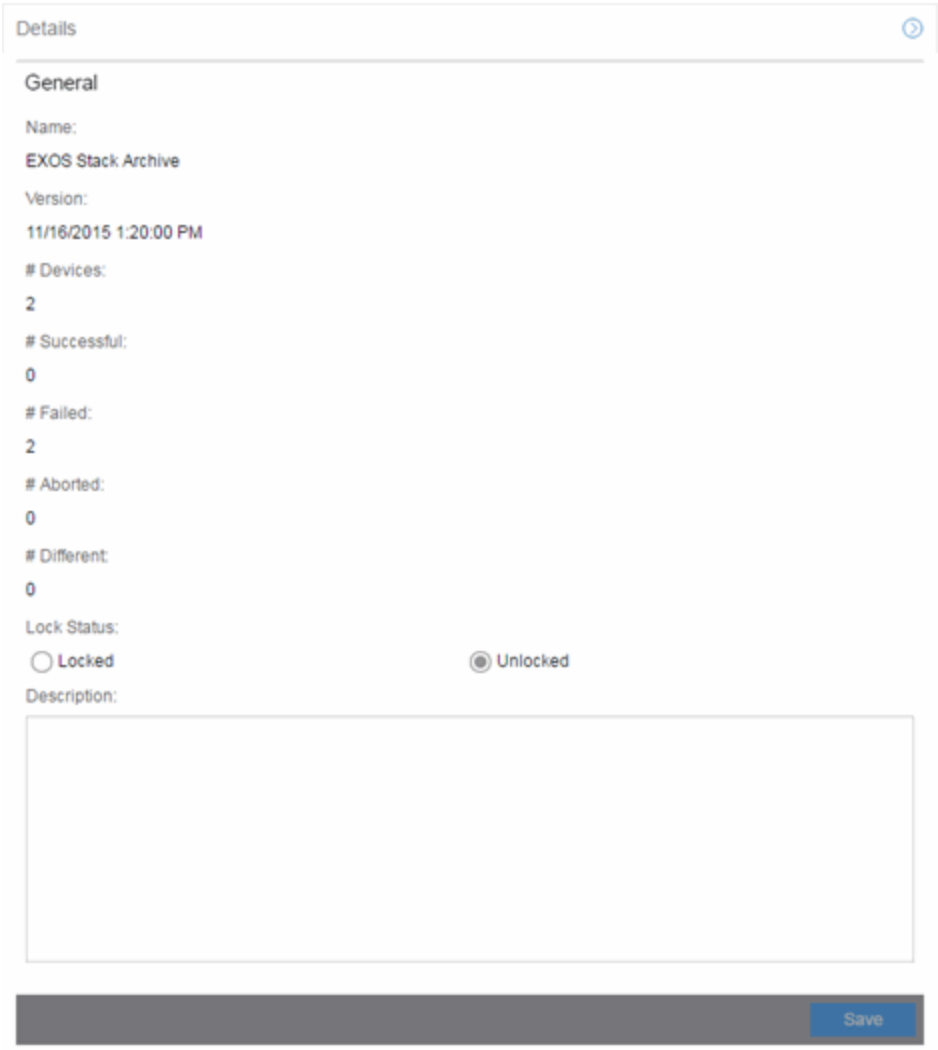
- Archive Version Right-Panel
- Archive File Right-Panel

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.



Archive 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

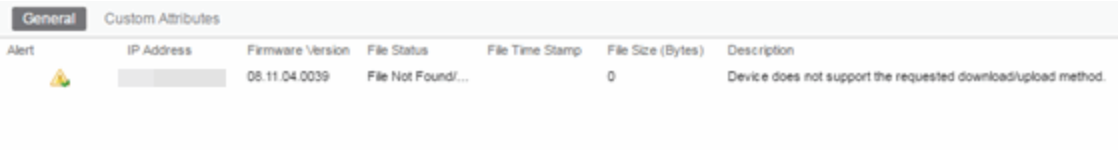
The Archive File panel appears when you select an archive configuration file in the left-panel of the **Archive** tab. It contains information about specific archive configurations.

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 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.

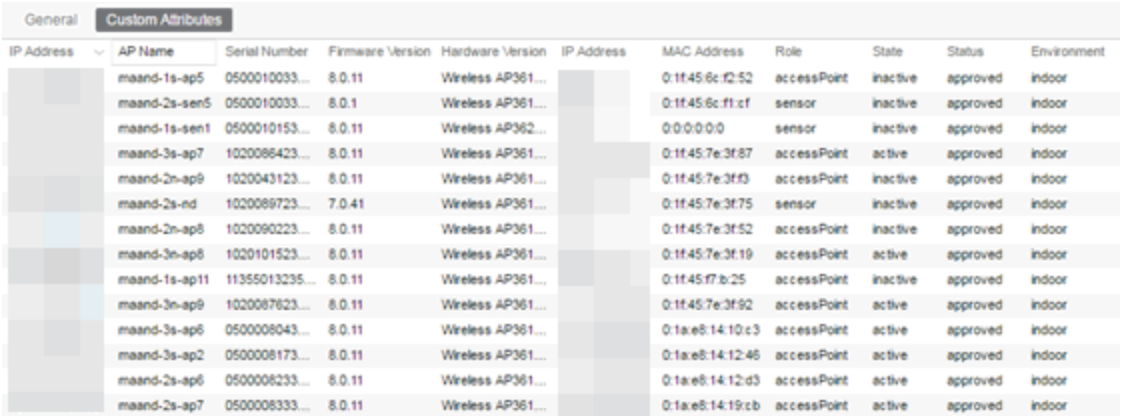
File Size
: The size of the saved configuration in bytes.

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 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


Details
General
Attributes
Name:
summit 670 archive
IP Address:
Device Type:
X670-48x
Version:
11/16/2015 1:20:00 PM
Status:
Failure
Device Status:
Contact
File Status:
File Not Found/Missing
File Name:
File Timestamp:
N/A
Contains Custom Attrs:
true
Contains Capacity Planning Data:
true
Description:
The device was unable to contact the TFTP server. Check that the TFTP server is running and connectivity is okay.
Memo:
Save

Name
: The name of the archive operation.

IP Address
: The IP address of the device whose data is saved, followed by the SNMP context, if applicable.

Device Type
: The device's model number or hardware type.

Version
: The date and time the archive operation occurred.

Status
: The status of the operation: Success or Failure.

Device Status
: The status of the device when the archive operation occurred: Contact or No Contact.

File Status
: The status of the config file: File Found or File Not Found/Missing. File Not Found/Missing indicates that 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.

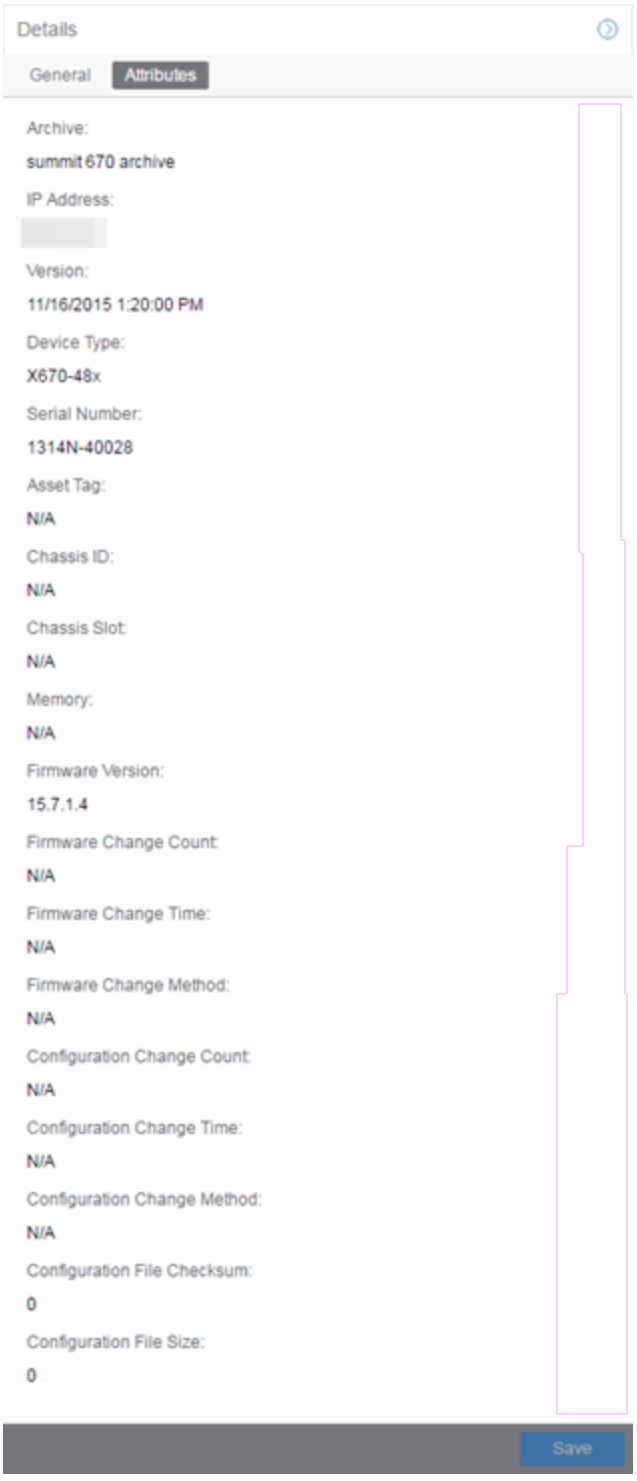
Description

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.

Configuration Archive



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. The asset tag is defined in the device's General Tab.

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

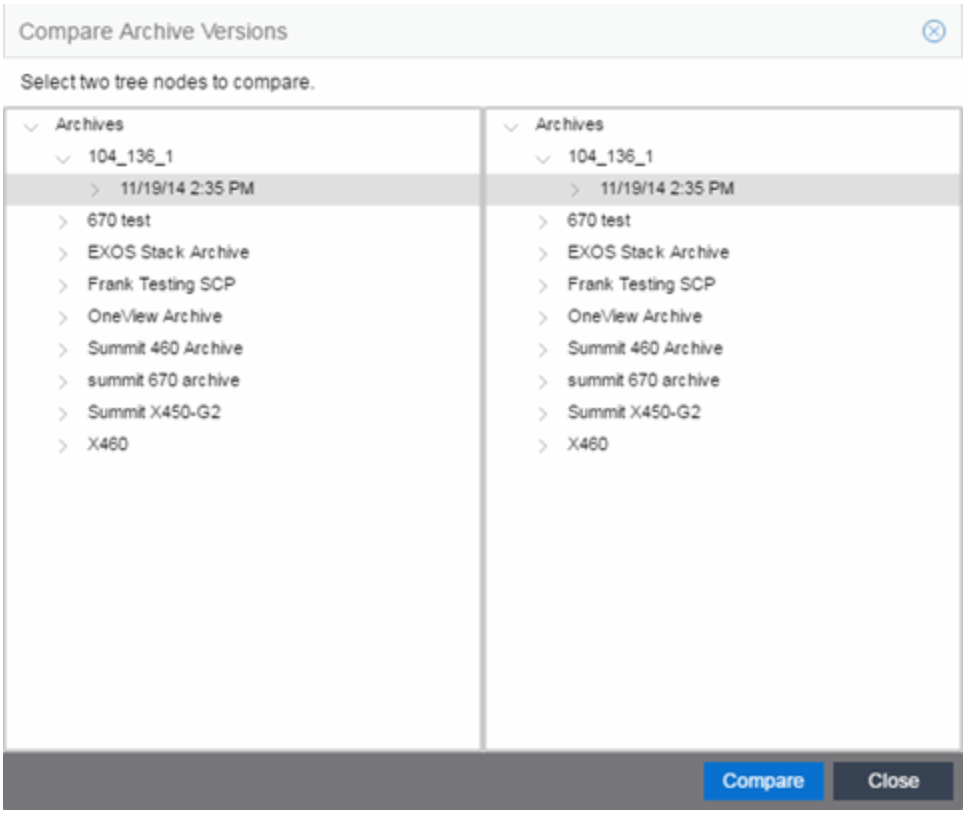
For information on related tasks:

- How to Archive
- How to Restore an Archive

Select 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 Button
: Performs the comparison and opens the Compare Archive Versions window, where you can view the comparison results.

Close Button
: Closes the window.

Related Information

For information on related windows:

- Compare Configuration Files Window
- Configuration File Viewer

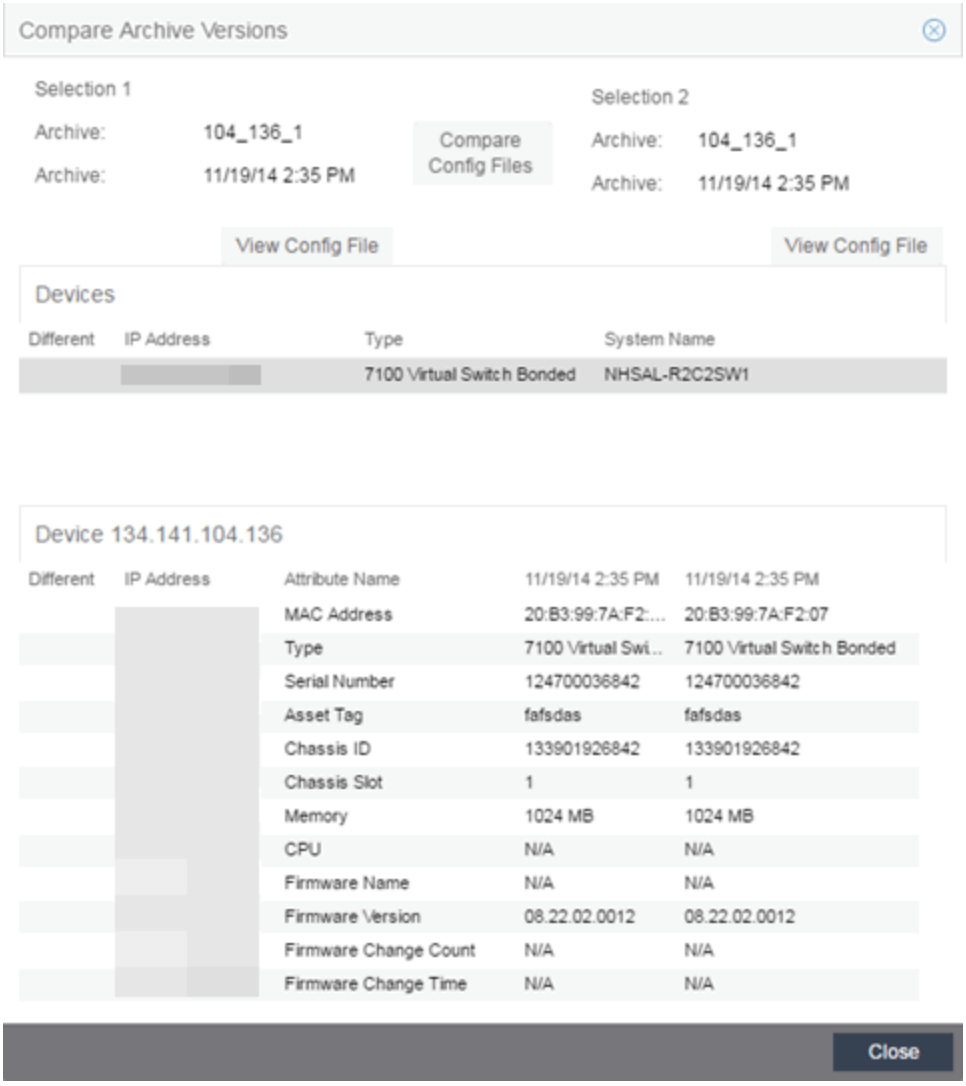
For information on related tasks:

- 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 . For more information, see How to Compare Archives.

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.

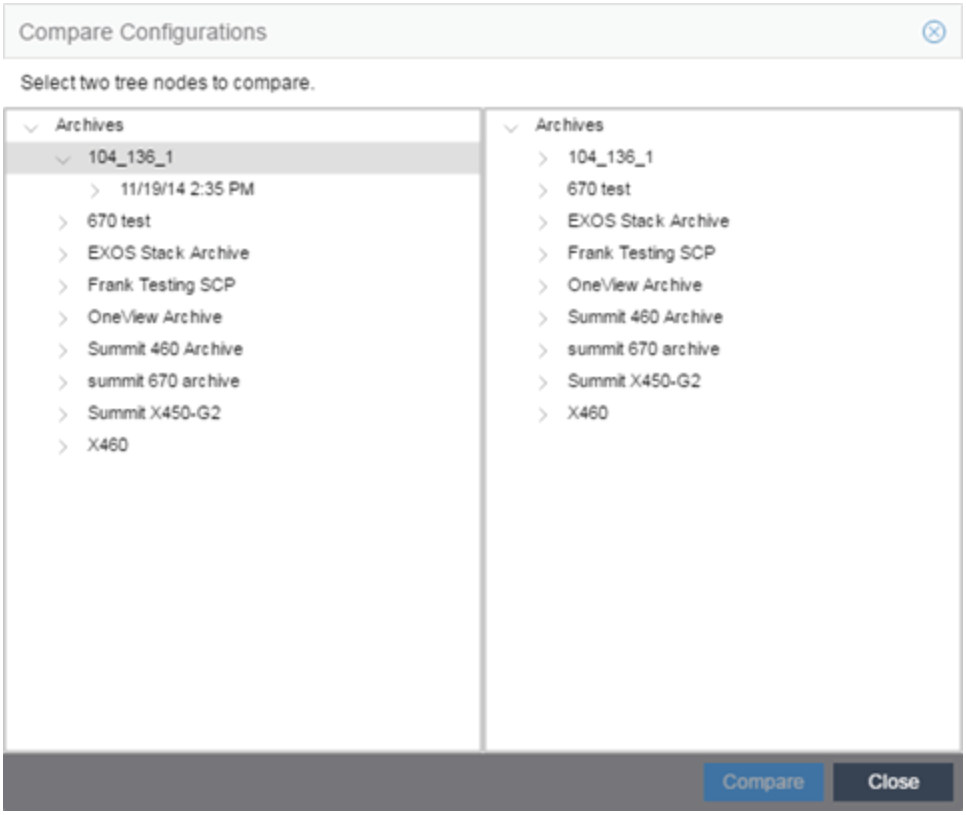
Related Information

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

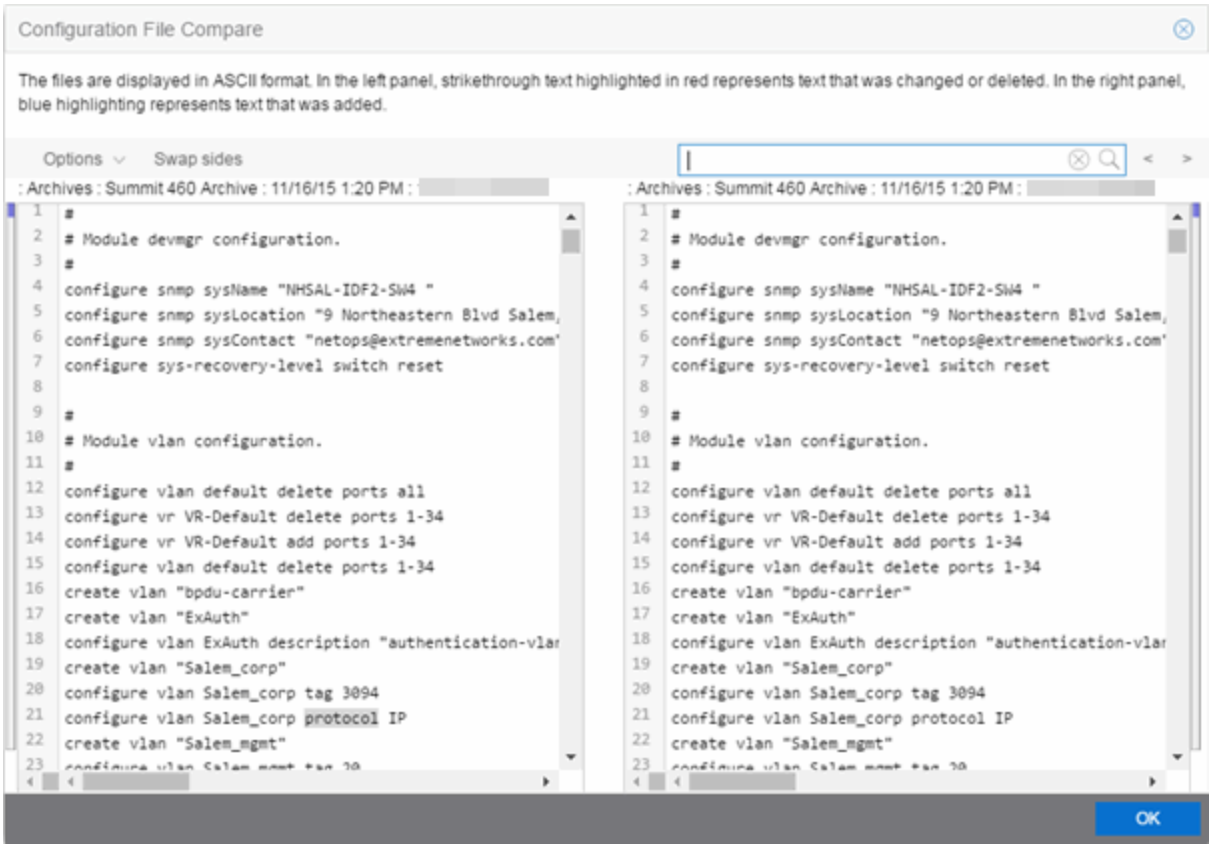
Configuration File Compare

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

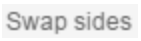
Use the **Search** box at the top of the window to search for strings of characters in the configuration files.

Clear Search Button

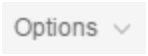
Click this button to clear the search parameters from the **Search** box.

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 

Clicking this button switches the sides on which each archive configuration is located.

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:

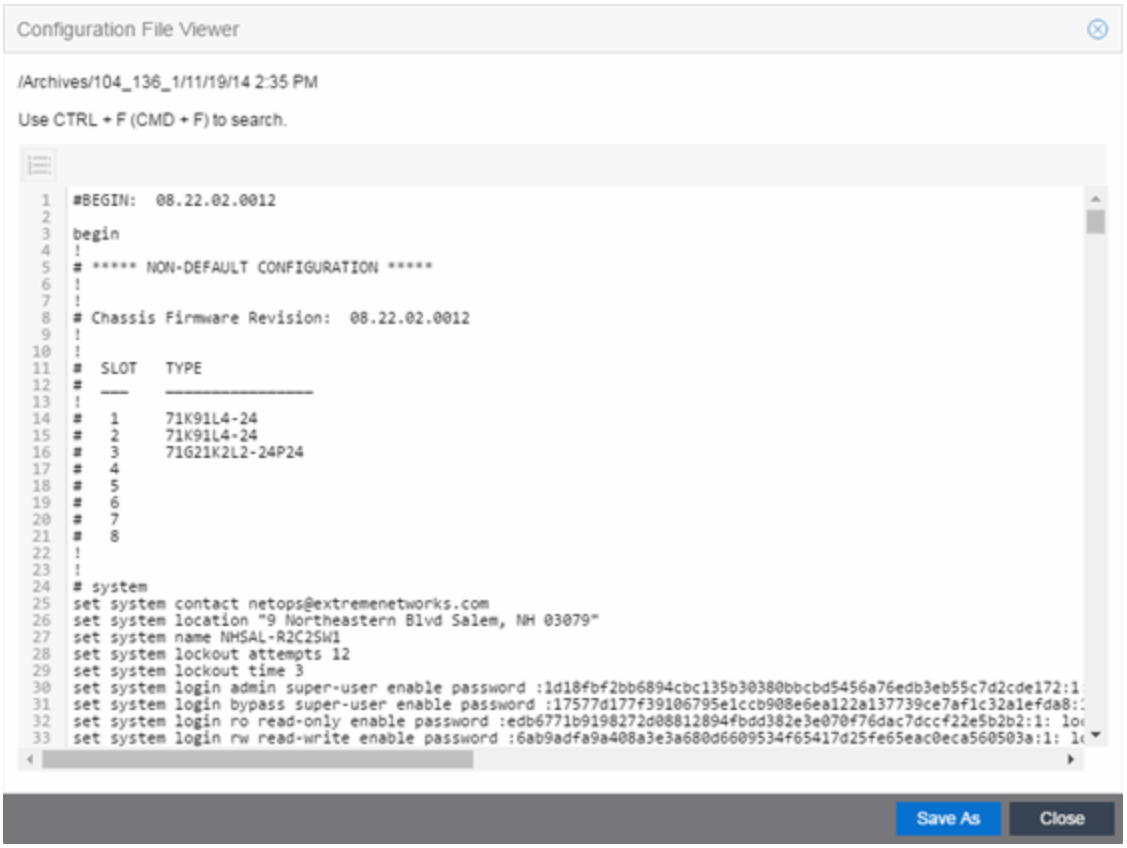
- How to Archive
- How to Compare Archives

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 As Button

Click the **Save As** button to automatically save the configuration file to your default download folder in CFG format.

Close Button
: Closes the Configuration File Viewer window and returns you 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

Archive Wizard

Use the Archive Wizard 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 wizard 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, Management Center generates an event log message. Using the 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.

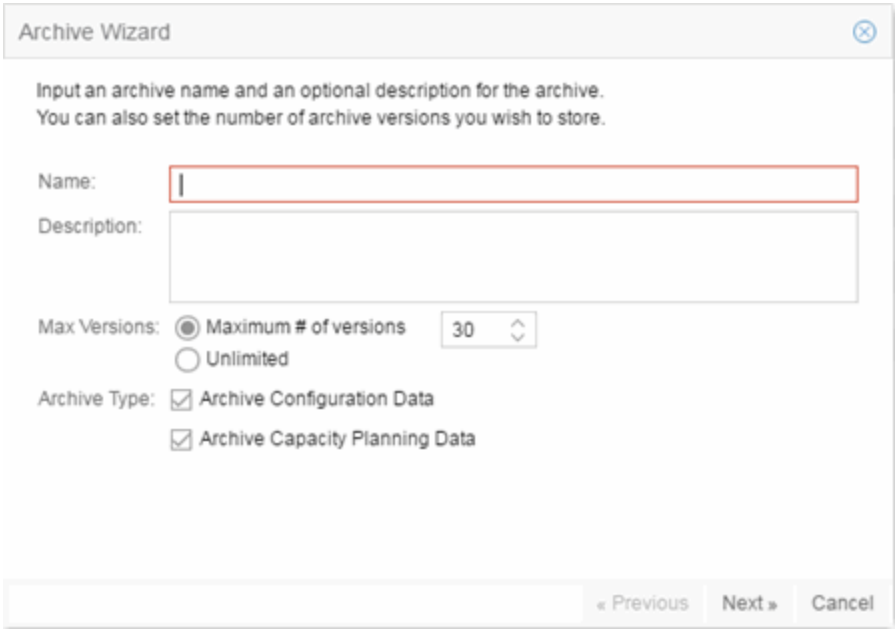
Once an archive operation is created, it is listed by name in the left-panel Archive Mgmt tab under the Archives folder. Below the archive name are the archive versions, displayed by the date and time of the creation of the version. Under the versions are individual configurations, listed by the IP address 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 wizard, select the Archive Wizard 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, 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:

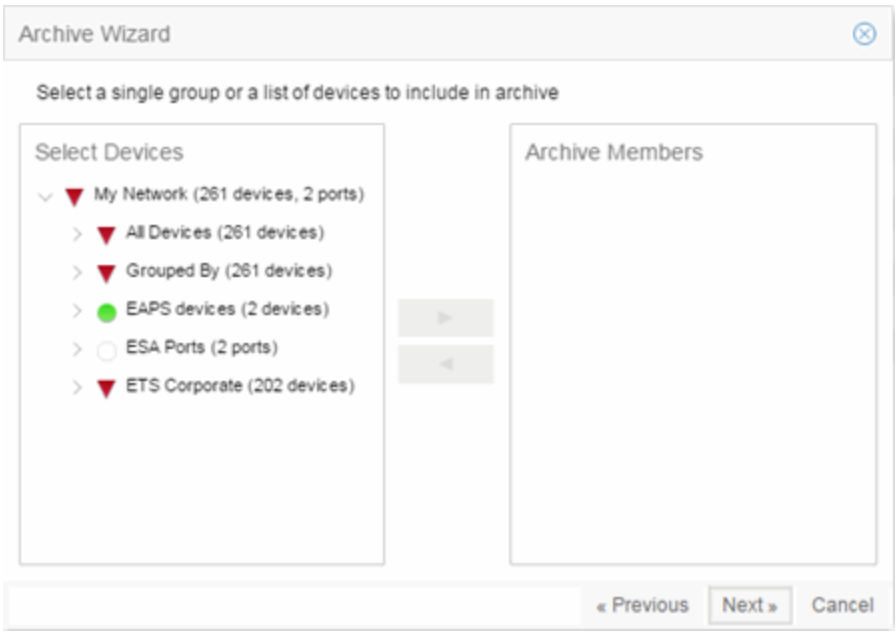
- Archive Configuration Data — Create archives (backup copies) of your devices' configurations you can restore to the devices at a later date.

- Archive Capacity Planning data — Create archives of port and FRU information.

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 **<**.

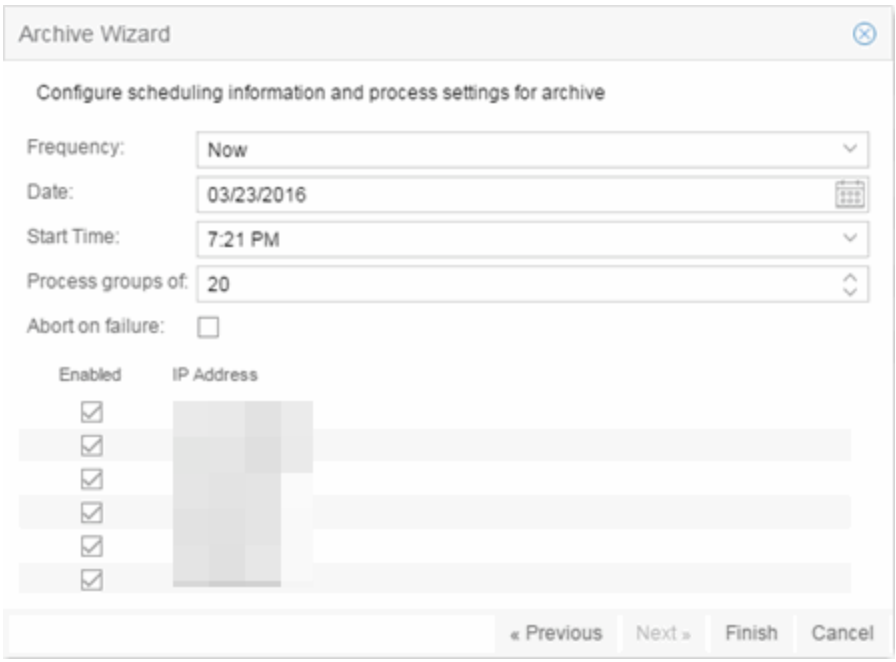
TIP: If you open the Archive Wizard from a device or device group in the left-panel, the selected device or device group automatically display under Archive Members.

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 Wizard

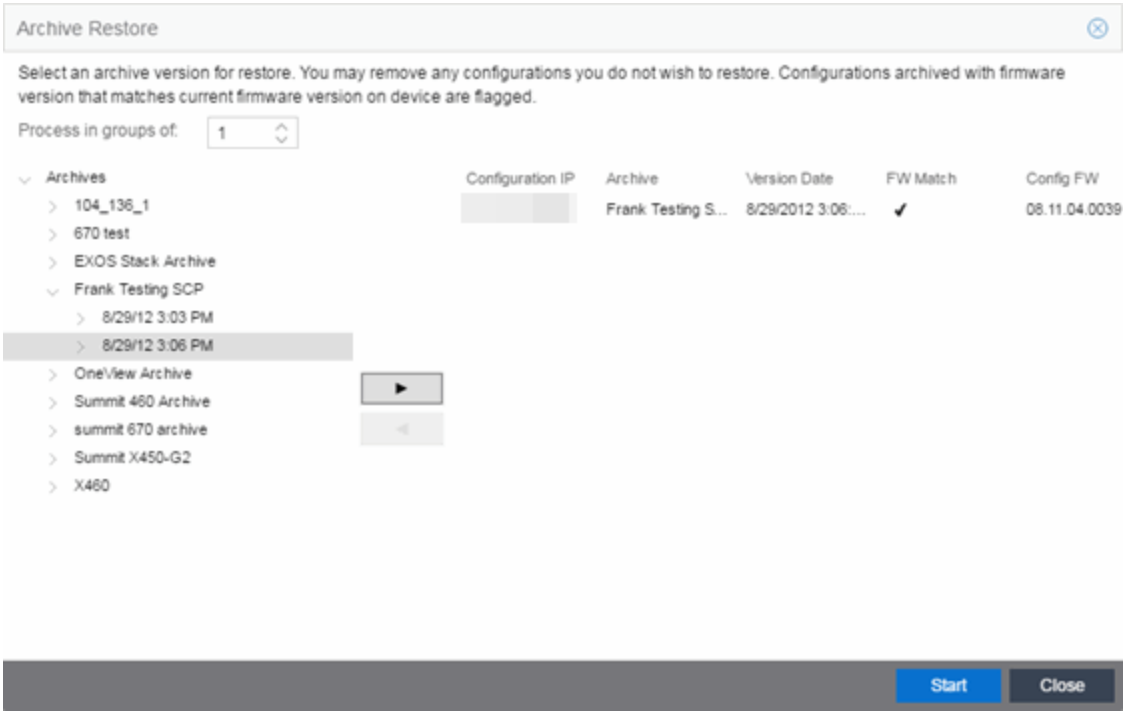
Use the Restore Wizard to restore saved (archived) device configuration files to one or more devices. Saved configurations are listed in the left-panel of the Archive tab under the appropriate archive and version. Each configuration displays an icon that identifies the type of saved data: device configuration 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 wizard, select an archive version or an archive configuration from the left-panel of the Archive tab or from the main panel and select Restore Wizard.

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 Archive 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 Wizard 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 reset automatically reset 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 groups of field. By default, the restores occur in sequential order (Process groups of: 1). This is to protect against possible isolation of other devices on the restore list.

CAUTION: Because some devices automatically reset 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 groups of** value of 1 (perform the restore serially,) unless you know it is safe for the selected network devices to reset 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 an 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.

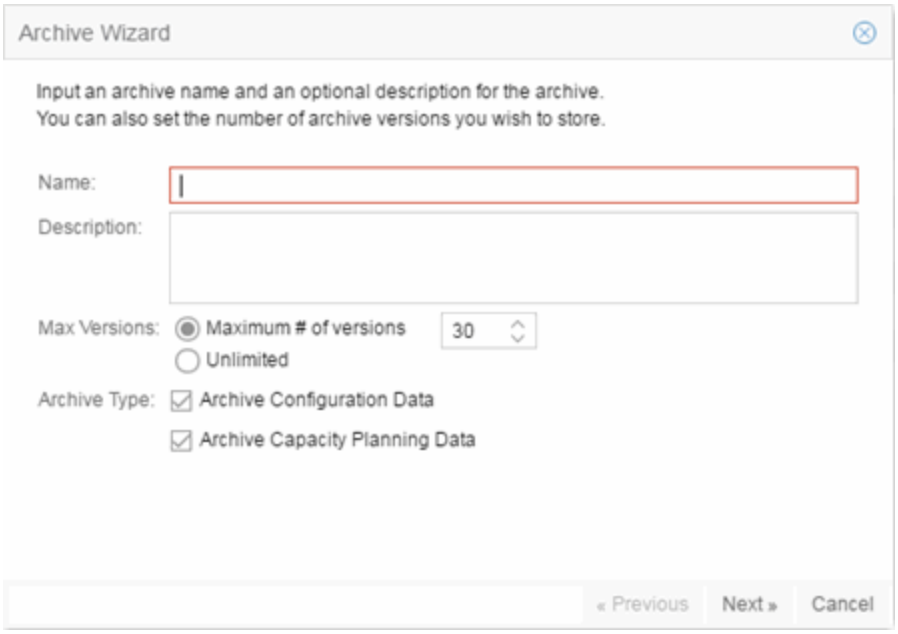
Instructions on:

- Using the Archive Wizard
- Saving a New Archive Version
- Editing an Archive
- Renaming an Archive
- Deleting an Archive

Using the Archive Wizard

Use the Archive Wizard 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.

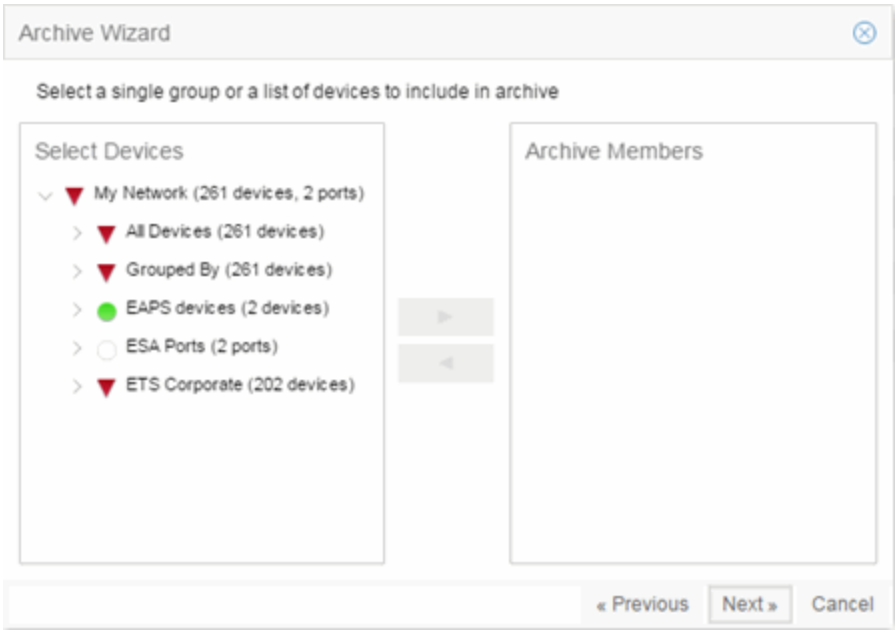
1. Select the Archive Wizard button from the left-panel. The Archive Wizard opens.



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 Maximum # of versions field or select Unlimited to retain all archives. Entering a value in the Maximum # of 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 to be used by the Capacity Planning tool to generate reports.

c. Click **Next**.
The next Select Devices window appears.



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.)

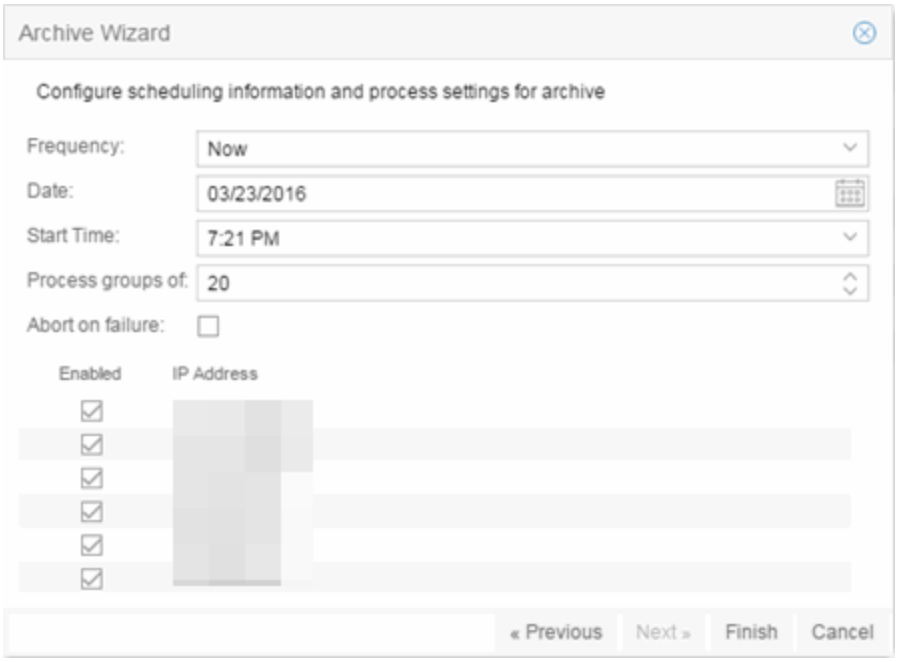
---

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 Archive Wizard from a selected device or device group in the left-panel Network Elements tab, the selected item are automatically displayed under Archive Members.

The Configuring Scheduling Information Process Settings for Archive window appears.



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 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. Select devices to be archived. Use the Enabled checkboxes to select or deselect devices to be archived. 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, 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. With an archive name selected in the left-panel of the Archives tab, select the right-panel Archive Name right-panel.
2. Edit the archive Description and use the Enabled checkboxes in the Devices table to select or deselect devices to be archived, if desired.
3. Click the Setup tab.
4. Select the number of devices to archive in parallel (simultaneously) in the Process Groups of field. Set the value to 1 to perform the operation serially, one device after another.
5. 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.

6. Specify either the maximum number of versions to be saved for this archive in the **Maximum # of versions** field or select **Unlimited** to retain all archives. Entering a value in the **Maximum # of 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.
7. 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.
8. Click the **Schedule** tab.
9. Select the **Frequency** with which the archive process occurs.
10. Select the **Date** to run the archive process and **Start Time** for the archive process.
11. 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:

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

How to Restore an Archive

You can restore saved (archived) device configuration files to devices using the Restore Wizard. 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. Select an archive version or an archive configuration from the left-panel of the Archive tab or from the main panel and select Restore Wizard. The Restore Wizard opens.
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) are available to be restored. Click the right arrow button >.
    b. The Configurations to Restore table lists the configurations. If you have selected an archive version and you 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 Wizard 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 groups of** field. By default, the restores occur in sequential order (Process groups of: 1). This is to protect against possible isolation of other devices in the restore list.

    CAUTION: Because some devices automatically reset 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 groups of** value at 1 (perform the restore serially), unless you know it is safe to the simultaneously reset 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 wizard.

Related Information

For information on related tasks:

- Restore Wizard
- How to Archive

How to Compare Archives

Extreme Management Center lets you compare two different archives for the same device and monitor any changes in device attributes. 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 Diff 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 Diff icon. If there are many devices being compared, a progress bar indicates the progress of the operation. You can stop the compare operation by pressing the Abort Compare button.
4. Once the compare operation is complete, select the device in the Summary table whose comparison results you wish to see. The results are displayed in the Device table at the bottom of the window.

In addition, the following buttons are available in the window only for archives that include device configuration data:

- View Config File — Opens the Configuration File Viewer and displays the archived 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.

Related Information

For information on related tasks:

- How to Archive
- How to Restore an Archive

For information on related windows:

- Compare Archives Window

Alarms and Events

The Alarms and 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 at the top of the screen provides links to additional information about your version of Extreme Management Center (formerly NetSight).

This Help topic provides information on the following topics:

Access Requirements

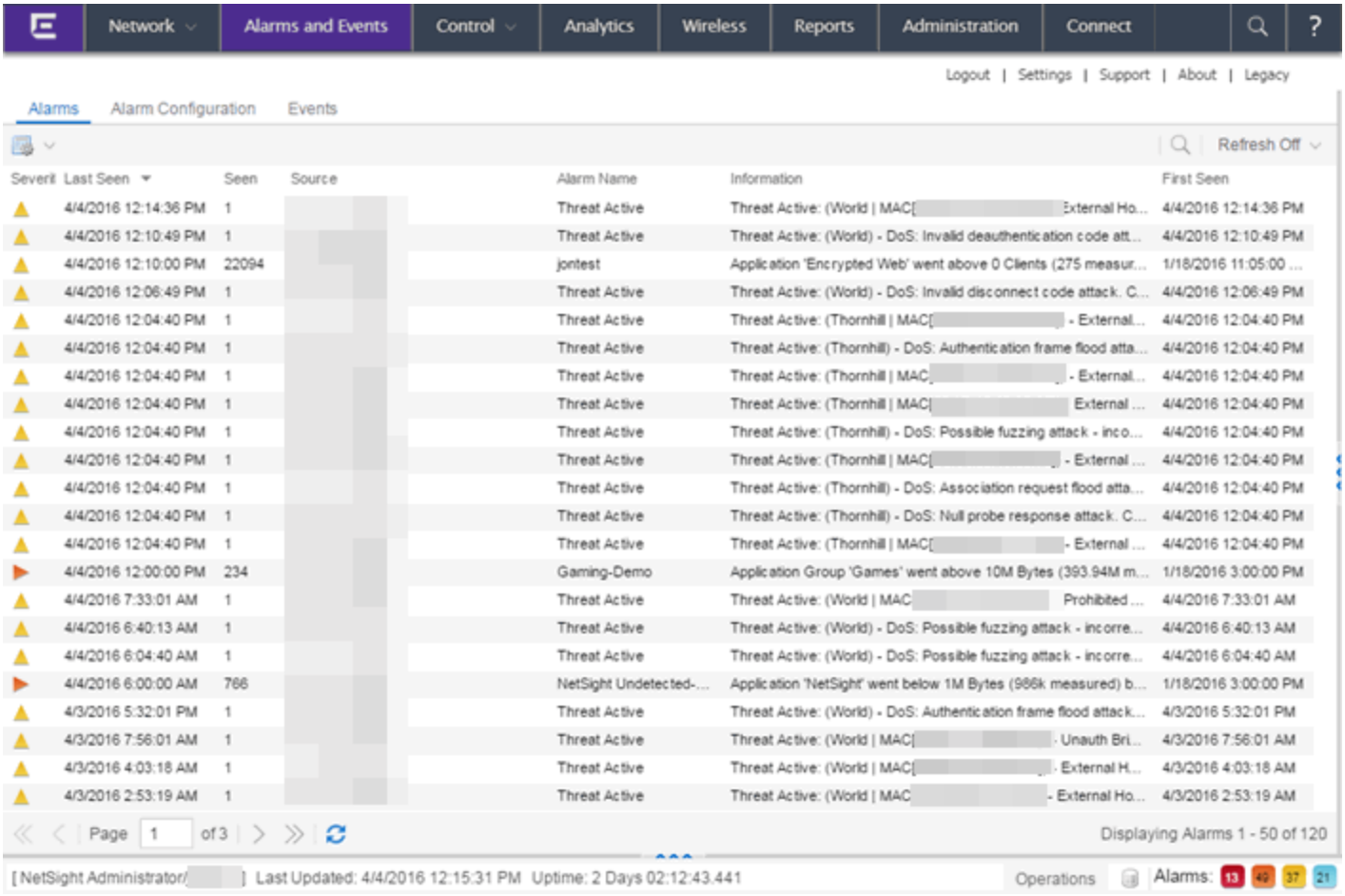
To view the information in the Alarms and Event logs, you must be a member of an authorization group assigned the appropriate Management Center capabilities:

- 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 How to Configure User Access to Extreme Management Center Applications and Extreme Management Center Access Requirements.

Alarms

Use the **Alarms and Events** tab to access an **Alarms** tab that displays the current alarms for the network.



In the **Alarms** tab:

- Right-click on the **Source** or **Alarm Name** column or click the **Gear** 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 **Source** or **Alarm Name** column or click the **Gear** icon ( ) and select **Alarm History** > **By Alarm Name** to view an Alarm History for a specific alarm.

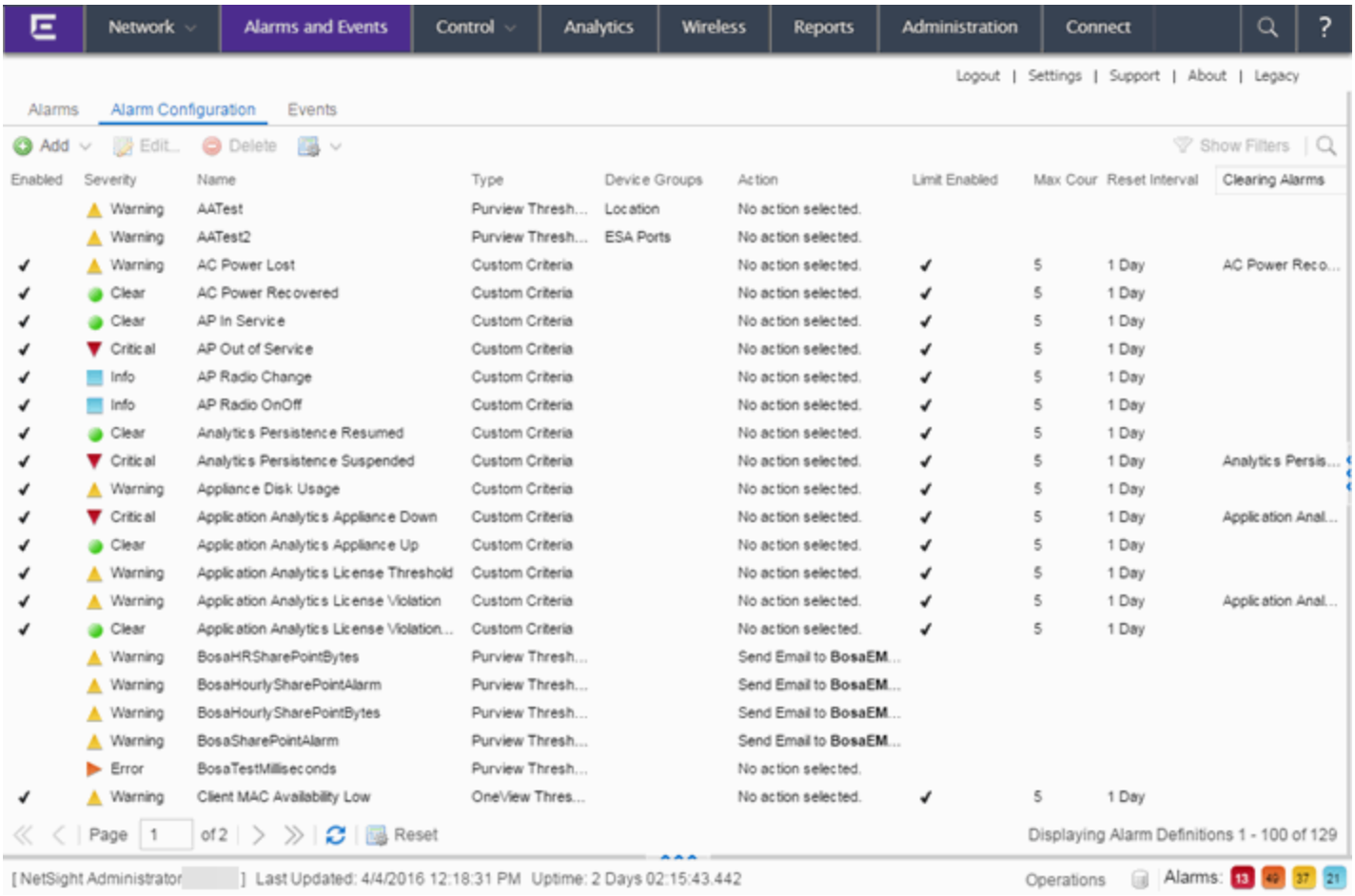
- Right-click on the **Source** or **Alarm Name** column or click the **Gear** icon ( ) and select **Alarm History** > **All** to view the Alarm History for all devices.
- Right-click on an alarm to clear the selected alarm or to clear all alarms. Supply a reason the alarm cleared, if necessary. which is recorded in the Alarm History.
- Right-click on an alarm or select an alarm and click the **Gear** 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.

Extreme Management Center

Every 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.

Alarm Configuration

The **Alarm Configuration** tab in the **Alarms and 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.

Management Center ships with a set of default alarm definitions, which you can use as is, or delete or modify them as desired.

For additional information, see How to Configure Alarms in Extreme Management Center.

Alarm Configuration Column Definitions

Enabled — A checkmark in the Enabled column indicates the alarm definition is active. Disable an alarm definition to deactivate it 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.

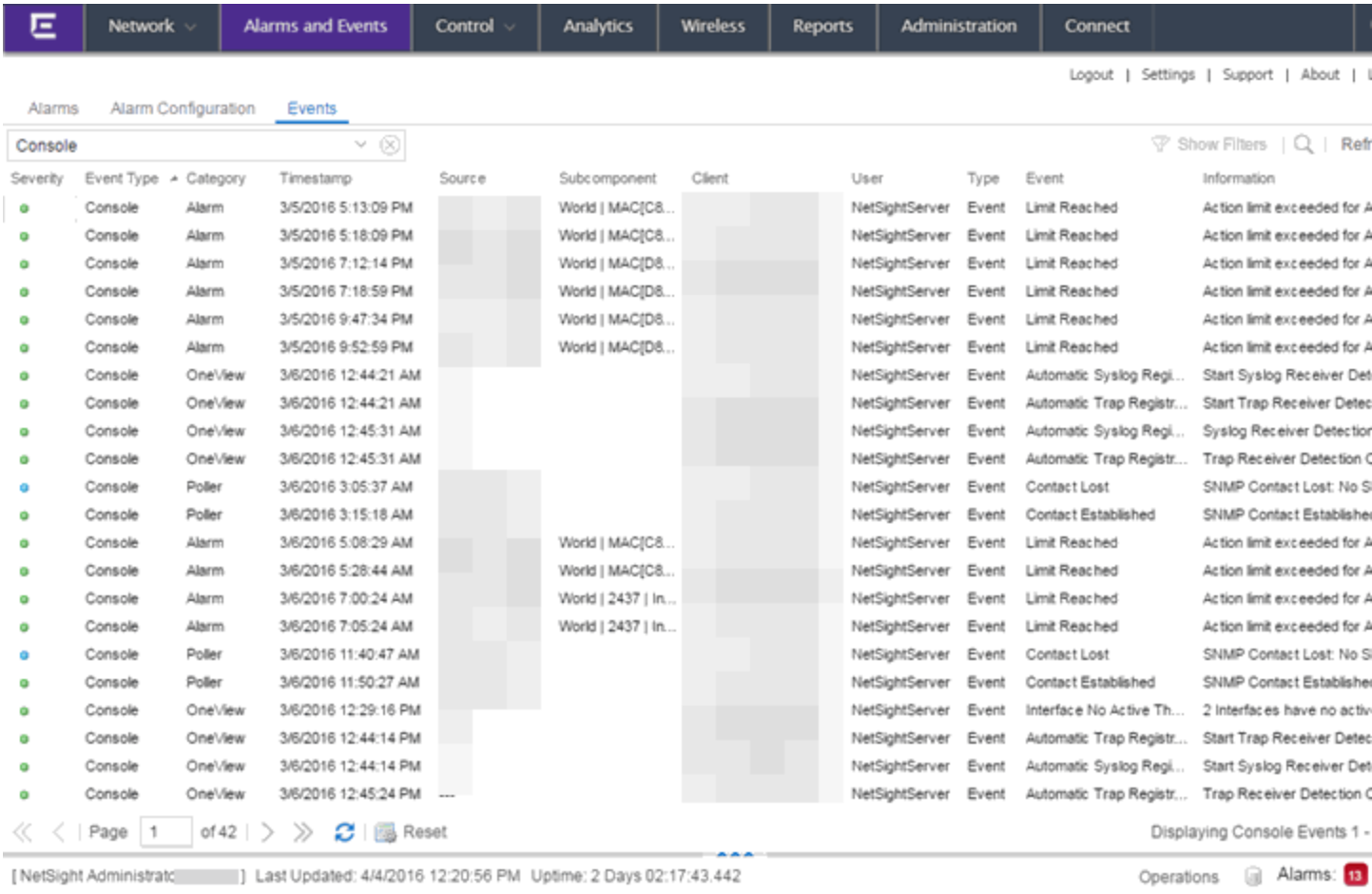
Max Count — If Limit Enabled is checked, this column indicates the number of times an action is performed for this alarm. Once the limit is reached, the alarm is still recorded, but no further actions are performed until the Reset Interval expires. If you configure multiple action types, the limit is 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. You can reset the action counters for all current alarms related to this alarm definition using the Reset All button. For example, if there is a Flow Limit Alarm on three devices, it resets the limits on those three alarms.

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 and Events tab to access the event log, as well as the event logs for Management Center, legacy applications, and Extreme Access Control Audit events and Wireless Audit events. In addition, you can access an event log for Management Center Scheduler events.



Use the drop-down menu at the top of the table to filter events based on application.

The Management Center event logs for Management Center and legacy components (Console, Automated Security, Inventory, Policy Control Console, Policy, NAC Manager, and Wireless) present the same data as the event logs in the actual applications.

The Access Control Audit event log provides information on Access Control Registration events such as when a device or user is added during the registration process, or an end-system is added/removed/updated via the registration administration web page.

The Access Control Engine event log displays engine events.

NOTE: Installed certificates using an MD5 RSA signature algorithm now generate an event in 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 Administration tab. The event log includes task execution events and errors.

The Admin event log displays Management Center server and database administrative events, and 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.

Timestamp — 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.

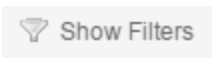
User — The user that performed the action that triggered the event.

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.

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

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.

Extreme Networks Mobile IAM (Identity and Access Management) is a comprehensive BYOD solution that provides total security, full IT control, and predictable network experience for all users. Mobile IAM provides the controls required to grant network access to BYOD devices, with the same fine-grained security controls that are applied to wired and wireless IT managed devices.

The Mobile IAM solution provides complete software for:

- Identification all of the devices connected to your network
- Access and inventory management
- Context-based policy enforcement
- End-to-end management from a single, easy-to-use management application
- Auditing and reporting

The Mobile IAM solution is delivered through an Extreme Access Control gateway engine and configured in NAC Manager. The engine is available as a physical or virtual engine to best meet your deployment needs. The solution can also include installation and integration services that are sold separately.

Contact your Extreme Networks sales representative for more information about Mobile IAM.

Additionally, the Legacy menu in the Control tab drop-down menu provides access to the following Java-based legacy applications:

- NAC Manager
- Policy Manager
- Automated Security 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

For additional information about authorization capabilities, see How to Configure User Access to Extreme Management Center Applications and Extreme Management Center Access Requirements.

Navigating the Control Tab

Clicking on **Control** in the Menu Bar at the top of Management Center opens the **Control** tab. The **Control** tab provides access to four sub-tabs:

- Dashboard — Displays summary Management Center data including end-system data, system-level information, system events, Access Control Appliance 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 at the top of the screen provides links to additional information about your version of 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. For additional information, see the Policy tab help topic.

Access Control

The **Access Control** tab lets you manage the end user connection experience and control network access based on a variety of criteria including authentication, user name, MAC address, time of day, and location. The **Access Control** tab comes with a default Access Control Configuration which is automatically assigned to your Access Control engine. You can use this default configuration as is, or make changes to the default configuration, if desired. For additional information, see Access Control tab.

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. See End-Systems for more information. 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

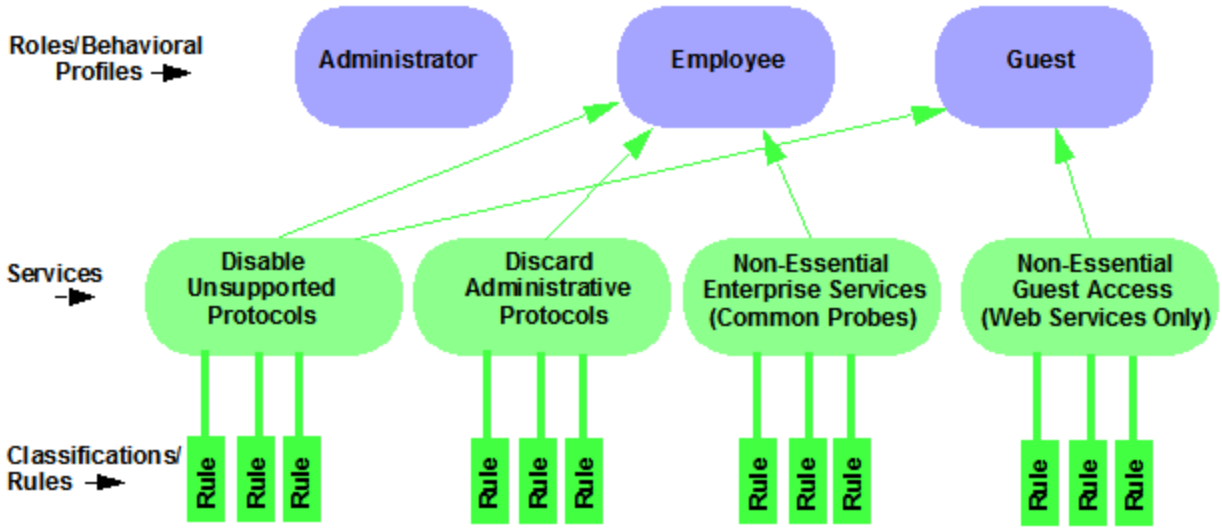
The Policy tab, contained in the Control tab of Extreme Management Center is a configuration tool that simplifies the creation and enforcement of policies on networks, enabling network engineers, information technology administrators, and business managers to work together to create the appropriate network 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.

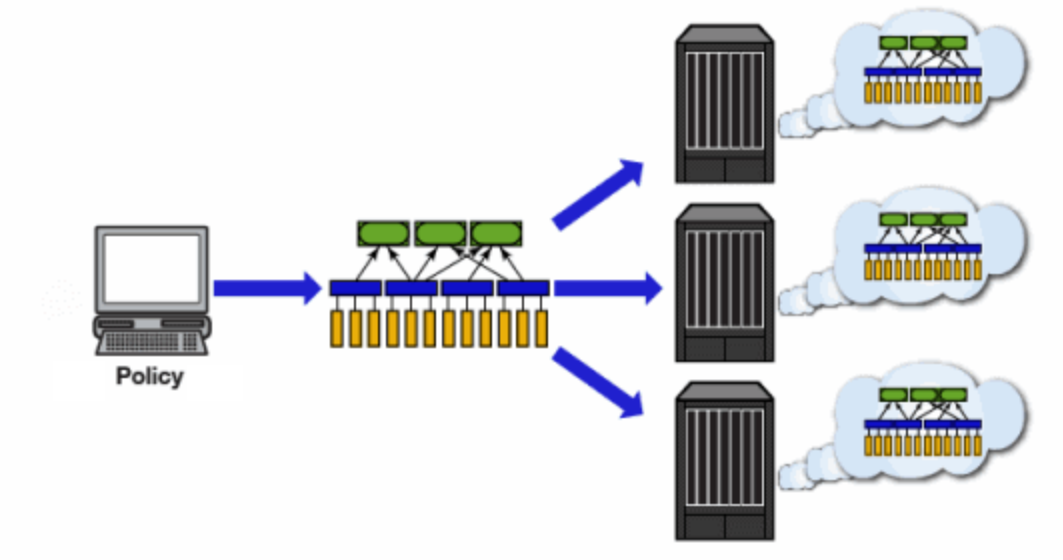
Use the following summary to guide you through the basic steps for using the Policy tab.

1. Create your Policy Domains (see How to Create and Use Domains.)
2. Add your devices to the 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
- Accessing Policy Tab Help

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.

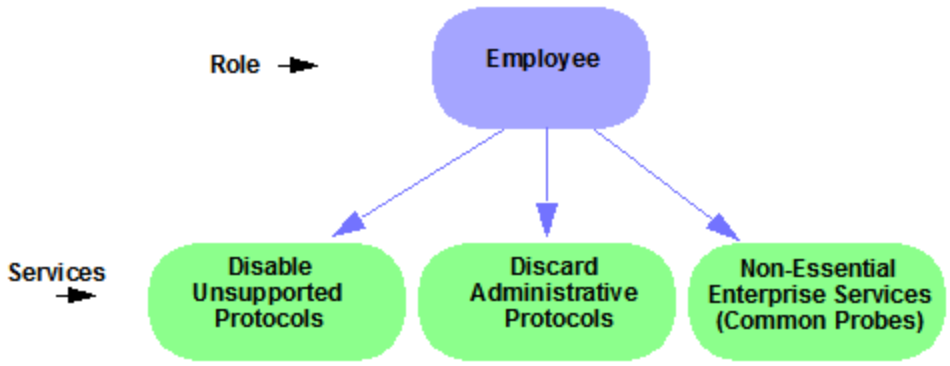
Understanding Roles

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.



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** tab.
2. Right-click the Roles folder, and select **Create Role**.
3. Enter the role name **`Office Assistant`** in the highlighted box and press **Enter**.

For more information:

- Role
- How to Create a Role

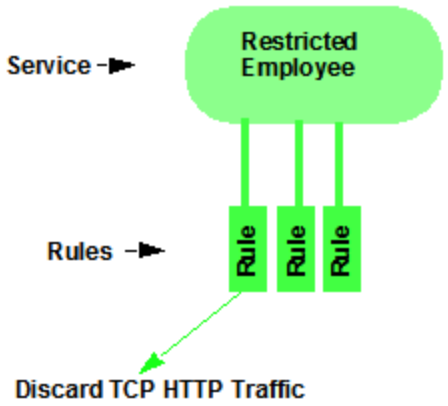
Understanding Services

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:

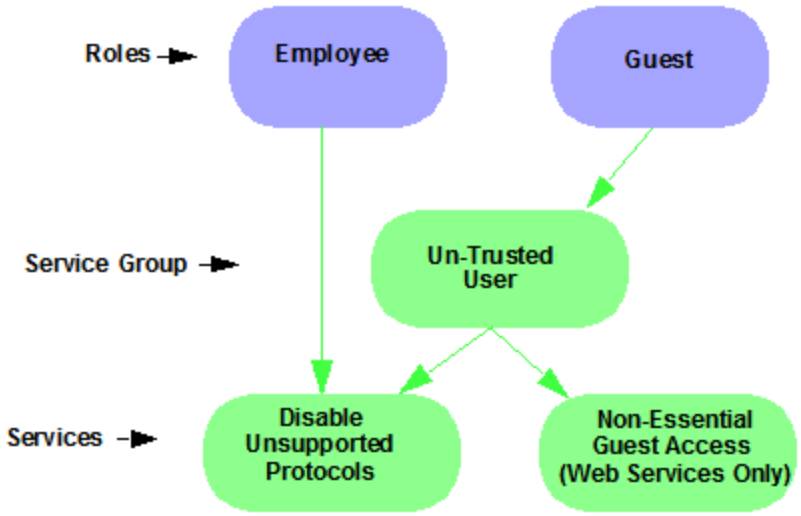
1. Click on the left-panel **Roles/Services** tab in the **Policy** tab main window.
2. Expand the **Service Repository** folder and then the **Local Services** folder.
3. Expand the **Services** folder to view a list of services.
4. Expand a service or two to see the individual classification rules 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 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 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 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.

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.

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 (formerly NetSight) **Policy** tab.

- General Considerations
  - Authenticating without Policy
  - Terminating Role Override Sessions
  - Port-Level MAC to Role Mappings
  - Import From Device
  - Flood Control
- C1 Considerations
  - Policy Support
  - Rule Limits
- N-Series Considerations
  - Role Precedence for the N-Series Platinum
- C2 and B2 Considerations
- C3 and B3 Considerations
- Mixed-Stack C2/C3 and B2/B3 Considerations
- 7100 Considerations
- Extreme Access Control Controller Configuration
- Wireless Controller Configuration

General Considerations

Authenticating without Policy

This section discusses how authentication works in a network where end users must authenticate, but there are no roles (policy) for authenticated users defined on the network devices.

The following table shows Authentication Behavior for each device type when the authenticated role is not defined on the device:

Authentication Type	K-Series, S-Series, N-Series Gold and Platinum	E6/E7	E1	RoamAbout R2 RoamAbout AP3000	C2/B2
802.1X	Successful	Successful	Successful	Successful	Successful
MAC	Successful	Successful	Successful	Successful	Successful
Web-Based	Successful	Successful on firmware version 5.06.x. Failed on older firmware versions.	Successful	Web-Based Auth Not Supported	Successful

The following table shows Authenticated Traffic Behavior for each device type when the authenticated role is not defined on the device:

Authentication Type	N-Series Gold and Platinum 4.11 and earlier	K-Series, S-Series, N-Series 5.01 and later Gold and Platinum	E6/E7	E1	RoamAbout R2 RoamAbout AP3000	C2/B2
802.1X	1	3	2	2	3	2
MAC	1	3	2	2	3	2
Web-Based	1	3	2	2	Web-Based Auth Not Supported	2

1 - Traffic is forwarded based on the 802.1Q PVID and 802.1p priority for the port, regardless of whether the port has been assigned a default role. Authenticated users display a current role of "None" in the Port Usage tab.

2 - Traffic is forwarded based on the port's default role and authenticated users will display the default role as their current role in the Port Usage tab. If no default role has been assigned to the port, the port's 802.1Q PVID and 802.1p priority are used, and the current role will be "None."

3 - Traffic is forwarded based on the Invalid Role Action configuration at the device level in the Policy tab.

Terminating Role Override Sessions

On Port Usage tabs, you cannot terminate Role Override (IP) or Role Override (MAC) sessions created through the CLI (command line interface).

Port-Level MAC to Role Mappings

Enforcing port-level MAC to Role mappings could potentially remove rules that were created by Management Center Automated Security Manager (ASM) 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 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 (created by ASM)
Authenticated role
MAC-to-Role mapping
IP override policy (created by ASM)
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 (created by ASM)
MAC-to-Role mapping
IP override policy (created by ASM)
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

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

Access Control Controllers are shipped with a default policy configuration already configured on the device. To modify this default policy configuration, you must create a domain for the Access Control Controller, assign the Access Control Controller to the domain, then import the policy configuration from the device into the Policy tab (File > Import > Policy Configuration from Device). You

can then alter the policy configuration to define the authorization levels for the Extreme Access Control process, as appropriate for your environment. If assessment will be enabled in the Extreme Networks Access Control solution, you must add classifications rules to the Quarantine and Assessing policies to 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 Access Control Controller.

NOTE: If you are using assisted remediation and quarantined end-users will be required to download remediation files via FTP, you will also need to add a rule to the Quarantine policy configuration that opens up ports 49152-65535. If you are concerned with security, you can configure your FTP server to use a smaller range of ports.

Modifying the Downstream Default Policy

Depending on the network configuration or circumstances, it's possible that traffic from the upstream side could be rerouted to the Access Control Controller where it would be authenticated using the upstream source IP address. To avoid this problem, add a Layer 3 IP Address Source rule to the downstream default policy configured on the Access Control Controller, using the upstream IP subnets (or critical servers located in the upstream) and containing the traffic to a VLAN.

Configuring LAG on Extreme Access Control Controllers

This section provides instructions for configuring LAG (link aggregation) on your Access Control Controller appliance. The instructions vary depending on whether you are configuring LAG on a Layer 2 or Layer 3 Access Control Controller.

Configuring LAG on Layer 3 Extreme Access Control Controllers - Upstream Ports

1. Configure LAG on the Access Control Controller PEP (Policy Enforcement Point) using the CLI (Command Line Interface).
2. Use the **Policy** tab to assign the appropriate upstream role as the default role on the port. For instructions, see Assigning Default Roles to Ports.

Configuring LAG on Layer 3 Extreme Access Control Controllers - Downstream Ports

1. Configure LAG on the Access Control Controller PEP (Policy Enforcement Point) using the CLI (Command Line Interface).
2. In the **Policy** tab options (Tools > Options), display the Ports panel and uncheck the Hide Logical Ports option.
3. Use the **Policy** tab to assign the appropriate downstream role as the default role on the port. For instructions, see Assigning Default Roles to Ports.

Configuring LAG on Layer 2 Extreme Access Control Controllers - Upstream Ports

1. Configure LAG on the Access Control Controller PEP (Policy Enforcement Point) using the CLI (Command Line Interface).
2. In the **Policy** tab options (Tools > Options), display the Ports panel and uncheck the Hide Logical Ports option.
3. Use the **Policy** tab to assign the appropriate upstream role as the default role on the port. For instructions, see Assigning Default Roles to Ports.

Configuring LAG on Layer 2 Extreme Access Control Controllers - Downstream Ports

1. Configure LAG on the Access Control Controller PEP (Policy Enforcement Point) using the CLI (Command Line Interface).
2. In the **Policy** tab options (Tools > Options), display the Ports panel and uncheck the Hide Logical Ports option.
3. Use the **Policy** tab to assign the appropriate downstream role as the default role on the port. For instructions, see Assigning Default Roles to Ports.
4. Use the CLI to set the following command: nodealias maxentries 4096 <lag port>.

ExtremeWireless Controller Configuration

The following sections present information regarding support for the ExtremeWireless Controller in the **Policy** tab. Review the following considerations prior to configuring policy on wireless controller devices.

Version Supported

The Policy tab only supports Wireless Controller version 8.01.03 and higher.

Policy Rules

This section describes wireless controller support for policy rules.

Supported Rule Types

The Wireless Controller supports the following traffic classification rule types:

- Ethertype
- MAC Address Source/Destination/Bilateral
- Priority
- IP Type of Service
- IP Protocol Type[1]
- ICMP
- IP Address Source/Destination/Bilateral
- IP Socket Source/Destination/Bilateral
- IP UDP Port Source/Destination/Bilateral
- IP UDP Port Source/Destination/Bilateral Range
- IP TCP Port Source/Destination/Bilateral
- IP TCP Port Source/Destination/Bilateral Range

[1]Not all IP Protocols are supported for the wireless controller. Supported IP Protocols for this rule type are: ICMP, TCP, UDP, GRE, ESP, AH.

"No Change" Filter Sets

The wireless controller 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

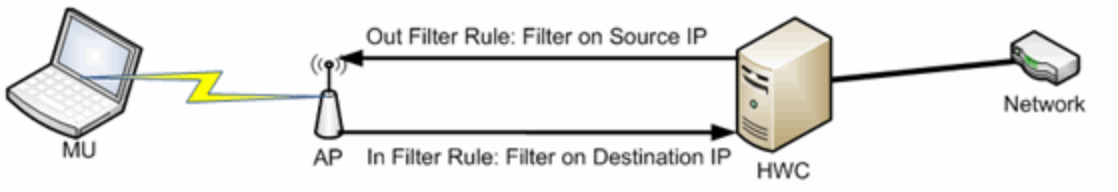
The following list defines the wireless controller support for rule actions:

- 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."

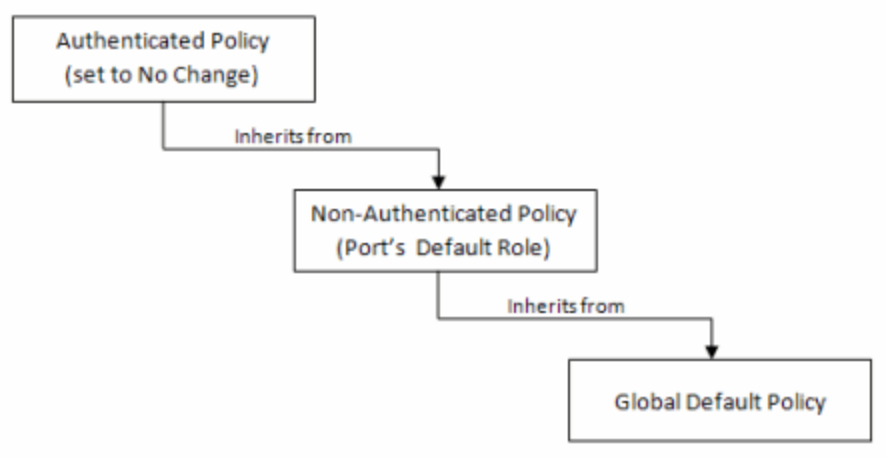
This internal VLAN cannot be used in your Policy tab domain configuration to tag traffic. If the VID for the internal VLAN is used in your domain configuration, the Policy tab enforce fails with an error message in the Event Log indicating the internal VID cannot be used.

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.

Policy Concepts

This topic explains concepts used in the **Policy** tab.

Information on:

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).

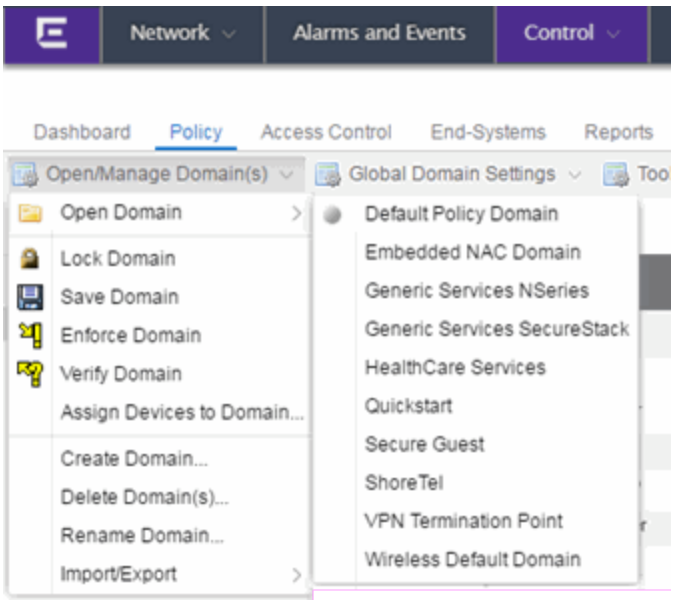
Policy Domains

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 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. 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.)

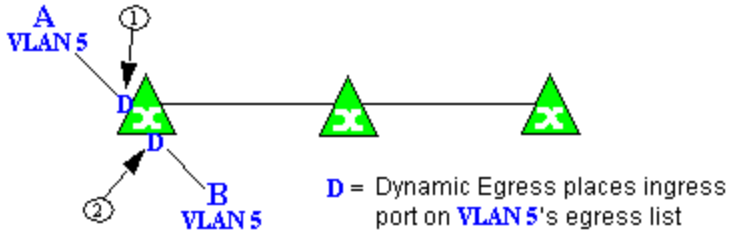
If an endstation is talking to a "silent" endstation which does not send responses, like a printer, you need to add the silent endstation's ingress port to the VLAN's egress list manually using local management. Dynamic Egress and GVRP take care of adding the other ingress ports to the VLAN's egress 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

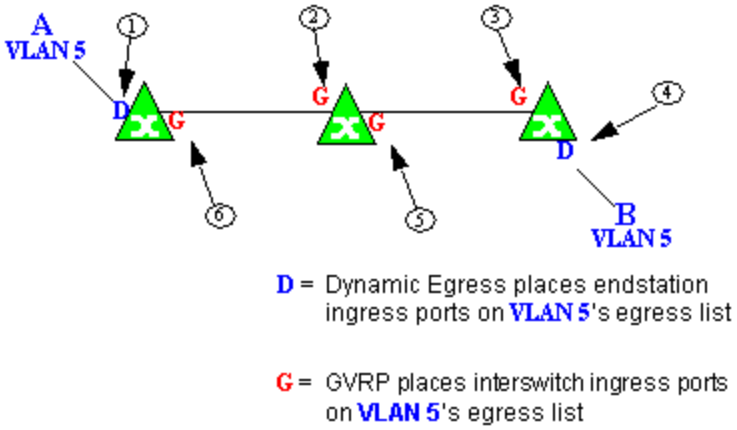
In this example, Dynamic Egress is enabled for VLAN 5. When source endstation A is tagged with VLAN 5, Dynamic Egress places A's ingress port (1) on VLAN 5's egress list. When destination endstation B's traffic is tagged with VLAN 5,

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

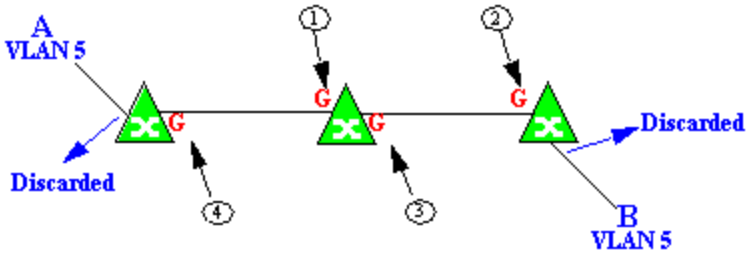
In this example, Dynamic Egress is enabled for VLAN 5, and the destination endstation, B, is on a different device from the source endstation, A. When A is tagged with VLAN 5, Dynamic Egress places A's ingress port (1) on VLAN 5's egress list. GVRP then places interswitch ingress ports (2) and (3) on 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.

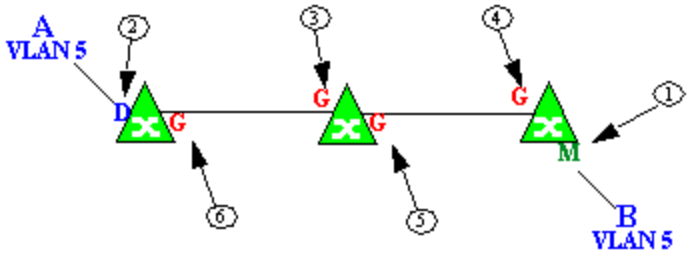


G = GVRP places interswitch ingress ports on VLAN 5's egress list

VLAN 5 Traffic for A and B discarded - A's and B's ingress ports not on VLAN's egress list

Example 4: Silent Endstation

In this example, Dynamic Egress is enabled for VLAN 5, but the destination endstation, B, is a "silent" endpoint, like a printer. Endstation B does not send responses, so the Administrator must place B's ingress port on VLAN 5's egress list manually (1). When A is tagged with VLAN 5, Dynamic Egress places A's ingress port (2) on VLAN 5's egress list. GVRP then places interswitch ingress ports (3) and (4), then (5) and (6) on VLAN 5's egress list. Endstation A is then able to communicate with the printer.



M = Administrator manually places B's ingress port on VLAN 5's egress list

D = Dynamic Egress places A's ingress port on VLAN 5's egress list

G = GVRP places interswitch ingress ports on VLAN 5's egress list

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, 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 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 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 Management Center application identification reports and analysis.

For information on configuring traffic mirroring, see the Role tab and the Rule General tab.

Port Groups

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 Management Center Administrator profile to communicate with devices. Because of this, the 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 Server Information window Locks tab. You can also revoke locks from this panel. For more information, see Viewing Locks.

Related Information

For information on related concepts:

- Traffic Classification Rules

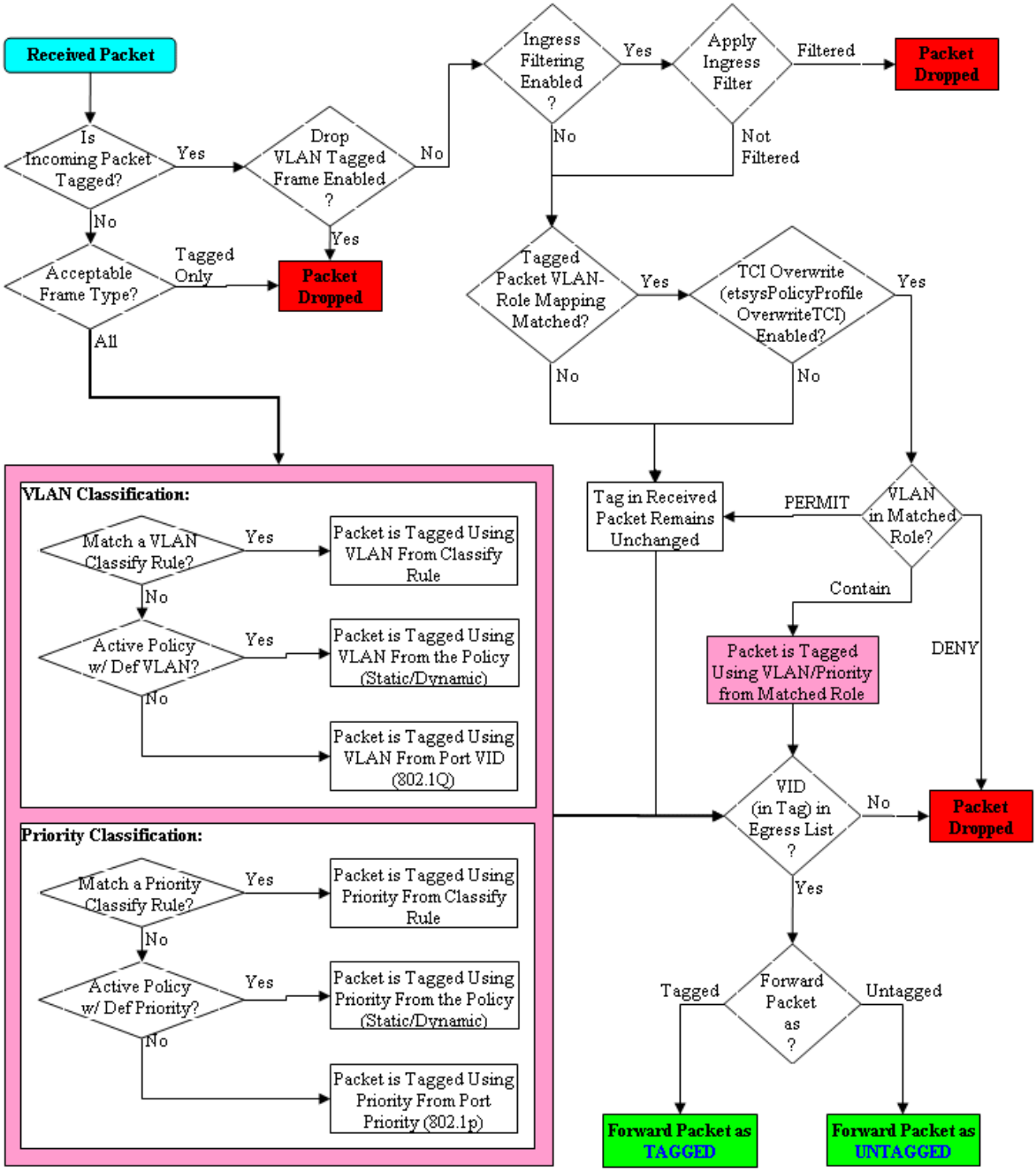
For information on related tasks:

- Creating a Role
- How to Create a VLAN

For information on related windows:

- Create VLAN Window

Packet Flow Diagram



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

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
ARP	0x0806
Reverse ARP	0x8035
Novell IPX 1	0x8137
Novell IPX 2	0x8138
Banyan	0x0bad
AppleTalk	0x809b
AppleTalk ARP	0x80f3

Well-known Ethertypes	Values
IPv6	0x86dd
Decnet Phase 4	0x6003

DSAP/SSAP

This classification type is based on the specific protocol type of each frame defined in the DSAP and SSAP fields. Select a protocol from the list of well-known values, or select Other and manually enter a custom two-byte value in hexadecimal format (0xFFFF). The LSB of the DSAP address specifies Individual(0) or Group(1), while the LSB of the SSAP address specifies Command(0) or Response(1). For the SNAP frame type, you may enter Advanced DSAP/SSAP configurations. The advanced fields are not supported on legacy devices and are ignored.

Well-known DSAP/SSAP Types	Values
IP	0x0606
IPX	0xe0e0
NetBIOS	0xf0f0
Banyan Vines	0xbcbc
SNA	0x0404
SNAP	0xAAAA
Other	a two-byte value

VLAN ID

This classification type is based on an exact match of the VLAN tag contained within a frame. Select a VLAN ID (VID) from the list of VLANs defined in the Policy tab. If you select Other, you must enter a single VID or specify a range of VIDs in decimal form. Range rules are not supported on legacy devices.

Priority

This classification type is based on an exact match of the Priority tag contained within a frame. Select a Priority value 0 - 7 from the list of well-known values, or select Other and enter a value in decimal form.

Layer 3 -- Network Classification Types

Layer 3 Network classification types allow you to define classification rules based on specific information contained within the Layer 3 header of an IP or IPX frame.

IP Time to Live (TTL)

This classification type is based on an exact match of the TTL field contained in the IP header of a frame. The TTL field indicates the maximum number of router hops the packet can make before being discarded. The TTL field is set by the packet sender and reduced by every router on the route to its destination. If the TTL field reaches zero before the packet arrives at its destination, then the packet is discarded. IP Time to Live rules are only supported on K-Series and S-Series devices.

IPX Network Source, IPX Network Destination, IPX Network Bilateral

These classification types are based on specific information contained within the Layer 3 header of an IPX frame. It is a four-byte user-defined value that represents the IPX source, destination, or bilateral (either source or destination) network number. This value must be a valid IPX network address in hexadecimal form. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

IPX Socket Source, IPX Socket Destination, IPX Socket Bilateral

These classification types are based on specific information contained within the Layer 3 header of an IPX frame. It is a two-byte, user-defined value that represents the IPX source, destination, or bilateral (either source or destination) socket numbers. This value is used by higher layer protocols to target specific applications running among hosts. Select an IPX Socket type from the list of well-known values, or select Other and manually enter the value in decimal form. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

Well-known IPX Socket Types	Values
NCP	1105
SAP	1106
RIP	1107
NetBIOS	1109
Diagnostics	1110
NSLP	36865
IPX Wan	56868
Other	0-65535

IPX Class of Service

This classification type is based on specific information contained within the Layer 3 header of an IPX frame. This is a one-byte field used for transmission control (hop count) by IPX routers. Enter a valid IPX Class of

Service in decimal form, 0-255. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

IPX Packet Type

This classification type is based on specific information contained within the Layer 3 header of an IPX frame. Select an IPX Packet type from the list of well-known values or select Other and manually enter the value in decimal form. You can enter a range of values, however range rules are not supported on legacy devices or N-Series Gold.

Well-known IPX Packet Types	Values
Hello/SAP	0
RIP	1
Echo Packet	2
Error Packet	3
NetWare 386	4
SeqPackProt	5
NetWare 286	17
Other	0-31

IPv6 Address Source, IPv6 Address Destination, IPv6 Address Bilateral

These classification types are based on an exact match of the source, destination, or bilateral (either source or destination) IPv6 address information contained within the IPv6 header of each frame. Enter a valid IPv6 address and optional mask ("/n") in the Value field.

IPv6 Socket Source, IPv6 Socket Destination, IPv6 Socket Bilateral

These classification types are based on an exact match of a specific source, destination, or bilateral (either source or destination) IPv6 address and a UDP/TCP port number (type) contained within the IPv6 header of each frame. Enter an IPv6 address in the Value field. Then, select a UDP/TCP type from the list of well-known values, or select Other and manually enter the value in
form. (UDP/TCP port numbers are defined in RFC 1700.) If you select Other, you can enter a range of values.

Well-known UDP/TCP Types	Values
FTP Data	20
FTP	21

Well-known UDP/TCP Types	Values
SSH	22
Telnet	23
SMTP	25
TACACS	49
DNS	53
BootP Server	67
BootP Client	68
TFTP	69
Finger	79
HTTP	80
POP3	110
Portmapper	111
NNTP	119
NTP	123
NetBIOS Name Service	137
NetBIOS Datagram Service	138
NetBIOS Session Service	139
IMAP2/IMAP4	143
SNMP	161
IMAP3	220
LDAP	389
HTTPS	443
R-Exec	512
R-Login	513
R-Shell	514
LPR	515
RIP	520
SOCKS	1080
Citrix ICA	1494
RADIUS	1812
RADIUS Accounting	1813
NFS	2049

Well-known UDP/TCP Types	Values
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

Well-known UDP/TCP Types	Values
TFTP	69
Finger	79
HTTP	80
POP3	110
Portmapper	111
NNTP	119
NTP	123
NetBIOS Name Service	137
NetBIOS Datagram Service	138
NetBIOS Session Service	139
IMAP2/IMAP4	143
SNMP	161
IMAP3	220
LDAP	389
HTTPS	443
R-Exec	512
R-Login	513
R-Shell	514
LPR	515
RIP	520
SOCKS	1080
Citrix ICA	1494
RADIUS	1812
RADIUS Accounting	1813
NFS	2049
X11 (Range Start)	6000
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

Well-known IP Protocol Types	Values
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

Well-known UDP Types	Values
SMTP	25
TACACS	49
DNS	53
BootP Server	67
BootP Client	68
TFTP	69
Finger	79
HTTP	80
POP3	110
Portmapper	111
NNTP	119
NTP	123
NetBIOS Name Service	137
NetBIOS Datagram Service	138
NetBIOS Session Service	139
IMAP2/IMAP4	143
SNMP	161
IMAP3	220
LDAP	389
HTTPS	443
R-Exec	512
R-Login	513
R-Shell	514
LPR	515
RIP	520
SOCKS	1080
Citrix ICA	1494
RADIUS	1812
RADIUS Accounting	1813
NFS	2049
X11 (Range Start)	6000
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
IMAP3	220
LDAP	389

Well-known 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 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.

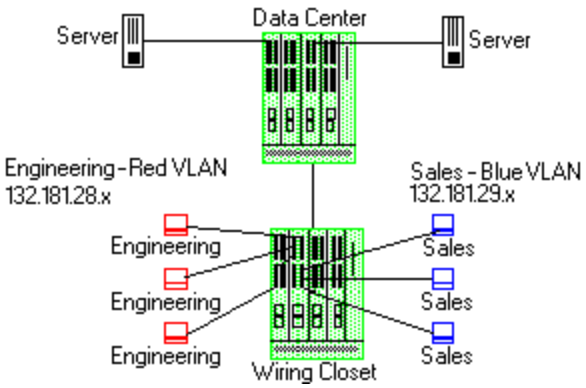
Examples of How Rules are Used

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.

IP Traffic Containment



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.

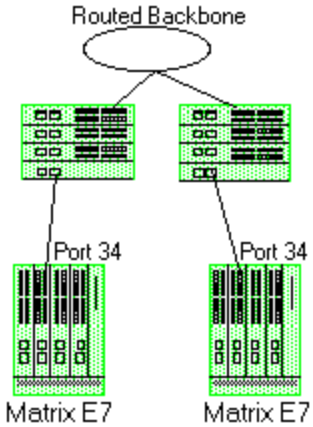
Rule 2 - Sales, which uses the 132.181.29.x subnet, will be assigned to the Blue VLAN.

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.

OSPF/RIP Traffic Filtering



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.

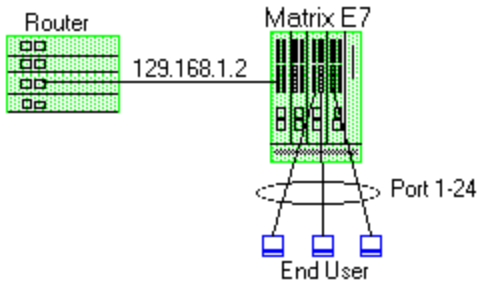
Rule 2 (Layer 4) - Any frame received with a Bilateral UDP port number of 520 (RIP) will be discarded.

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.

Router Traffic Security



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.

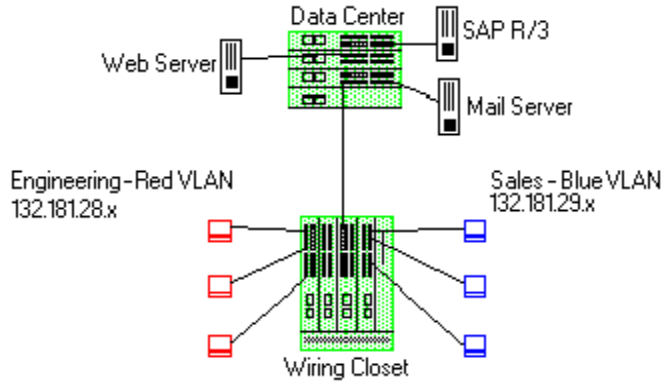
Rule - Any frames received by the switch with a destination IP address of the router (129.168.1.2) will be discarded.

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.

Prioritization



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

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
- Rate Limits
- Transmit Queues
- Flood Control

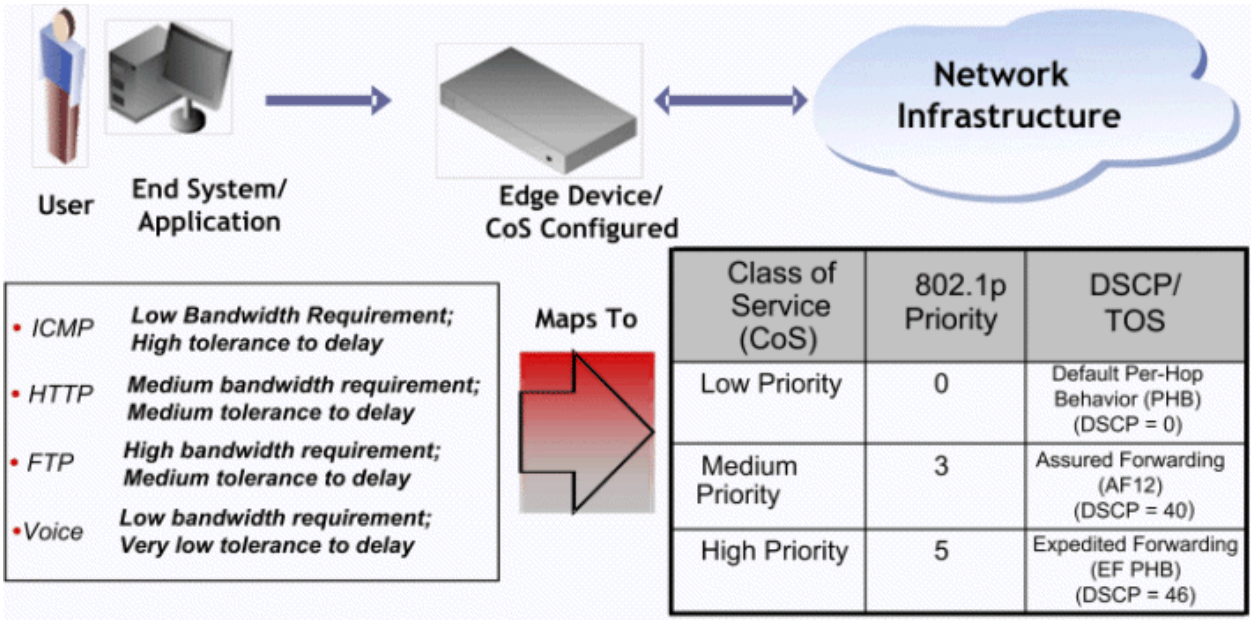
Class of Service Overview

Class of Service (CoS) provides the ability to give certain network traffic preferential treatment over other traffic. It classifies traffic into categories such as high, medium, and low, where high-priority traffic gets the best service while low-priority traffic is "drop eligible."

Class of Service helps you manage the bandwidth requirements of a given network flow with the available port resources on your network devices. (In a CoS context, a flow is a stream of packets classified with the same class of service as the packets transit the interface). Using CoS, you can:

- Assign different priority levels to different packet flows.
- Mark or re-mark the packet priority at port ingress with a Type of Service (ToS).
- Sort flows by transit queue. Higher priority queues get preferential access to bandwidth during packet forwarding.
- Limit the amount of bandwidth available to a given flow by either dropping (rate limiting) or buffering (rate shaping) packets in excess of configured limits.

The following figure shows how you can manage network bandwidth requirements by assigning different classes of service to different types of network traffic.



The ICMP protocol, used for error messaging, has a low bandwidth requirement, with a high tolerance for delay and jitter, and is appropriate for a low priority setting. HTTP and FTP protocols, used respectively for browser-generated and file transfer traffic, have a medium to high bandwidth requirement, with a medium to high tolerance for delay and jitter, and are appropriate for a medium priority level. Voice (VoIP), used for voice calls, has a low bandwidth requirement, but is very sensitive to delay and jitter and is appropriate for a high priority level.

Implementing CoS

CoS determines how a given network flow is assigned bandwidth as it transits your network devices. As a preliminary step to using CoS, it is important that you understand the characteristics of the flows on your network and associate these flows with your policy roles. In this sense, CoS is the third step in a three step process:

1. Understand your network flows using NetFlow.
2. Associate your network flows with a **Policy** tab role.
3. Configure your classes of service and associate them with the rules contained in your roles.

Configuring CoS

The **Policy** tab lets you configure multiple classes of service that include one or more of the following components:

- 802.1p priority
- IP type of service (ToS) value
- drop precedence
- inbound and outbound rate limits
- outbound rate shaper per transmit queue.
- flood control rate limits

After you have created and defined your classes of service, they are then available when you make a class of service selection for a rule action (**Rule** tab), a role default (**General** tab), or an automated service (**Automated Service** tab).

To view and configure CoS, open the **Class of Service Overview** tab from the **Policy** tab. It is pre-populated with eight static classes of service, each associated with one of the 802.1p priorities (0-7). You can use these classes of

service as is, or configure them to include ToS, drop precedence, rate limit, and/or transmit queue values. In addition, you can also create your own classes of service (user-defined CoS).

Rate Limits

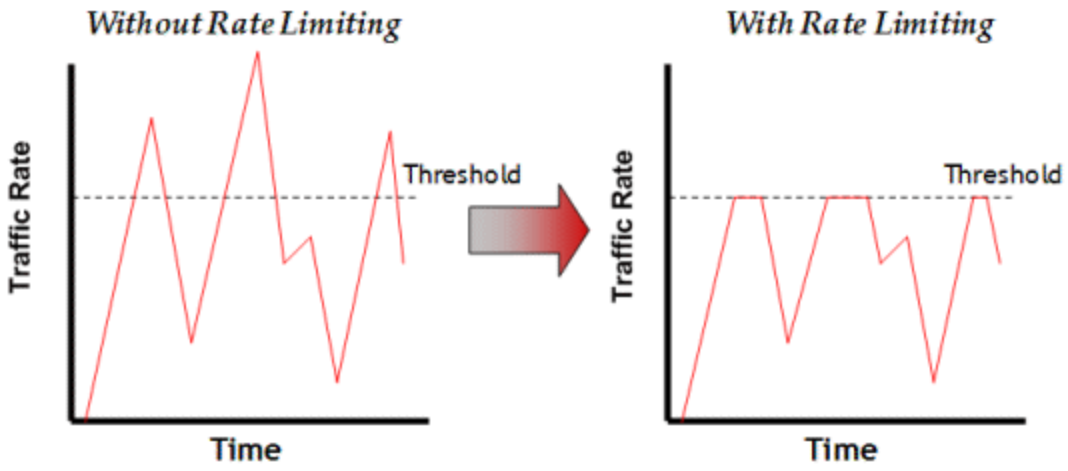
Rate limits are one component of a **Policy** tab class of service. They control the transmit rate at which traffic enters and exits ports in your network. All traffic mapped to a Class of Service on a given port share the bandwidth specified by the rate limit.

For instructions on how to configure rate limits, see How to Define Rate Limits.

Rate limits are tied directly to roles and rules, and are written to a device when the role/rule is enforced. When rate limits are implemented, all traffic on the port that matches the rule with the associated rate limit cannot exceed the configured limit. If the rate exceeds the configured limit, frames are dropped until the rate falls below the limit.

The rate limit remains on the port only as long as the role using the rate limit is active on the port either as the authenticated role or as the port's default role.

The following figure shows how bursty traffic is clipped above the assigned threshold when rate limiting is applied.



The CoS can be configured to perform one or all of the following actions when a rate limit is exceeded:

- Generate System Log on Rate Violation - a syslog message is generated when the rate limit is first exceeded.

- Generate Audit Trap on Rate Violation - an audit trap is generated when the rate limit is first exceeded.
- Disable Port on Rate Violation - the port is disabled when the rate limit is first exceeded.

The Policy tab class of service also provides the ability to create rate limit port groups. Port groups let you specify different rate limits within the same class of service. For example, you might create a port group for edge ports and a port group for core ports, and assign two different rate limits. For more information on rate limit port groups, see Creating Class of Service Port Groups.

Transmit Queues

Transmit queue configuration is defined within a class of service and associated with a specific role via a rule action or as a role default. It is implemented based on the role assigned to a port. All traffic received on a port and matching a rule with the associated class of service is forwarded using the defined transmit queue configuration.

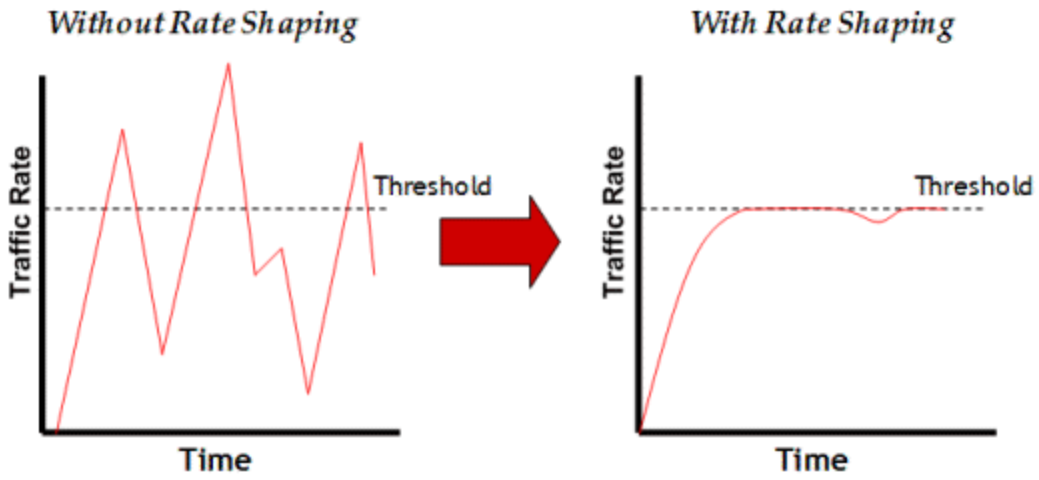
For instructions on how to configure transmit queues, see How to Configure Transmit Queues.

There are three components to transmit queue configuration:

- Transmit Queue Configuration 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

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.

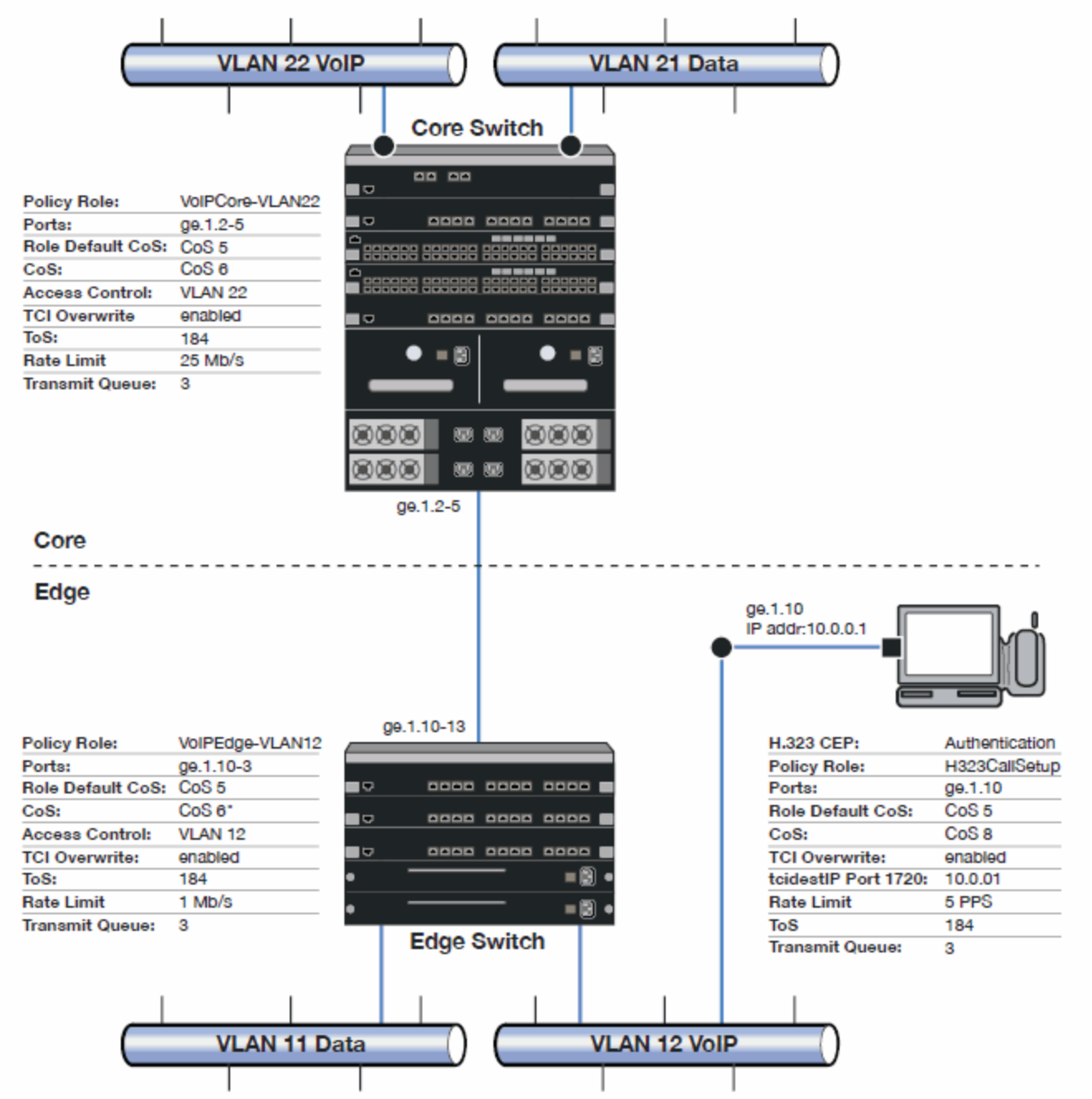
To simplify the discussion of the configuration process, this example is limited to the VoIP configuration context. The following table provides a set of sample

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

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 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 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)

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)

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)

ToS/DSCP Value Definition Chart

Use this chart to compare ToS and DSCP values.

ToS (Dec)	ToS (Hex)	ToS (Binary)	ToS Precedence (Binary)	ToS Precedence (Decimal)	ToS Precedence Name	ToS Delay Flag	ToS Throughput Flag	ToS Reliability Flag	DSCP (Binary)	DSCP (Hex)	DSCP (Decimal)	DSCP Class
0	0x00	00000000	000	0	Routine	0	0	0	000000	0x00	0	none
32	0x20	00100000	001	1	Priority	0	0	0	001000	0x08	8	cs1
40	0x28	00101000	001	1	Priority	0	1	0	001010	0x0A	10	af11
48	0x30	00110000	001	1	Priority	1	0	0	001100	0x0C	12	af12
56	0x38	00111000	001	1	Priority	1	1	0	001110	0x0E	14	af13
64	0x40	01000000	010	2	Immediate	0	0	0	010000	0x10	16	cs2
72	0x48	01001000	010	2	Immediate	0	1	0	010010	0x12	18	af21
80	0x50	01010000	010	2	Immediate	1	0	0	010100	0x14	20	af22
88	0x58	01011000	010	2	Immediate	1	1	0	010110	0x16	22	af23
96	0x60	01100000	011	3	Flash	0	0	0	011000	0x18	24	cs3
104	0x68	01101000	011	3	Flash	0	1	0	011010	0x1A	26	af31
112	0x70	01110000	011	3	Flash	1	0	0	011100	0x1C	28	af32
120	0x78	01111000	011	3	Flash	1	1	0	011110	0x1E	30	af33
128	0x80	10000000	100	4	FlashOverride	0	0	0	100000	0x20	32	cs4
136	0x88	10001000	100	4	FlashOverride	0	1	0	100010	0x22	34	af41
144	0x90	10010000	100	4	FlashOverride	1	0	0	100100	0x24	36	af42
152	0x98	10011000	100	4	FlashOverride	1	1	0	100110	0x26	38	af43
160	0xA0	10100000	101	5	Critical	0	0	0	101000	0x28	40	cs5
184	0xB8	10111000	101	5	Critical	1	1	0	101110	0x2E	46	ef

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
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

How To Use Policy

The How To section contains Help topics that give you instructions for performing tasks in the Policy tab.

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 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
- Using Console to Import Devices
- Adding a Single Device
- Deleting Devices from the Database

Using Console to Discover Devices

Console Discover lets you to discover your network devices and add them to the 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 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 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 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 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 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 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 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 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 Create a Port Group

The **Policy** tab allows you to group ports into user-defined port groups, similar to the way you can group services into service groups. Port groups enable you to configure multiple ports on the same device or on different devices, simultaneously. A port can be a member of more than one group.

When you create a user-defined port group, you select individual ports to add to the group.

The **Policy** tab also provides you with Pre-Defined Port Groups which are automatically populated according to port characteristics. See Pre-Defined Port Groups for more information.

Instructions on:

- Creating a Port Group
- Adding Ports to a Port Group
- Removing Ports from a Port Group

Creating a Port Group

1. In the left panel, 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

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) and the Extreme Management Center Automated Security Manager to create an automatic response to threats detected on the network. Once the Quarantine role has been enforced to the network, and both the Extreme Networks IPS and the Automated Security Manager are 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. In this case however, the Automated Security Manager determines a network threat, identifies the responsible port, and applies the Quarantine role to the port.

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: Because it is used by the Automated Security Manager, 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

When the Automated Security Manager detects a threat on the network, it automatically assigns the Quarantine role as the default role on that port. However, 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 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.

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 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, 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, 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
- Modifying a Service Name
- Modifying the Roles for a Service
- Modifying the Rules for a Manual Service
- Modifying an Automated Service

Modifying a Service Description

You can edit the description for the service by selecting it and 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.

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 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, 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 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 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 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.

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

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 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 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.
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 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 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 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 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 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
- Disabling/Enabling a Rule

- Deleting a Rule

Creating a Rule

When you create a rule using the Rule tab, you first create and name the rule using the **Create Rule** menu option, then define its characteristics in the right panel. You can also use the right panel to modify an exiting rule's characteristics.

1. In the **Policy** tab left panel, select the **Roles/Services > Service Repository** tab.
2. Expand either the **Local** or **Global Services** folder, depending on whether the rule is going to be used locally or by all users.
3. Expand either the **Service Groups** or **Services** folder and 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 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 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.

Policy Tab Windows

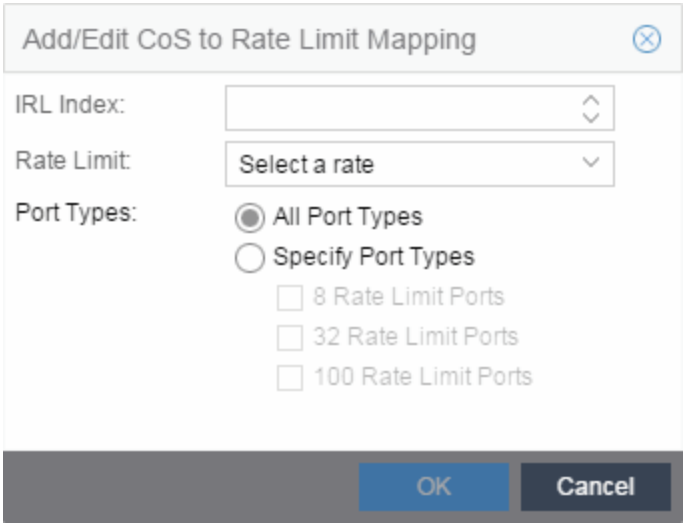
The Windows Help section contains Help topics describing Policy tab windows and their field definitions.

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)

Add Devices (VLAN Islands)

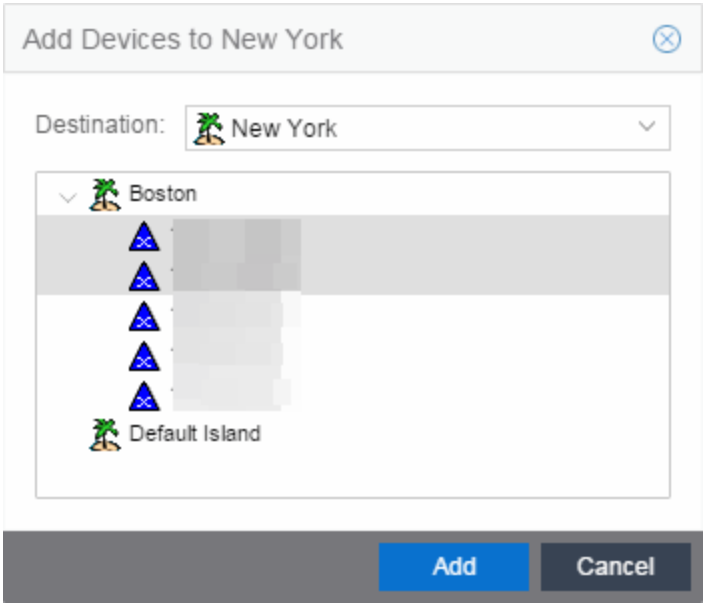
This window enables you to add devices to VLAN islands.

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

Add/Remove Ports

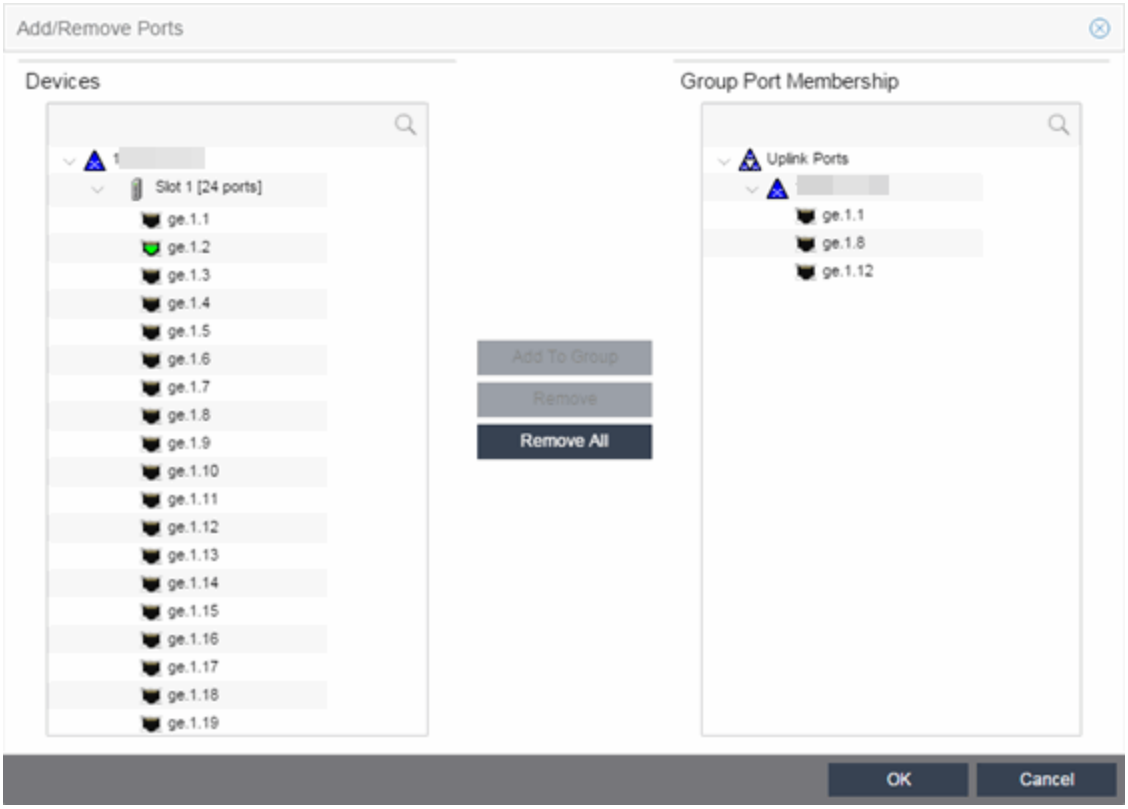
In this window, you can add and remove ports to and from port groups. Initially, all ports are grouped into a Default port group. When you create new port

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

Add/Remove Services (Roles)

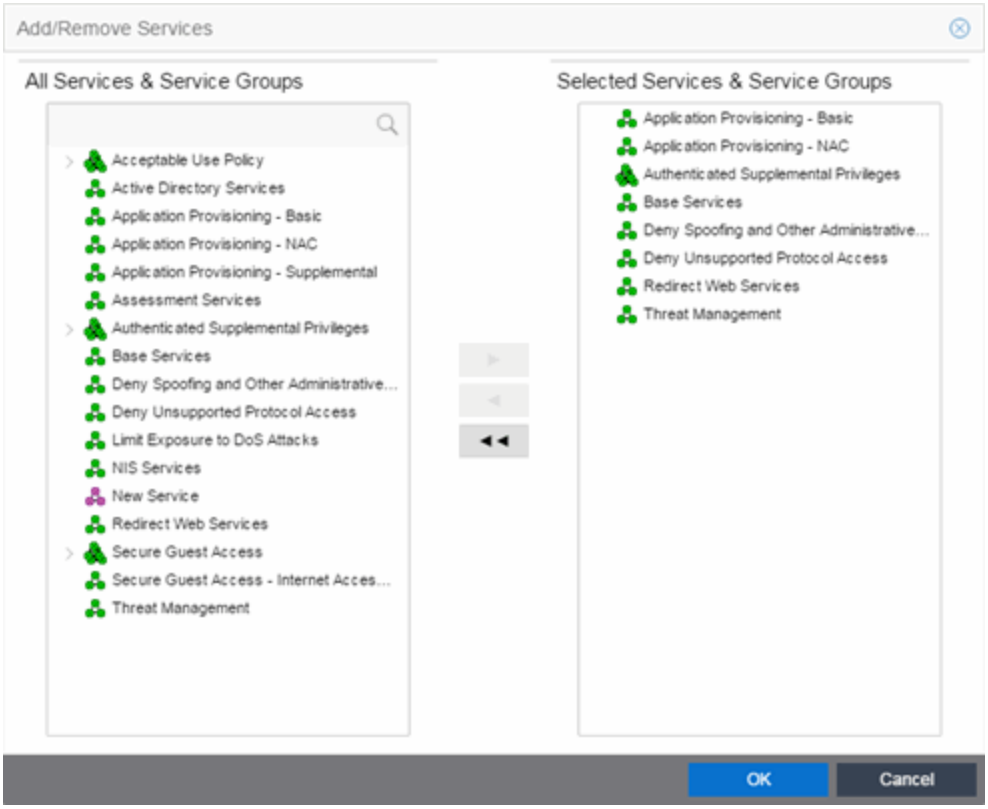
Add and remove services and service groups from roles using the Add/Remove Services window.

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

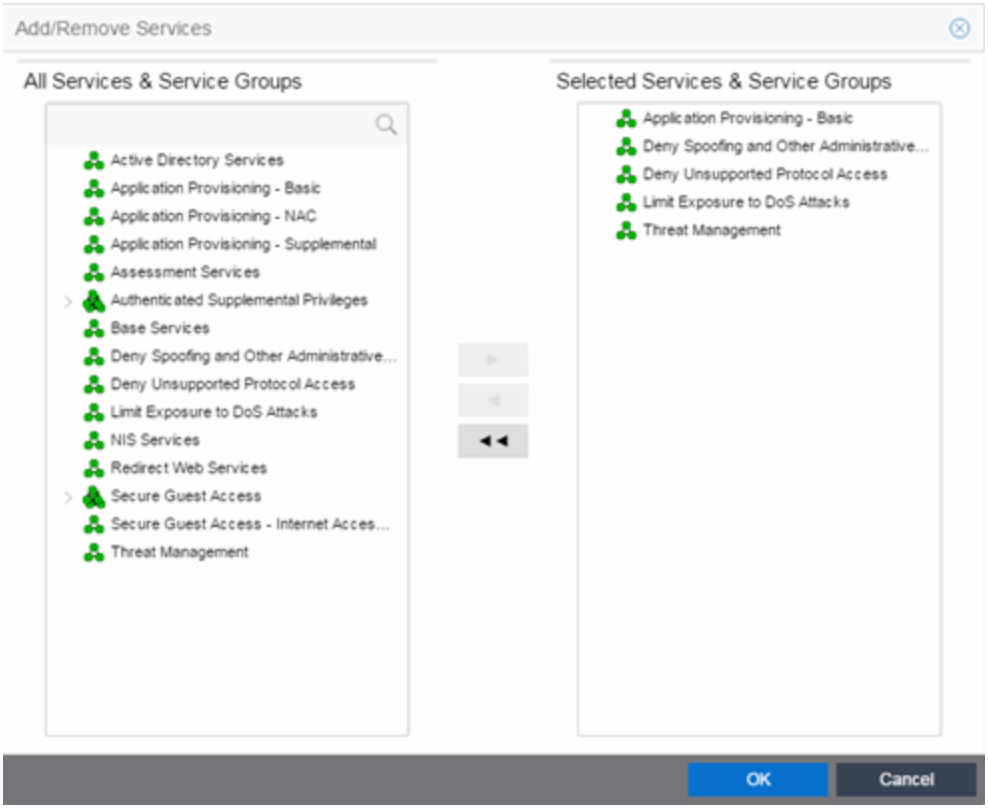
For information on related tasks:

- Adding Services to a Role
- Removing Services from a Role

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:

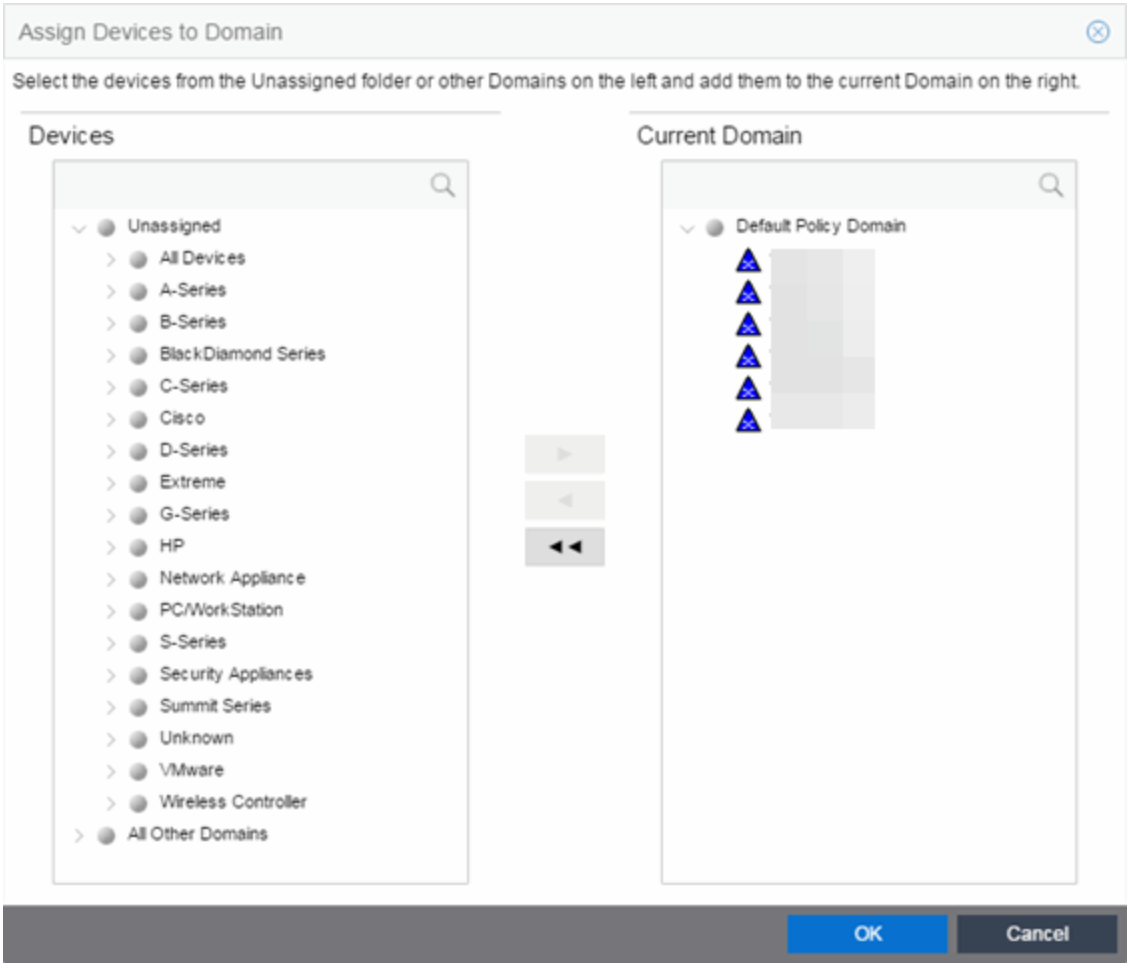
- Adding Services to a Service Group
- Removing Services from a Service Group

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 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 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:

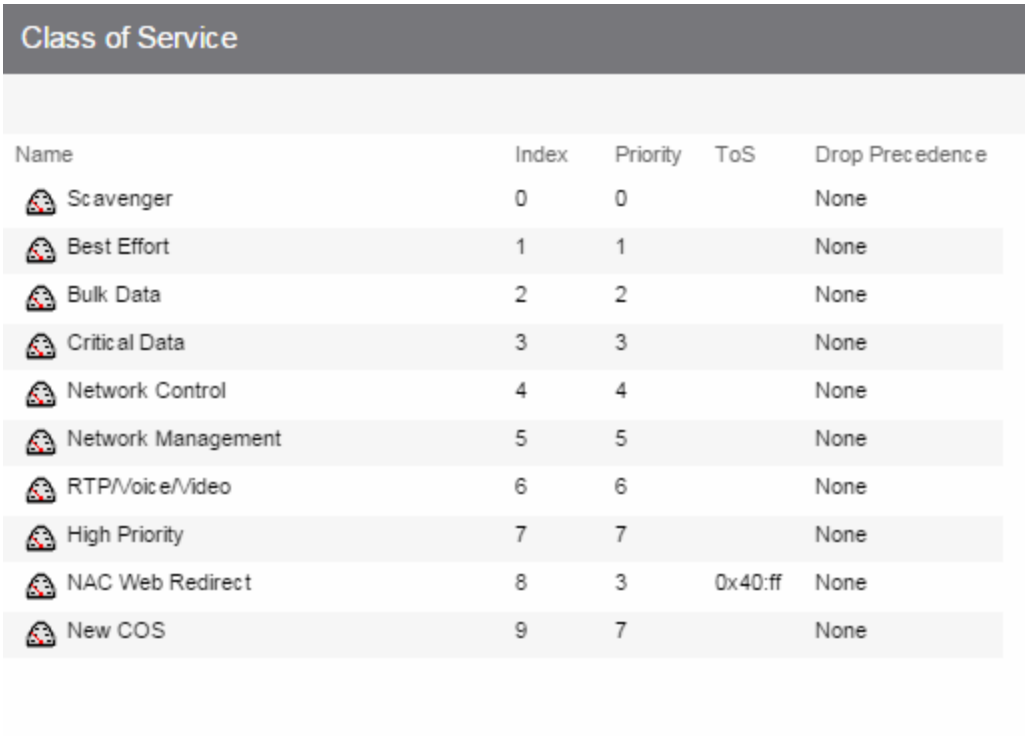
- How to Add and Delete Devices
- How to Create and Use Domains

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:

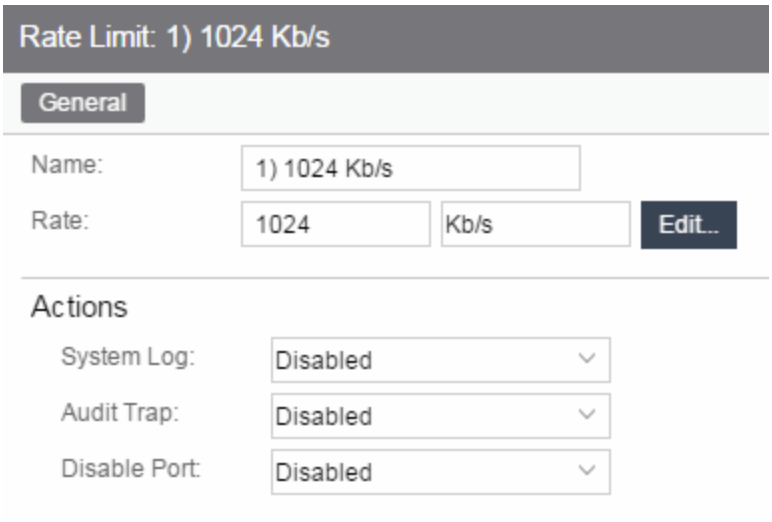
- General Tab (Class of Service)

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:

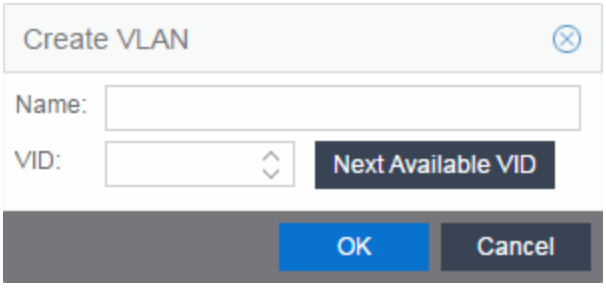
- Rate Limits

For information on related tasks:

- How to Define Rate Limits

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.

OK Button
: Creates the VLAN.

Related Information

For information on related concepts:

- Dynamic Egress
- Policy VLAN Islands

For information on related tasks:

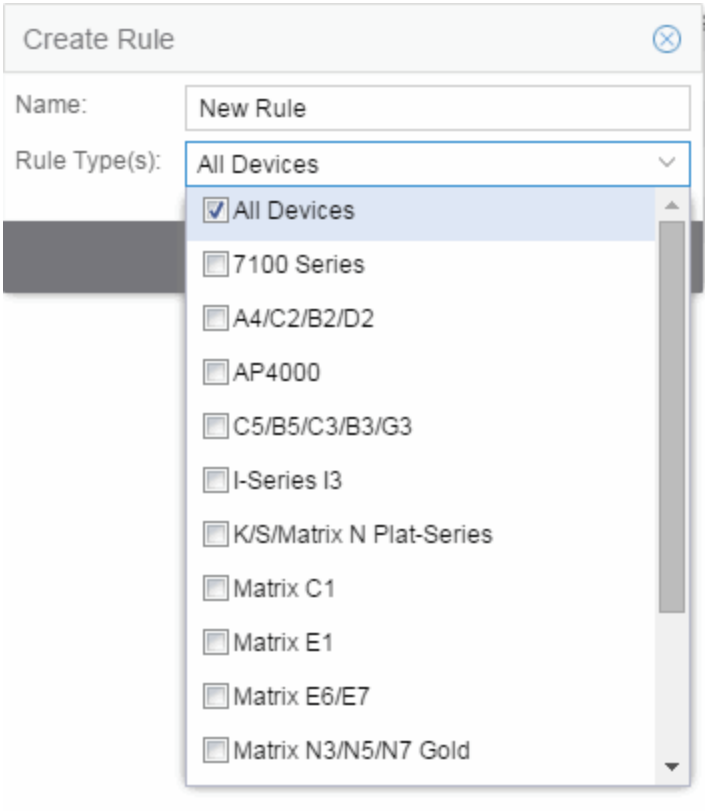
- How to Create a VLAN
- How to Create a Policy VLAN Island

For information on related windows:

- General Tab (Role)

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.

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)

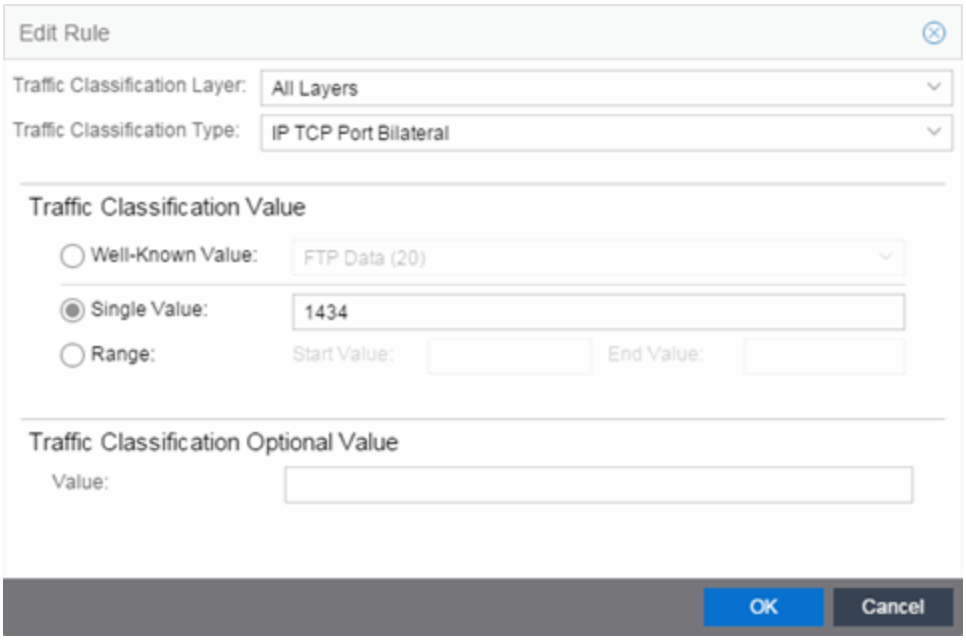
Edit Rule

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:

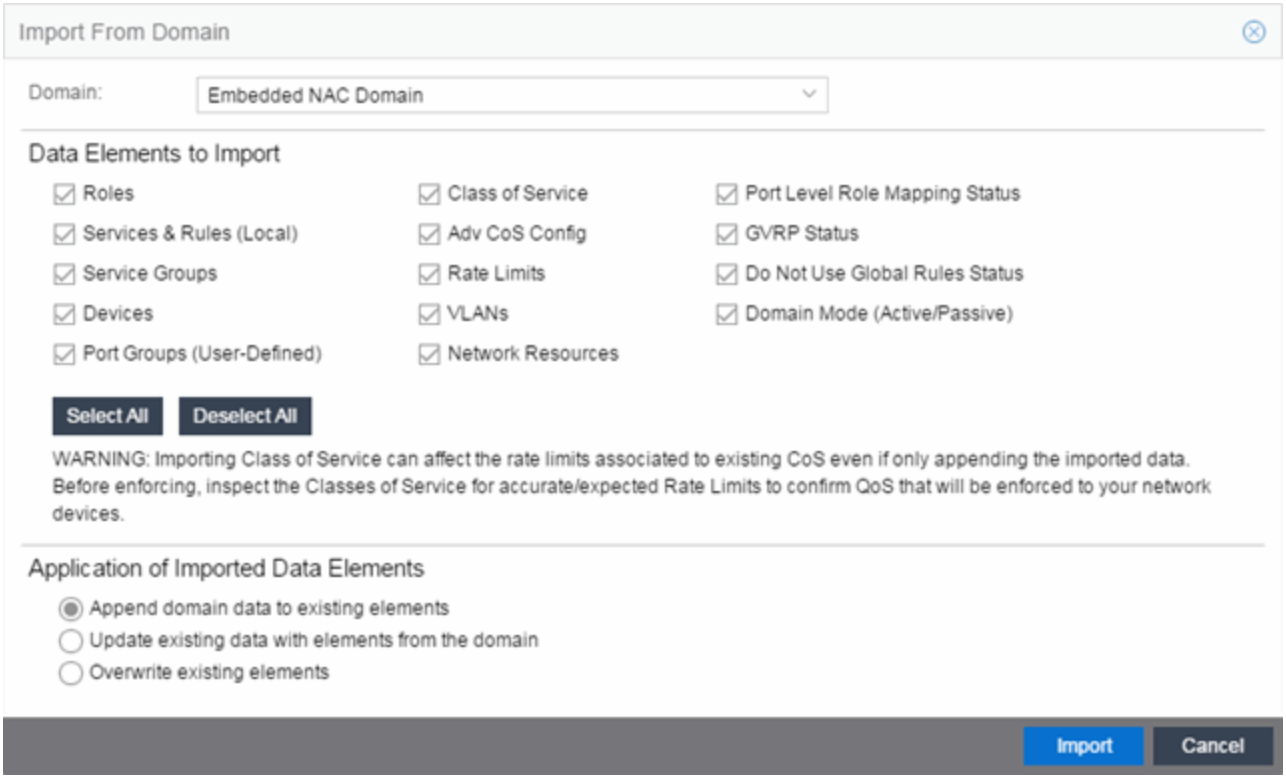
- How to Create or Modify a Rule

For information on related windows:

- General Tab (Rule)

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 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

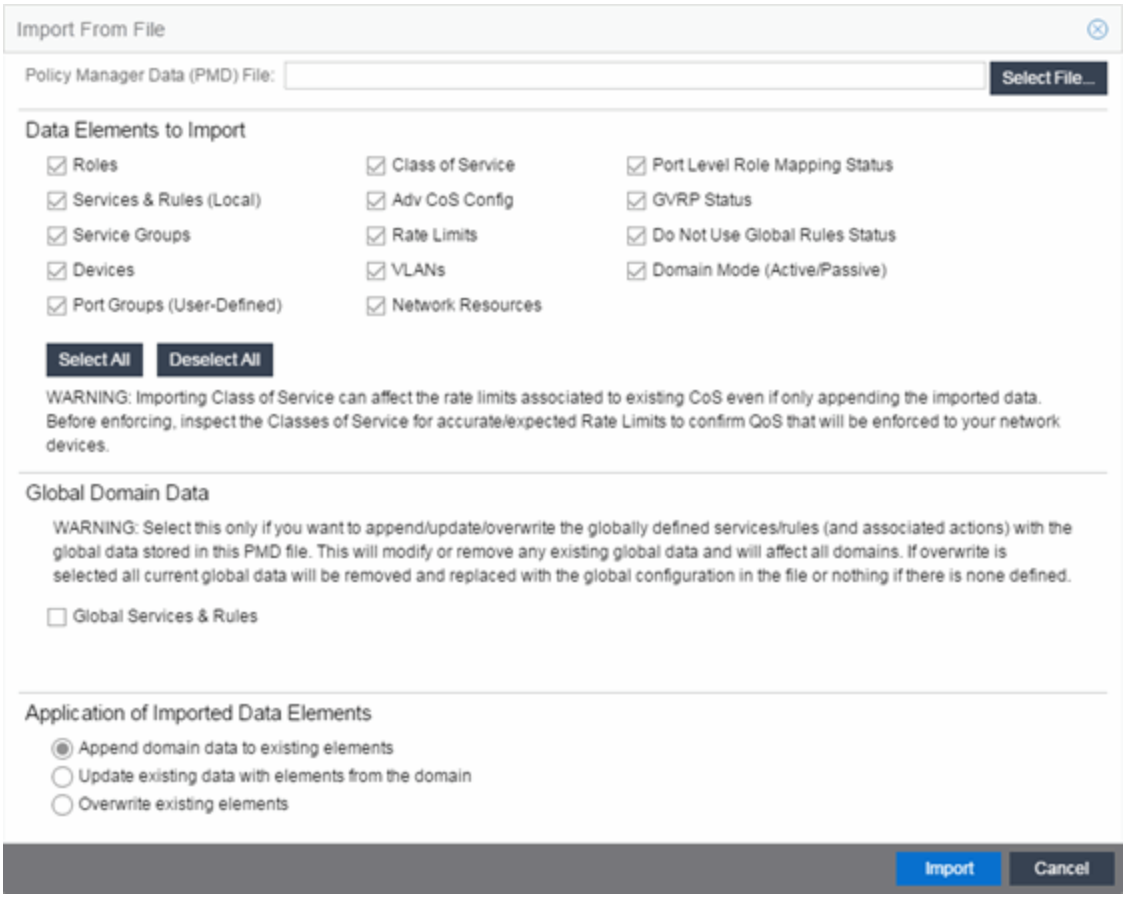
For information on related windows:

- 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 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:

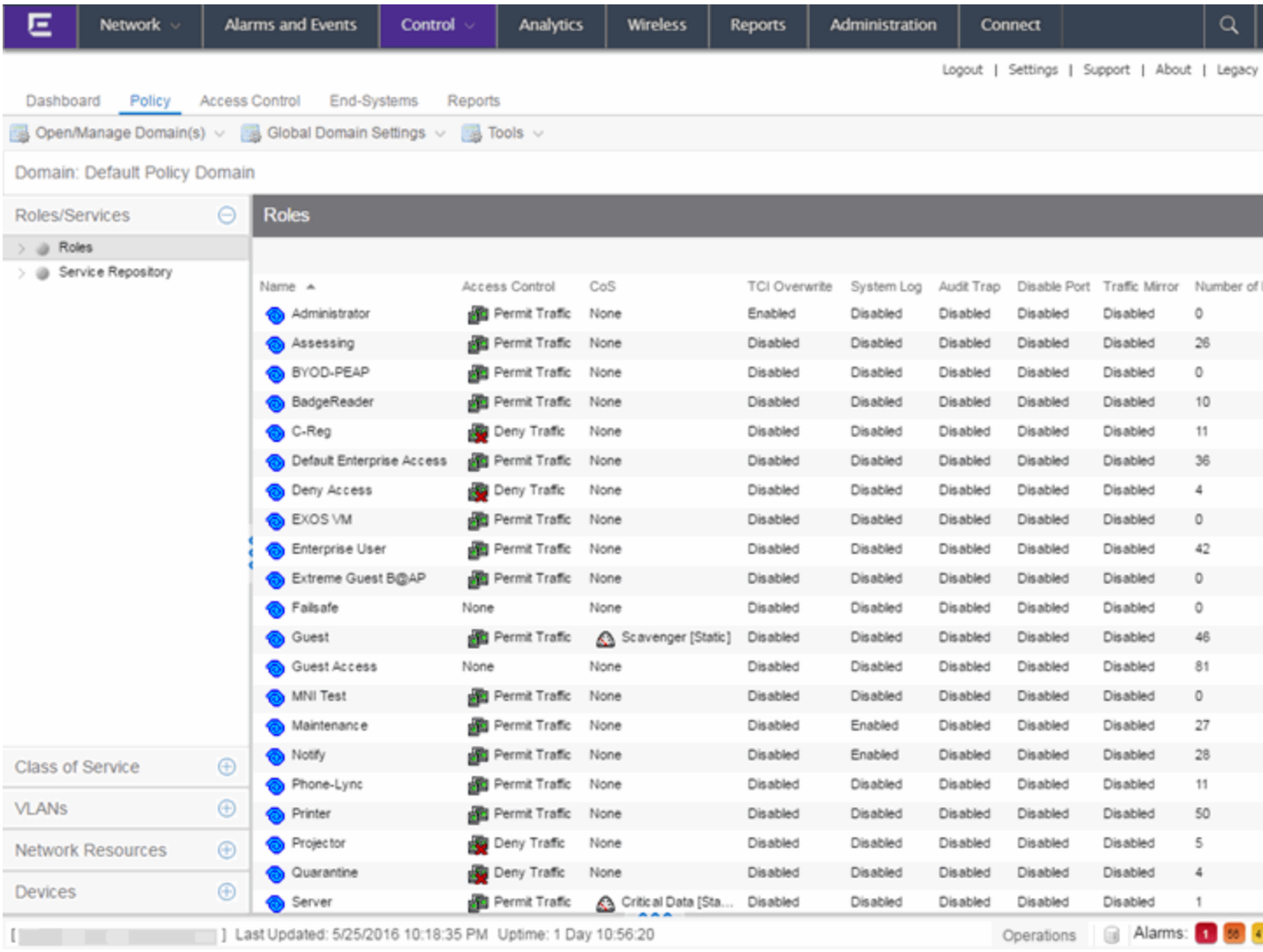
- Import From Domain Window

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

Icon	Definition	Icon	Definition
	Device/Wireless Device		Port Group
	Port		Frozen Port
	Role		Quarantine Role
	Rule		Disabled Rule
	Device-specific Rule		Service Group
	Automated Service		Manual Service
	Network Resource Group		Slot/Logical Ports/Ports
	Contain VLAN		Deny VLAN
	VLAN or Network Resource Island		Island VLAN
	Warning		CoS (Class of Service)
	802.1p Priority		IP Type of Service Value
	CoS Port Group		Rate Limit
	Transmit Queue		Network Resource Topology

Open/Manage Domain Menu Icons

The following icons appear in the Open/Manage Domains drop-down 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:

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:

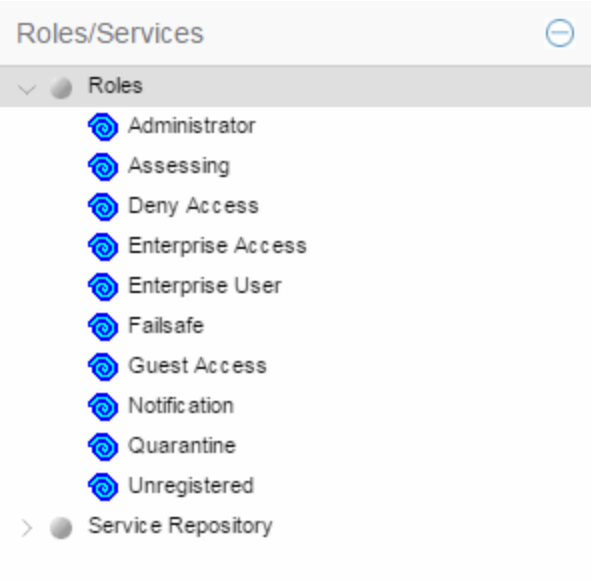
- Roles/Services Tab
- Network Elements/Port Groups Tab
- Access Control Configuration
- Class of Service Configuration
- Network Resources Configuration

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.

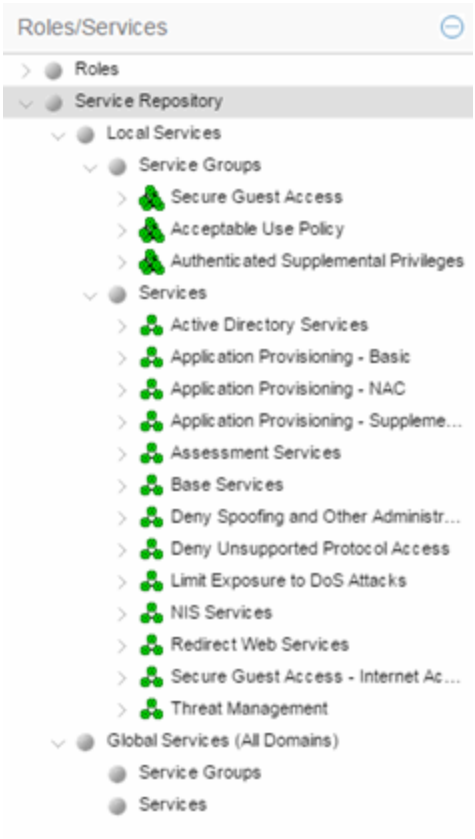


Roles Folder
: This folder contains the roles defined for the current domain. See How to Create a Role for more information.

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.

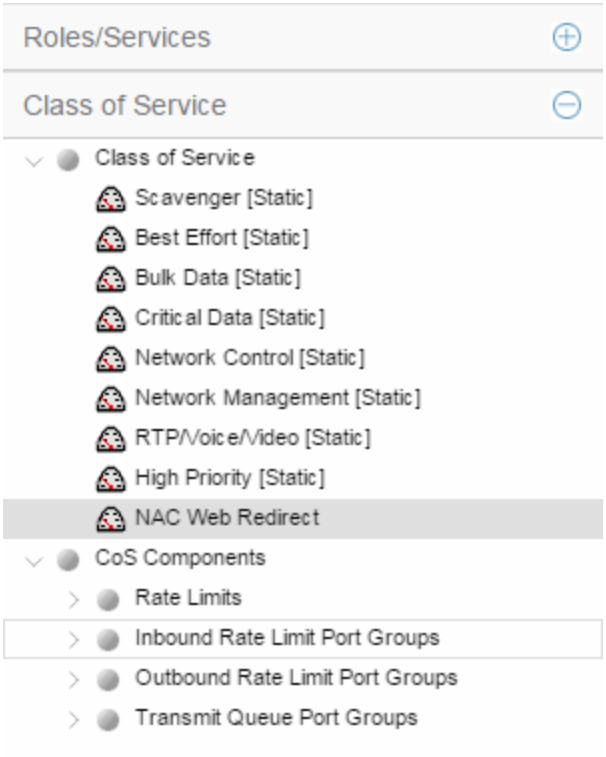
Manual Service
: Individual Manual services are listed under the Services Folder. Expand the service to see the rules associated with it.

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.

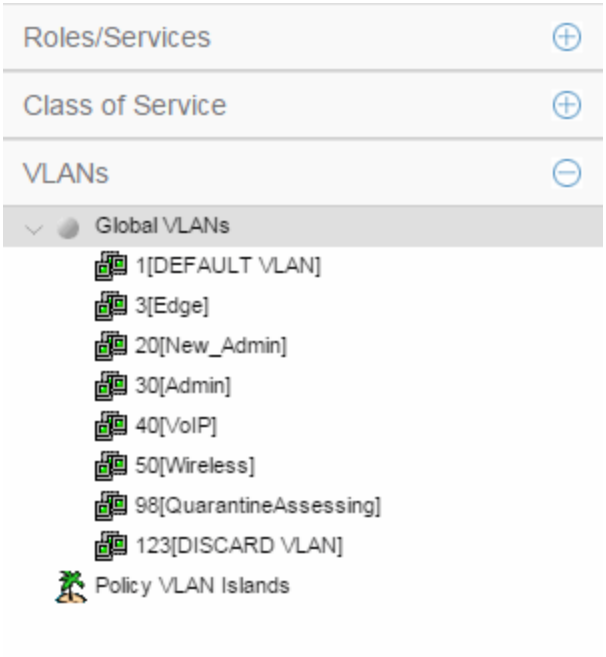
Inbound Rate Limit Port Groups
: This folders contains the currently defined inbound rate limit port groups. Select a port group in the left panel and view information about that group in the right-panel tabs. For more information, see Creating Class of Service Port Groups.

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.

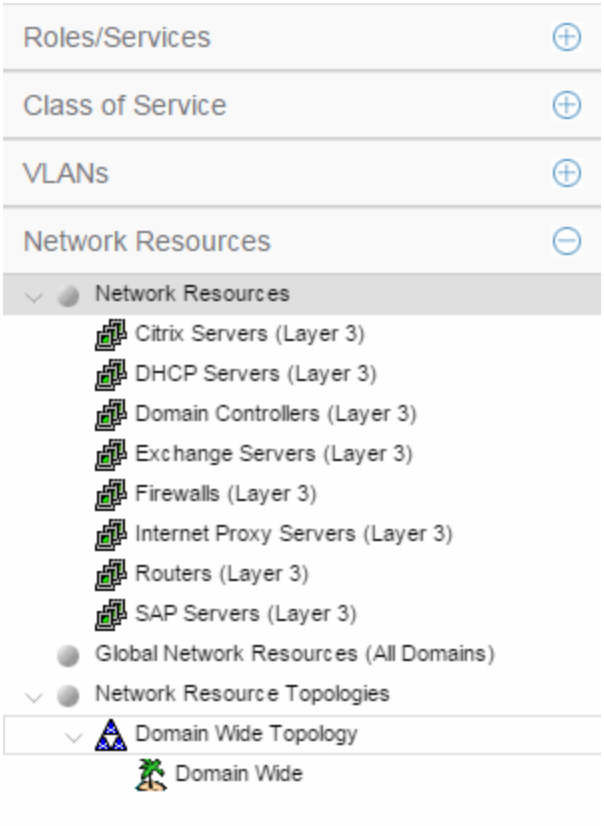
Island VLANs Folder
: This folder appears only when the Policy VLAN Islands feature is enabled, and contains your currently defined Island VLANs for this domain.

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.

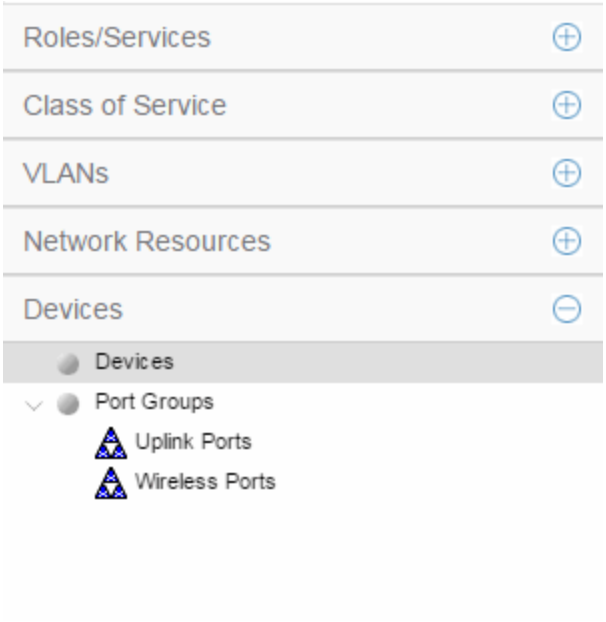
Topology Island
: A topology island is a group of devices that have a unique network resource list, allowing you to set up network resource access based on the location where end users authenticate.

Devices 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 Folder
: This folder 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 Folder

This folder 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.

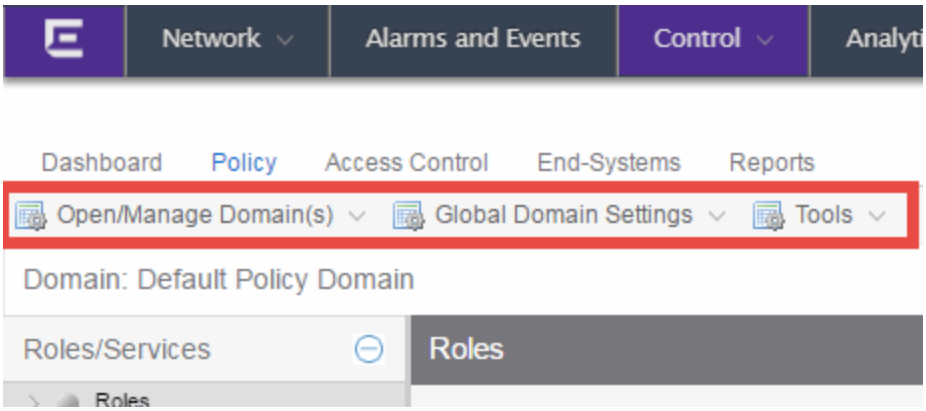
Related Information

For information on related windows:

- Main Window
- Right Panel

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.

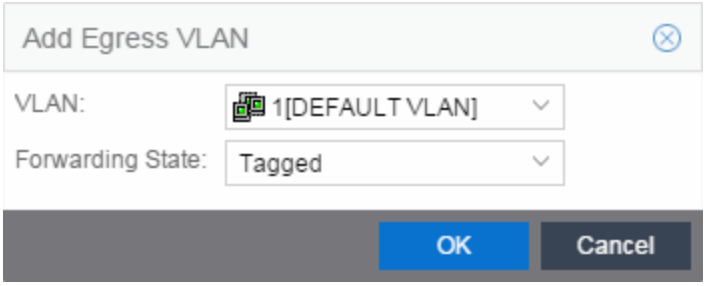
Related Information

For information on related windows:

- Main 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 (formerly NetSight)® Extreme Access Control

The Access Control tab provides secure, policy-based management for Extreme Networks Mobile IAM and Extreme Access Control solutions. It configures and manages Mobile IAM and 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 a Extreme Management Center software license.

The Access Control tab contains three main navigation trees in the left-panel:

- Access Control Engine Groups
- All Access Control Engines
- Access Control Configurations

Access Control Engine Groups

The Access Control Engine Groups tree presents groups of Access Control engines you configure into engine groups. Information for engine groups is organized into four tabs in the right-panel, each showing different information relating to the engine group selected:

- Details — Displays basic information about the engine group as well as information about how the engines in the group are configured.
- Switches — Shows the switches monitored by the gateway engines in the group and allows you to add, delete, and edit the switch configuration.
- End-Systems — Displays end-systems monitored by the Access Control engines in the selected engine group.
- Access Control Engines — Displays the Access Control engines added to the engine group. Right-clicking an engine in the table displays a menu from which you can configure the engine.

All Access Control Engines

The All Access Control Engines tree displays all of your Access Control engines. Selecting an engine displays information in three tabs:

- Details — Displays basic information about the engine, provides a summary of the interface, and allows you to disable Access Control authentication and assessment.
- End-Systems — Displays end-systems monitored by the Access Control engine.
- Switches — Shows the switches monitored by the gateway engine and allows you to add, delete, and edit the switch configuration.

Access Control Configurations

The 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 Access Control Configuration which is automatically assigned to your Access Control engines. You can use this default configuration as is, or make changes to the default configuration, if desired.

Configure a registration that forces any new end-system connected on the network to provide the user's identity in a web page form before being allowed access to the network. End users are automatically provisioned network access on demand without time-consuming and costly network infrastructure reconfigurations. In addition, IT operations gains visibility into the end-systems and their associated users (e.g. guests, students, contractors, and employees) on the network.

Via the 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 Access Control configurations to use for different network deployment circumstances (e.g. type of end-systems on the network, network topology, authentication method deployed, etc.). The second table displays details and information for each of the different suggested Access Control configurations. The information in the tables assumes that DHCP is deployed on the network.

Suggested Access Control Configuration for Different Deployments

Policy/VLAN Switch Configuration	Number of Devices Allowed to Connect to Authentication-enabled Edge Port	Type of End-Systems	Authentication Method Deployed	Switch Support IEEE 802.1X MIB	Switch Support, Session Timeout and Termination Action RADIUS Attributes	Suggested Configuration
- Policy Only (*without* changing of VLANs)	*	*	*	*	*	A

Policy/VLAN Switch Configuration	Number of Devices Allowed to Connect to Authentication-enabled Edge Port	Type of End-Systems	Authentication Method Deployed	Switch Support IEEE 802.1X MIB	Switch Support, Session Timeout and Termination Action RADIUS Attributes	Suggested Configuration
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs)	Multiple	Microsoft XP SP1 with KB822596 installed[1]	802.1X[2]	Yes	*	A
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs)	Multiple	*	802.1X[2]	Yes	*	B
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs)	Multiple	*	802.1X[2]	No	Yes	C
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs)	Multiple	*	802.1X[2]	No	No	D
- 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

Policy/VLAN Switch Configuration	Number of Devices Allowed to Connect to Authentication-enabled Edge Port	Type of End-Systems	Authentication Method Deployed	Switch Support IEEE 802.1X MIB	Switch Support, Session Timeout and Termination Action RADIUS Attributes	Suggested Configuration
- VLAN only - Policy and VLAN - Policy Only (*with* changing of VLANs) *[for 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.

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.				

Configuration	Port Link Control	Assessing Session Timeout	Assessing Policy Configuration	DHCP Server Configuration Considerations	Other Considerations
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.				
D	Disabled	Disabled	Initial Scan Only	- Set short lease times (e.g. 1 min) for the unauthenticated, Assessing, and Quarantine VLANs - Normal lease times can be configured for the Accept (Production) VLANs	Set short reauthentication interval manually on edge switches (e.g. 2 min)
	NOTE: This is not a very scalable configuration model, and therefore should not be implemented for a network with a large number of end-systems.				
E	Enabled	Disabled	*	No	N/A
	NOTE: End-system will be reauthenticated and will renew its IP address via DHCP with link down/up execution.				

Configuration	Port Link Control	Assessing Session Timeout	Assessing Policy Configuration	DHCP Server Configuration Considerations	Other Considerations
F	Enabled	Disabled	Initial Scan Only	- Set short lease times (e.g. 1 min) for the unauthenticated, Assessing, and Quarantine VLANs - Normal lease times can be configured for the Accept (Production) VLANs	N/A
	NOTES: End-system will be reauthenticated with link down/up execution and will automatically re-establish network connectivity via DHCP upon lease expiration of the IP address in the unauthenticated, Assessing, and Quarantine VLANs. When a compliant end-system on the Production VLAN is subsequently quarantined after failing a re-assessment, the end-system will be reauthenticated and will renew its IP address via DHCP with link down/up execution.				
G	Disabled	*	*	*	RFC 3576 Reauthentication Enabled
	NOTES: 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 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 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 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 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 a 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 Access Control Profile to "Use Assessment Policy During Initial Assessment Only," and set the DHCP lease time for the IP address pools that correspond to the VLAN(s) associated to the Quarantine and Assessing access policies, as well as the default VLAN associated to the unauthenticated state of the port, to a low value (e.g. 1 minute). This forces an end-system to send DHCP Request messages every 30 seconds while it is unauthenticated, being assessed, and quarantined. Upon passing assessment, the end-system is dynamically assigned an IP address on the production VLAN shortly after assessment is complete, establishing connectivity to the network on the production VLAN.

- Access Control Gateway DHCP Snooping:
  - Option 1: Locate the Access Control Gateway on the same subnet as the DHCP server. If the Access Control engine is in the same subnet (relay router interface) as the end-system, it is able to hear ACK responses from the DHCP server, 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 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 a Access Control Gateway learns a MAC/IP address pair, it sends a message to all other Access Control Gateways, so only one Access Control Gateway needs to live on each subnet with a DHCP server on it, to leverage this technique.

- Option 2: Add the Access Control Gateway IP address as a helper address on default gateway routers. To increase the accuracy of the MAP-to-IP resolution, the 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 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 Access Control Gateway's IP address can be added along with the actual DHCP server IP addresses. When a Access Control Gateway learns a MAC/IP address pair, it sends a message to all other Access Control Gateways, so only one 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 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 Access Control Gateways.

- Access Control Gateways should not be selected for ASM search. Do not use the Access Control Gateway as a search device in ASM. ASM should be configured to search other devices in the network for the IP-to-MAC-to-port bindings, such as gateway routers for IP-to-MAC bindings and access edge switches for MAC-to-port information.

- 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 Web Browsers for end-systems connecting through Access Control. The following web browsers are supported for end-systems connecting to the network through Extreme Networks Access Control:
  - Microsoft Edge and Internet Explorer version 11
  - Mozilla Firefox 34 and later
  - Google Chrome 33.0 and later

- RADIUS Configuration on E1 Devices. The Access Control engine opens an SSH/Telnet session on the E1 device and enable RADIUS by running a script of CLI commands. CLI credentials for the device are obtained from the device profile and must be configured in the Authorization/Device Access tool.

- RADIUS Authentication and Accounting Configuration on ExtremeXOS Devices. 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. Access Control uses CLI to configure RADIUS accounting on Enterasys fixed switching devices (A-Series, B-Series, C-Series, D-Series, G-Series, and I-Series). CLI credentials for the device are obtained from the device profile and must be configured in the Authorization/Device Access tool. This does not apply to A4, B5, and C5 devices running firmware version 6.81 and higher. Those devices support RADIUS accounting configuration using SNMP. For more information, see How to Enable RADIUS Accounting.

Considerations When Implementing Policy Roles

This section describes the communication that takes place between Access Control engines and end-systems connecting to the network. This communication should be taken into account when defining and deploying policy roles and rules on your network. It is particularly critical because certain policy roles and rules 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 Access Control engines.

IP resolution via NetBIOS
MAC Resolution via NetBIOS
 Access Control engine UDP Port 137 <==> End-System Port 137

Remediation and Registration
 Access Control engine (TCP or UDP) Port 80 <==> End-System Port (determined on the client) - HTTP
 Access Control engine (TCP or UDP) Port 443 <==> End-System Port (determined on the client) - HTTPS

Access Control Agent Discovery via HTTP
 Access Control engine Port TCP 8080 <==> End-System Port (determined on the client)
Access Control Agent Heartbeat via HTTPS
 Access Control engine Port TCP 8443 <==> End-System Port (determined on the client)

Access Control Agent-less Assessment
 All ports determined by the selected test set.

The following software is optional and 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 (Access Control) to use the source IP. If a logical IP address is used, then Access Control is unable to reauthenticate end-systems.

- If you have configured Assisted Remediation, you must perform the following steps if your network includes wireless controllers:
    - Enable the "ToS override for Access Control" option configured through Wireless Manager in the Edit WLAN Service > Authentication Mode Configuration > Settings window.
    - If Policy Manager is **not** being used to configure policy on the wireless controller, use Wireless Manager to manually add the following rule to the VNS Quarantine, Assessing, and Unregistered filters to 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 (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 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 Access Control engine is configured as a secondary DNS server in the DHCP scope, in addition to the primary DNS server on the network. When an end-system is required to register or undergo remediation, access to the primary DNS server is blocked and the end-system sends its DNS requests to the DNS proxy on the Access Control 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 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 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 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 Access Control Gateway.
- If an assessment policy is defined for all assessments, the user is redirected to the 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 Access Control engine. You can enable diagnostics for DNS proxy by going to the Access Control engine administration web page and enabling the DNS Proxy diagnostic group to provide troubleshooting information. Launch the Access Control engine administration web page by using the following URL: https://<Access ControlengineIP>:8443/Admin. The default user name and password for access to this web page is "admin/Extreme@pp." 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.

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 Access Control is a centralized network access control solution located in the **Access Control** tab that combines authentication, vulnerability assessment, and location services to authorize network access and determine the appropriate level of service for an end-system. The Access

Control solution ensures that only valid users and devices with appropriate security postures at the proper location are granted access to your network. For end-systems which are not compliant with defined security guidelines, the Access Control solution provides assisted remediation, 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 Access Control solution. The Access Control tab and Access Control engines work in conjunction to implement network access control. The Access Control tab provides one centralized interface for configuring the authentication, authorization, assessment, and remediation parameters for your Access Control engines. After these configurations are enforced, the Access Control engines can detect, authenticate, assess, authorize, and remediate end-systems connecting to the network according to those configuration specifications.

Extreme Access Control Engines

The Access Control engine is required for all Extreme Networks Access Control deployments. It provides the ability to detect, authenticate, and effect the authorization of end devices attempting to connect to the network. It also integrates with, or connects to, vulnerability assessment services to determine the security posture of end-systems connecting to the network. Once authentication and assessment are complete, the Access Control engine effects the authorization of devices on the network by allocating the appropriate network resources to the end-system based on authentication and/or assessment results.

If authentication fails and/or the assessment results indicate a non-compliant end-system, the Access Control engine can either totally deny the end-system access to the network or quarantine the end-system with a highly restrictive set of network resources, depending on its configuration. The Access Control engine also provides the remediation functionality of the Access Control solution by means of the remediation web server that runs on the engine. Remediation informs end users when their end-systems have been quarantined due to network security policy non-compliance, and allows end users to safely remediate their non-compliant end-systems without assistance from IT operations.

Use Scenario

The 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 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 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 Access Control with the 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, 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, 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, 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 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 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 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 Access Control Features: Authentication and OS/Device Fingerprinting, but no Registration or Assessment.
	4500	Configured Access Control Features: All features excluding Assessment.
	3000	Configured Access Control Features: All features including Assessment.
IA-A-300	12000	Configured Access Control Features: Authentication and OS/Device Fingerprinting, but no Registration or Assessment.
	9000	Configured Access Control Features: All features excluding Assessment.
	6000	Configured Access Control Features: All features including Assessment.

Model	Number of End-Systems Supported	Notes
IA-V	See Notes	The IA-V is included with the Management Center Advanced (NMS-ADV) license and is used in conjunction with a Access Control Enterprise license (IA-ES-12K). For more information, see Extreme Access Control Enterprise Licensing.
NAC-V-20	3000	The NAC-V-20 is a virtual engine and requires a Access Control VM license in the Management Center Server. For more information, see the Suite-Wide Tools Server Information Window Help topic section on Extreme Access Control VM license.
NAC-A-20	3000	
SNS-TAG-ITA	3000	
SNS-TAG-HPA	3000	
SNS-TAG-LPA	2000	

It is important to configure Access Control Gateway redundancy for each switch. This is achieved by configuring two different 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 Access Control Gateways, it is suggested that one half of the switches connecting to the gateways are configured with "Access Control Gateway A" as the primary and "Access Control Gateway B" as the secondary, and the second half are configured with "Access Control Gateway B" as the primary and "Access Control Gateway A" as the secondary. In this way, 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 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 Access Control Gateway. The 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 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 Access Control Gateway requests an assessment of the end-system, if assessment is configured. Once authentication and assessment are complete, the 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 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 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 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 Access Control Engines — Lists all 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.
- 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 Access Control Configuration which is automatically assigned to your Access Control engines. You can use this default configuration as is, or make changes to the default configuration, if desired.

The Access Control Configuration determines what Access Control Profile will be assigned to an end-system connecting to the network. It contains an ordered list of rules that are used by the configuration to assign a 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 a Access Control Configuration provide very granular control over how end-systems are treated as they come onto the network. The following criteria can be used to define the rules used in your Access Control Configuration:

- Authentication Type - for example, 802.1X or MAC authentication.

- End-System Groups - 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 Access Control Profiles:

- Administrator
- Allow
- Default
- Guest Access
- Notification
- Pass Through
- Quarantine
- Registration Denied Access
- Secure Guest Access
- Unregistered

If desired, you can edit these profiles or you can define your own profiles to use for your Access Control Configurations. For more information, see the Manage 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 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 Access Control Profiles, these access policies define a set of network access services that determine exactly how an end-system's traffic is authorized on the network. How access policies are implemented depends on whether your network utilizes Access Control Controller engines and/or Access Control Gateway engines.

For end-systems connected to EOS policy-enabled switches, 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 Access Control Gateways to send a

VLAN ID instead of a policy role to those switches using Tunnel RADIUS attributes.

For Access Control Controller engines, authorization of the end-system is implemented locally on the Access Control Controller engine by assigning a policy role to the end-system, as specified by the access policy. In this scenario, all policy roles must be defined in the Access Control Controller policy configuration.

Here is a description of each the Access Control tab access policy, and some guidelines for creating corresponding policy roles in the Policy tab.

Accept Policy: The Accept access policy is applied to an end-system when it has been authorized locally by the Access Control 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. 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. Access Control Controllers are shipped with a default policy configuration that includes a Quarantine policy role.

Failsafe Policy: The Failsafe access policy is applied to an end-system when it is in an Error connection state. An Error state results if the end-system's IP address could not be determined from its MAC address, or if there was an assessment error and an assessment of the end-system could not take place. For EOS policy-enabled switches, a corresponding policy role (created in the Policy tab) allocates a nonrestrictive set of network resources to the connecting end-system so it can continue its connectivity on the network, even though an error occurred

in the Access Control Solution operation. For RFC 3580-compliant switches, the Failsafe access policy may be mapped to the Production VLAN. Access Control Controllers are shipped with a default policy configuration that includes a Failsafe policy role.

Assessment Policy: The Assessment access policy 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. 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 Access Control Gateway engines and/or Layer 2 Access Control Controller engines. (Registration is not supported on the Layer 3 Identity and Access Controller engines.) Registration provides flexibility in implementation by offering the following capabilities:

- Determine "valid" end users by prompting each end user for a username with additional information such as full name and 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 Access Control Solution utilizes a Registration Web Server installed on the Access Control engine to provide this registration functionality to end-systems. Note that an Access Control engine may implement both assisted remediation and registration concurrently.

There are specific network configuration steps that must be performed when using Registration in your Access Control Solution. In addition, you must configure Registration in the **Access Control** tab. For more information, see How to Set up Registration.

How Registration Works

Here is a description of how Registration works in the Extreme Networks Extreme Access Control (Access Control) Solution:

- An unregistered end-system attempts to connect to the network and is assigned the unregistered access profile without being assessed by the Access Control engine. For example, if connected to a Layer 2 Access Control Controller, the end-system may be assigned to the "Unregistered" policy as defined in the Access Control Controller's default policy configuration. If connected to an EOS policy-enabled switch, the end-system 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 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 Access Control Configuration.
- The end-system is then automatically re-authenticated to the network by the Access Control engine. Upon re-authentication, the end-system is authenticated, assessed, and authorized as defined by the profile specified in the Access Control Configuration for the newly registered system. If the profile specifies to assess the end-system, an assessment of the end-system takes place at this time.

Assessment

The Extreme Networks 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.

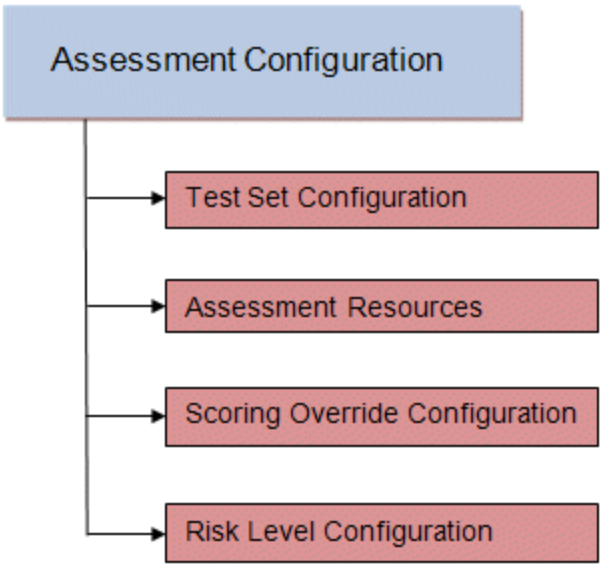
When an assessment is performed on an end-system, a *Health Result* is generated. For each health result, there may be several *Health Result Details*. A health result detail is a result for an individual test performed during the assessment. Each health result detail is given a score ranging from 1 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 Access Control Profiles. In addition, the Access Control tab provides a default assessment configuration that is already set up with default assessment parameters and is ready to use in your Access Control Profiles.

Before beginning to configure assessment on your network, 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 Access Control Configuration.
- Extreme Access Control Assessment Phased Deployment Guide - This guide describes the phased approach to introducing assessment into your Access Control deployment using Informational, Warning, and Quarantine assessment. The guide also provides information on the Access Control tab tools that can be used to monitor and evaluate assessment results, and diagnose and troubleshoot problems.
- How to Configure Assessment - Provides step-by-step instructions for configuring assessment using the phased approach described in the Access Control Assessment Phased Deployment Guide. Instructions are provided for configuring phased assessment using agent-less or agent-based assessment, or a combination of both.
- How to Deploy Agent-Based Assessment - If you are deploying agent-based assessment, this Help topic provides the configuration steps specific to deploying agent-based assessment in a Windows and Mac network environment. It includes instructions for configuring agent deployment and

provides information about the agent icon and notification messages that appear on the end-user's system. It also includes instructions on performing a managed deployment or installation of the agent.

- How to Set Up Assessment Remediation - Because Warning and Quarantine assessment provides end-system remediation, you must enable remediation for your Access Control Configuration. This Help topic provides the specific steps that must be performed when setting up assisted remediation in your network.

Assessment Remediation

Remediation is a process that informs end users when their end-systems have been quarantined due to network security policy non-compliance, and 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 Access Control engine.

There are specific network configuration steps that must be performed when using assisted remediation in your Access Control Solution. In addition, you must configure assisted remediation in the Access Control tab. For more information, see How to Set up Assessment Remediation and Portal Configuration Help topics.

How Remediation Works

Here is a description of how assisted remediation works in the Extreme Networks 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 Access Control engine and a web page indicating that the end-system is currently being assessed is displayed.
- When the assessment is complete, the assessment server sends the results to the Access Control engine. If the end-system failed assessment, the end-system is authorized with the level of network access defined by the Quarantine access policy configuration.
- When the quarantined end user opens a web browser to any web site, its traffic is dynamically redirected to the Access Control engine.
- The Access Control engine returns a web page formatted with self-service remediation information for the quarantined end-system. This web page indicates the reasons the end-system was quarantined and the remediation steps the end user must take.
- After taking the appropriate remediation steps, the end-user 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 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 a Extreme Management Center user's access to 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 Management Center end-system information and configuration.

When an end-system authenticates to the network, Access Control rules are used to assign a 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 Management Center.

A user's authorized zones are determined by their Management Center user group membership. User groups are created and configured in the 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 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 Management Center user group membership.

A third component that should be taken into consideration is the ability to limit user access to Management Center using authorization group capabilities. For example, you can assign a user group the Management Center End-Systems Read Access capability to allow read-only access to 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 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 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 Access Control configuration information to one or more Access Control engines. Any time you add or make a change to the Access Control Configuration, the engines need to be informed of the change through an enforce, otherwise the changes do not take effect. When an engine needs to be enforced, the Enforce icon  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 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 Access Control Configuration, 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 Access Control Controllers, a MAC address can be locked to the Controller PEP IP address and port, or just the PEP IP address, but this only controls the movement of the end-system between the downstream ports on the PEP (IP address and port) and not the actual edge of the network.
-- On Layer 3 Access Control Controllers, there 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.

Automated Security Manager Blacklist

Extreme Management Center Automated Security Manager (ASM) can be configured to notify the Access Control tab in response to a real-time security threat from an end-system on the network. The Access Control tab automatically adds the end-system's MAC address to the Blacklist end-system group,

effectively putting the end-system in quarantine and preventing the end-system from accessing the network from any location. If ASM notifies the Access Control tab that the security threat is no longer present, then the Access Control tab removes the end-system from the Blacklist group and the end-system is dynamically re-authenticated to the network. Use ASM's Create/Edit Rule window (accessed from the Rule Definition view of the Automated Security Manager Configuration window) to configure the "Notify Identity and Access" action.

You can view ASM blacklists under the End-System Group folder in the Access Control Configurations tree, by selecting Tools > Management and Configuration > Advanced Configurations from the menu bar. In the left-panel tree, expand the Rule Components folder and the End-System Group folder, and click on Blacklist. An ASM blacklist entry will have a description of "ASM." In addition, the Access Control tab generates a health result for the end-system when it is blacklisted by ASM. In the Health Result Summaries table, the health result reason states "ASM Denied" and lists the Sender ID, Signature, and Sender Name. In the Health Result Details table, one health result detail is generated with a Test Case ID of 200001, and a risk level of HIGH with a score of 10. All ASM Blacklist health result details will use the same Test Case ID of 200001.

Mobile IAM

Extreme Networks Mobile IAM (Extreme Access Control Management) is a comprehensive BYOD solution that provides total security, full IT control, and predictable network experience for all users. Mobile IAM provides the controls required to grant network access to BYOD devices, with the same fine-grained security controls that are applied to wired and wireless IT managed devices.

The Mobile IAM solution provides complete software for:

- identification all of the devices connected to their network
- access and inventory management
- context-based policy enforcement
- end-to-end management from a single, easy-to-use management application
- auditing and reporting

The Mobile IAM solution is delivered through an Access Control gateway engine and Extreme Management Center version 4.3, and configured in the Access Control tab. The engine is available as a physical or virtual engine to best meet

your deployment needs. The solution can also include installation and integration services that are sold separately.

Contact your Extreme Networks sales representative for more information about Mobile IAM.

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 Management Center server IP address.
End-System Keywords	
$macAddress	The end-system's current MAC address.
$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.

Keyword	Returned Value
$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.
$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.

Keyword	Returned Value
$switchPortId	The name of the switch port the end-system is currently connected to (for example, ge.1.1).
$oldswitchPortId	The name of the switch port the end-system was previously connected (for example, ge.1.1).
$authType	The latest authentication method used by the end-system to connect to the network.
$oldauthType	The previous authentication method used by the end-system to connect to the network.
$allAuthTypes	A comma-separated list of authentication types currently used for this end-system in its current location. The list is only provided if there is more than one authentication type.
$oldallauthTypes	A comma-separated list of authentication types previously used for this end-system in its current location. The list is only provided if there is more than one authentication type.
$nacProfileName	The Access Control profile currently assigned to the end-system.
$oldnacProfileName	The Access Control profile previously assigned to the end-system.
$reason	The reasons why the end-system is assigned its current Access Control profile or is in a particular state.
$oldreason	The reasons why the end-system was assigned its previous Access Control profile or is in a particular state.
$policy	The access policy currently assigned to the end-system, if on a policy-based switch.
$oldpolicy	The access policy previously assigned to the end-system, if on a policy-based switch.
$firstSeentime	The first time the end-system was seen by the Access Control engine.
$lastSeenTime	The last time the end-system was seen by the Access Control engine.
$oldlastSeenTime	The previous last time the end-system was seen by the Access Control engine.
$nacApplianceIp	The IP address of the Access Control engine on which the end-system authenticated.

Keyword	Returned Value
$oldnacApplianceIp	The IP address of the previous Access Control engine on which the end-system authenticated.
$nacapplianceGroupName	The engine group for the Access Control engine where the end-system was last heard.
$oldnacApplianceGroupName	The previous engine group for the Access Control engine where the end-system was last heard.
$lastScanTime	The last time a scan was performed on the end-system.
$lastScanResultState	The resulting state of the last scan: ACCEPT, QUARANTINE, or empty.
$ssid	The Service Set Identifier (SSID) of the wireless network to which the end-system is connected.
$oldssid	The Service Set Identifier (SSID) of the wireless network to which the end-system was previously connected.
$wirelessAp	The name of the Wireless Access Point (AP) to which the end-system is connected. If the AP's name is unavailable, then the AP's MAC address is reported. If the MAC address is unavailable, then the AP's serial number is reported.
$oldwirelessAp	The name of the Wireless Access Point (AP) to which the end-system was previously connected. If the AP's name is unavailable, then the AP's MAC address is reported. If the MAC address is unavailable, then the AP's serial number is reported.
$ifAlias	The ifAlias of the switch port to which the end-system is currently connected.
$oldifAlias	The ifAlias of the switch port to which the end-system was previously connected.
$ifDescription	The ifDescription of the switch port to which the end-system is currently connected.
$oldifDescription	The ifDescription of the switch port to which the end-system was previously connected.
$ifName	The ifName of the switch port to which the end-system is currently connected.
$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.

Keyword	Returned Value
$custom2	The text from the Custom 2 end-system information column.
$custom3	The text from the Custom 3 end-system information column.
$custom4	The text from the Custom 4 end-system information column.
$regName	The registered username supplied by the end user during the registration process.
$regEmail	The email address supplied by the end user during the registration process.
$regPhone	The phone number supplied by the end user during the registration process.
$regData1	The text from the Custom 1 registration field supplied by the end user during the registration process.
$regData2	The text from the Custom 2 registration field supplied by the end user during the registration process.
$regData3	The text from the Custom 3 registration field supplied by the end user during the registration process.
$regData4	The text from the Custom 4 registration field supplied by the end user during the registration process.
$regData5	The text from the Custom 5 registration field supplied by the end user during the registration process.
$regDeviceDescr	The device description supplied by the end user during the registration process.
$regSponsor	The registered device's sponsor.
$memberOfGroups	The current list of MAC end-system groups listed in the Groups end-system information column.
$oldmemberOfGroups	The previous list of MAC end-system groups listed in the Groups end-system information column.
$groupDescr1	The entry description that was entered when the end-system was added to a MAC-based end-system group.
$groupDescr2	The entry description that was entered when the end-system was added to a MAC-based end-system group.
$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.
$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.

Keyword	Returned Value
$createdBy	The name of the user that created the user group.
$creationTime	The time and date the user group was created.
$description	A description of the user group (if one was defined when the group was created).
$added	A comma-separated list of user entries that were added to the group during the change.
$removed	A comma-separated list of user entries that were removed from the group during the change.
$lastModifiedTime	The last time the user group was modified.
$oldlastModifiedTime	The previous last time the user group was modified.
$lastModifiedBy	The name of the user who most recently edited the user group.
$oldlastModifiedBy	The name of the user who had previously edited the user group.
$revisionCounter	The current revision count (the number of changes that have been made) for the user group.
$oldrevisionCounter	The previous revision count (the number of changes that have been made) for the user group.
$listtype	One of the following types: Username, LDAP User Group, RADIUS User Group.
End-System Group Keywords	
$name	The name of the end-system group.
$createdBy	The name of the user that created the end-system group.
$creationTime	The time and date the end-system group was created.
$description	A description of the end-system group (if one was defined when the group was created).
$added	A comma-separated list of end-system entries that were added to the group during the change.
$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.

Keyword	Returned Value
$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

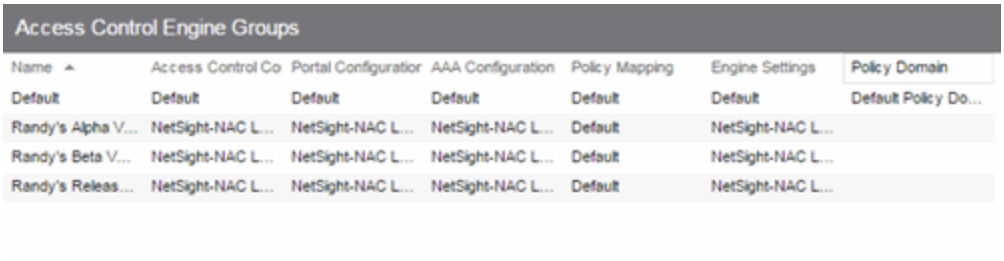
For information on related windows:

- Extreme Access Control Options Panel

Access Control Engine Groups

The Access Control Engine Groups panel is displayed in the right panel when you select the Access Control Engine Groups folder in the left panel. (The Access Control Engine Groups folder is only displayed if you have created engine groups.) The tab displays a table of information about the engine groups in the folder.

Use the table options and tools to filter, sort, and customize table settings. You can access the options by clicking the down arrow in the right corner of any column header.



Name

The name of the engine group.

Access Control Configuration

The Access Control Configuration currently selected for this engine group.

Portal Configuration

If your network is implementing Registration or Assisted Remediation, the Portal Configuration that defines the branding and behavior of the website used by the end user during the registration or remediation process.

AAA Configuration

The AAA Configuration used by this engine group.

Policy Mapping

The Default policy mapping can be viewed in the Access Control Configurations tree (under Access Control Profiles) or accessed from the Edit 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.

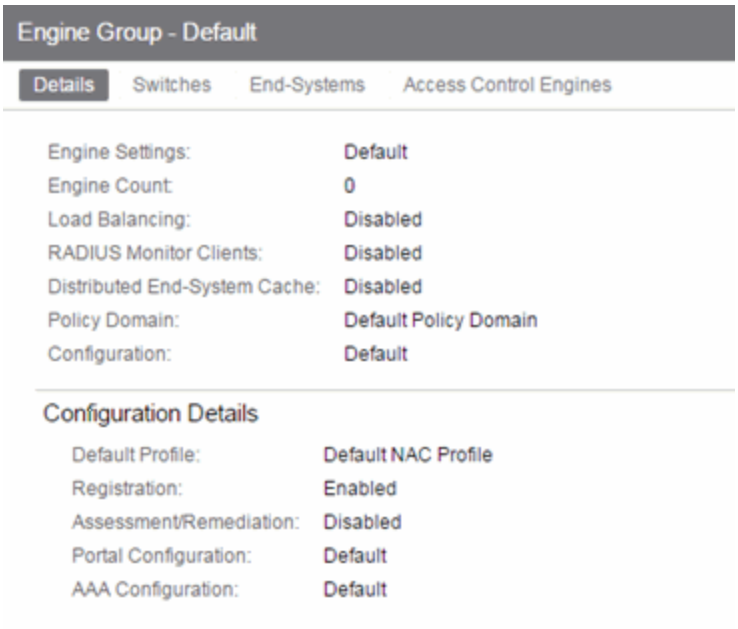
Related Information

For information on related windows:

- Edit Portal Configuration Window

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.



Engine Settings

The engine settings configuration being used by your Access Control engines. Engine settings are configurable through the Access Control Configurations view, by expanding the **Access Control Configurations** tree from the left panel.

Engine Count

The number of engines in the engine group.

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 Access Control gateway engines. This can be

useful in Access Control deployments with a large number of switches, where manual delegation of switch resources would be cumbersome.

RADIUS Monitor Clients
: Displays whether RADIUS Monitor Clients are enabled for the Access Control engines in the folder.

Distributed End-System Cache
: Displays whether the Distributed End-System Cache option is enabled for the Access Control engines in the folder.

Configuration
: The name of the Access Control Configuration being used by your Access Control engines. The Access Control Configuration determines the Access Control Profile assigned to an end-system connecting to the network.

Default Profile
: The name of the Default Profile specified in the Access Control Configuration. The Default Profile serves as a "catch-all" profile for any end-system that doesn't match one of the rules listed in the Access Control Configuration.

Registration
: Whether a registration/web access feature is enabled or disabled for the Access Control Configuration.

Assessment/Remediation
: Whether the assessment/remediation feature is enabled or disabled for the Access Control Configuration.

Portal Configuration
: The name of the Portal Configuration specified in the Access Control Configuration. If your network is implementing Registration or Assisted Remediation, the Portal Configuration defines the branding and behavior of the website used by the end user during the registration or remediation process.

AAA Configuration
: The name of the AAA Configuration specified in the Access Control Configuration.

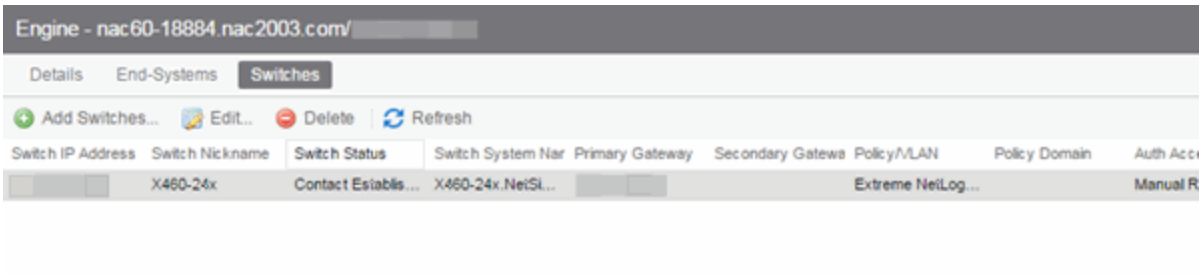
Switches

This tab provides information about the switches assigned to a Extreme Access Control Gateway engine or 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 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 Access Control Gateway. If load balancing has been configured for the engine group, the 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 Access Control Gateway. If load balancing has been configured for the engine group, the 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. Access Control learns about these session via RADIUS accounting. This allows Access Control to be in a listen mode, and to display access control, location information, and identity

information for end-systems without enabling authentication on the switch.

- Manual RADIUS Configuration — RADIUS configuration was performed manually on the switch using Policy Manager or CLI.

Switch Type
: Specifies the switch type: a switch that authenticates layer 2 traffic via RADIUS to an out-of-band Access Control 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 Access Control engine, providing real-time connection status in 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 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 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:

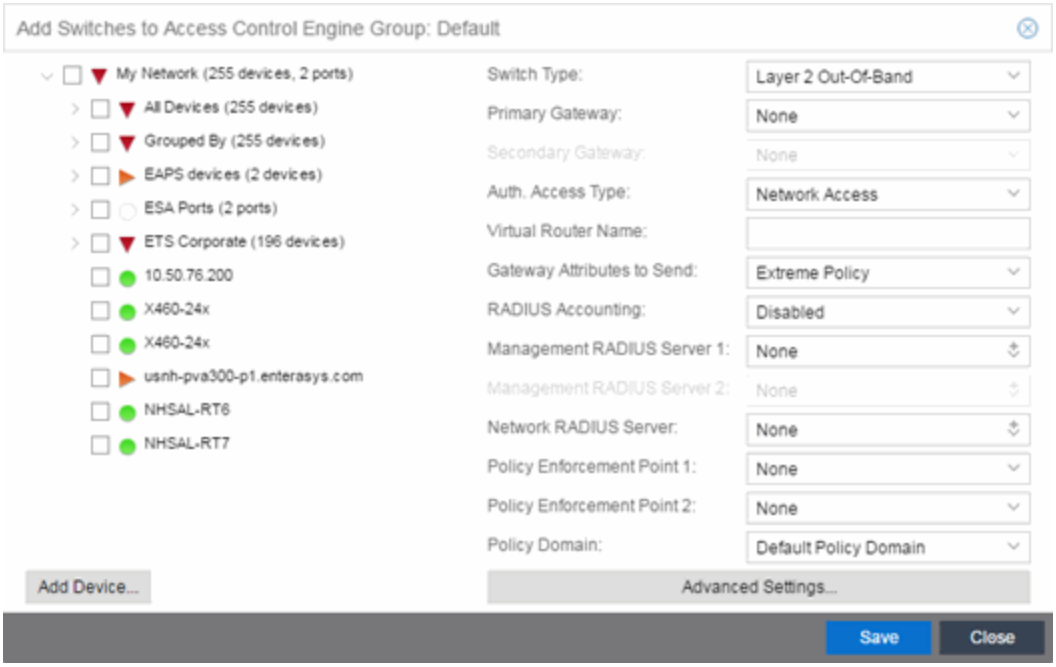
- Add Switches to a Extreme Access Control Engine Group Window
- Edit Switches in Extreme Access Control Engine Group Window

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 Access Control Gateway for the switches; Extreme Management Center does not require the secondary Access Control Gateway to be set. If only the primary 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 Access Control Gateway. In this scenario, if contact with the Access Control Gateway fails, authentication traffic would bypass the 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 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 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 Access Control engine, Access Control removes the end-system authentication from their prior port/switch. This allows VMs that quickly move from one server to another and then back again to still have their location updated in Management Center, because only one authenticated session is allowed per end-system in Management Center.
- Layer 2 RADIUS Only — In this mode, 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 a 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 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 Access Control Gateway for the selected switches. If load balancing has been configured for the engine group, the 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 Access Control Gateway for the selected switches. If load balancing has been configured for the engine group, the Management Center server determines the primary and secondary gateways at Enforce, and this field displays Determined by Load Balancer.

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

Auth. Access Type

Use the drop-down 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. 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 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 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 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. Management Center learns about these session via RADIUS accounting. This allows 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 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 - 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 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 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 Access Control engine, providing real-time connection status in 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 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 Access Control engine. (This option is only available if a Secondary Gateway is not specified.) Select from the RADIUS servers you have configured in 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 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

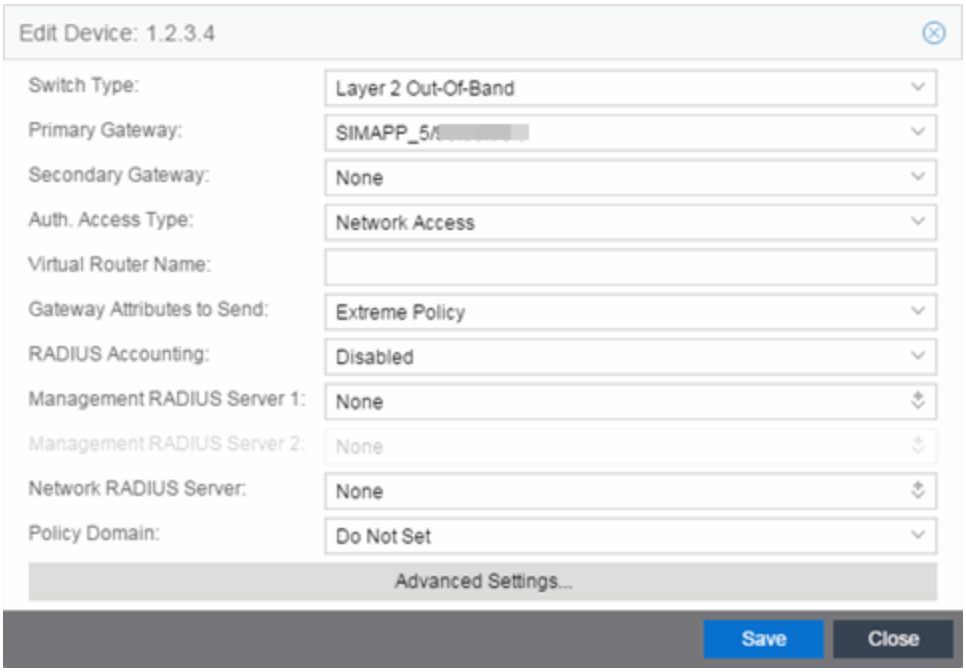
For information on related windows:

- Switches Tab
- Edit Switches in Engine Group Window

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 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 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 Management Center, because only one

authenticated session is allowed per end-system within Management Center.

- Layer 2 RADIUS Only — In this mode, 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 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 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 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. 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 Access Control, make sure that an appropriate administrative access configuration is in place by assigning a profile such as "Administrator Access Control Profile" to grant proper access to users. Also, verify that the current switch CLI credentials for the admin user are defined in the database against which Access Control authenticates management login attempts.
- Switching from an Auth type of "Any Access" or "Management Access" back to "Network Access" can restrict access to the switch after an enforce is performed. Verify that the current switch CLI credentials for the admin user are defined locally on the switch.

- Any Access — the switch can authenticate users originating from any access type.
- Management Access — the switch can only authenticate users that have requested management access via the console, Telnet, SSH, or HTTP, etc.
- Network Access - the switch can only authenticate users accessing the network via the following authentication types: MAC, PAP, CHAP, and 802.1X. If RADIUS accounting is enabled, then the switch also monitors Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. If there are multiple sessions for a single end-system, the session with the highest precedence will be displayed to provide the most accurate access control information for the user. The Access Control authentication type precedence from highest to lowest is: Switch Quarantine, 802.1X, CHAP, PAP, Kerberos, MAC, CEP, RADIUS Snooping, Auto Tracking.
- Monitoring - RADIUS Accounting — the switch will monitor Auto Tracking, CEP (Convergence End Point), and Switch Quarantine sessions. Management Center learns about these session via RADIUS accounting. This allows 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 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 — 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 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 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 Access Control engine, providing real-time connection status in Management Center. It also allows 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 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 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.

Advanced Settings
: Select this button to open the Advanced Switch Settings window.

Related Information

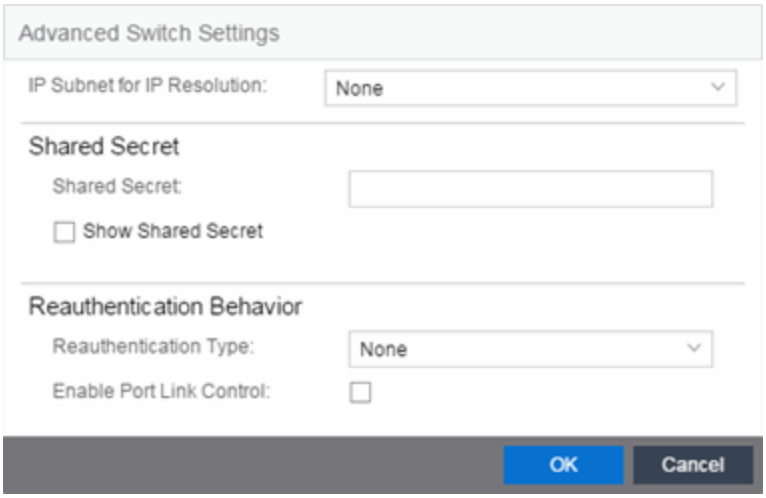
For information on related windows:

- Switches Tab
- Add Switches to an Engine Group Window
- Advanced Switch Settings Window

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

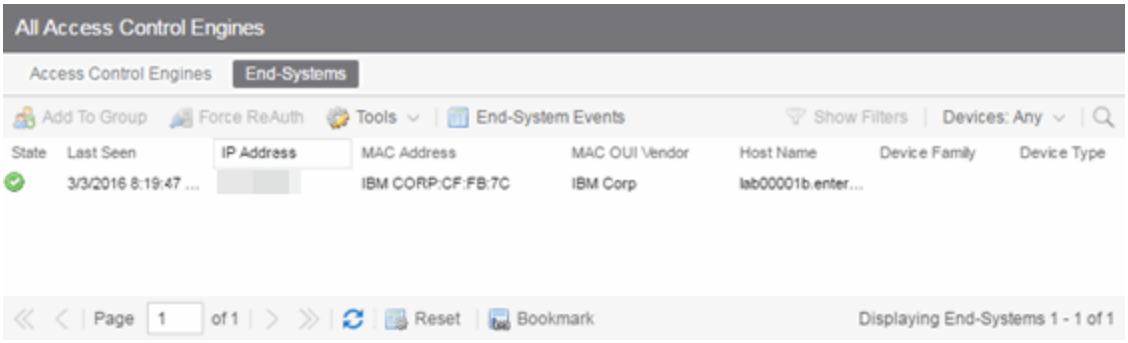
End-Systems

The End-Systems tab presents end-system connection information for a single Extreme Access Control engine, all Access Control engines, or all the engines in an engine group, depending on what you select in the left-panel tree. You can also monitor end-system events and view the health results from an end-system's assessment.

The End-Systems tab is the first tab displayed when accessing the Control > Access Control tab. A high-level overview of the functionality found in the Access Control tab is also available. For additional information, see Access Control.

To access this tab, select a single Access Control engine, the All 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 Access Control profile was set to Reject, the MAC Locking test failed, or the RADIUS server was reachable but rejected the authentication request.
- Disconnected — All sessions for the end-system are disconnected. This state is only applicable for end-systems connected to switches that have RADIUS accounting enabled.
- Error — Indicates one of nine problems:
  - the MAC to IP resolution failed, if assessment is enabled
  - the MAC to IP resolution timed out, if assessment is enabled
  - all RADIUS servers are unreachable
  - the RADIUS request was non-compliant
  - all assessment servers are unavailable
  - the assessment server can't reach the end-system
  - no assessment servers are configured
  - the assessment server is not compatible with the current version of Access Control
  - the username and password configured in the Assessment Server panel of the Access Control options (Administration > Options > Access Control > Assessment Server) are incorrect for the assessment server.

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 a Access Control Controller engine, this is the 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 Access ControlController engine, this is the Access Control Controller PEP (Policy Enforcement Point) port. However, for Layer 3 Access Control Controller engines this column is blank.

  If you add or update the port alias on the switch, you must enforce the Access Control engine in order for the new information to be displayed in the End-Systems table.

  If you don't want the port alias displayed, remove the PORT_DESCRIPTION_FORMAT variable from the /opt/nac/server/config/config.properties file. If this variable is removed, only the switch port number is displayed.

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 Access Control Controller engines, this column will list "IP.") For additional information about the authentication methods the end-system used to authenticate, see All Authentication Types.

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.

Profile
: The name of the 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 Access Control engine.

First Seen
: The first time the end-system was seen by the 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.

I & A Engines/Source IP
: The Access Control engine to which the end-system is connecting.

Engine Group
: This column is only displayed if you have multiple engine groups. It displays what engine group the Access Control engine was in when the end-system event was generated. For example, if the engine was in Engine Group A when an end-system connected, but then later the engine was

moved to Engine Group B, this column would still list Engine Group A for that end-system's entry.

Switch Location
: The physical location of the switch to which the end-system connected. If the end-system is connected to a Access Control Controller engine, this is the 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 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. For additional information, see End-System Zones.

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 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 window 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 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 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

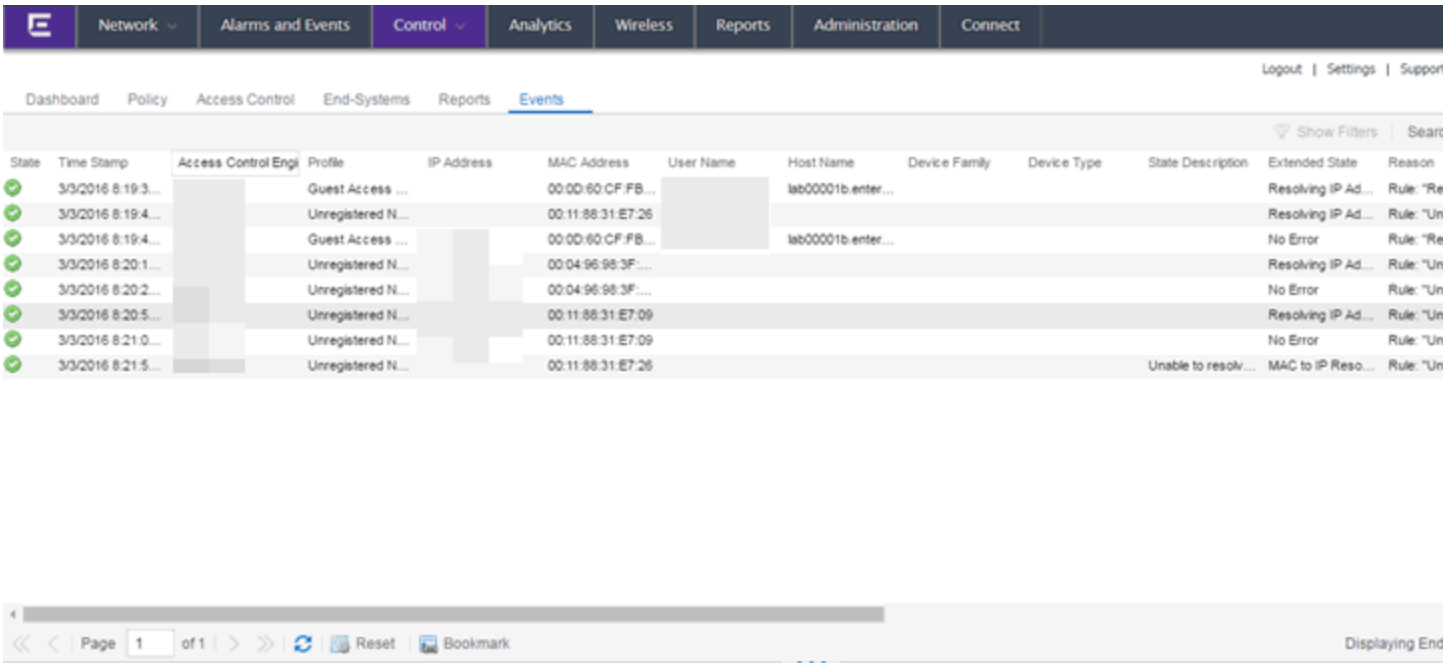
The menu at the top of the window contains most of the options available via a right-click previously mentioned in the Actions section above, as well as the End-System Events button, described below.

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 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 Access Control Options view (Administration > Options > Access Control > End-Systems Event Cache).

NOTE: The **End-System Events** tab displays events up to the most recent delete event for the end-system, if one exists. If you want to see events that happened prior to the most recent delete event, use the **Search for Older Events** button.



State

The end-system's connection state:

- Scan — The end-system was scanned.
- Accept — The end-system was granted access with either the Accept policy or the attributes returned from the RADIUS server.
- Quarantine —The end-system was quarantined because the assessment failed.
- Reject — The end-system was rejected because the assigned Access Control profile was set to Reject, the MAC Locking test failed, or the RADIUS server was reachable but rejected the authentication request.
- Disconnected — This end-system session was disconnected, however other sessions for the end-system may still be active. For example, the end-system may have a disconnected session with an authentication type of 802.1X, but still have an active MAC authentication session. This state is only applicable for end-systems connected to switches that have RADIUS accounting enabled.
- Error — Indicates one of nine problems:
  - the MAC to IP resolution failed
  - the MAC to IP resolution timed out
  - all RADIUS servers are unreachable

- the RADIUS request was non-compliant
- all assessment servers are unavailable
- the assessment server can't reach the end-system
- no assessment servers are configured
- the assessment server is not compatible with the current version of Management Center
- the username and password configured in the Assessment Server panel of the Access Control options (Administration > Options > Access Control > Assessment Server) are incorrect for the assessment server

Time Stamp
: The date and time the end-system connected.

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 a Access Control Controller engine, this is the Access Control Controller PEP (Policy Enforcement Point) IP address.

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

Switch Port
: The switch port number to which the end-system is connected. If the end-system is connected to a Layer 2 Access Control Controller engine, this is the Access Control Controller PEP (Policy Enforcement Point) port. However, for Layer 3 Access Control Controller engines this column is blank.

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 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 Access Control Controller engines, this column displays the policy assigned to the end-system for its authorization.

Profile
: The name of the 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 a Access Control Controller engine, this is the 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 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 Access Control Options view (Administration > Options > Access Control > End-System Event Cache). The search is ended when any one of the parameters is reached.

- Maximum number of results to return from search
- Maximum time to spend searching for events (in seconds)
- Maximum number of days to go back when searching

Related Information

For information on related topics:

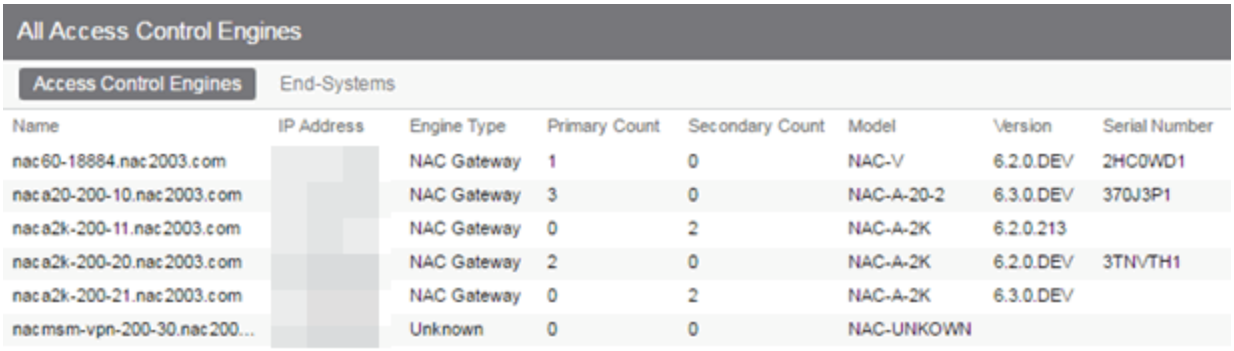
- Add MAC Lock Window
- End-System Details Window

All Access Control Engines

The All Access Control Engines tab is displayed in the right panel when you select the All Access Control Engine tree in the left panel or when you select the Access Control Engines tab when an Access Control Engine Group is selected. The panel displays a table of information about the engines in the folder or group. Right-click an engine for a menu of options.

Use the table options and tools to filter, sort, and customize table settings. You can access the options by clicking the down arrow in the right corner of any column header.

NOTE: The Access Control Engine administration web page allows you to access status and diagnostic information for an Access Control engine. Access the administration web page using the following URL: https://*Access ControlEngineIP*:8444/Admin. The default user name and password for access to this web page is "admin/Extreme@pp."



Name

The name of the Access Control engine (assigned when the engine is created).

IP Address

The Access Control engine's IP address.

Engine Type

The Access Control engine type: Access Control Gateway, Extreme Access Control Layer 2 (L2) Controller, or Access Control Layer 3 (L3) Controller.

Primary Count

The number of switches for which the Access Control engine is the primary engine.

Secondary Count
: The number of switches for which the Access Control engine is the secondary engine.

Model
: The Access Control engine's model number.

Version
: The Access Control engine's version number.

CPU Load (0-100%)
: The percentage of the engine's CPU currently being used. This value gives you an indication of how busy the engine is and helps you determine if your network needs additional engines, or if you need to change your network configuration so that the load is more evenly distributed among your existing engines.

Memory Used
: The amount of memory used by the engine.

Memory Available
: The amount of memory available on the engine.

Connected Agents
: The number of assessment agents connected to the engine.

Capacity
: The engine's current capacity, which is the number of end-systems that have authenticated within the last 24 hours out of the maximum number of authenticating end-systems supported for the engine.

Related Information

For information on related windows:

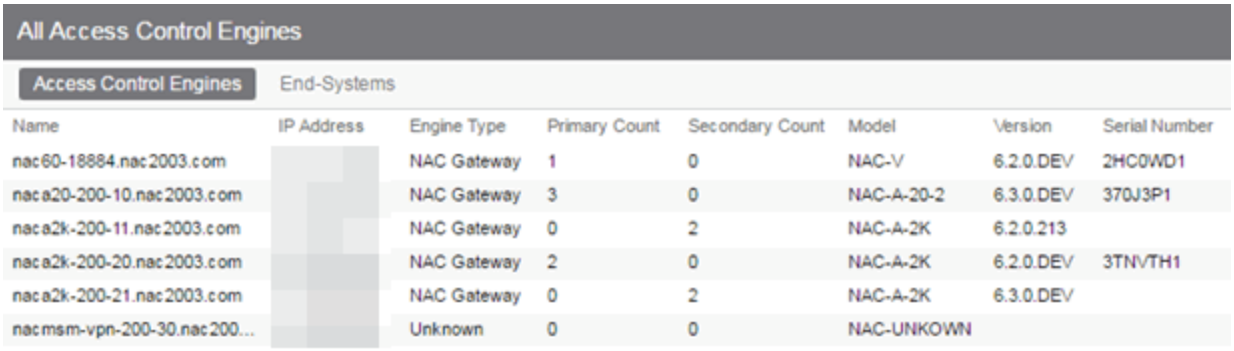
- End-Systems Tab

All Access Control Engines

The All Access Control Engines tab is displayed in the right panel when you select the All Access Control Engine tree in the left panel or when you select the Access Control Engines tab when an Access Control Engine Group is selected. The panel displays a table of information about the engines in the folder or group. Right-click an engine for a menu of options.

Use the table options and tools to filter, sort, and customize table settings. You can access the options by clicking the down arrow in the right corner of any column header.

NOTE: The Access Control Engine administration web page allows you to access status and diagnostic information for an Access Control engine. Access the administration web page using the following URL: https://*Access ControlEngineIP*:8444/Admin. The default user name and password for access to this web page is "admin/Extreme@pp."



Name

The name of the Access Control engine (assigned when the engine is created).

IP Address

The Access Control engine's IP address.

Engine Type

The Access Control engine type: Access Control Gateway, Extreme Access Control Layer 2 (L2) Controller, or Access Control Layer 3 (L3) Controller.

Primary Count

The number of switches for which the Access Control engine is the primary engine.

Secondary Count
: The number of switches for which the Access Control engine is the secondary engine.

Model
: The Access Control engine's model number.

Version
: The Access Control engine's version number.

CPU Load (0-100%)
: The percentage of the engine's CPU currently being used. This value gives you an indication of how busy the engine is and helps you determine if your network needs additional engines, or if you need to change your network configuration so that the load is more evenly distributed among your existing engines.

Memory Used
: The amount of memory used by the engine.

Memory Available
: The amount of memory available on the engine.

Connected Agents
: The number of assessment agents connected to the engine.

Capacity
: The engine's current capacity, which is the number of end-systems that have authenticated within the last 24 hours out of the maximum number of authenticating end-systems supported for the engine.

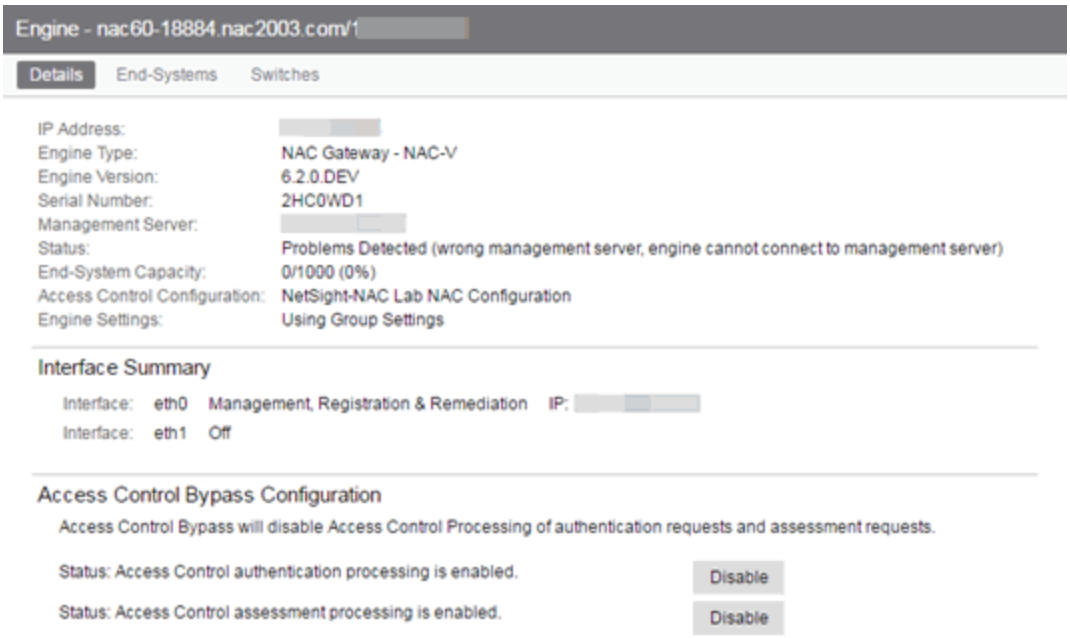
Related Information

For information on related windows:

- End-Systems Tab

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 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 Access Control engine, including its name, IP address, type (Access Control Gateway or Layer 2/Layer 3 Access Control Controller), the engine version, the IP address of the Extreme Management Center Management server, and the Access Control engine status.

End-System Capacity

This field lists the engine's current capacity, which is the number of end-systems that authenticated within the last 24 hours out of the maximum number of authenticating end-systems supported for the engine.

Access Control Configuration

Displays the Access Control Configuration assigned to the engine. The Access Control Configuration determines the Access Control Profile

assigned to an end-system connecting to the network.

Engine Settings
: 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.

Access Control Bypass Configuration
: The Access Control Bypass Configuration feature allows you to bypass Access Control processing of authentication requests from end-systems connecting to the network and also disable the Access Control assessment process. For Access Controlauthentication bypass, Access Control either configures the switch to authenticate directly to a RADIUS server to which Access Control is configured to proxy authentication requests, or it disables RADIUS authentication on the switch. This capability is useful for troubleshooting purposes. For example, if there is a problem with a Access Control Configuration, the Disable button lets you remotely disable Access Control functionality until the problem is resolved. You can then use the Enable button to re-enable Access Control functionality on the engines. When Access Control authentication or assessment is disabled, the Access Control engine name and IP address display in red text in the left-panel tree indicating the engine is in Bypass mode.

  For Access Control Gateway engines, when you select the option to disable Access Control authentication processing, if proxy RADIUS servers are configured for authentication in a Basic AAA Configuration, the Access Control Engine configures the switches to send RADIUS packets directly to the primary and secondary RADIUS servers (from the Basic AAA Configuration), instead of talking to the RADIUS proxy through the Access Control 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 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 Access Control authentication processing is disabled.

NOTES: If you have disabled Access Control authentication processing and then enforce with new switches, the new switches are configured to send RADIUS packets directly to the primary and secondary RADIUS servers. These switches are reconfigured to talk to the RADIUS proxy when you enable Access Control; a second enforce is not necessary.

Bypass is not an option for switches set to Manual RADIUS Configuration or ExtremeWireless controllers not configured for RADIUS strict mode.

For Access Control Controller engines, when you disable Access Control authentication, then the Access Control Controller does not send RADIUS packets directly to the RADIUS servers. Authentication is disabled on the Access Control Controller and end-systems do not need to authenticate to the network. Traffic from the end-systems bypass the Access Control Controller and go directly onto the network.

The Status fields provide the current status of the Access Control authentication or assessment process. The authentication status field also includes a link to the Verify RADIUS Configuration on Switches feature. This feature is available for Access Control Gateway engines and Layer 2 Access Control Controllers, and can be used to alert you to any RADIUS configurations that are out of sync and could cause RADIUS authentication problems on the network.

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 a Access Control Profile to a connecting end-system based on rule criteria.

This Help topic provides information for accessing and configuring Access Control Configuration Rules:

Accessing 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 Access Control Configuration and select Rules. The table of your Access Control rules is displayed in the right panel. See below for an explanation of the table columns.
5. Use the toolbar buttons at the top of the right-panel to create a new rule or edit existing rules. See below for a description of each button.

Viewing Rules in the Table

The Rules table displays the rule name, whether the rule is enabled, and summary information about the rule. It also shows the 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 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 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 Management Center. Click on a rule group name to open a window where you can edit the group's parameters.

Zone
: This column displays the end-system zone you configured. End-system zones allow you to group end-systems into zones, and then limit a 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. You can see definitions for these columns below.

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.

▲ Up ▼ Down Move Rule Up/Down

Move rules up and down in the list to determine rule precedence.

Add... 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.

Edit... Edit Rule

Opens the Edit Rule window where you can edit the rule criteria for a selected rule.

Delete Delete Selected Rules

Deletes any rules selected in the table.

Related Information

For information on related windows:

- AAA Configuration
- Portal Configuration

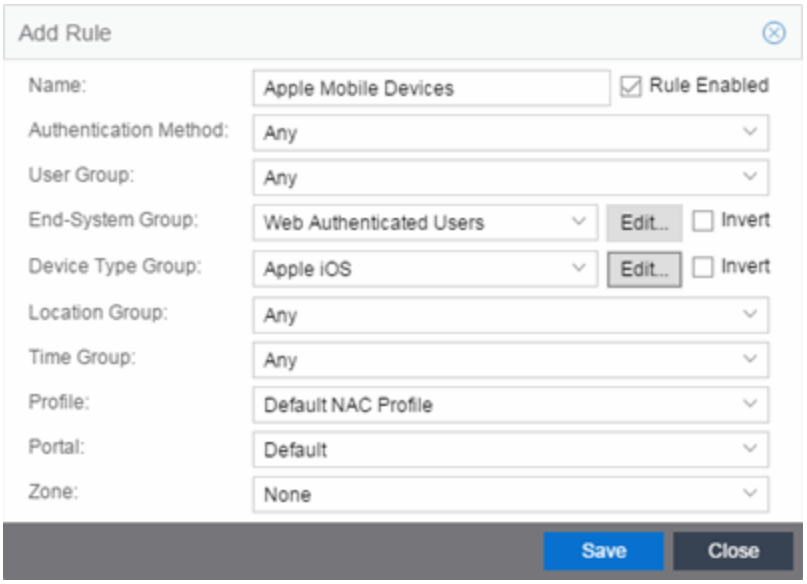
Add/Edit Rule

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 Access Control profile that is specified.

To access this window:

1. Open the Control tab in Extreme Management Center.
2. Click the Access Control tab.
3. In the left-panel tree, select Access Control Configurations > Default > Rules. A table of rules for the Access Control configuration is displayed in the right panel.
4. 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 Access Control profile for authenticated registered users on mobile devices. Descriptions of the different fields and options in the window are provided below.



NOTES: For the following rule criteria:
-- If you select **Any** then the criteria is ignored during the rule match process.
-- If you select the Invert checkbox, it is considered a rule match if the end-system does **not** match the selected value.

Name
: Enter a name for a new rule or change the name of an existing rule, if desired.

Rule Enabled
: Select this checkbox to enable this rule in the Access Control configuration.

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.

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.

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.

Profile
: Select the Access Control profile assigned to any end-system matching this rule.

Portal
: Select the portal configuration presented to any end-system matching this rule.

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 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.

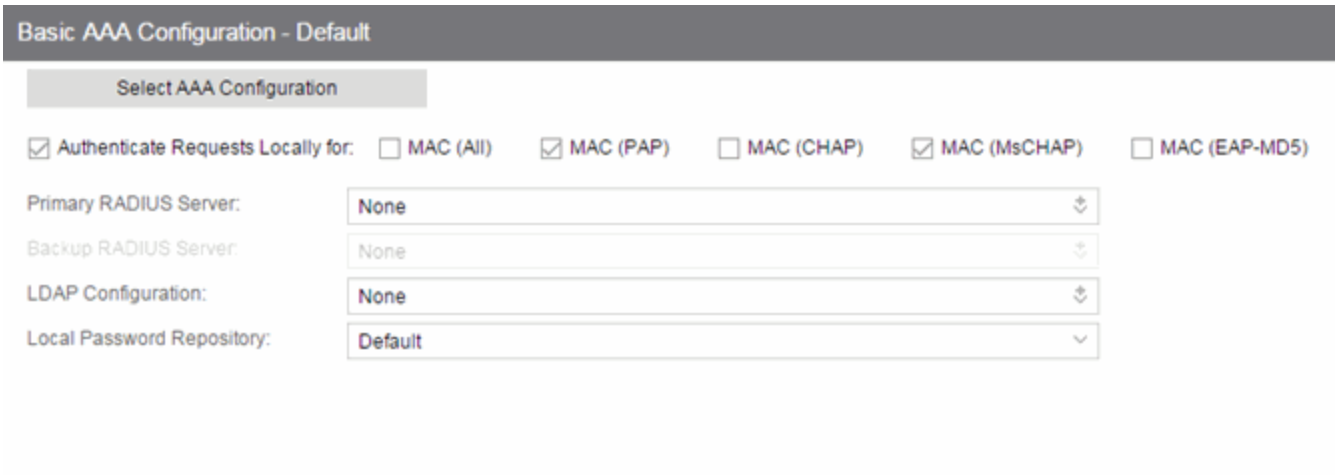
Accessing the AAA Configuration

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. In the left-panel tree, expand the Access Control Configurations tree and expand an Access Control Configuration at the top of the tree.
4. Select AAA within the tree. The AAA Configuration is displayed in the right panel.
5. If needed, click the Select AAA Configuration button at the top of the panel to open the Select AAA Configuration drop-down menu in the right panel to select the configuration you want for your Access Control Configuration.
6. 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.
7. 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 Access Control engine. Select this option if all MAC authentication requests are to be authorized, regardless of the MAC authentication password (except MAC (EAP-MD5) which requires a password that is the MAC address). The Accept policy is applied to end-systems that are authorized locally.

Select one or more MAC authentication types:

- MAC (All) — includes MAC (PAP), MAC (CHAP), MAC (MsCHAP), and MAC (EAP-MD5) authentication types.
- MAC (PAP) — this is the MAC authentication type used by Extreme Networks wired and wireless devices.
- MAC (CHAP)
- MAC (MsCHAP)
- MAC (EAP-MD5) — this MAC authentication type requires a password, which must be the MAC address.

Primary/Backup RADIUS Servers

If your Access Control engines are configured to proxy RADIUS requests to a RADIUS server, use these fields to specify the primary and backup

RADIUS servers to use. Use the drop-down 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:

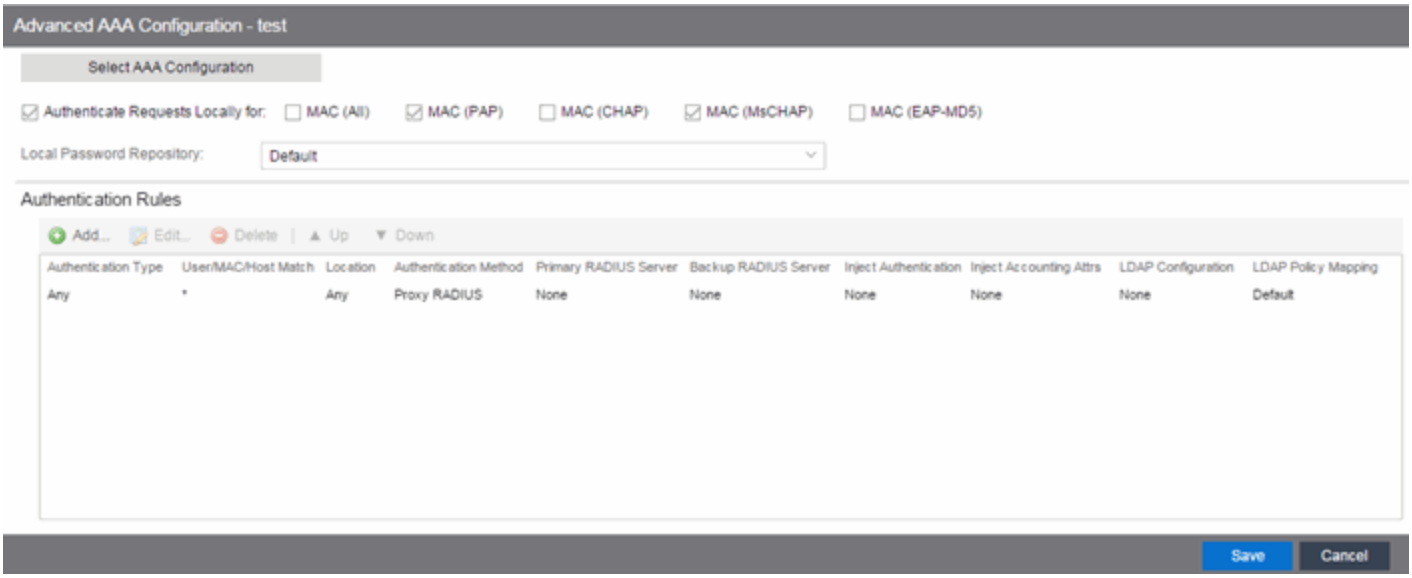
- authentication type
- username/user group
- MAC address/end-system group
- hostname/hostname group
- location group
- authentication method
- RADIUS user group
- LDAP user group

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

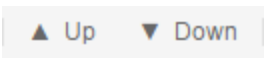
Use this field to specify the local password repository you want for this AAA configuration. Extreme Management Center supplies a default repository that can be used to define passwords for administrators and sponsors accessing the Registration administration web page and the sponsor administration web 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 Access Control engine joins in order to authenticate users to all Active Directory domains configured for that engine or select Auto Detect to let the Access Control engine determine the domain. Auto Detect starts at the first entry set to LDAP Authentication in the table and attempt to join that domain. If it cannot join that domain, it goes to the next entry set to LDAP Authentication and attempt to join that domain, and so on until one succeeds.

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... **Add New Mapping**

Opens the Add User to Authentication Mapping window where you can define a new mapping.

Edit... **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.

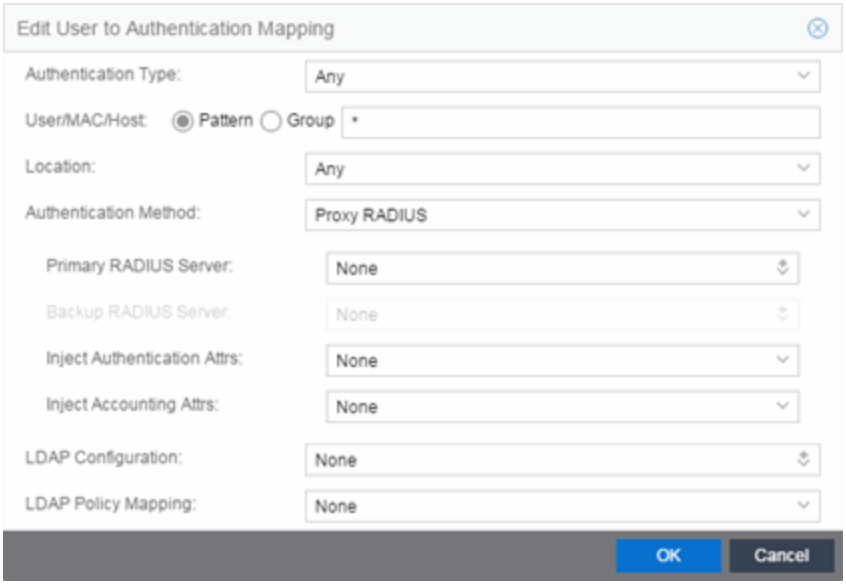
Related Information

For information on related windows:

- Add User to Authentication Mapping Window

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.

Inject Accounting Attrs — Use the drop-down menu to select attributes to inject when proxying accounting requests to the back-end RADIUS servers.

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.

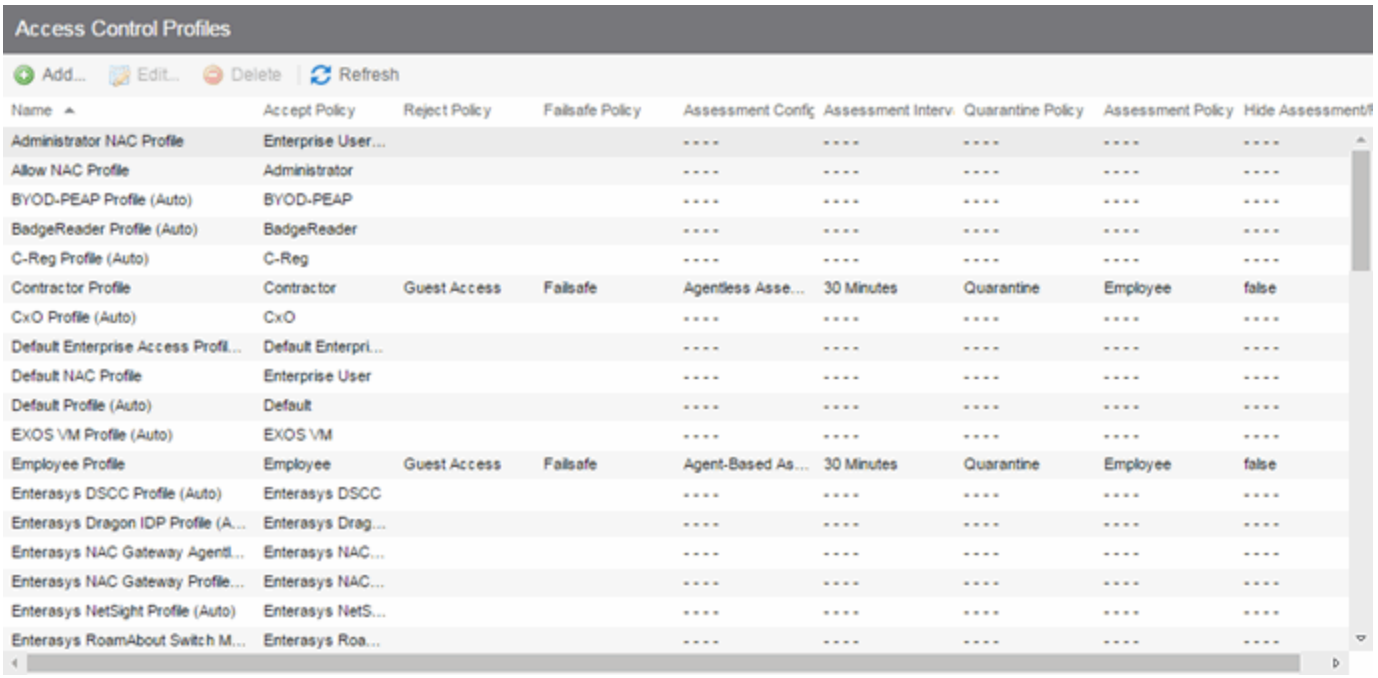
Related Information

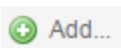
For information on related windows:

Extreme Access Control Profiles

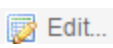
Extreme Management Center comes with ten system-defined Extreme Access Control profiles that define the authorization and assessment requirements for the end-systems connecting to the network. The system-defined profiles are: Administrator, Allow, Default, Guest Access, Notification, Pass Through, Quarantine, 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 Management Center database.

To access this window, select the Access Control Profiles left-panel option in the Access Control tab.

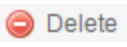


Add Button 

Use this button to open the New Extreme Access Control Profile window, where you can add a Access Control profile.

Edit Button 

Use this button to open the Edit Extreme Access Control Profile window, where you can edit an existing Access Control profile.

Delete Button 

Use this button to add a Access Control profile.

Name
: The name of the Access Control profile.

Accept Policy
: The Accept policy defined for this profile. An Accept policy is applied to an end-system when

  - an end-system has been authorized locally by the Access Control engine and has passed an assessment (if assessment in enabled).
  - authentication is configured to replace the attributes returned from the RADIUS server with the Accept policy.

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

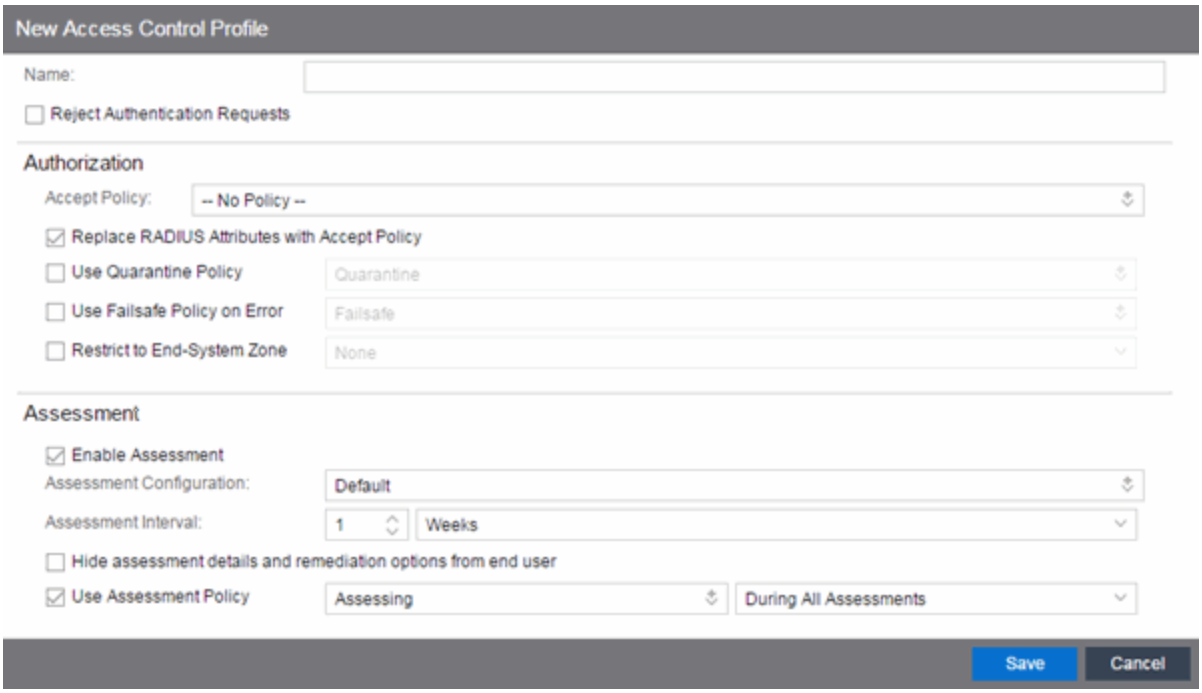
Extreme Access Control Profiles specify the authorization and assessment requirements for the end-systems connecting to the network. Profiles also specify the security policies that will be applied to end-systems for network authorization, depending on authentication and assessment results.

Extreme Management Center comes with ten system-defined Access Control profiles:

- Administrator
- Allow
- Default
- Guest Access
- Notification
- Pass Through
- Quarantine
- Registration Denied Access
- Secure Guest Access
- Unregistered

You can edit these profiles or you can define your own profiles to use for your Access Control configurations. Use this window to create a new profile, or edit an existing profile. When you create a new profile, it is added to the Manage 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 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 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 Access Control engine and has passed an assessment (if assessment in enabled).
- you have selected the **Replace RADIUS Attributes with Accept Policy** option.

If you select "No Policy", then the Access Control engine does not include a Filter ID or VLAN Tunnel Attribute in the RADIUS attributes returned to the

switch, and the default role configured on the port is assigned to the end-system. This option is necessary when configuring single user plus IP phone authentication supported on C2/C3 and B2/B3 devices.

Replace RADIUS Attributes with Accept Policy

When this option is checked, the attributes returned from the RADIUS server are replaced by the policy designated as the Accept policy. If the RADIUS server does not return a Filter ID or VLAN Tunnel attribute, the Accept policy is inserted. When this option is unchecked, the attributes returned from the RADIUS server are forwarded back "as is" and the Accept Policy would only be used to locally authorize MAC authentication requests. If the RADIUS server does not return a Filter ID or VLAN Tunnel attribute, no attributes are returned to the switch.

Use Quarantine Policy

Select this checkbox if you want to specify a Quarantine policy. The Quarantine policy is used to restrict network access for end-systems that have failed the assessment. You must have the Enable Assessment checkbox selected to activate this checkbox.

If a Quarantine policy is not specified and you have configured RADIUS in your AAA configuration, then the policy from the RADIUS attributes would be applied (unless Replace RADIUS Attributes with Accept Policy has been selected, in which case the Accept policy would be used.) If Authorize Authentication Requests Locally has been selected in your AAA configuration, then the Accept policy would be applied to those end-systems that are authorized locally. This allows an end-system onto the network with its usual network access even though the end-system failed the assessment.

Use Failsafe Policy on Error

Select this checkbox if you want to specify a Failsafe policy to be applied to an end-system when it is in an Error connection state. An Error state results if the end-system's IP address could not be determined from its MAC address, or if there was a scanning error and a scan of the end-system could not take place. A Failsafe policy should allocate a nonrestrictive set of network resources to the connecting end-system so it can continue its work, even though an error occurred in Access Control operation.

If a Failsafe policy is not specified and you have configured RADIUS in your AAA configuration, then the policy from the RADIUS attributes would be applied (unless Replace RADIUS Attributes with Accept Policy has been

selected, in which case the Accept policy would be used.) If **Authorize Authentication Requests Locally** has been selected in your AAA configuration, then the Accept policy would be applied to those end-systems that are authorized locally. This allows end-systems onto the network with their usual network access when an error occurs in Access Control operation.

Assessment

Enable Assessment

Select the **Enable Assessment** checkbox if you want to require that end-systems are scanned by an assessment server.

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 Access Control Configurations > 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

Manage 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 Access Control profiles.

When an end-system authenticates to the network, the Access Control profile is applied and the appropriate RADIUS response attributes are extracted from the mapping based on the switch the authentication request originated from. The attributes are returned to the switch in the RADIUS Access-Accept response.

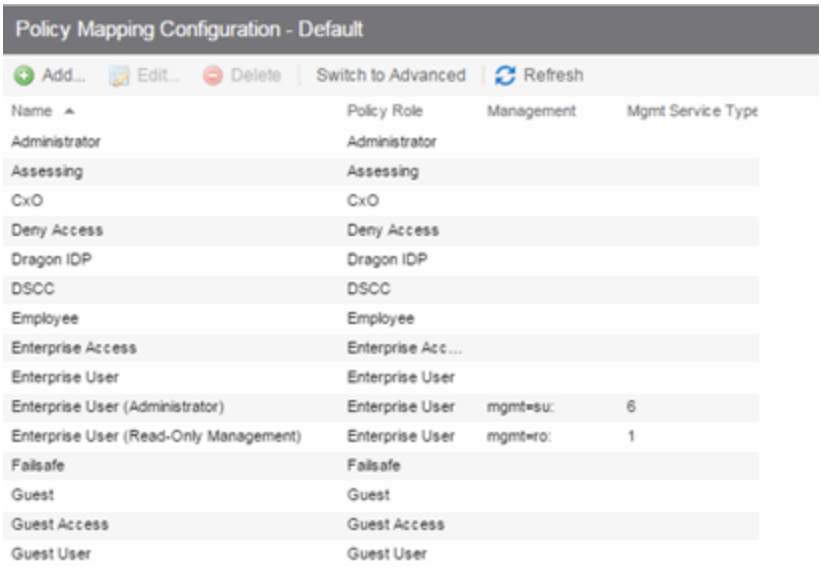
For more information on configuring policy mappings, see How to Set Up Access Policies and Policy Mappings. For a description of each Access Control access policy, and some guidelines for creating corresponding policy roles in the **Policy** tab, see the section on Access Policies in the Concepts file.

To access this window, click on the **Policy Mappings** left-panel option in the **Access Control Configurations** > **Access Control** left-panel menu.

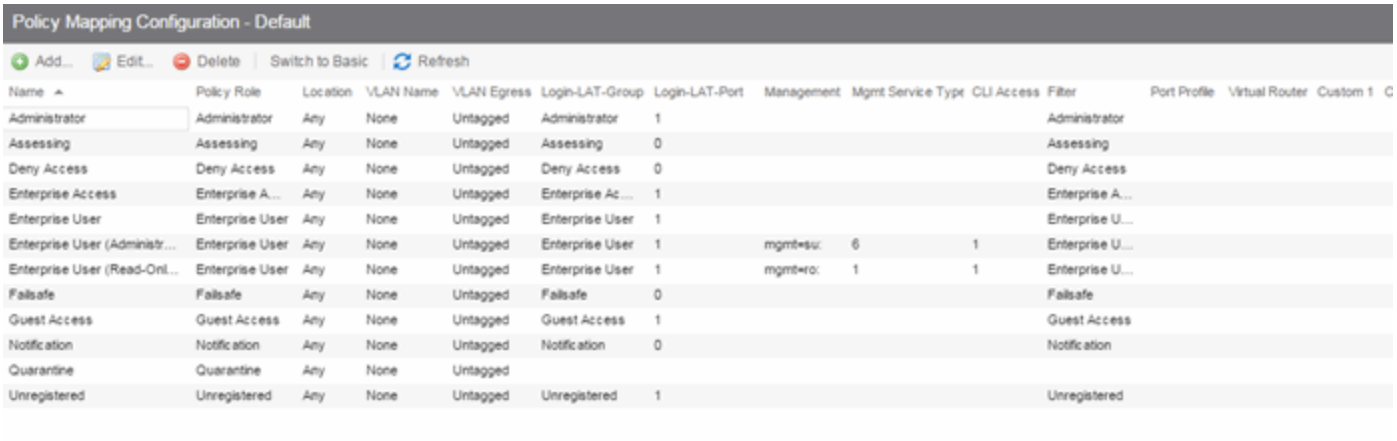
The columns displayed in this window vary depending on whether you are using a Basic or Advanced policy mapping configuration. For a definition of each column, see below.

Basic AAA Configuration

Basic AAA Configurations define the RADIUS and LDAP configurations for all end-systems connecting to your Access Control engines.



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 (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 Access Control rule and corresponding Access Control profile to be authorized to different accept attributes (policy/VLAN/Custom Attribute) based on the location the request originated from. For example, in the Policy Mapping Configuration screenshot above, the Administration policy mapping has five entries, with each entry assigning a different VLAN (for RFC 3580-enabled switches) for authentication requests matching the specified location. Requests originating from the 1st floor South location will be authorized to VLAN 100, and requests originating from the 2nd floor North location (matching the same Access Control rule) is authorized to VLAN 220. Using locations in this manner lets you authorize end-systems to different access criteria using a single Access Control rule, whereas the alternative would be to create multiple location-based Access Control rules each with a 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 Access Control engine. This is used in conjunction with the Registration and Assessment features of Access Control.

Management
: The authorization attribute returned for successful administrative access authentication requests that originate from network equipment configured to use RADIUS as the authentication mechanism for remote management of switches, routers, VPN concentrators, etc. Examples of management values for EOS devices are: "mgmt=su:", "mgmt=rw:", or "mgmt=ro:". The management attribute determines the level of access the administrator will have when authorized to access the device: superuser, read/write, or read-only.

Custom
: Some network devices require additional RADIUS response attributes in order to provide authorization or define additional parameters for the authenticated session. These additional attributes can be defined in the five available Custom option fields.

Related Information

For information on related windows:

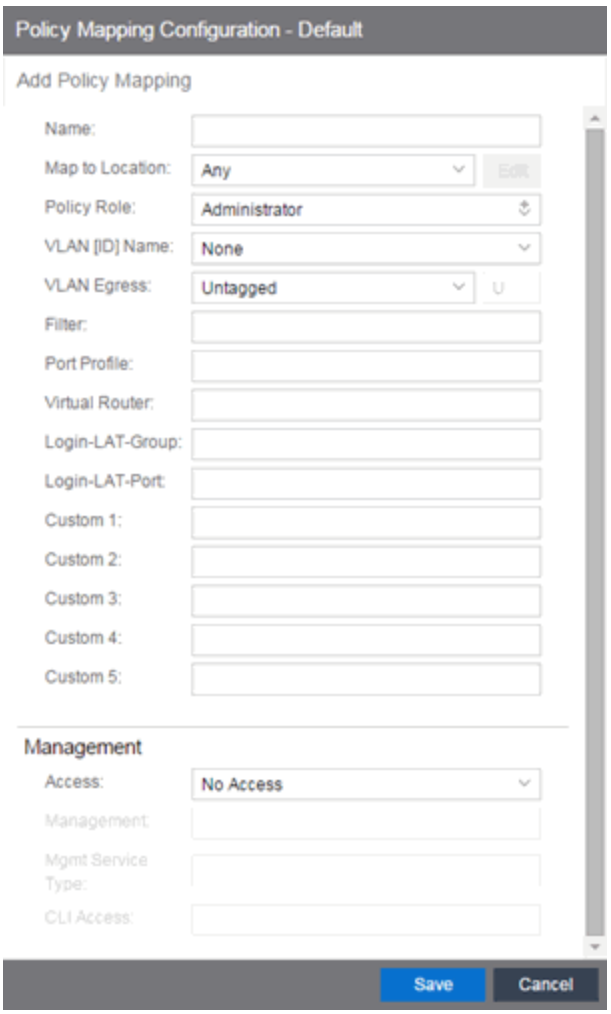
- Add/Edit Policy Mapping Window
- How to Set Up Access Policies and Policy Mappings

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.



Name
: Enter a name for the policy mapping.

Map to Location
: Allows you to specify a certain location for the mapping. You should first configure your locations using the Location Group (**Control** tab > **Access Control** > Access Control Configurations > Group Editor > Location Groups) or you can 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 Access Control Controller policy configuration. Roles from all your policy domains are listed; if there are duplicate names, only one is listed. The list is not case sensitive, so "Enterprise User" and "enterprise user" are considered duplicate policy names. All policy roles used in your mappings must be part of your Access Control) Controller policy configuration and/or defined in **Policy** tab and enforced to the EOS policy-enabled switches in your network.

NOTE: Entering a new policy role does **not** create a new role in the **Policy** tab.

VLAN [ID] Name
: Use the drop-down menu to select the appropriate VLAN associated with the policy. This list displays any VLANs defined in 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 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 Access Control engine. This is used in conjunction with the Registration and Assessment features of Access Control.

Custom
: If your network devices require additional RADIUS response attributes in order to provide authorization or define additional parameters for the authenticated session, you can define them in the five available Custom option fields.

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

Manage Assessment Settings

The Manage Assessment Settings panel is the main panel used to manage and configure the assessment servers performing the end-system assessments in your network. To access this window, select Access Control Configurations > Access Control Profiles > Assessment from the menu bar.

The window displays three tabs that provide information on:

- Assessment Configurations
- Assessment Servers
- Assessment Server Pools

Assessment Configurations

This tab lets you view a listing of your assessment configurations, and add, edit, or delete a configuration. 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 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

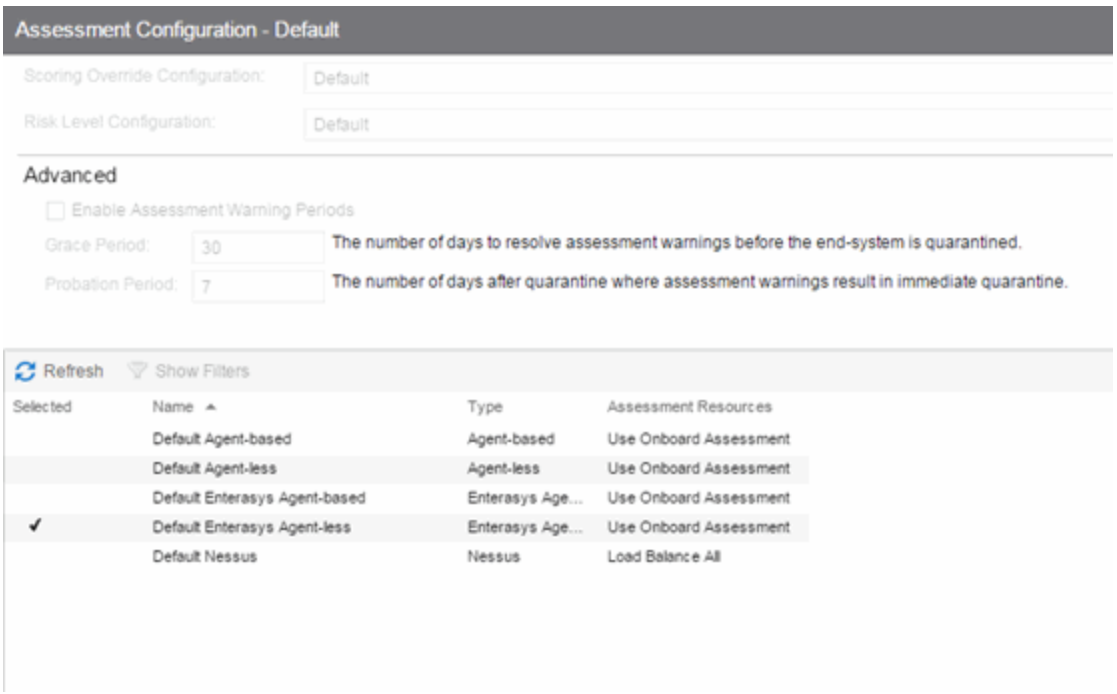
Edit Assessment Configuration

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 **Access Control Configurations > 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

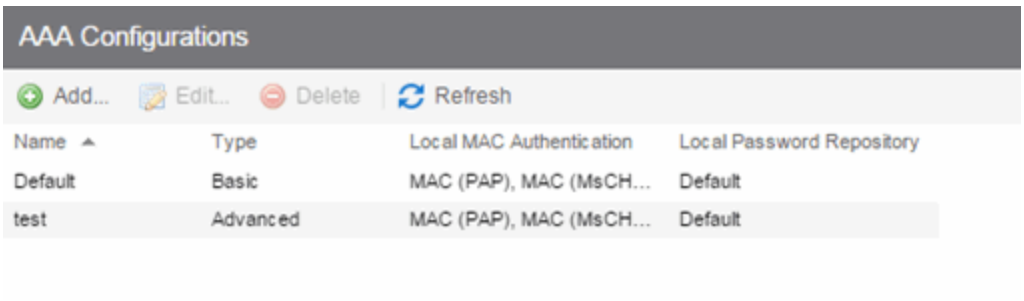
each network, select the unique test set as the Master test set and then select any number of secondary test sets to be included in the configuration as well.

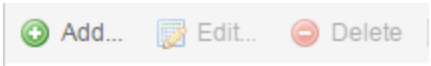
If the Master test set is deselected, then a new master is automatically selected. To specify a different test set as Master, deselect all test sets, select the desired Master test set first, and select the additional supporting test sets.

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 Access Control Configurations panel in the **Control** > **Access Control** tab by expanding the **Access Control Configurations** tree in the left-panel and expanding the AAA Configurations tree. Your configurations are listed within the tree.





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 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

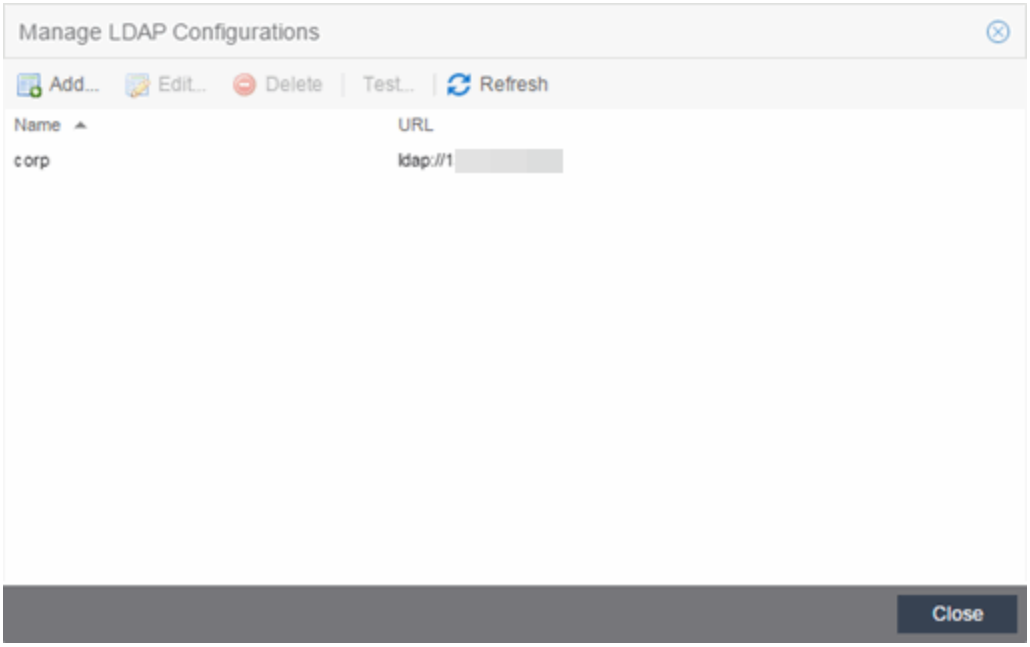
to define passwords for administrators and sponsors accessing the Registration administration web page and the sponsor administration web page. The default password is Extreme@pp.

Related Information

- AAA Configurations

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 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 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/Edit LDAP Configuration

Use the Add/Edit LDAP Configuration window to configure the LDAP servers on your network. You can access this window from the AAA Configuration window in the Access Control tab in Extreme Management Center, 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 Management Center database.

NOTE: If you are using LDAPS, your Management Center/Access Control environment must be configured to accept the new LDAPS server certificate. For additional information, see Server Certificate Trust Mode.

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.)

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 Control/Identity and Access environment must be configured to accept the new LDAPS server certificate. For additional information, see Server Certificate Trust Mode.

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 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. Use a DN (Distinguished Name) search root format.

Schema Definition

Provide information that describes how entries are organized in the LDAP server. You can enter your own definitions or use the defaults available by clicking the Populate Default Values button at the bottom of the window.

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 is stripped off the username prior to performing the lookup. For example, deselect this option when using the User Search Attribute: sAMAccountName. Two examples of the domain name being stripped off:
  user@domain.com -> user
  DOMAIN\user -> user
- User Authentication Type - Specifies the users authentication. 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 will use 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 Identity and Access 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

---

Related Information

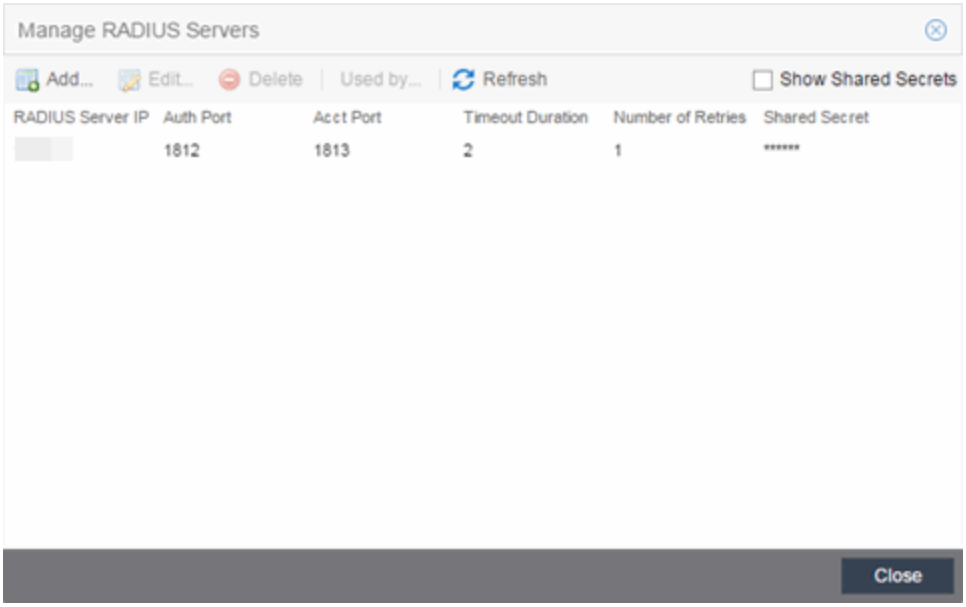
For information on related windows:

- 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 Management Center server authentication configurations and in Extreme Access Control AAA configurations.

You can access this panel by selecting RADIUS Servers from the Access Control Configurations > AAA Configurations > RADIUS Servers in the left-panel tree, or from the Edit Device window or AAA Configuration window. Any changes made are written immediately to the 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 Management Center server or 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 Access Control engine sends accounting requests; 1813 is the default port number.

Timeout Duration
: The amount of time, in seconds, the Management Center server or Access Control engine waits for the RADIUS server to respond to an authentication

or accounting request. Valid values are 2-60 seconds.

Number of Retries
: The number of times the Management Center server or Access Control engine resends an authentication or accounting request if the RADIUS server does not respond. Valid values are 0-20.

Shared Secret
: The shared secret used to encrypt and decrypt communication between the Management Center server or Access Control engine and the RADIUS server. In Access Control, this is also the shared secret used between the switch and the RADIUS server if the Access Control engine is bypassed or if you configured the Management RADIUS Server options when you added the switch.

Show Shared Secrets
: When checked, the shared secrets are shown in text. When unchecked, the shared secrets are shown as a string of asterisks.

Used By Button
: This button is only available when the panel is launched from Access Control. Opens the RADIUS Server(s) Used By window which shows where the selected servers are in use by AAA configurations.

Add Button
: Opens the Add RADIUS Server window where you can define a new RADIUS server.

Edit Button
: Opens the Edit RADIUS Server window where you can edit the values for the selected RADIUS server.

Delete Button
: Deletes the selected RADIUS server. You cannot delete servers currently in use.

Related Information

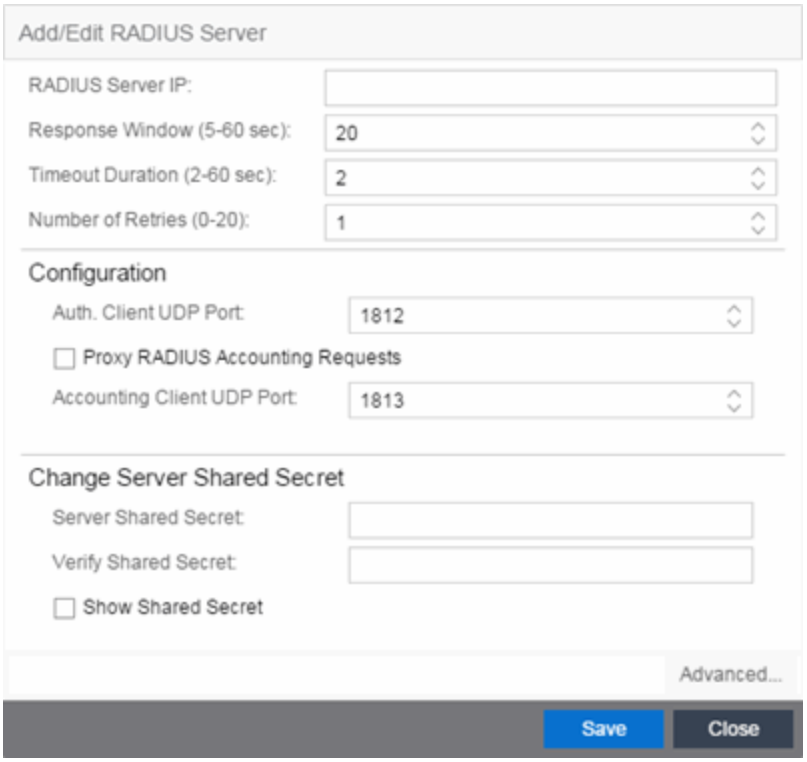
For information on related windows:

- 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 Management Center database.



RADIUS Server IP
: The IP address of the RADIUS server.

Response Window
: This setting is used by Access Control when proxying a RADIUS request to a backend RADIUS server. Access Control keeps a status on all backend RADIUS servers instead of going to the primary RADIUS server for every request. If a RADIUS server does not respond in the amount of time specified here, that server is marked as down until it can be verified as being up. See the Health Check section of the Advanced RADIUS Server

Configuration window for information on how Access Control determines the health of a RADIUS server.

Timeout Duration

The amount of time in seconds the Management Center server or Access Control waits for the RADIUS server to respond to an authentication or accounting request. Valid values are 2-60 seconds. This setting is only used for logging into Management Center via RADIUS or logging into the Access Control Captive Portal via RADIUS.

NOTE: The Access Control engine times out a RADIUS server if it takes more than "(retries +1) * timeout" or 20 seconds, whichever is greater, for the server to respond. For example, if the number of retries is set to 1 and the timeout duration is set to 2 (the default values), then the engine times out a RADIUS server if it takes longer than 20 seconds to respond, because that is the greater value (20 to 4). If the RADIUS server times out, then Access Control fails over to the backup RADIUS server until it determines that the primary server is back up. At that point, Access Control starts proxying RADIUS requests to the primary server again.

Number of Retries

The number of times the Management Center server or Access Control engine resends an authentication or accounting request if the RADIUS server does not respond. Valid values are 0-20. This setting is only used for logging into Management Center via RADIUS or logging into the Access Control Captive Portal via RADIUS.

Auth. Client UDP Port

The UDP port number (1-65535) on the RADIUS server that the Management Center server or Access Control engine sends authentication requests to; 1812 is the default port number.

Proxy RADIUS Accounting Requests

Select this checkbox to enable the Access Control engine to proxy RADIUS accounting requests to the RADIUS server. This option must be enabled if you are doing RADIUS accounting in an Access Control environment where the primary RADIUS server is being used for redundancy in a single Access Control engine configuration (Basic AAA configuration only).

Accounting Client UDP Port

The UDP port number (1-65535) on the RADIUS server that the Access Control engine sends accounting requests to; 1813 is the default port number.

Server Shared Secret
: The shared secret is a string of characters used to encrypt and decrypt communication between the Management Center server or Access Control and the RADIUS server. In Management Center, this is also the shared secret used between the switch and the RADIUS server if the Access Control engine is bypassed or if you configured the Management RADIUS Server options when you added the switch. The shared secret must be at least 6 characters long; 16 characters is recommended. Dashes are allowed in the string, but spaces are not.

Verify Shared Secret
: Re-enter the Server Shared Secret you entered above.

Show Shared Secret
: Displays the secret in the **Server Shared Secret** and **Verify Shared Secret** fields.

Advanced Button
: Use this button to open the Advanced RADIUS Server Configuration window, where you can configure advanced RADIUS settings used by Access Control when proxying access requests to a backend RADIUS server.

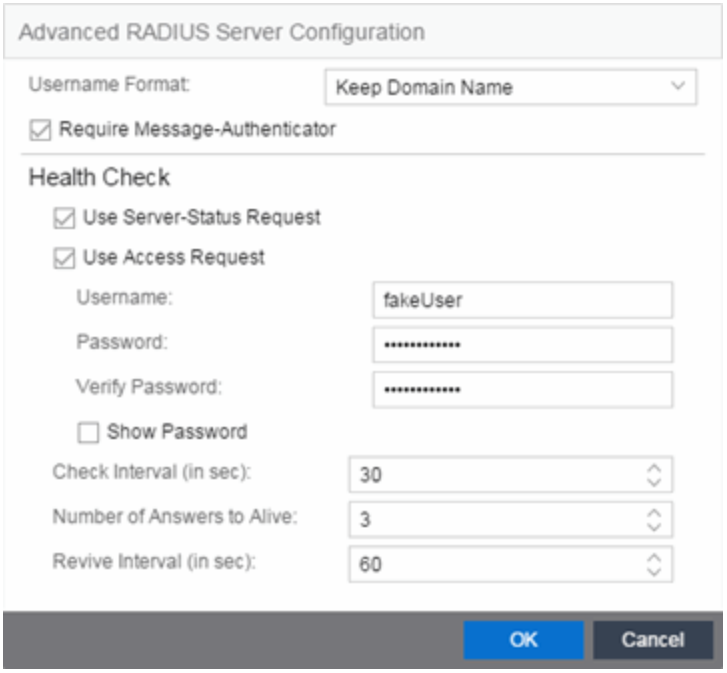
Related Information

For information on related windows:

- Manage RADIUS Servers Window
- Advanced RADIUS Server Configuration 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 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, Management Center adds the message authenticator when proxying the request.

Health Check Section

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, 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, 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 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 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

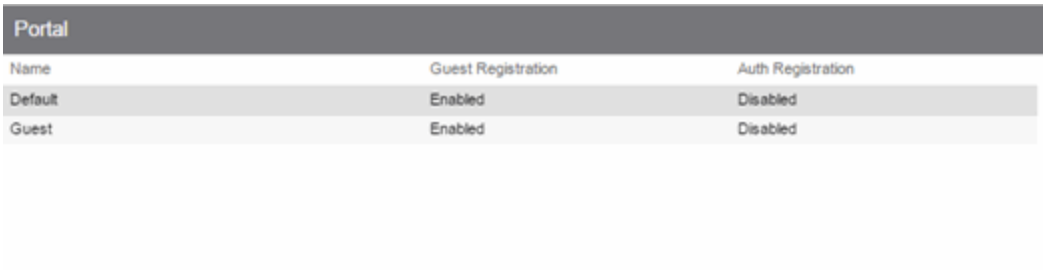
For information on related windows:

- Manage RADIUS Servers Window
- Add/Edit RADIUS Server Window

Portal Configurations

The Portal Configurations panel in the **Control** > **Access Control** tab lets you view and edit all the portal configurations defined in Extreme Management Center.

To access the Portal Configurations panel, select **Access Control Configurations** > **Portal** from the left-menu tree. If you expand the Portal tree, the Default portal configuration plus any other configurations you have defined are displayed.



Related Information

- Portal Configuration
- AAA Configuration
- Extreme Access Control Configuration Rules

Portal Configuration

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.

This Help topic provides the following information for accessing and configuring the Portal Configuration:

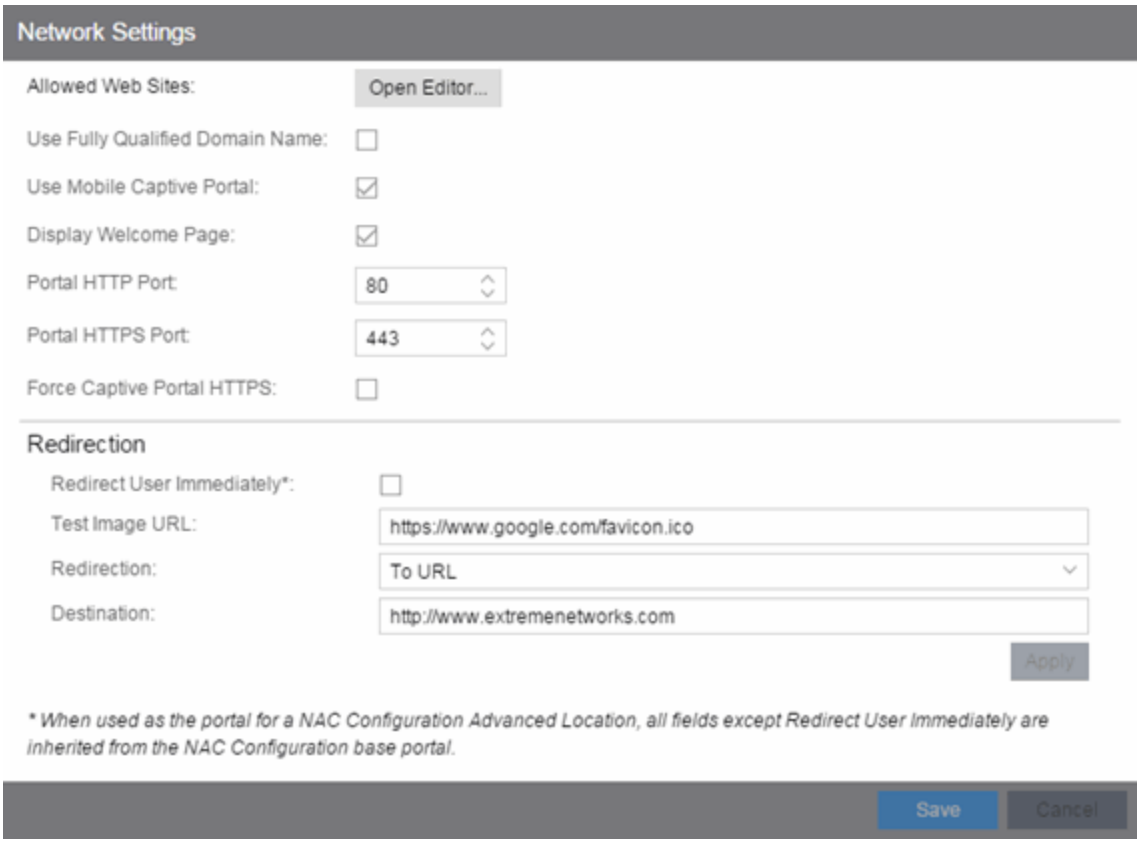
Accessing the Portal Configuration

Use the following steps to access the Portal Configuration:

1. Open the Control > Access Control tab.
2. In the left-panel tree, expand the Portal tree.
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.



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 Control engine. Enable this option only if all Access Control engines 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 Access Control engine use for HTTP web server traffic. Any change does not take effect on the Access Control engine until an Enforce is performed.

Portal HTTPS Port
: Specify which port the Management Center server and Access Control engine use for HTTPS web server traffic. Any change does not take effect on the Access Control engine until an Enforce is performed.

Force Captive Portal HTTPS
: Select this checkbox to force captive portal web pages to be served securely over HTTPS (instead of HTTP) to end users on the network. It is recommended this checkbox is enabled if Authenticated Registration is configured for the registration process. The default setting is unchecked, specifying to serve the captive portal web pages over HTTP.

Redirect User Immediately
: This option redirects end users to the specified test image URL as soon as they have network access. The redirect happens regardless of where the end user is in the connection process. If the end-system's browser can reach the test image URL, then it assumes the end user has network access and redirects the end user out of the captive portal. The test image URL should be an internal image on your own website that end users don't have access to until they're accepted. It is recommended that the test image URL is a link to an SSL site because if the Access Control captive portal is configured for Force Captive Portal HTTPS, the browser does not allow the attempt to an HTTP test image site. It is also recommended that the captive portal policies, (typically the Unregistered, Assessing, and Quarantine policies), are configured to deny HTTPS traffic. This prevents the test image

connection attempt from successfully completing and moving the end-system out of the captive portal prematurely. In the event access to the test image is available, the user may experience the captive portal reverting to the "click here to access the network page", and then upon selecting the link, returning to the previous page based on their state. This behavior continues until the user is finally accepted on the network.

NOTE: If using the portal for an Access Control Advanced Location, all portal configurations are inherited from the Access Control base portal.

Redirection

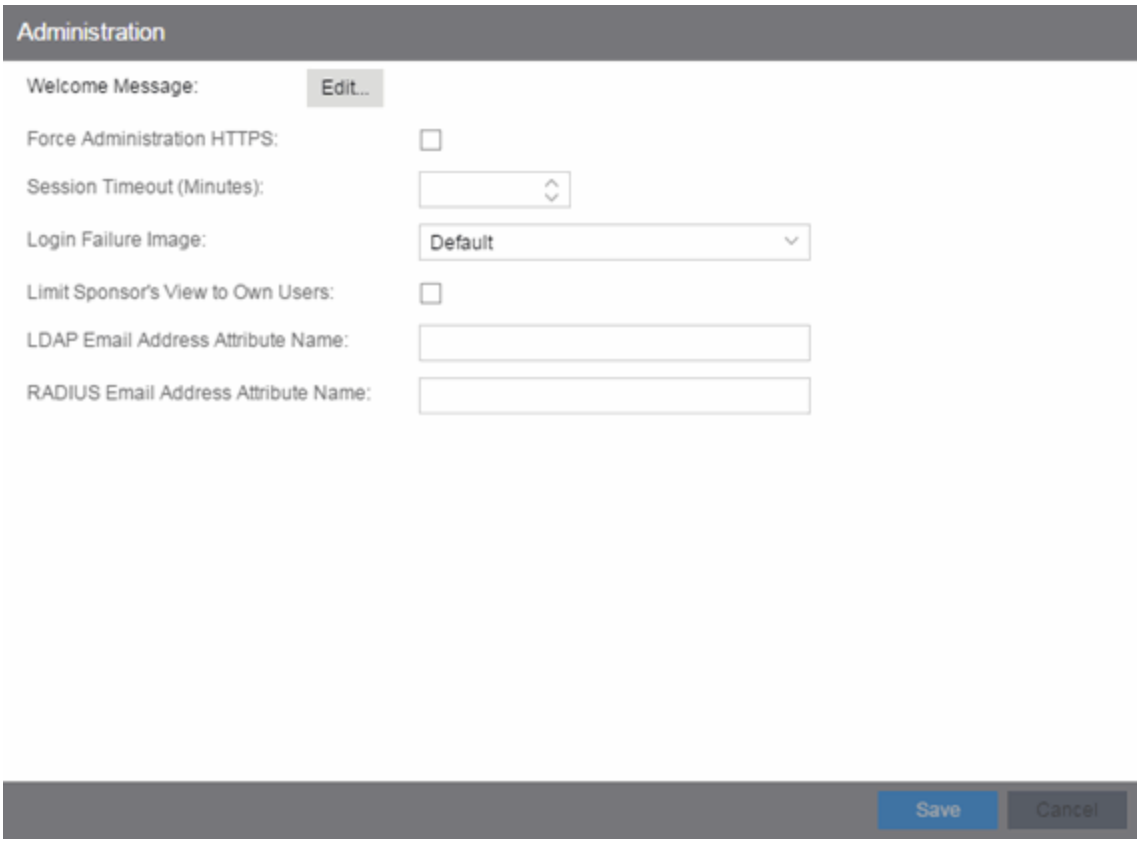
There are three Redirection options that specify where the end user is redirected following successful registration or remediation, when the end user is allowed on the network:

- To URL — This option lets you specify the URL for the web page where the end user is redirected. When selected, the Destination field displays, allowing you to indicate the URL of the web page.
- Disabled — This option disables redirection. The end user stays on the same web page where they were accepted onto the network.
- To User's Requested URL — This option redirects the end user to the web page they originally requested when they connected to the network.

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.



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)

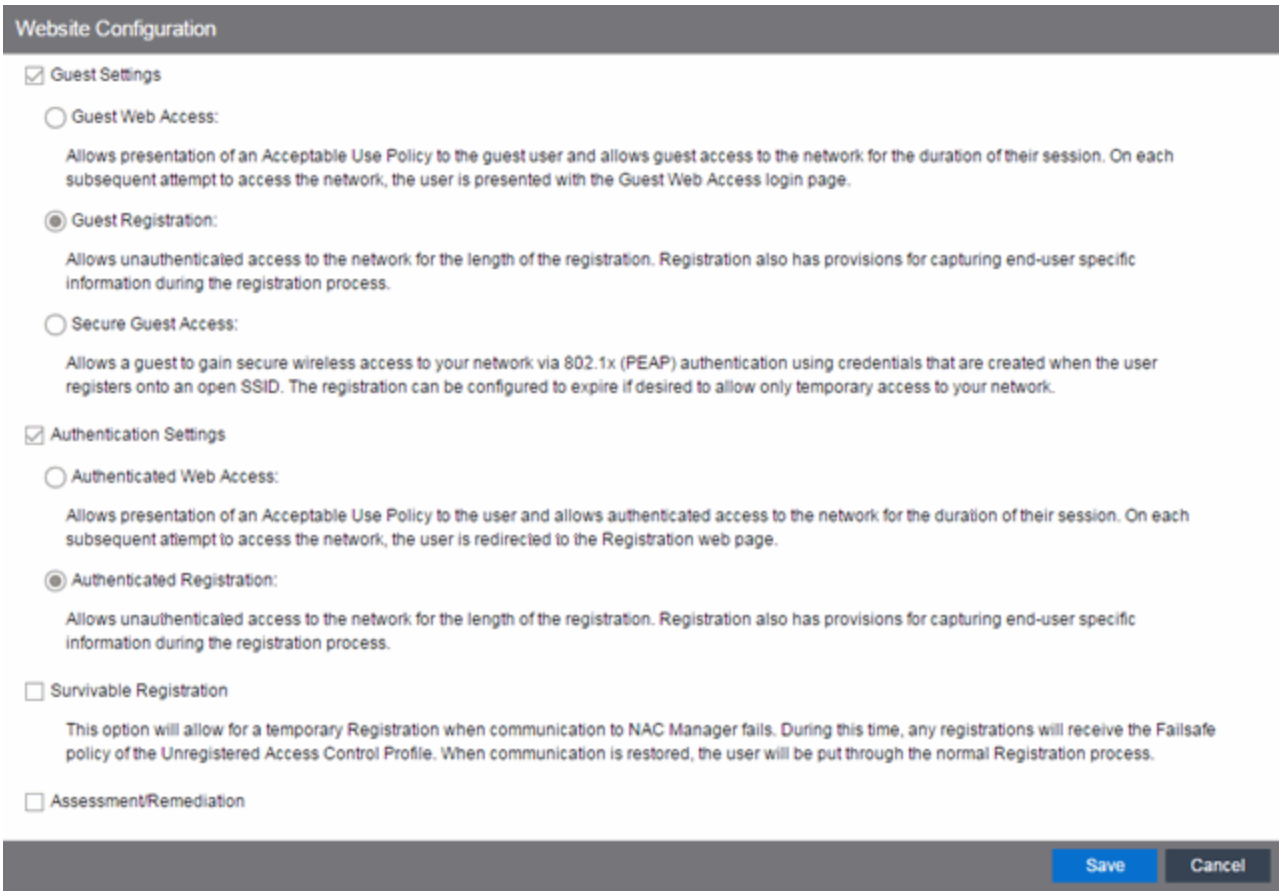
This field specifies the length of time an administrator can be inactive on the administration web page before automatically being logged out. The default value is 10 minutes.

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.

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

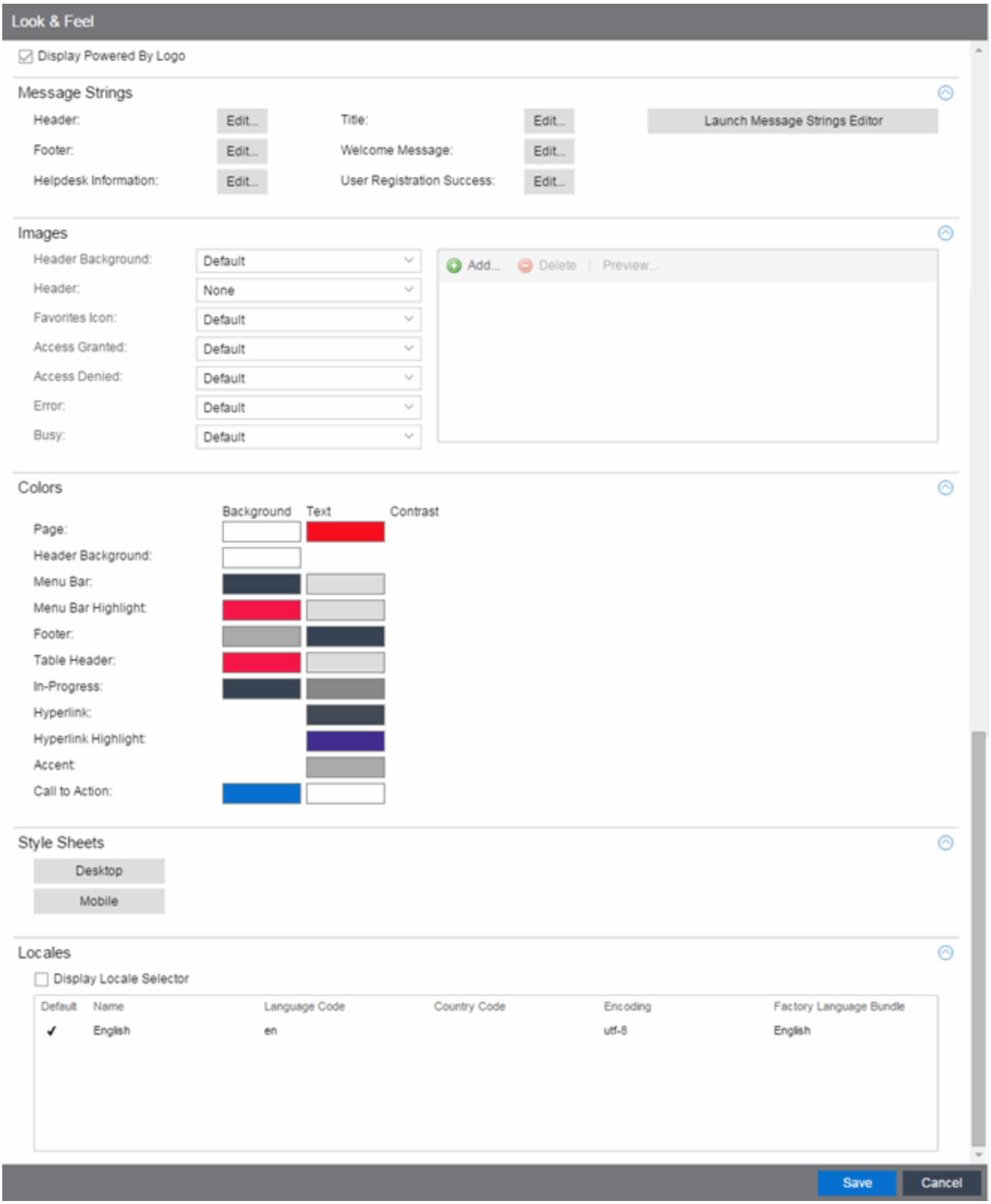
This feature provides temporary Registration for unregistered end-systems when the Extreme Management Center server is unreachable. If you select this checkbox, unregistered users that try to register while the Management Center server is unreachable are redirected to the Registration web page. After entering the required information, users are assigned the Failsafe policy and allowed on the network. Once the connection to the 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.

Look and Feel

Use this panel to configure common web page settings shared by both the Assessment/Remediation and the Registration portal web pages.


Look & Feel
Display Powered By Logo
Message Strings
Header:
Edit...
Title:
Edit...
Launch Message Strings Editor
Footer:
Edit...
Welcome Message:
Edit...
Helpdesk Information:
Edit...
User Registration Success:
Edit...
Images
Header Background:
Default
Header:
None
Favorites Icon:
Default
Access Granted:
Default
Access Denied:
Default
Error:
Default
Busy:
Default
Add...
Delete
Preview...
Colors
Background
Text
Contrast
Page:
Header Background:
Menu Bar:
Menu Bar Highlight:
Footer:
Table Header:
In-Progress:
Hyperlink:
Hyperlink Highlight:
Accent:
Call to Action:
Style Sheets
Desktop
Mobile
Locales
Display Locale Selector
Default
Name
Language Code
Country Code
Encoding
Factory Language Bundle
English
en
utf-8
English
Save
Cancel

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 Control engine 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.

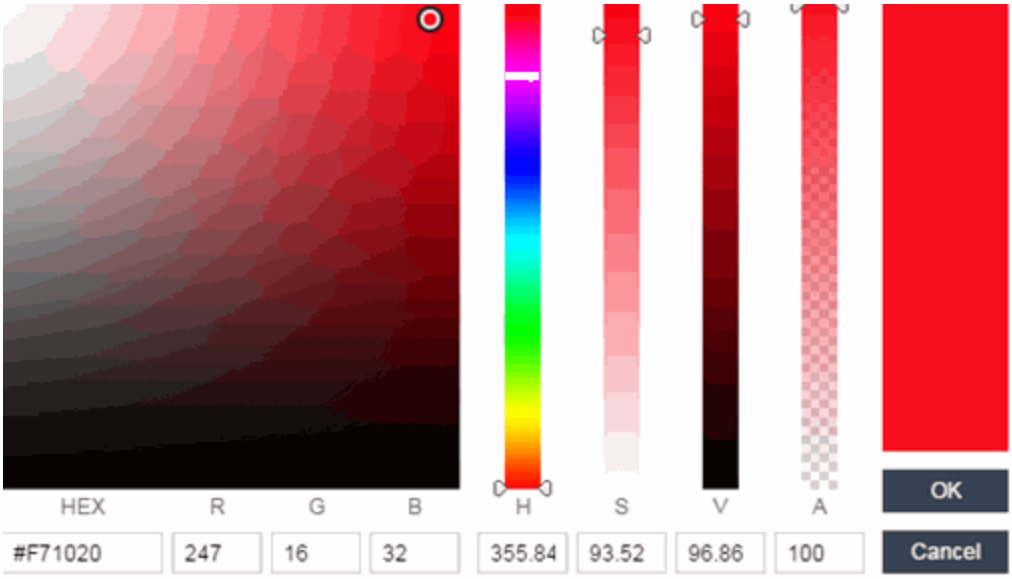
Colors

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.)

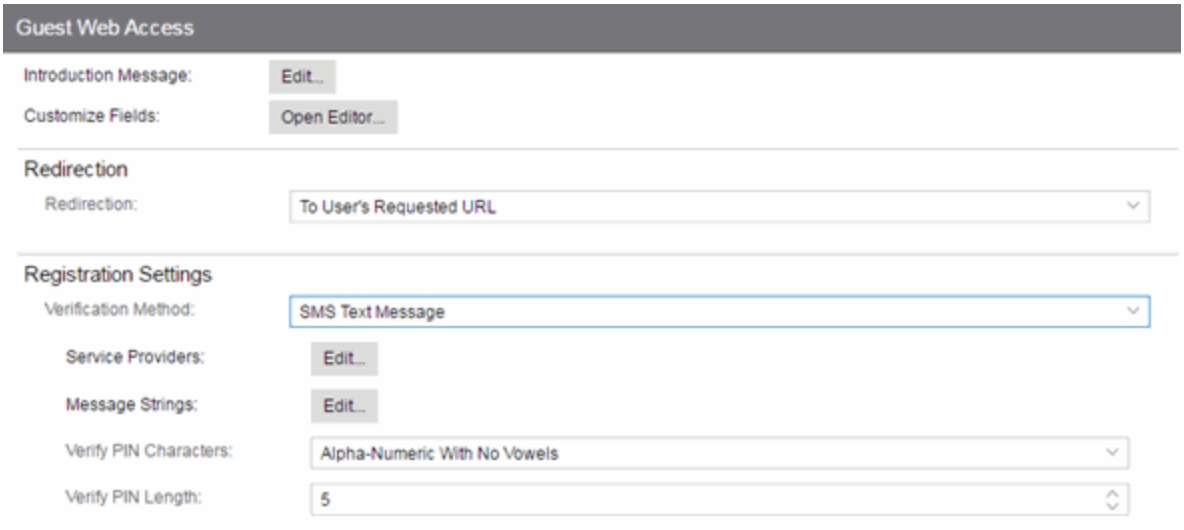
Guest Web Access

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.

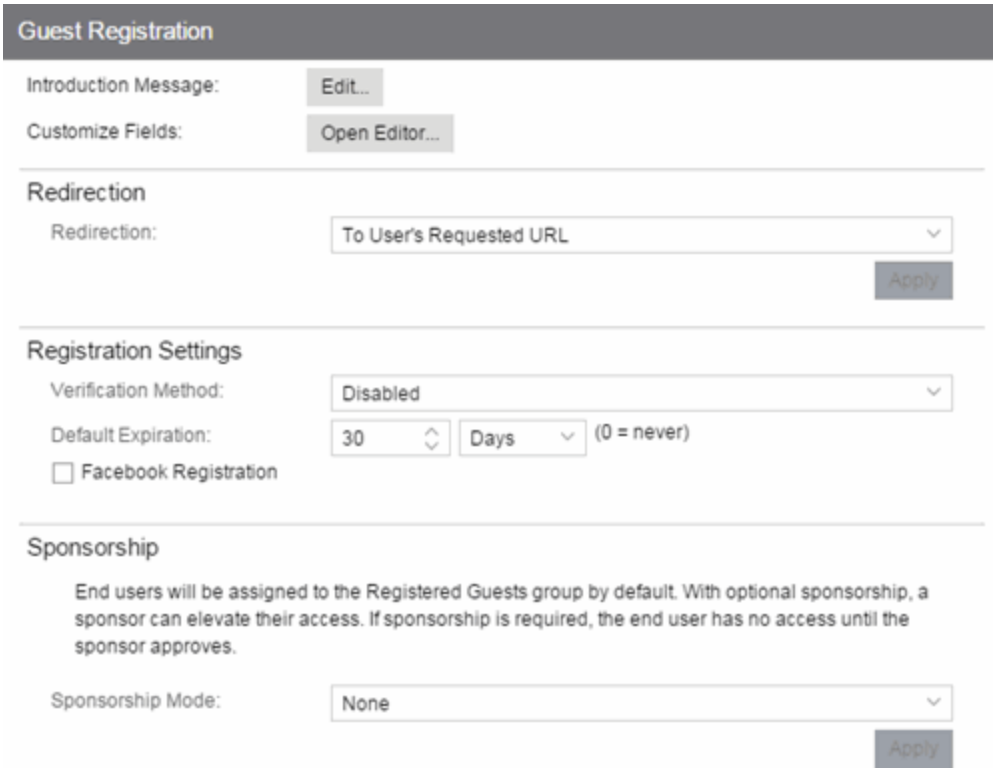
For all methods: set the Verify Pin Characters and Verify Pin Length options to define the characteristics and length of the verification code that is sent to the guest end user. This setting is shared by Guest Registration and Guest Web Access. Changing it for one access type also changes it for the other.

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.

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.



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.

Facebook Registration

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. For more information, see How to Implement Facebook Registration for steps on how to create a Facebook application. When you create an application you are given a Facebook App ID and Facebook App Secret to enter here.

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. For information on each option, see How to Configure Sponsorship for Guest Registration.

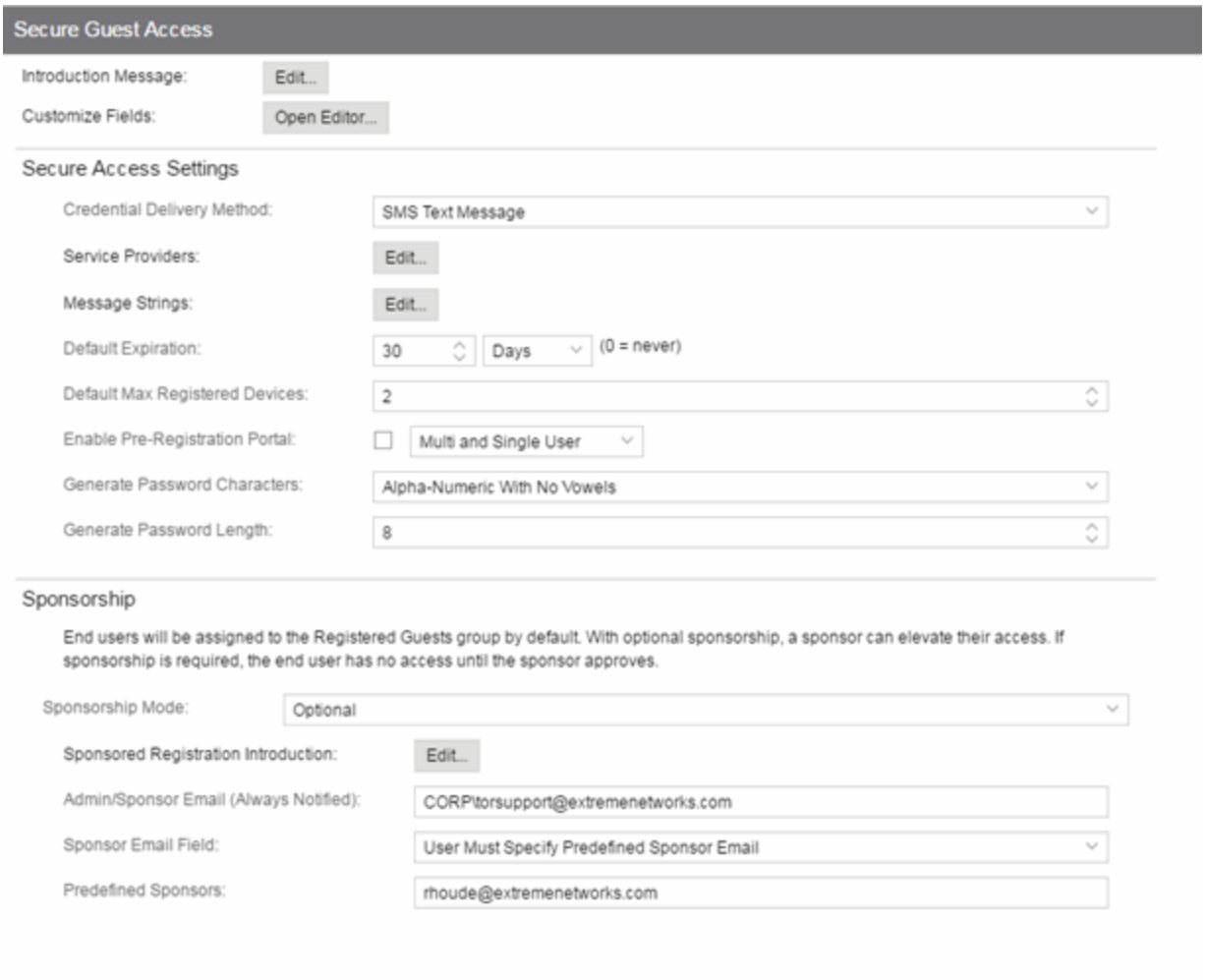
With sponsored registration, end users are only allowed to register to the network when approved by a "sponsor," an internal trusted user to the organization. Sponsorship can provide the end user with a higher level of access than just guest registration and allows the sponsor to fine-tune the level 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.

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.

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.

Implementing authenticated web access requires web redirection or DNS proxy.

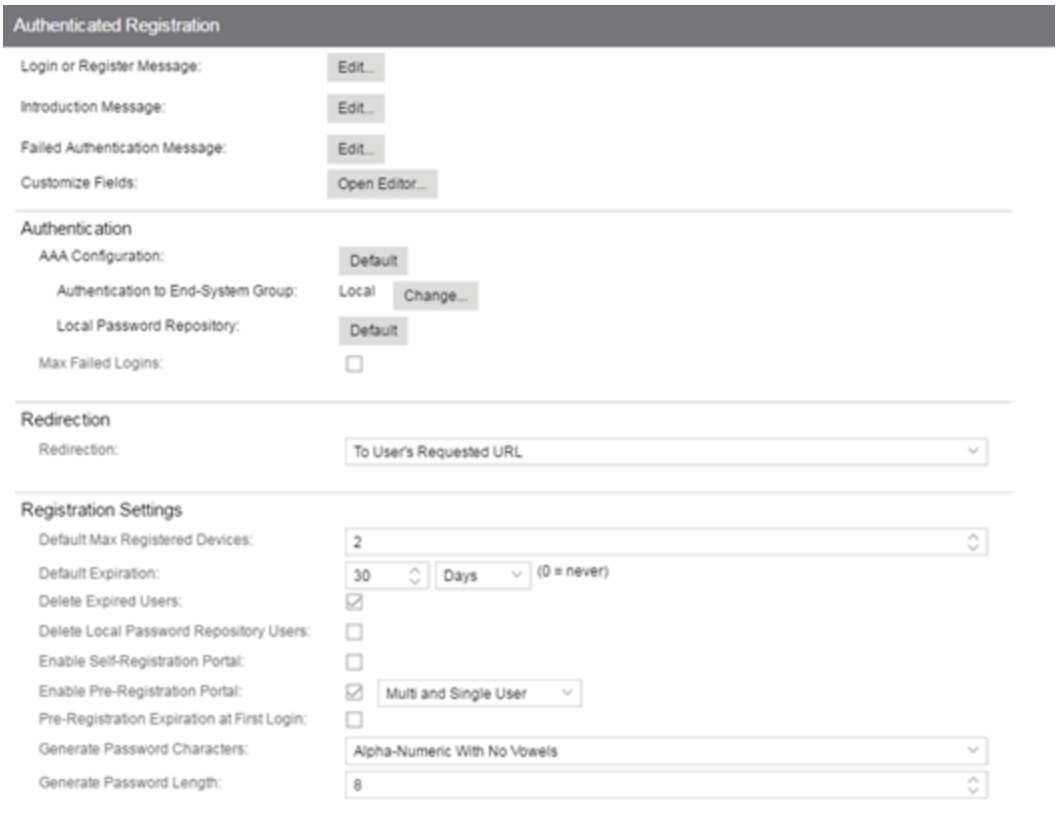
This functionality is not yet available.

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.



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.

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 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://<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

This option is available if you select **Enable Pre-Registration Portal**. 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). For more information, see How to Configure Pre-Registration.

Generate Password Characters

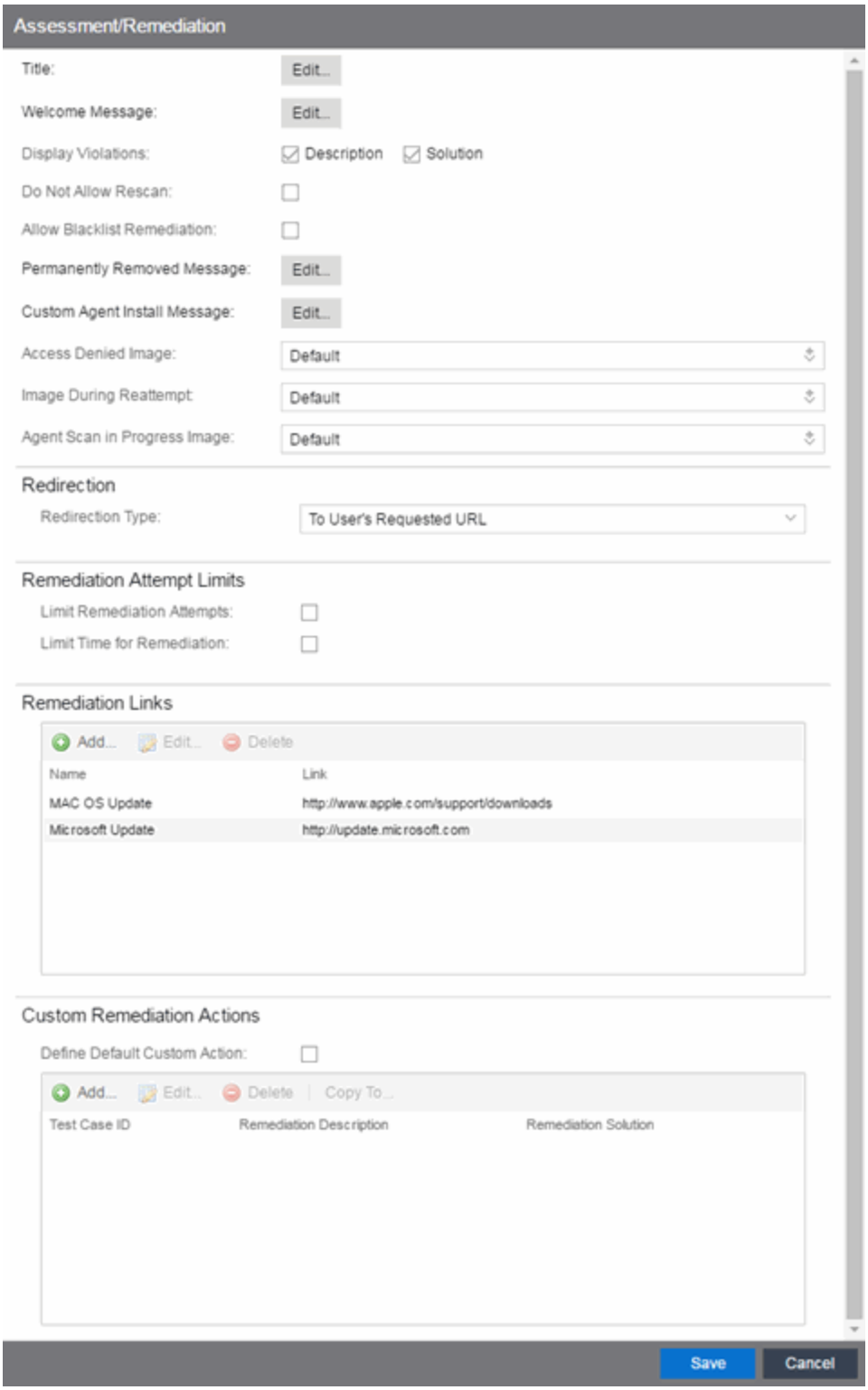
This option is available if you select **Enable Pre-Registration Portal**. During the pre-registration process, Management Center can automatically generate the password that the guest user uses when connecting to the network. The password is generated according to the specification selected here. This 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, 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. This setting is shared by Authenticated Registration and Secure Guest Access. Changing it for one access type also changes it for the other.

Assessment/Remediation

Use this panel to configure settings for 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 a 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://*Access ControlengineIP* /screen_ preview
Registration Administration Page Lets administrators view registered devices and users, and manually add, delete, and modify users.	https://*Access ControlengineIP* /administration
Registration Sponsor Page Lets sponsors view registered devices and users, and manually add, delete, and modify users.	https://*Access ControlengineIP* /sponsor
Pre-Registration Page The pre-registration web page lets selected personnel easily register guest users in advance of an event, and print out a registration voucher that provides the guest user with their appropriate registration credentials.	https://*Access ControlengineIP* /pre_ registration
Self-Registration Page Allows an authenticated and registered user to self-register additional devices that may not have a web browser (for example, game systems).	https://*Access ControlengineIP* /self_ registration

Related Information

For information on related help topics:

- How to Configure Verification for Guest Registration

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:

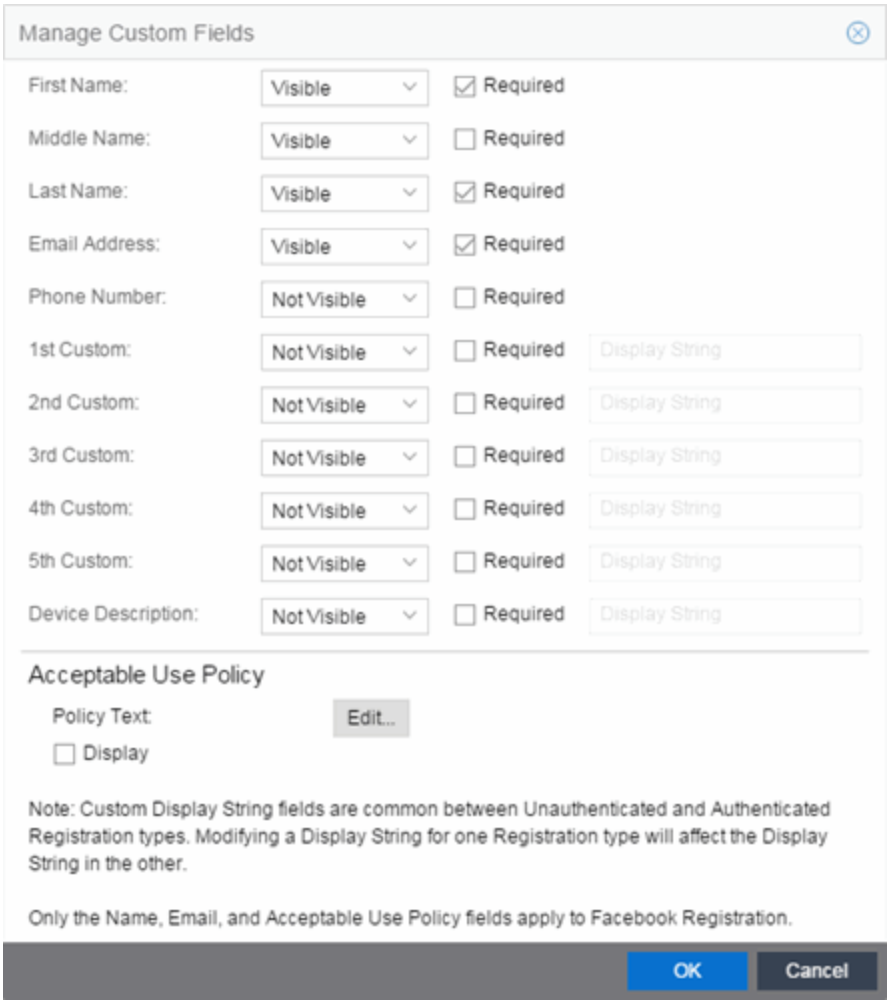
- Edit Portal Configuration Panel

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

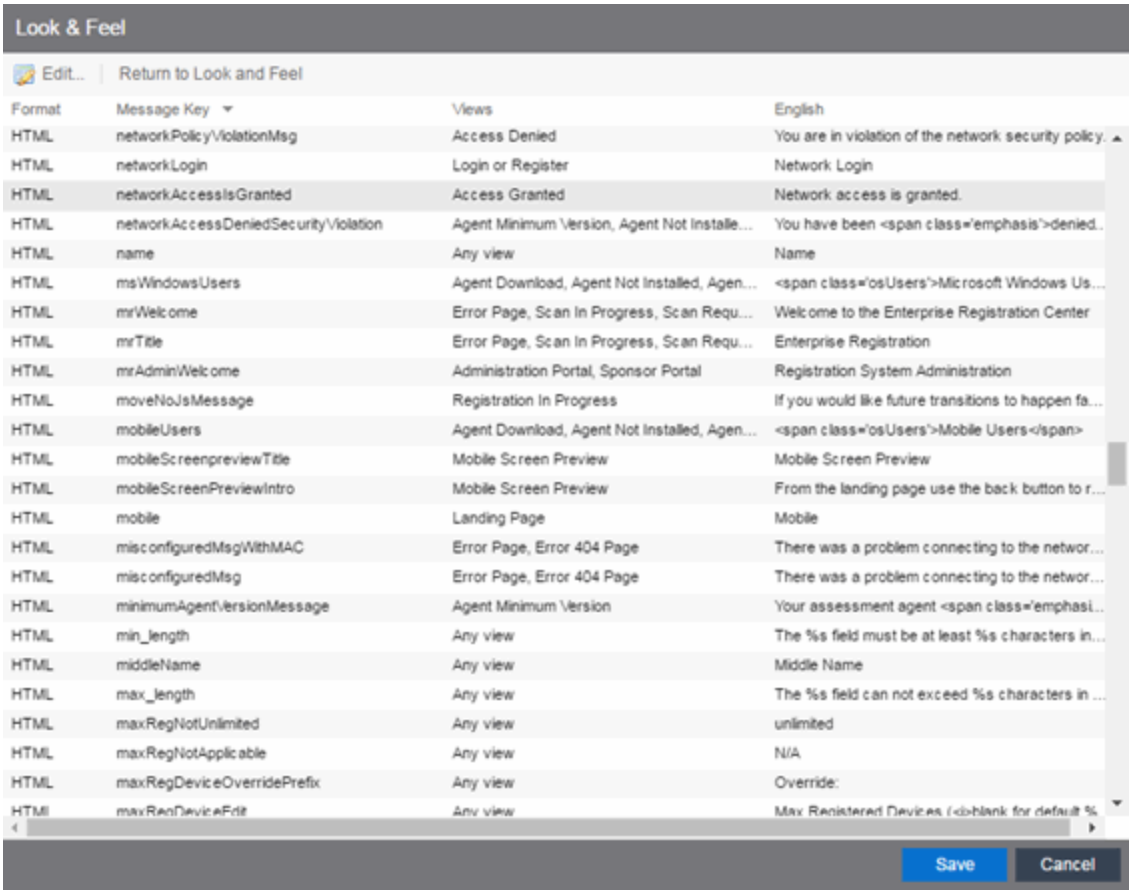
- Edit Portal Configuration Panel

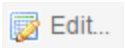
Message Strings Editor

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 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

Group Editor

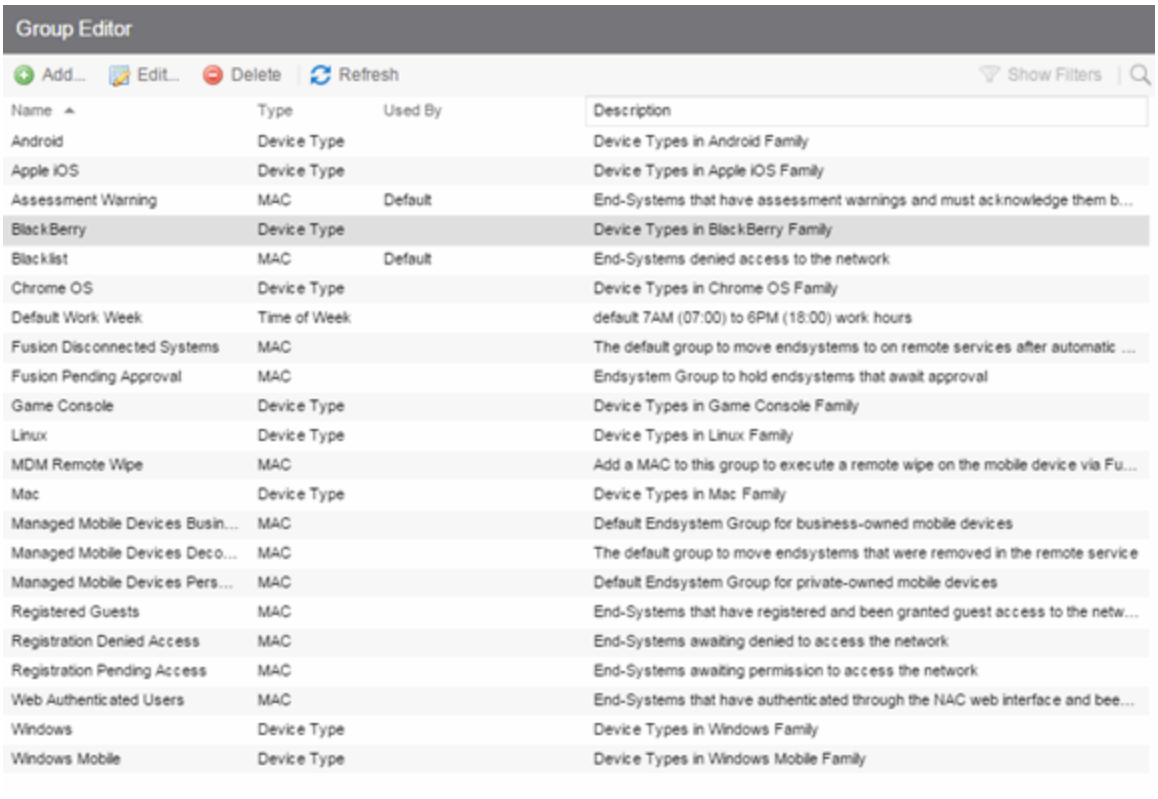
This panel lists the various rule groups used to define the criteria for the rules used in your Extreme Access Control configuration. You can use this window to view and edit the defined rule groups and also to add new rule groups for use in your Access Control configuration. Any changes made in this window are written immediately to the Extreme Management Center database.

Management Center comes with system-defined rule groups. 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.

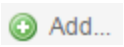
Select from the following rule group categories when you create a new rule group:

Category	Group Types	Value Types
Device Type Groups	Device Type	A list of device types.
End-System Groups	Hostname	A list of hostnames: 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.
	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.
User Groups	LDAP User Group	A list imported from an LDAP Server, organized by Organization Unit (OU).
	RADIUS User Group	A list of attributes returned by the RADIUS server.
	Username	A list of usernames which can be based on an exact match or a wild card.

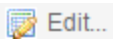
To access this window, open the Access Control tab and select Access Control Configurations > Group Editor in the left-panel.



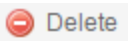
Name	Type	Used By	Description
Android	Device Type		Device Types in Android Family
Apple iOS	Device Type		Device Types in Apple iOS Family
Assessment Warning	MAC	Default	End-Systems that have assessment warnings and must acknowledge them b...
BlackBerry	Device Type		Device Types in BlackBerry Family
Blacklist	MAC	Default	End-Systems denied access to the network
Chrome OS	Device Type		Device Types in Chrome OS Family
Default Work Week	Time of Week		default 7AM (07:00) to 6PM (18:00) work hours
Fusion Disconnected Systems	MAC		The default group to move endsystems to on remote services after automatic ...
Fusion Pending Approval	MAC		Endsystem Group to hold endsystems that await approval
Game Console	Device Type		Device Types in Game Console Family
Linux	Device Type		Device Types in Linux Family
MDM Remote Wipe	MAC		Add a MAC to this group to execute a remote wipe on the mobile device via Fu...
Mac	Device Type		Device Types in Mac Family
Managed Mobile Devices Busin...	MAC		Default Endsystem Group for business-owned mobile devices
Managed Mobile Devices Deco...	MAC		The default group to move endsystems that were removed in the remote service
Managed Mobile Devices Pers...	MAC		Default Endsystem Group for private-owned mobile devices
Registered Guests	MAC		End-Systems that have registered and been granted guest access to the netw...
Registration Denied Access	MAC		End-Systems awaiting denied to access the network
Registration Pending Access	MAC		End-Systems awaiting permission to access the network
Web Authenticated Users	MAC		End-Systems that have authenticated through the NAC web interface and bee...
Windows	Device Type		Device Types in Windows Family
Windows Mobile	Device Type		Device Types in Windows Mobile Family

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 

Use this button to delete existing rule groups.

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 Access Control Configurations > Group Editor > Device Type Groups left-panel tree.

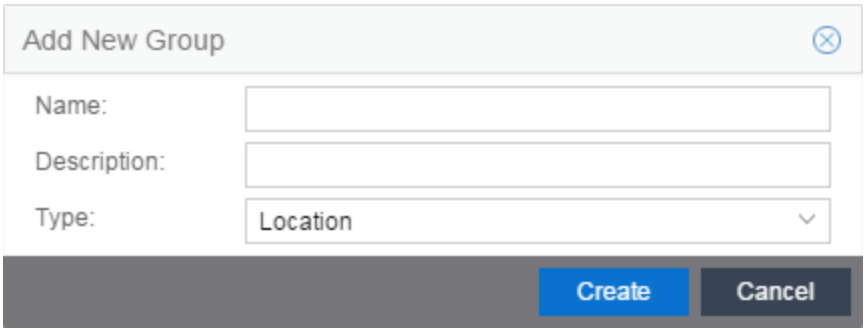
Device type groups are comprised of entries that Extreme Access Control uses to determine if an end-system's device type matches the group. Entries can be a specific device type or a wildcard, such as Windows 7 or win*. If an entry does not already contain a wildcard, Management Center creates a wildcard 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.

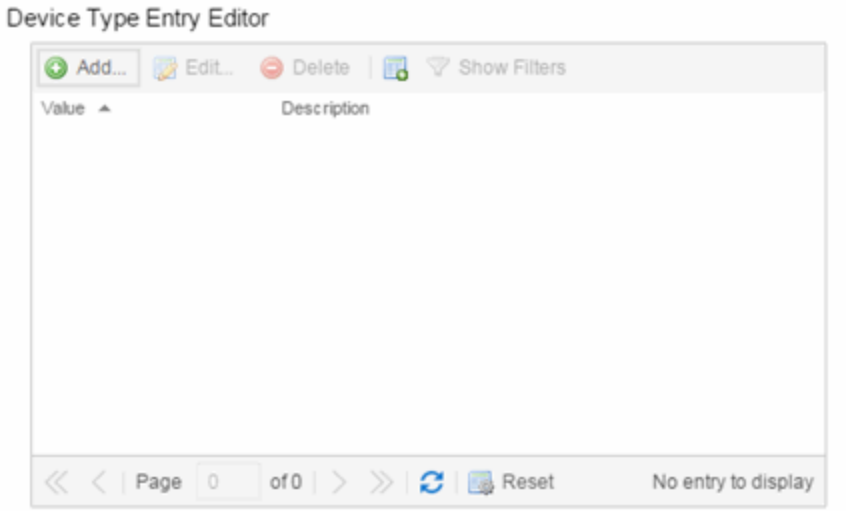
Description

Enter a description of the device type group.

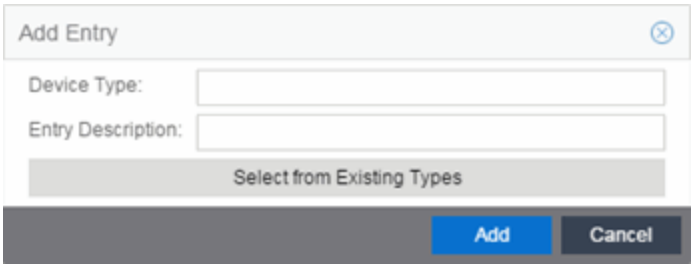
Type

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 Windows 7 or win*. 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

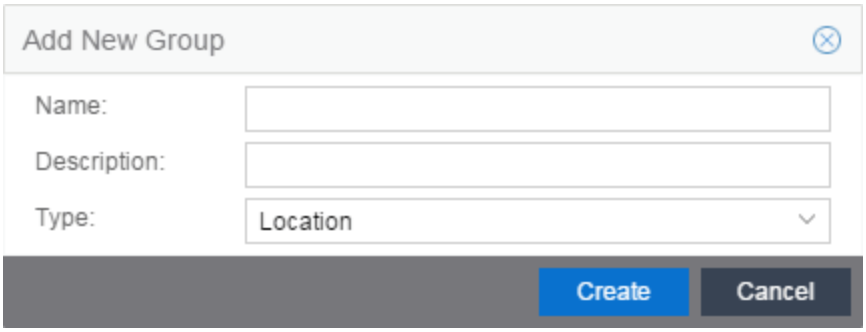
Add/Edit End-System Group

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 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.

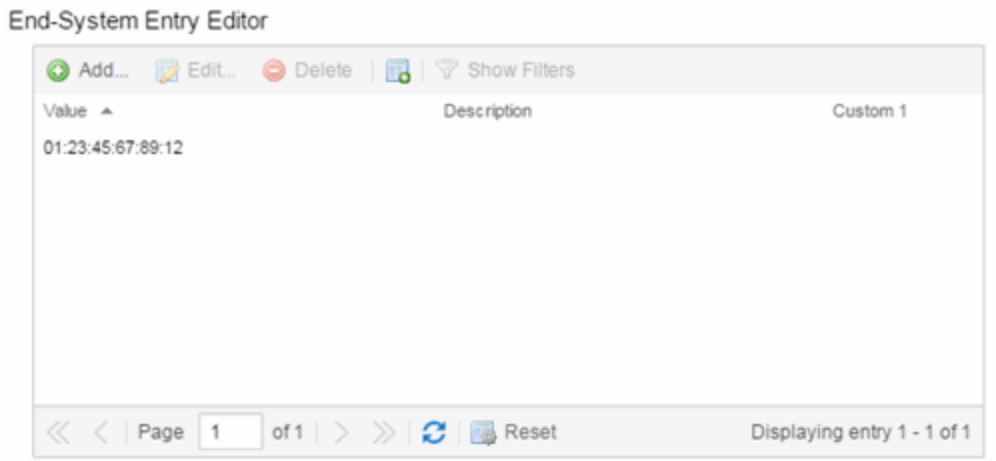
Description

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
: Select **End-System** to create an end-system group. 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 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.

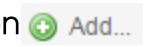
Click **Create** to display the End-System Entry Editor section of the window. This section varies depending on the **Type** selected.



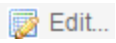
Value
: The MAC address, IP address, Hostname, or Attribute value of the end-system.

Description
: The description of the end-system group.

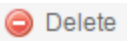
Mode
: For LDAP Host Groups, the mode option lets you specify whether to match any or match all of the LDAP attributes listed below. You can also use "Exists" to just check to see if a host is present in LDAP.

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:

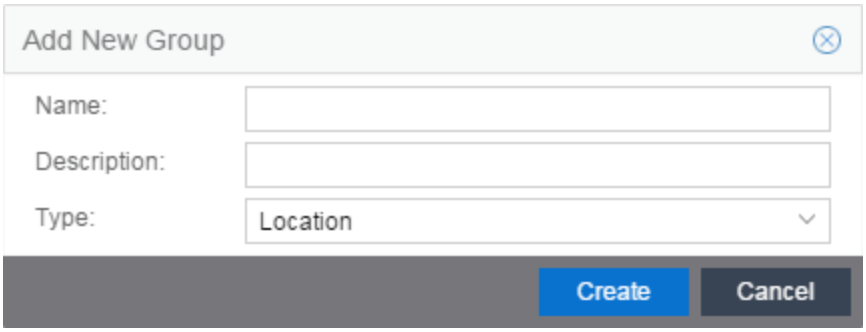
- Create Rule Window
- Manage Rule Groups Window

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 Access Control tab and selecting 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.

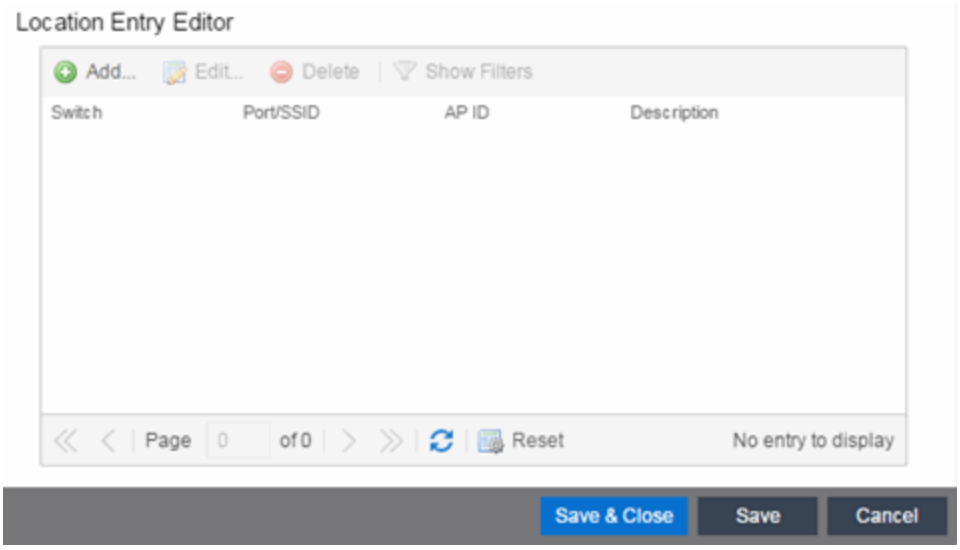


Name
: Enter a name for a new location group. You cannot edit the name of a group.

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.

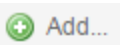


Switch
: The IP address of the switches added to the location.

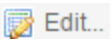
Port/SSID
: The port or port range for a wired switch or the SSIDs for a wireless switch.

AP ID
: The access point identifiers for a wireless switch.

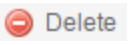
Description
: The description of the location group.

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

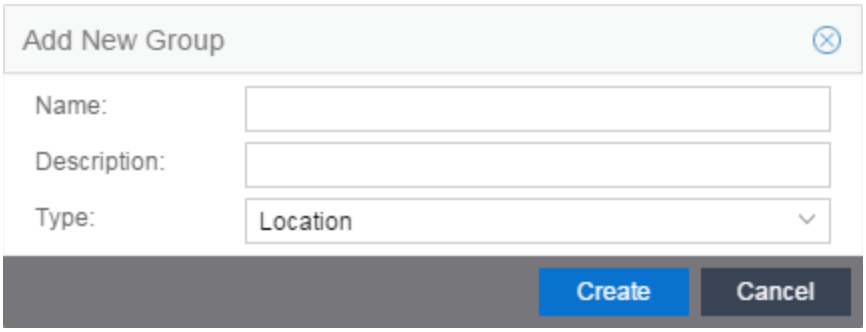
For information on related windows:

- Create Rule Window
- Manage Rule Groups Window

Add/Edit 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.



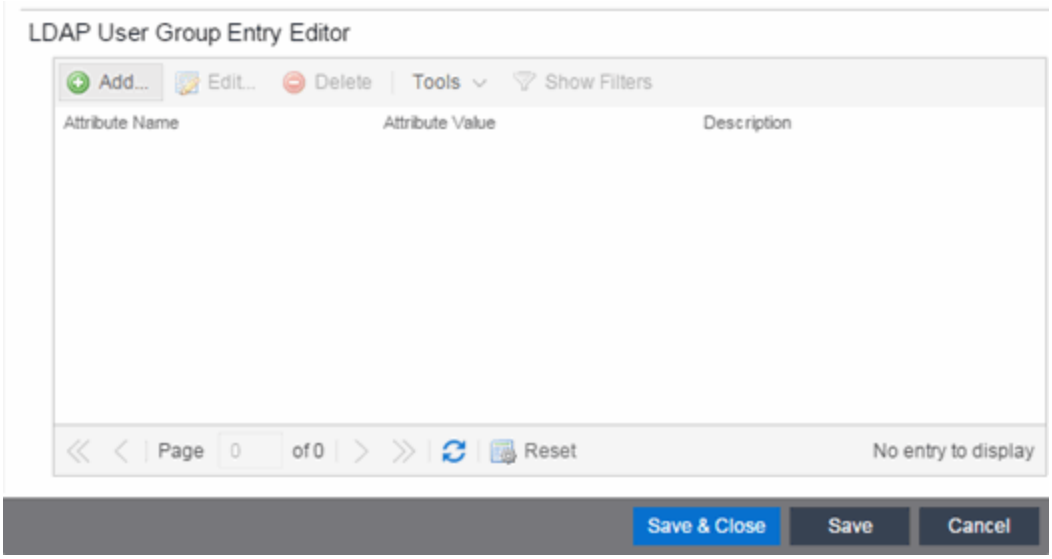
Name
: Enter a name for a new user group. You cannot edit the name of a group.

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.

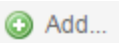
For LDAP User Groups, you can also select **Exists**, as the username can be used to verify this criteria after the initial authentication (i.e., using Registration). The **Exists** mode is not available for RADIUS User Groups because they cannot be verified after an initial registration as the user credentials are not stored on the Extreme Access Control engine for re-verification.

Attribute Name

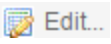
The name of the LDAP or RADIUS Attribute.

Value

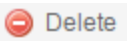
The Attribute value of the user group or username.

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

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 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 Access Control engine assessment requests.

This password must match the password specified in the Access Control Options as the Assessment Agent Adapter Credentials (Administration > Options > Identity and Access > Assessment Server). If you change the password on the assessment agent adapter, change assessment agent adapter credentials in the Access Control options as well, or connection between the engine and assessment servers is lost and assessments is not performed.

To change the assessment agent adapter password:

1. Go to the install directory for the assessment agent adapter on the assessment server. This can be a Nessus server or the Access Control engine if you are using on-board agent-less assessment. On a Access Control engine, the install directory is **/opt/nac/saint**.
2. Run the **sha1.sh** script (on a Access Control engine, the script is located in located in **/opt/nac/saint/util**) using the new password as the argument. The script produces a hash string that looks something like: 9ba2db465ff11b0bdfd188f7ee87b10fc3a145dc
3. Open the **users.properties** file (on an Access Control engine, the file is located in **/opt/nac/saint/users.properties**) and replace the existing hash string with the new one:
   `admin=<new string>`
4. Restart the assessment agent adapter. On a 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 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 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 Access Control engines.
  In this scenario, each service provider customer has their own 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.

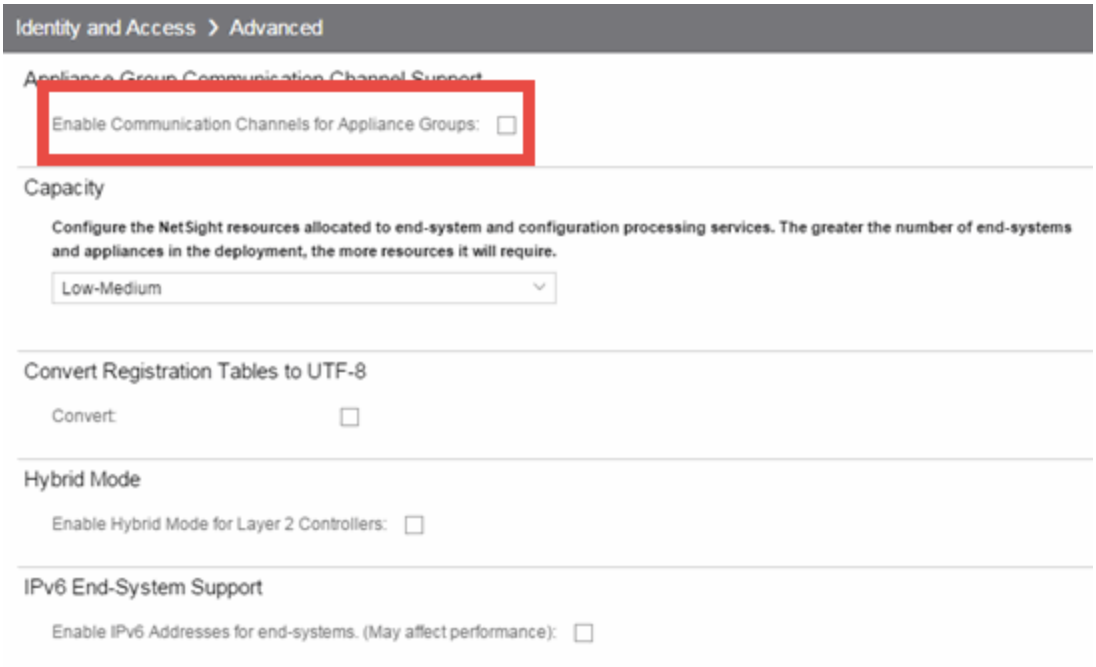
NOTES: In order to enable this feature, both the Management Center server and all the Access Control engines must be running Management Center version 4.4 or higher. This feature is not supported if there are any engines on the network running older versions.

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 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 Access Control Options window (**Administration > Options**).
2. In the 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 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 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 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.

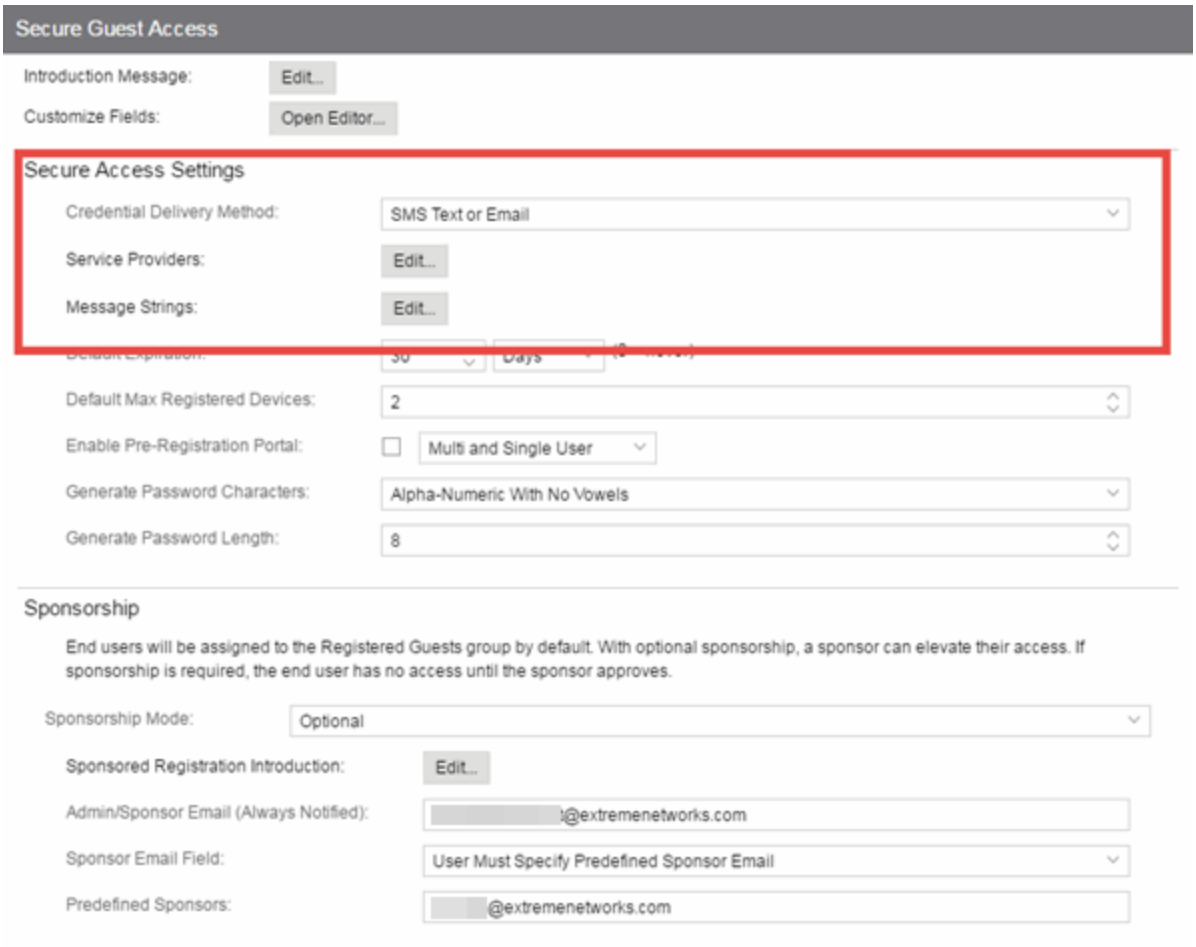
The following table provides a description of each credential delivery method and lists their custom field requirements.

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**.

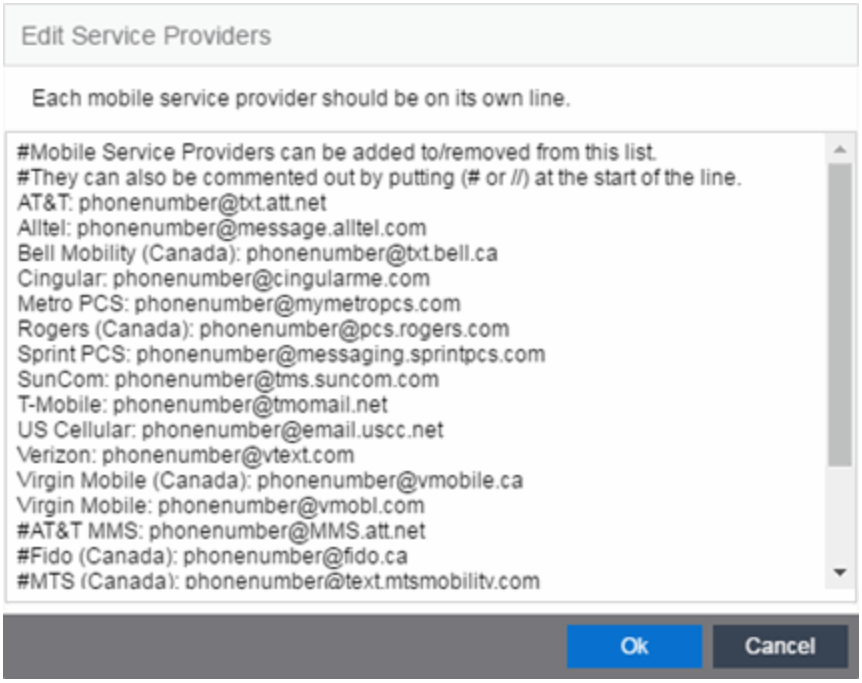
User Verification Method	Description	Custom Field Requirement
SMS Gateway or Email	The SMS Gateway provider must support SMTP API. The SMS Gateway provider converts the email to an SMS text message. The end user must enter a mobile phone number or email address on the Registration web page.	The Phone 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.



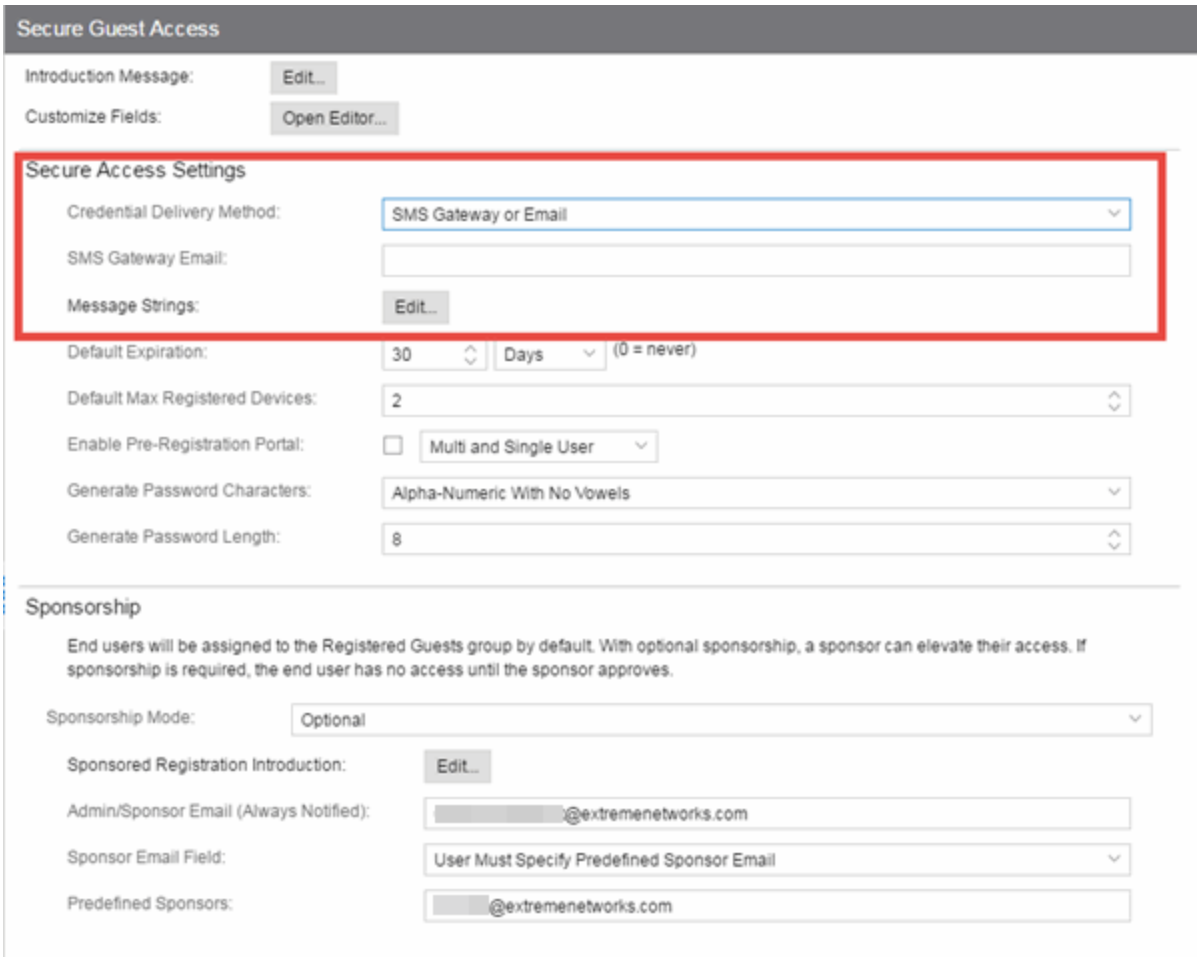
You can comment out entries by preceding each line with either a # or // to allow temporary editing of the file without removing the text.

The list requires one service provider entry per line, using the following format: <Provider>:phonenumber@<specificdomain>.

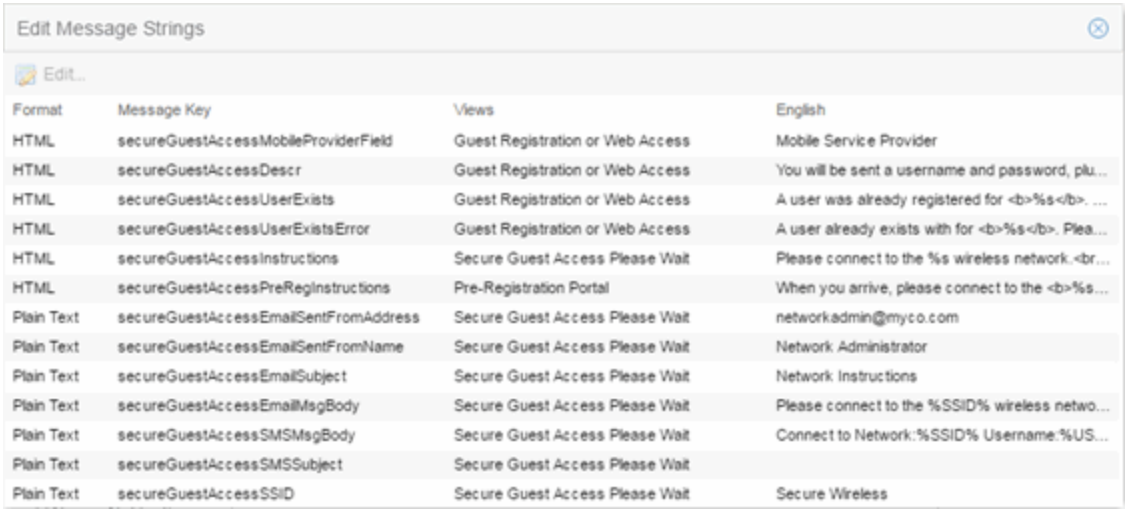
When the end user registers, they only see the <Provider> portion in the drop-down menu of providers on the Registration web page.

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.

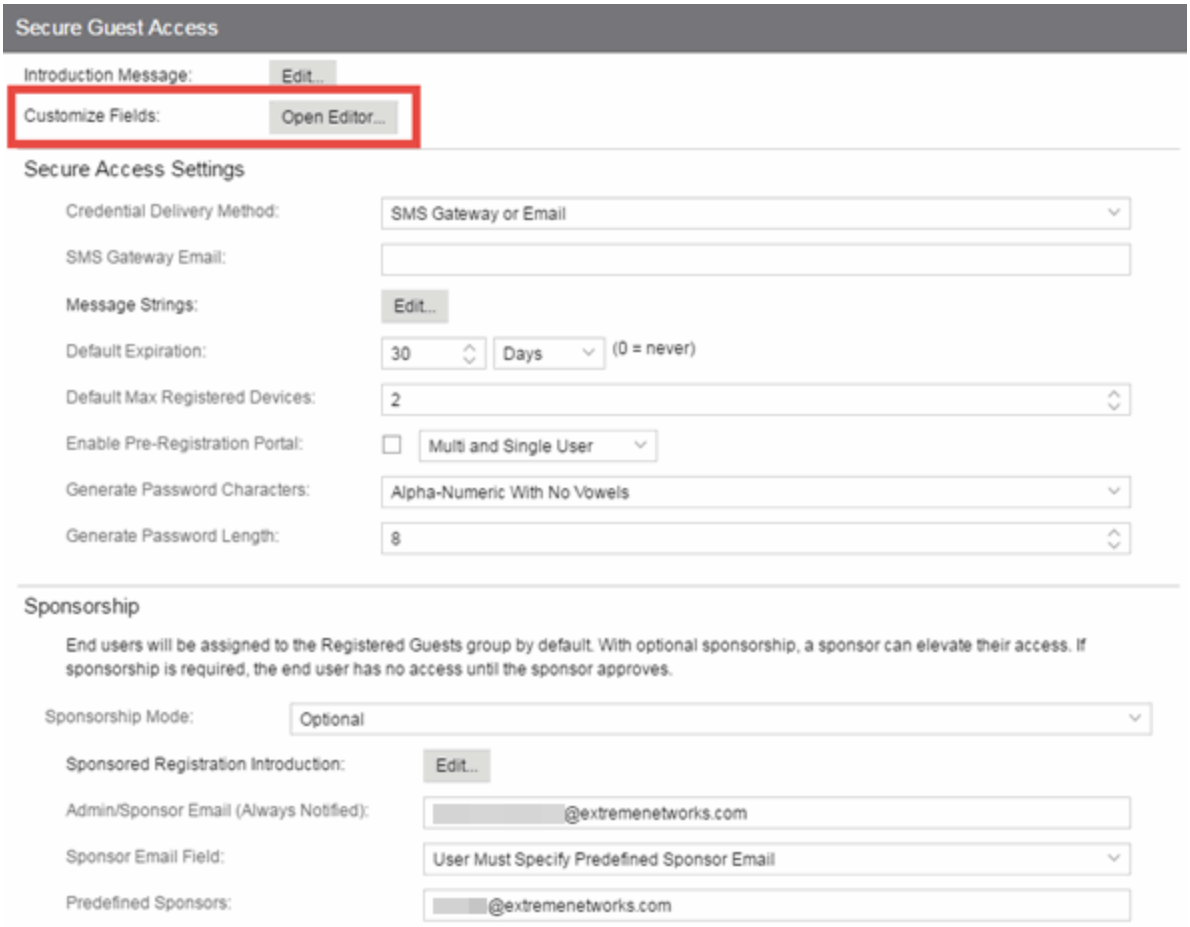
- Email — This method uses the following strings:
  - secureGuestAccessEmailMsgBody — the default message shouldn't need to be changed.
  - secureGuestAccessEmailSentFromAddress — you need to change the default message to the appropriate email address for your company.
  - secureGuestAccessEmailSentFromName — 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

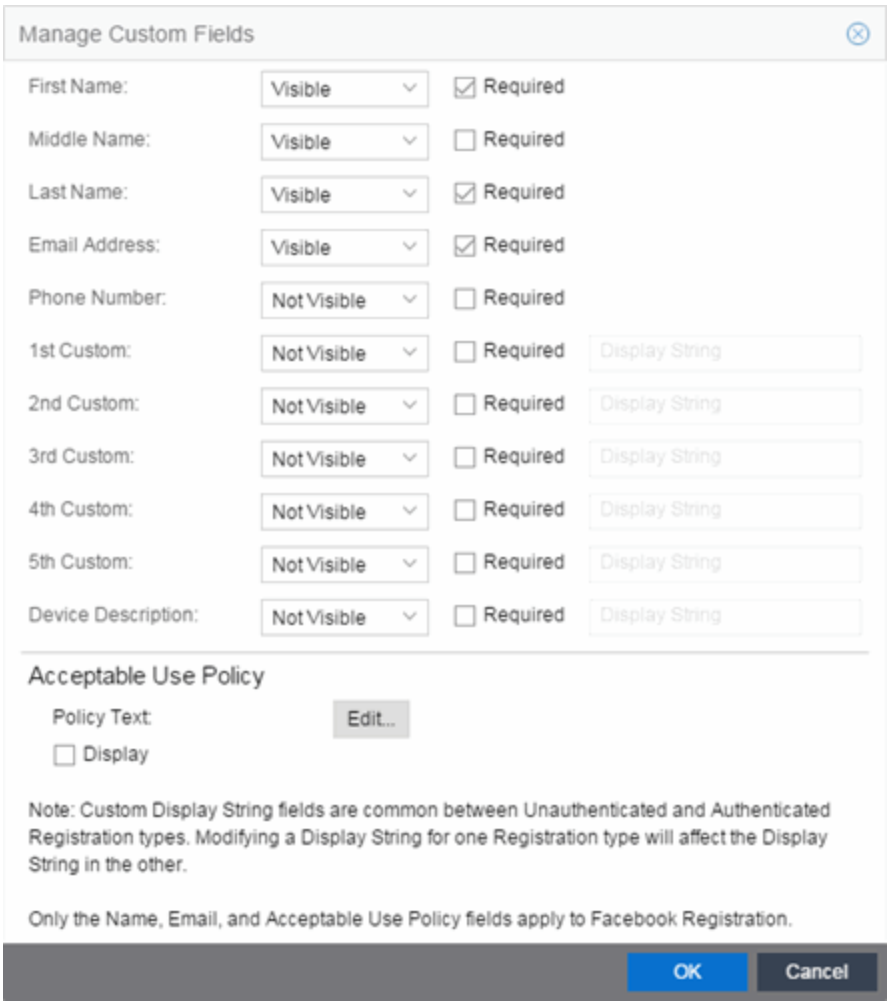
Click **OK** to close the window.

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.

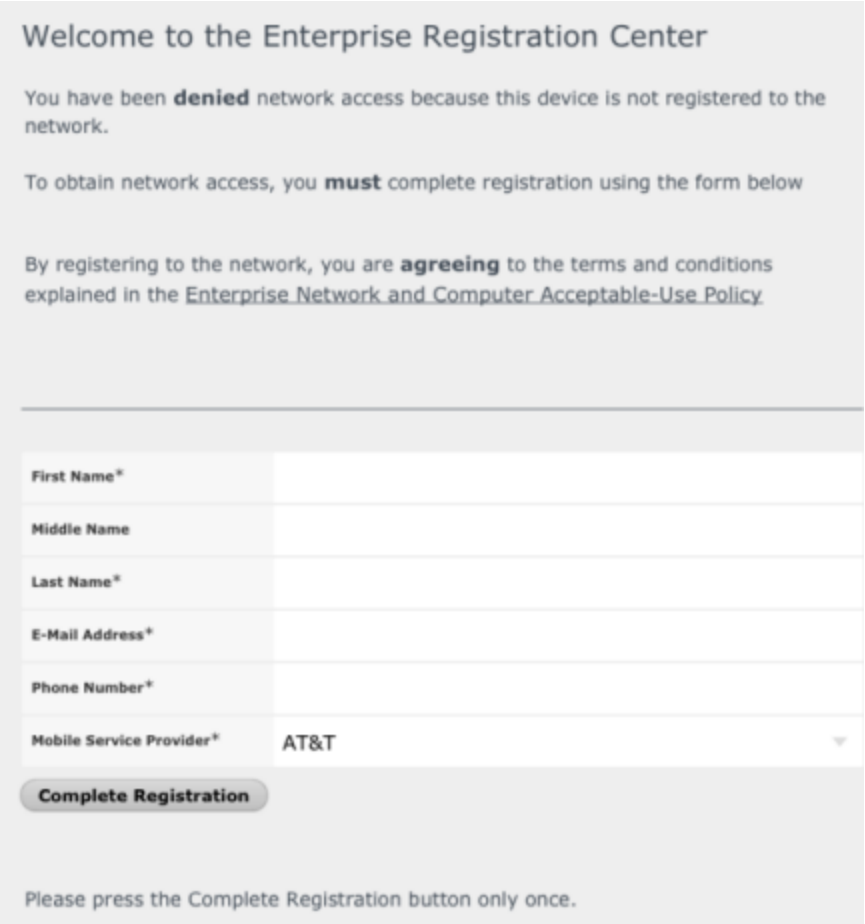


8. Click **OK** to close the window.
9. Back in the Portal Configuration, click **Save** to save your changes.
10. Enforce the new portal configuration to your engine(s).

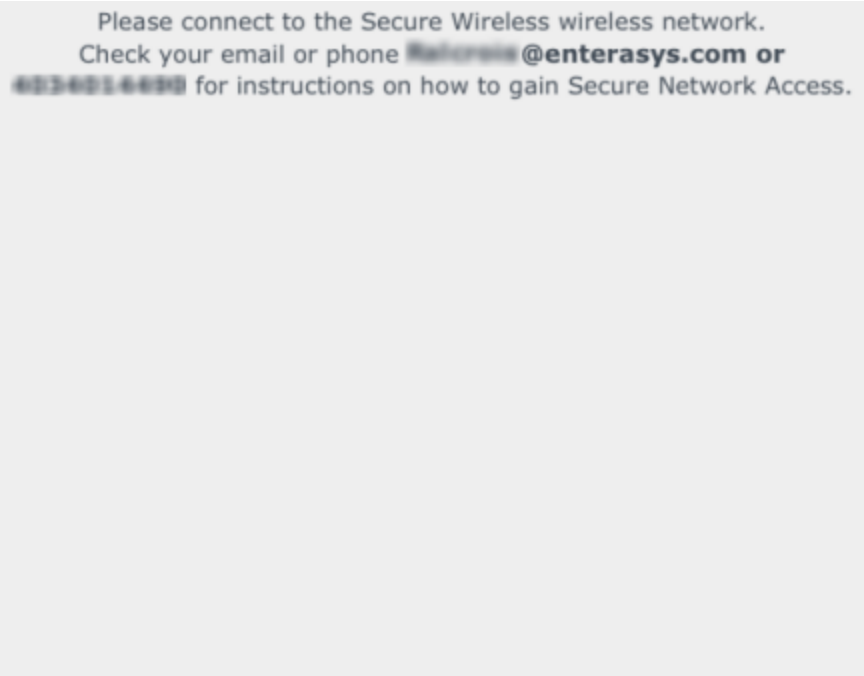
Credential delivery is now configured for your secure guest access.

How Secure Guest Access Works

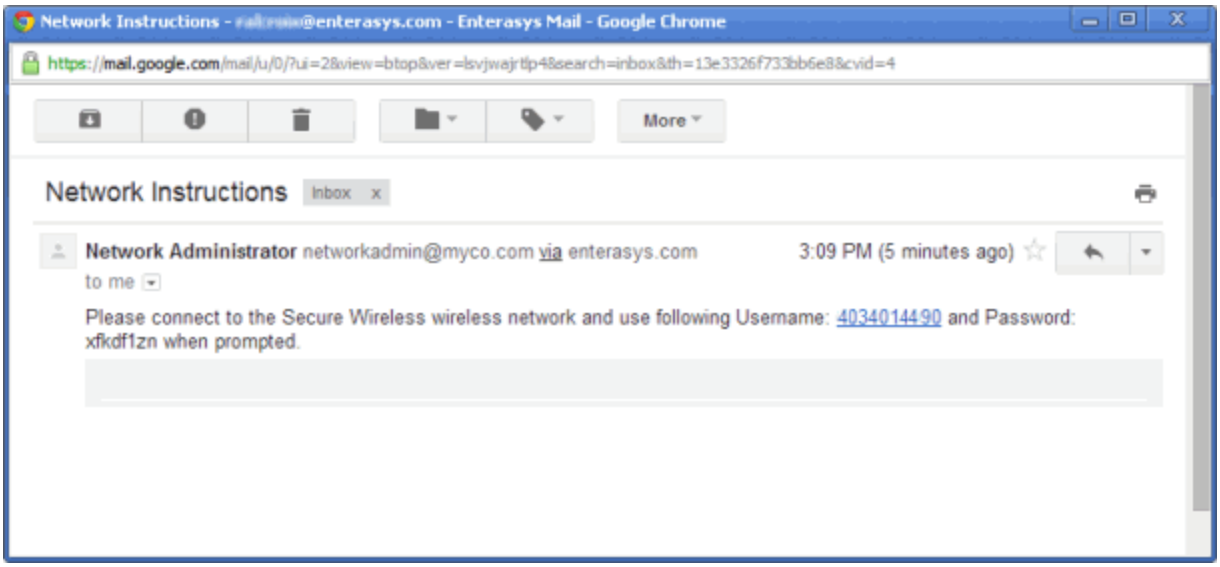
When a guest attempts to access the network, the Registration web page asks for their email address and/or phone number, and any other required/configured information.



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 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.

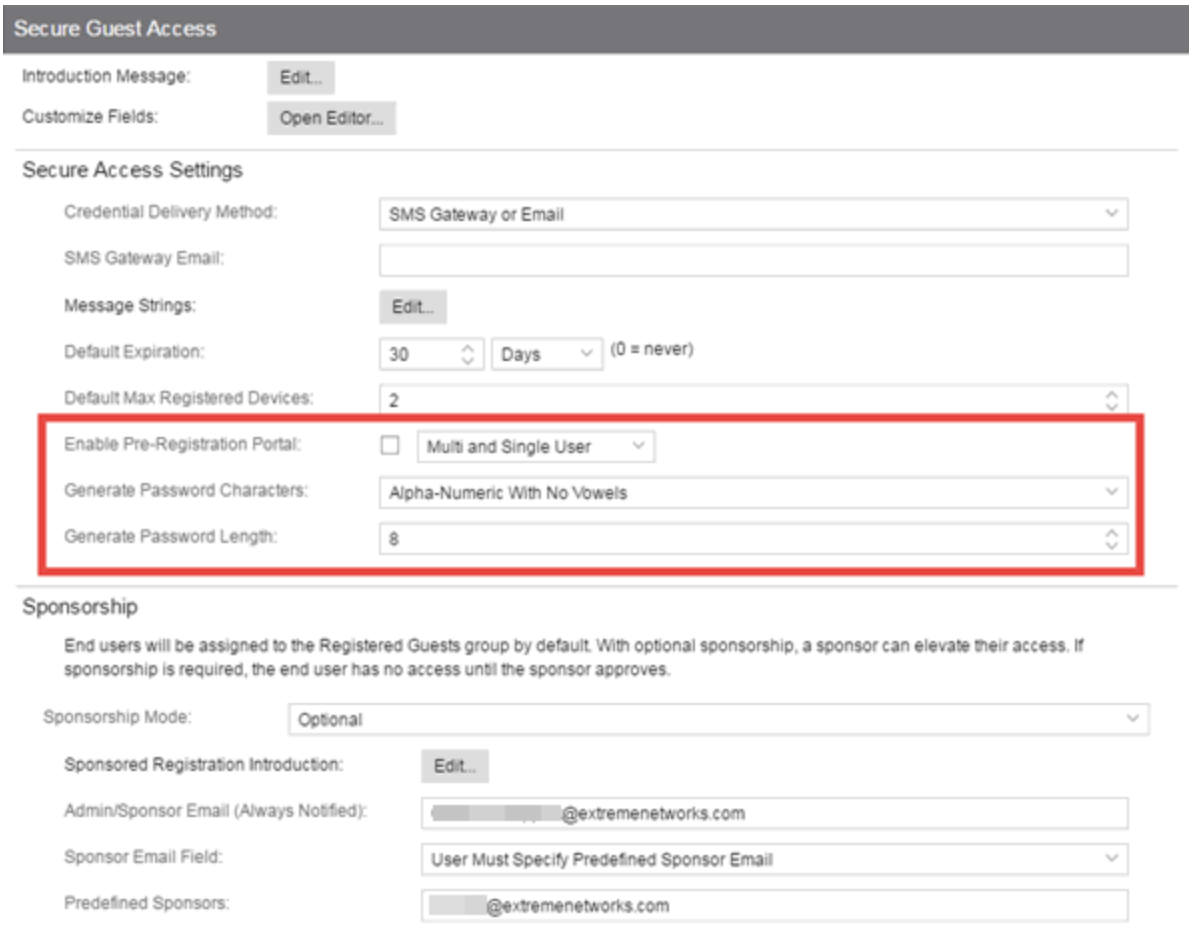
Pre-registration allows IT to delegate control of the network registration process to less technical personnel such as company receptionists, administrative assistants, or training personnel. Using the pre-registration web portal, selected personnel can easily register guest users in advance of an event, 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:

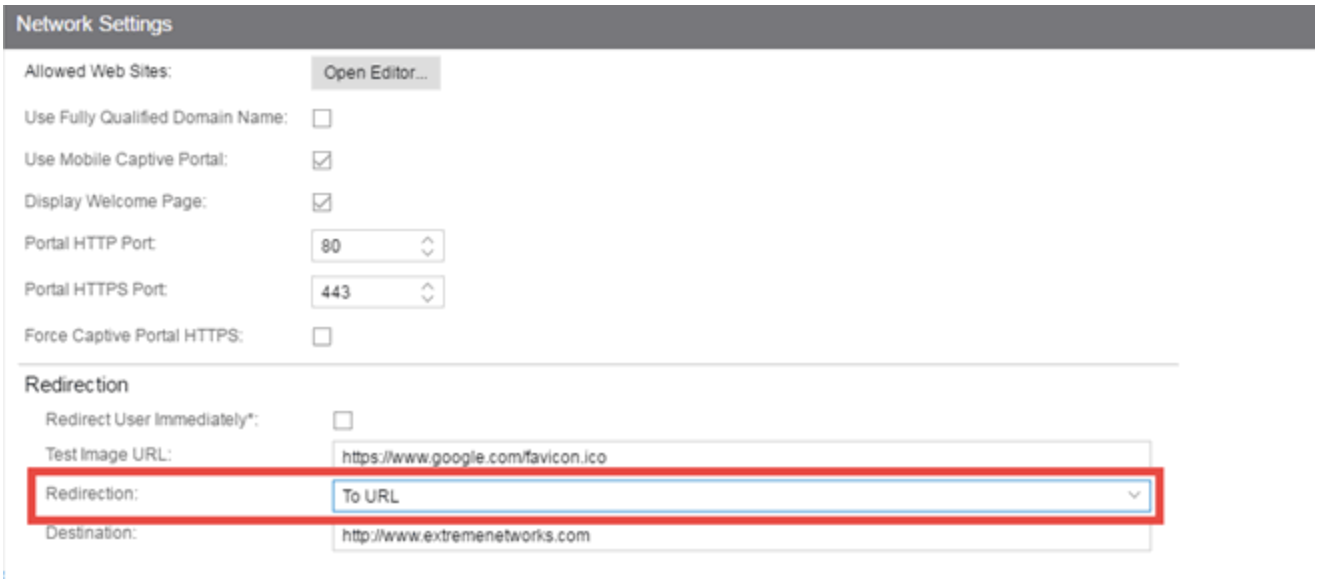
Configuring Pre-Registration

Following are instructions for configuring pre-registration in your portal configuration.

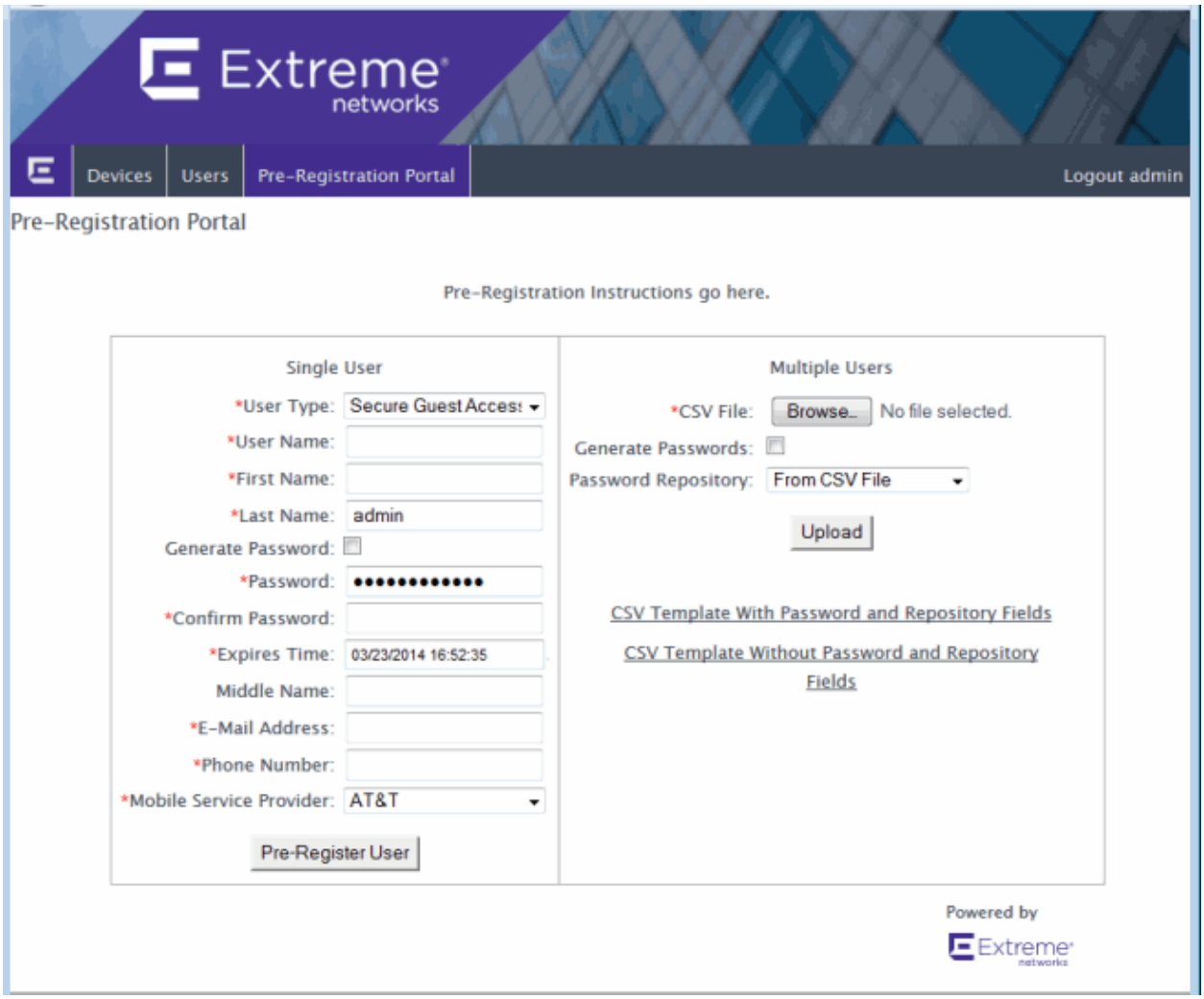
1. Open the **Control** > **Access Control** tab.
2. In the left-panel tree, expand the I&A Configurations > Portal > Website Configuration navigation tree.
3. Click on Secure Guest Access or Authenticated Registration (depending on the access type you are configuring).



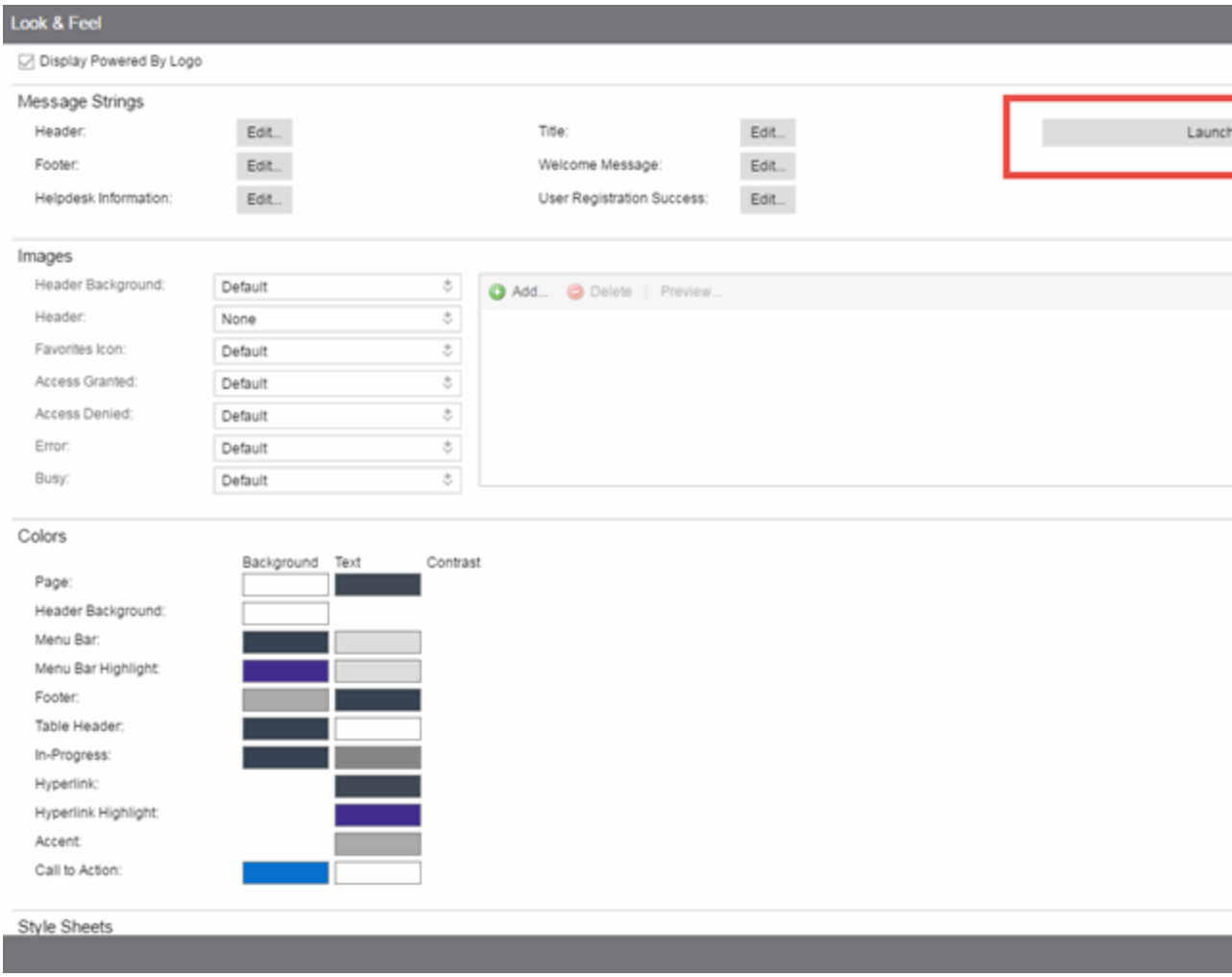
4. Select the **Enable Pre-Registration Portal** checkbox and specify whether personnel are able to register a single user, multiple users, or both single and multiple users.
5. Set the **Generate Password Characters** and **Generate Password Length** options. Extreme Access Control uses these options 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 Access Control Configuration to your engines.
8. Access the Pre-Registration Portal by entering the following URL in a browser window:
   `https://<Access ControlEngineIP>/pre_registration`

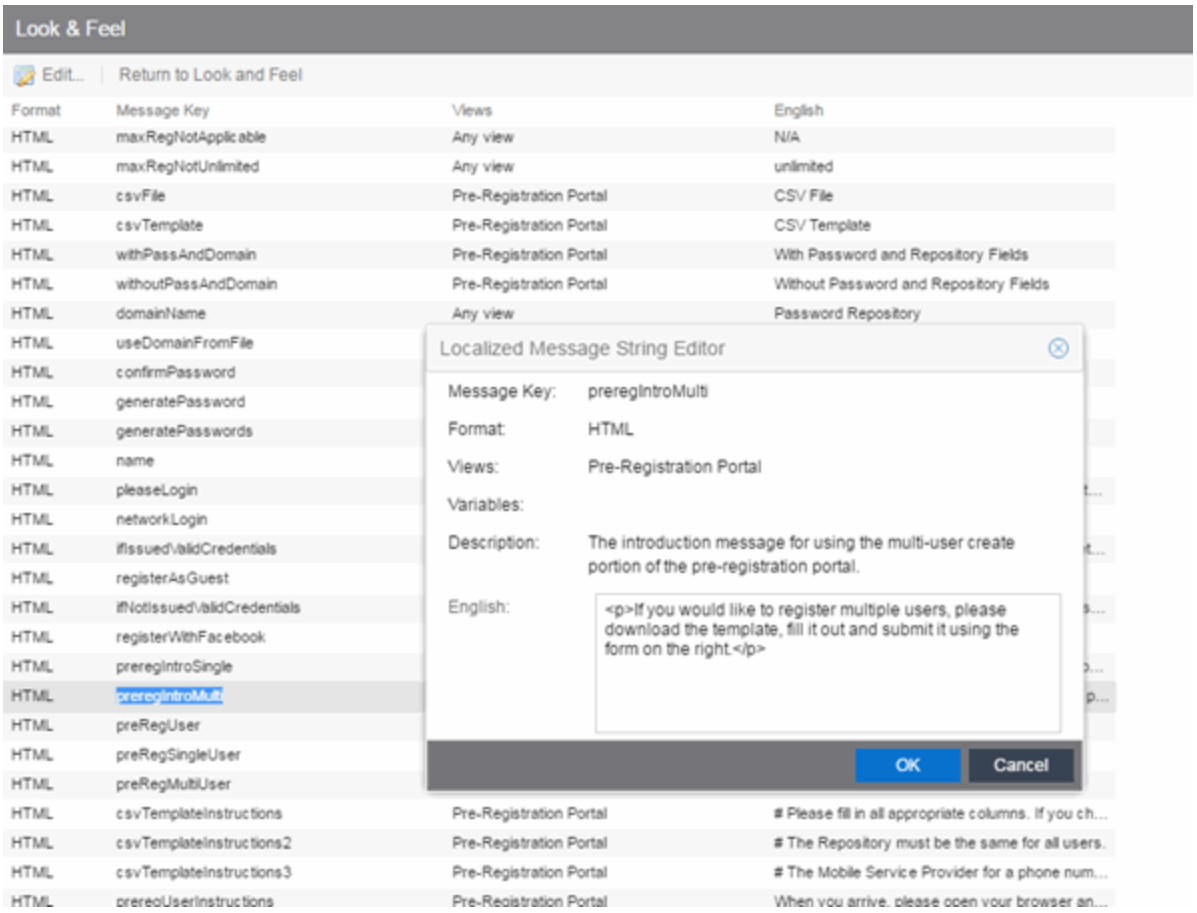


9. At the top of the portal web page are instructions for the people performing the pre-registrations. To modify and edit these instructions:
    a. In the **Control** > **Access Control** tab, select I&A Configurations > Portal in the left-panel navigation tree.
    b. Select a Portal Configuration and select Website Configuration > Look & Feel to open the Look & Feel panel.



c. 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

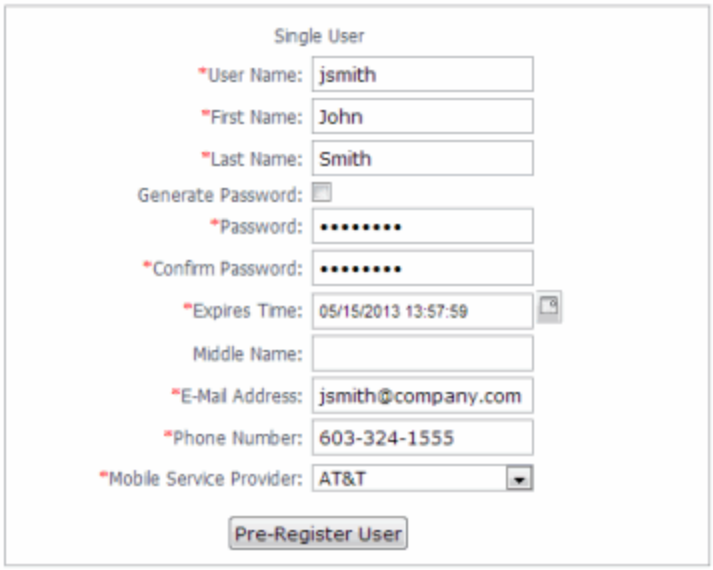
After you have configured pre-registration, provide the URL for the Pre-Registration Portal (`https://<Access ControlEngineIP>/pre_registration`) to the personnel who are pre-registering guests. This may be network administrators or it may be personnel such as company receptionists,

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.

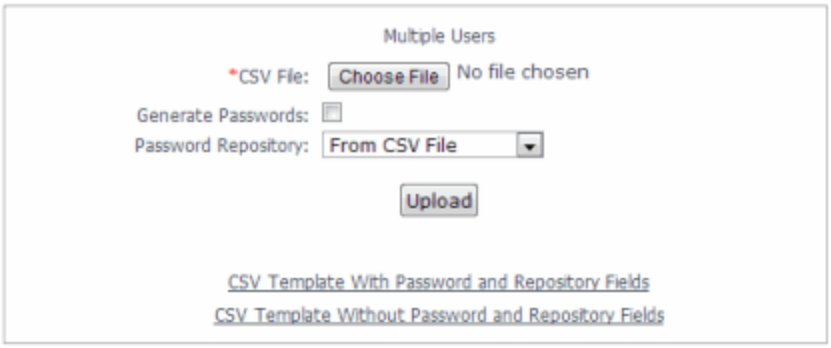
IMPORTANT: The voucher must be printed out immediately, as there is no way to go back and print out a voucher once you leave the web page. If you do not print out the voucher, the voucher needs to be created by hand. In the event that the "Generate Password" option was used, you need to modify the guest 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.

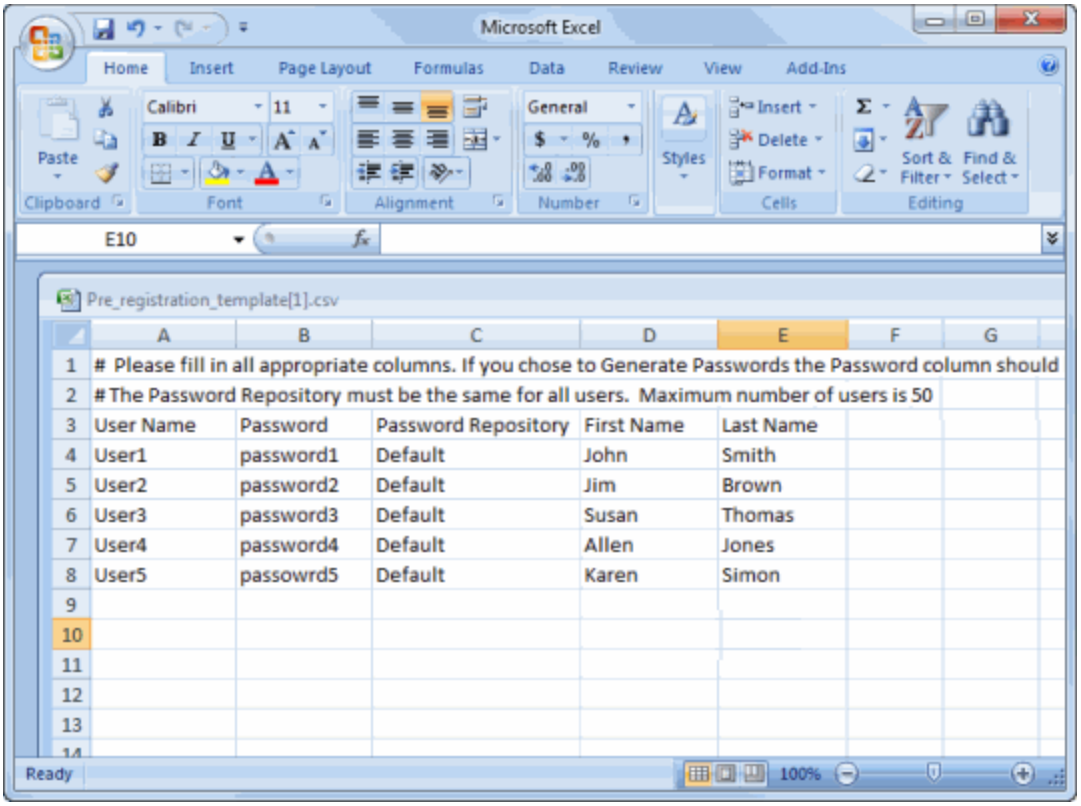
Pre-Registering Multiple Users

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.

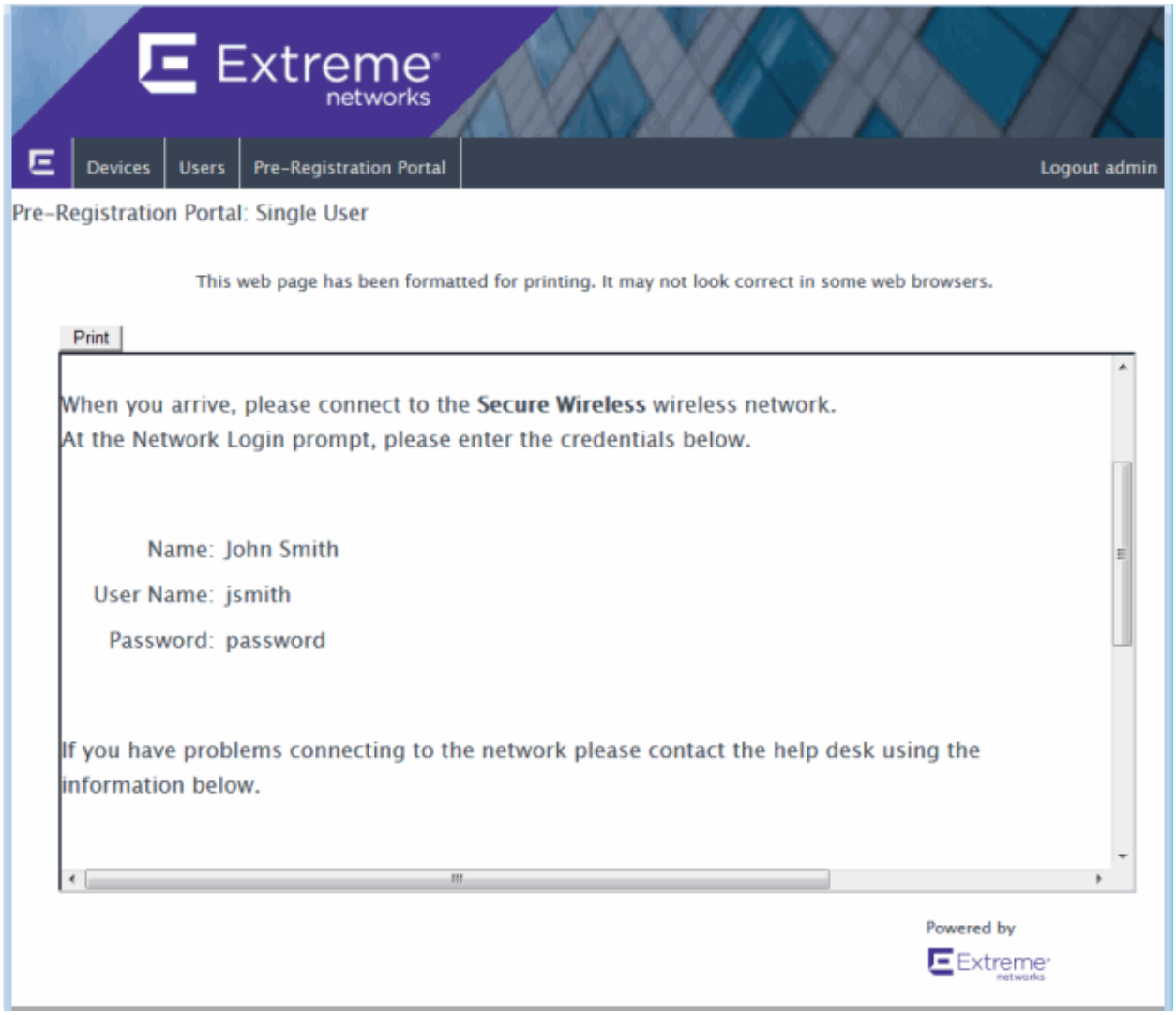
2. When you have finished entering the guest user information, save and close the file.
3. Back in the Multiple Users panel, enter the path and filename for the CSV file by using the Browse button to browse to the file on your system.
4. If your CSV file includes a Password Repository, use the Password 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

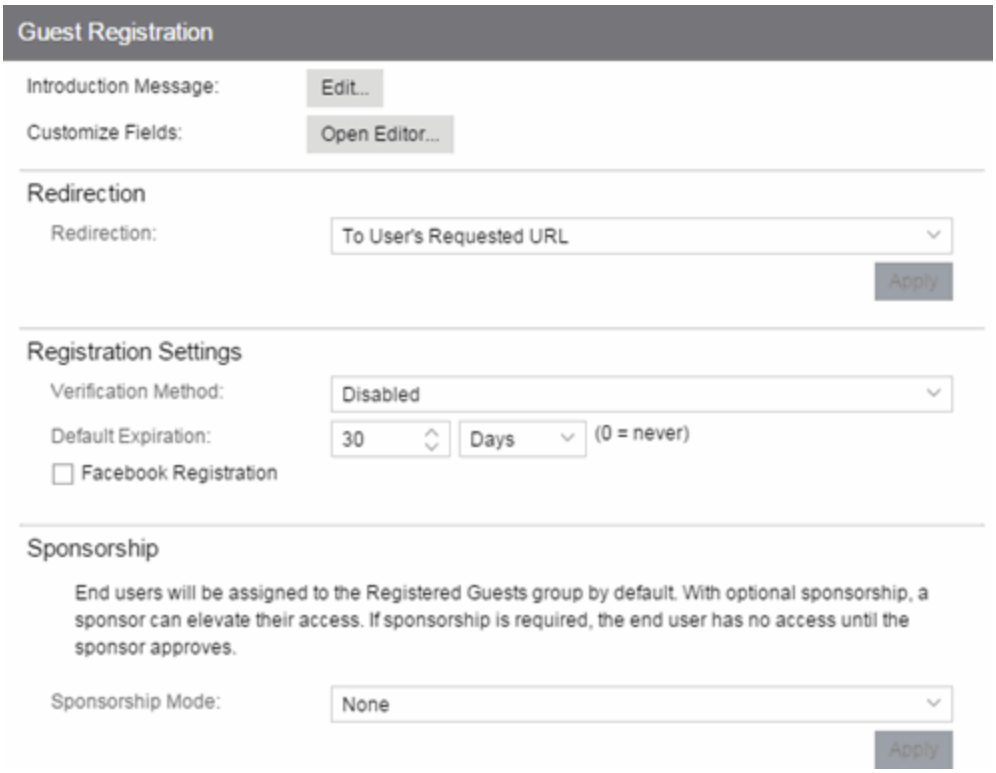
How to Configure Sponsorship for Guest Registration

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 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.

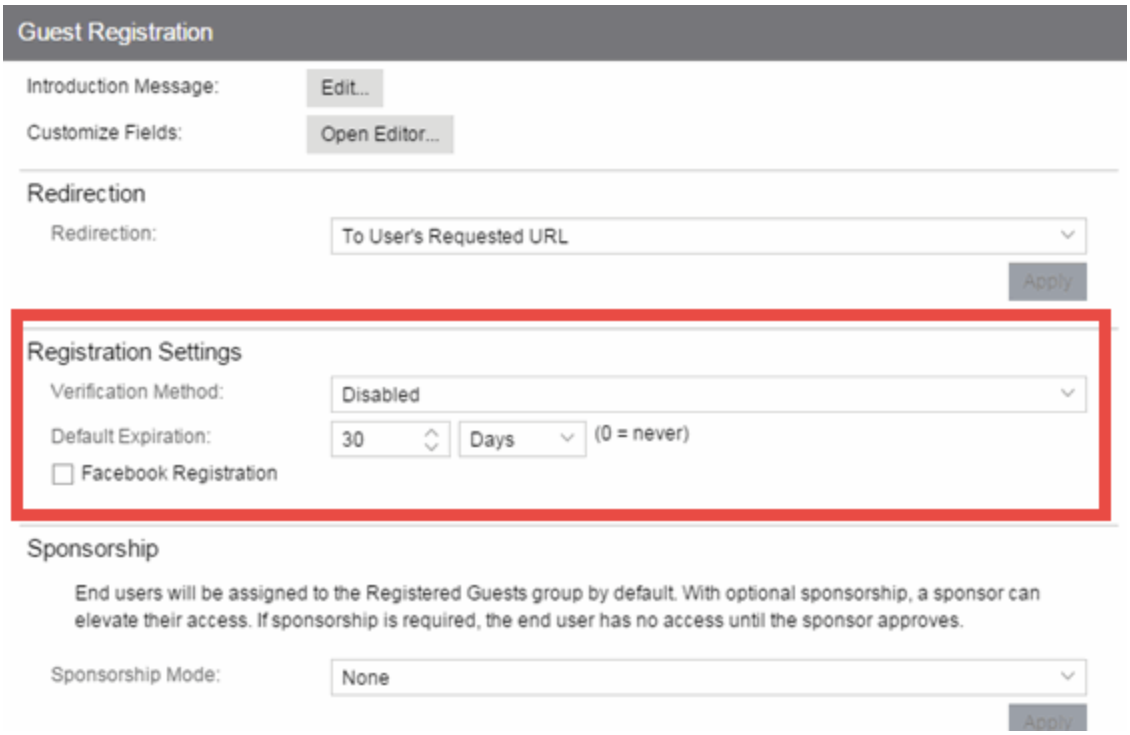
The following table provides a description of each verification method and lists their custom field requirements.

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

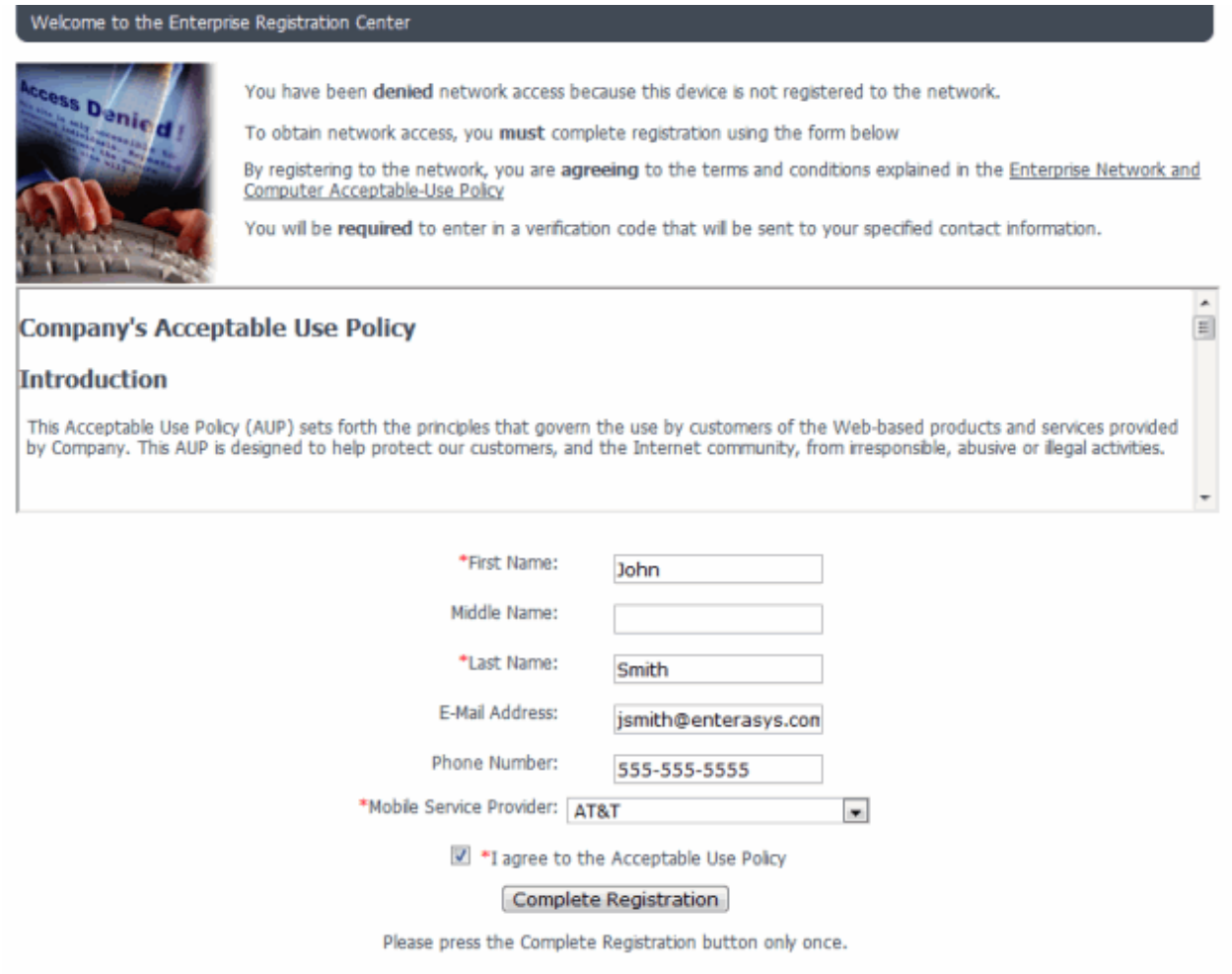
changes, the correct configuration of the custom fields are verified. These settings are shared by Guest Web Access, Guest Registration, and Secure Guest Access. Changing them for one access type also changes them for the others. For more information, see the Manage Custom Fields Window.

Click OK to close the window.

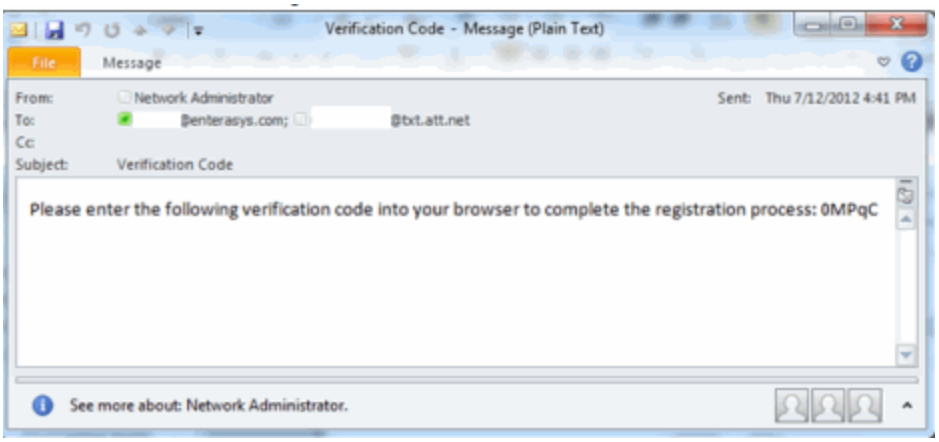
8. Back in the Portal Configuration, click Save to save your changes. Close the Portal Configuration window. Enforce the new portal configuration to your engine(s). Verification is now configured for your guest registration.

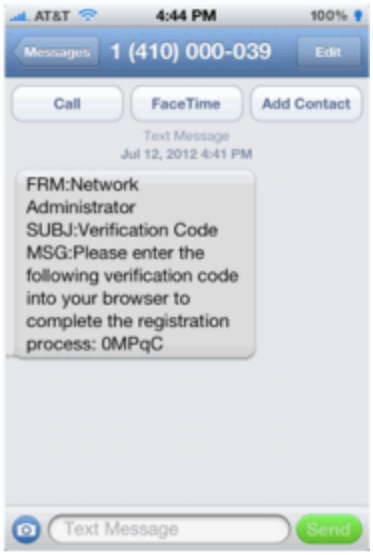
How User Verification Works

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.

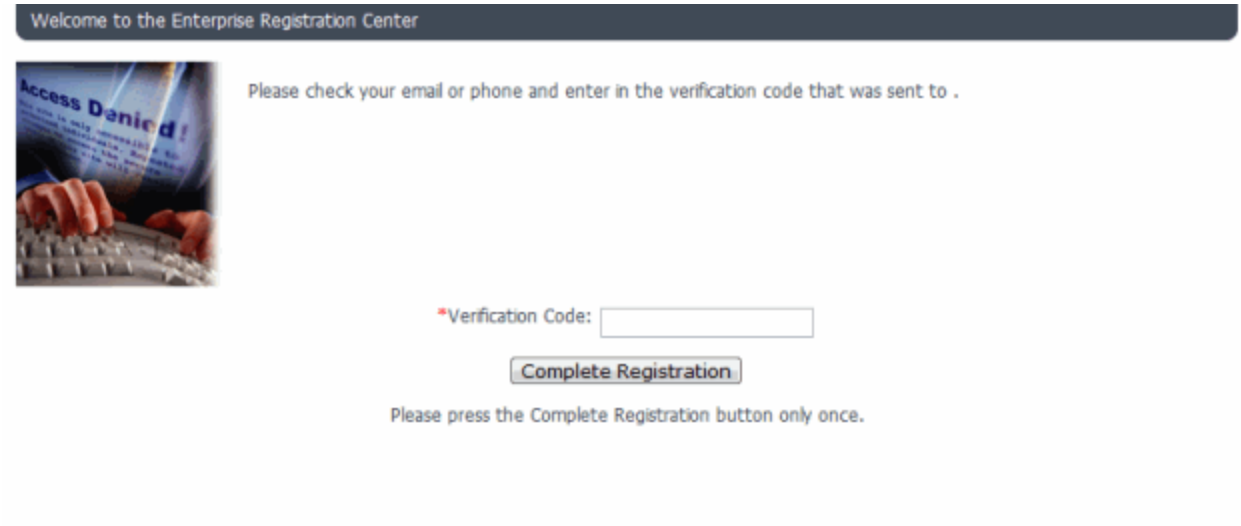


When they click the Complete Registration button, they are sent a verification code via an email or a phone text message.





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 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 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 Access Control engine version 4.0 or higher to take advantage of RADIUS accounting functionality in Management Center.

For Extreme Networks stackable and standalone devices (A-Series, B-Series, C-Series, D-Series, G-Series, and I-Series), 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 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 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 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 Access Control engine IP address as the IP address of the RADIUS server. Refer to your wireless controller User Guide for instructions on enabling RADIUS accounting via the ExtremeWireless Assistant, or the CLI Reference Guide for the exact CLI command syntax to use.

For third-party switching devices:

a. RADIUS accounting must be enabled manually on the device using the device CLI (command line interface).

b. Be sure to configure the Access Control engine IP address as the RADIUS accounting server. Refer to your device documentation for the exact command syntax.

2. If you are doing RADIUS accounting in an Access Control environment where the primary RADIUS server is being used for redundancy in a single Access Control engine configuration (Basic AAA configuration only), then enable the Proxy RADIUS Accounting Requests option in the Edit RADIUS Server window.

   a. In the Edit Basic AAA Configurations window, use the Configuration Menu button in the Primary RADIUS Server field to open the Manage RADIUS Servers window.

   b. Select the RADIUS Server and 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 Management Center End-Systems tab and Dashboard.

Considerations for Fixed Switching Devices

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 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 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 Access Control Engine Group Window
- Edit Switches in Access Control Engine Group Window

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.

Guest Registration using Facebook has two main advantages:

- It provides 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. 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.

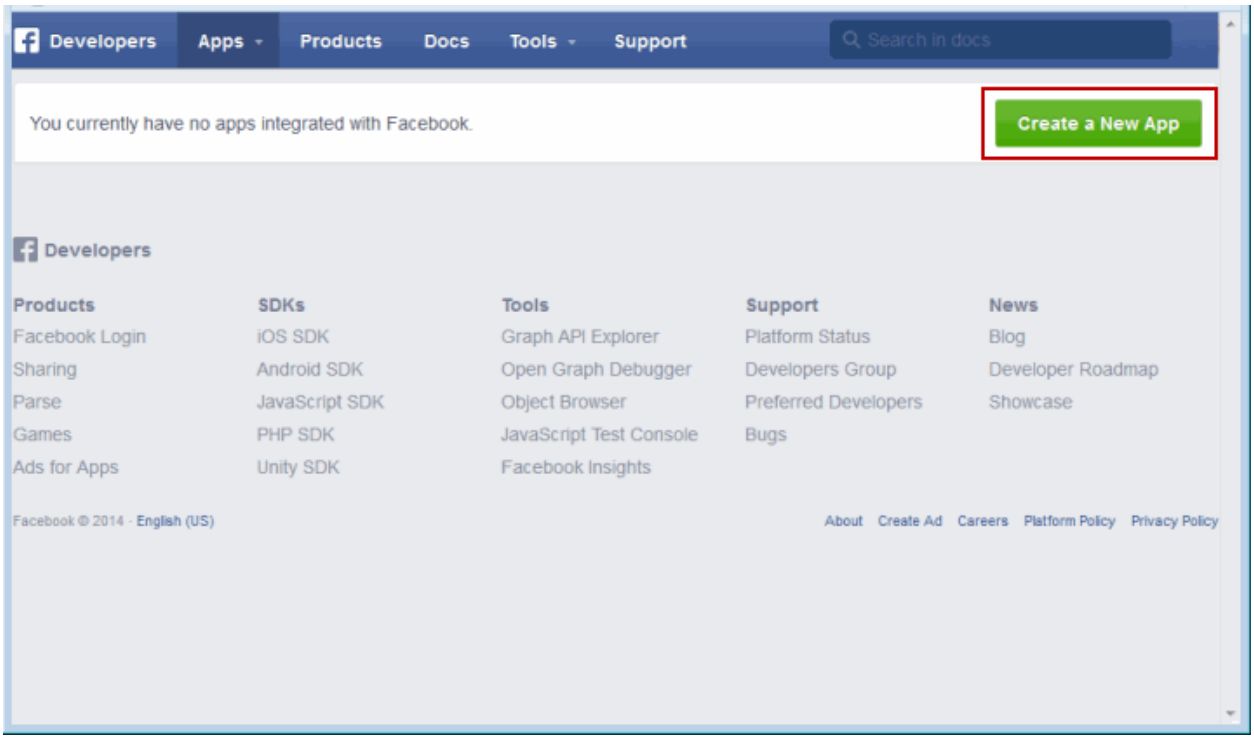
- The Extreme Access Control engine must have Internet access in order to retrieve user information from Facebook.
- The Access Control Unregistered access policy must allow access to the Facebook site (either allow all SSL or make allowances for Facebook servers).

- 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

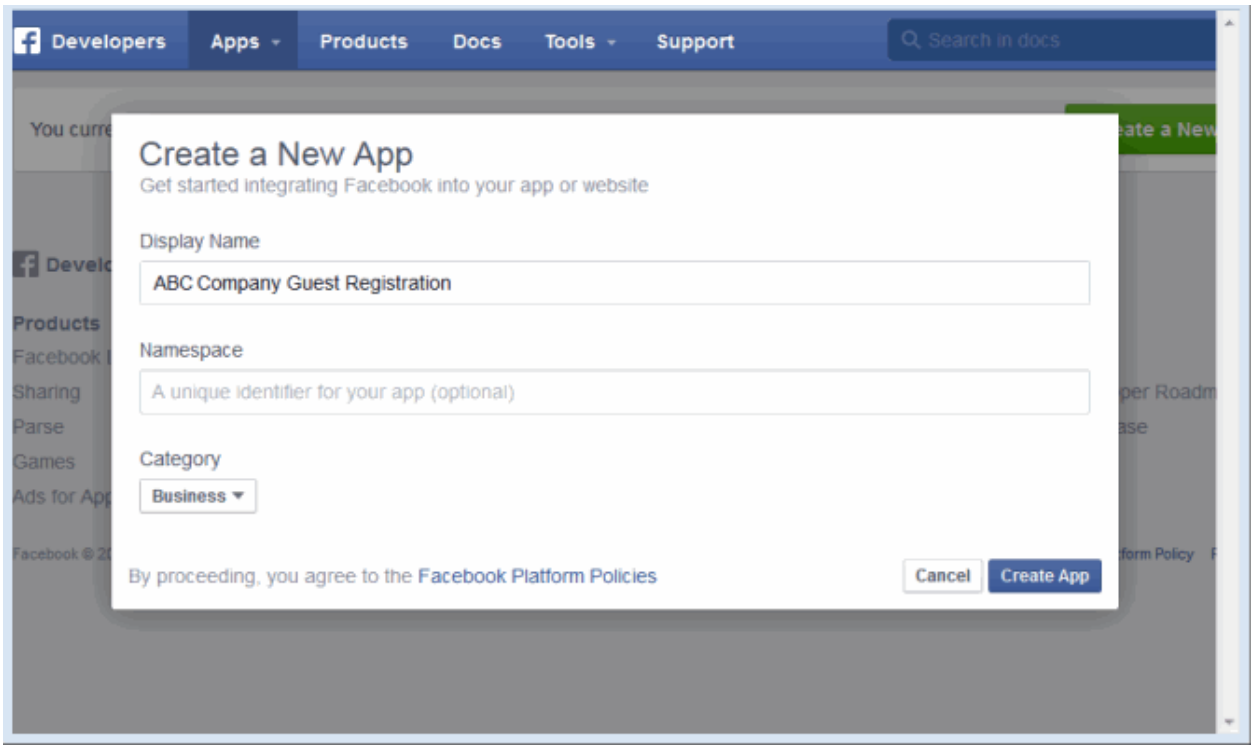
When implementing guest registration using Facebook, you must first create a Facebook application. This generates an Application ID and Application Secret that are required as part of the Extreme Management Center OAuth process. Use the following steps to create a Facebook application.

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 Create New App button to open the Create a New App dialogue.

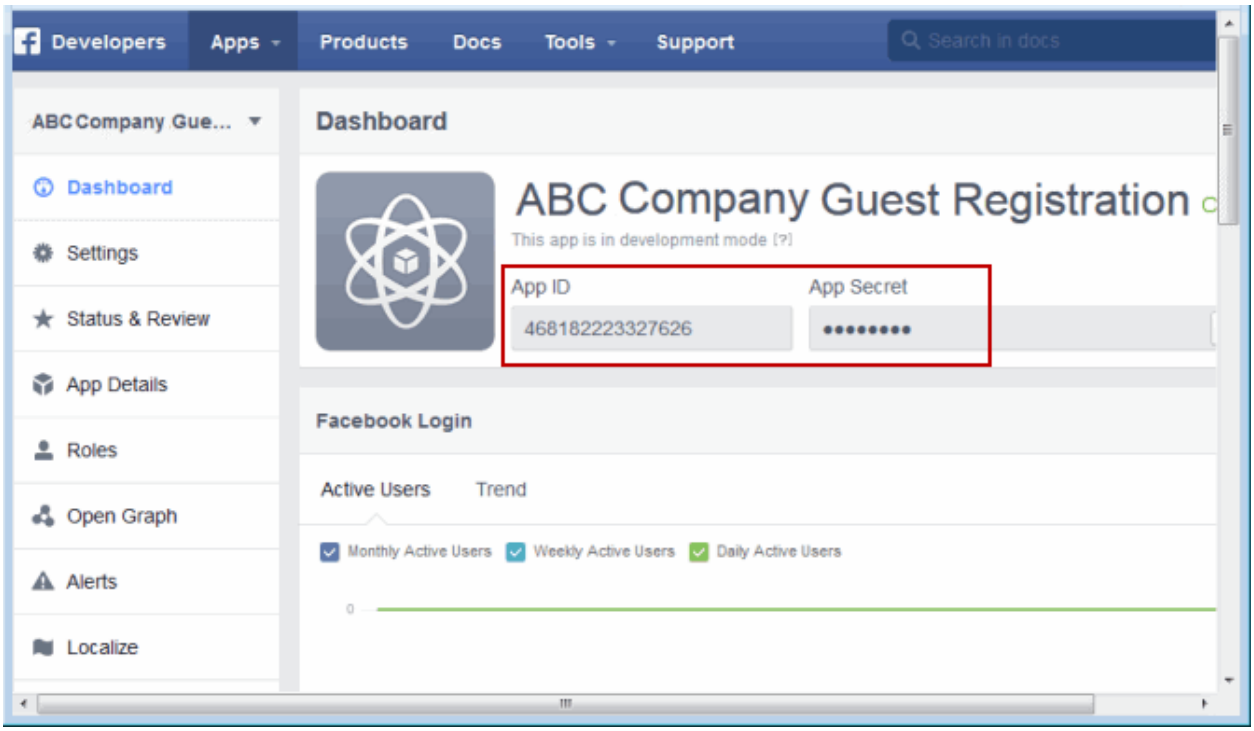


3. The Create a New App window opens. Enter a Display Name and select a category for your app. The Display Name is the name of the app presented to the end-user when they grant Management Center access to their

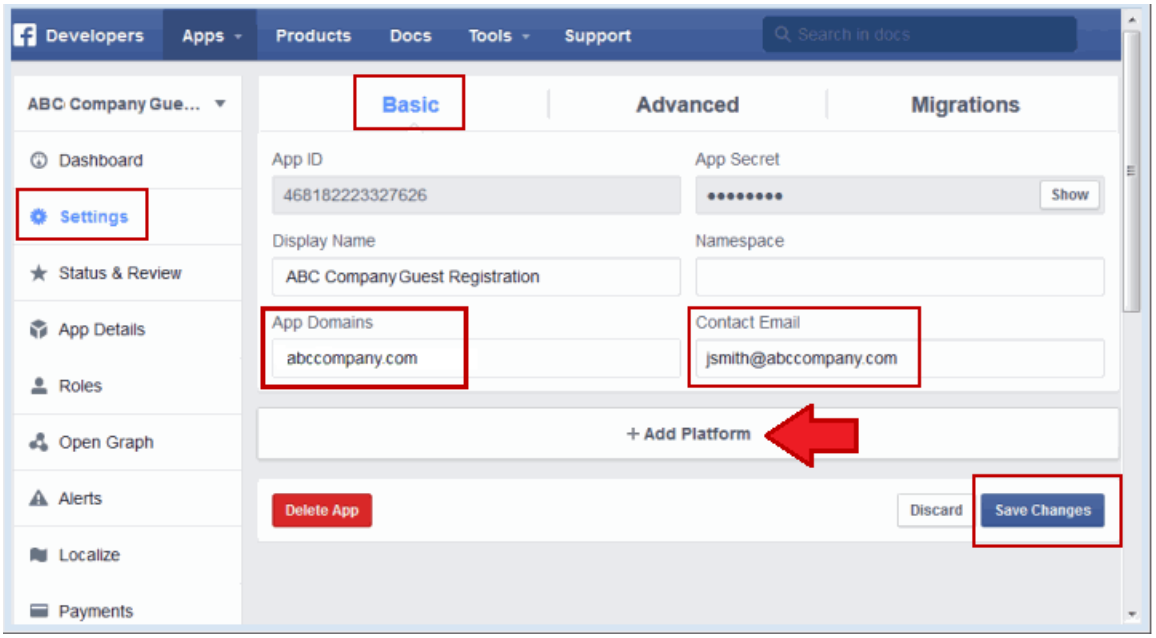
Facebook information and should clearly indicate what its purpose is, for example, Extreme Networks Guest Registration. Click **Create App**.



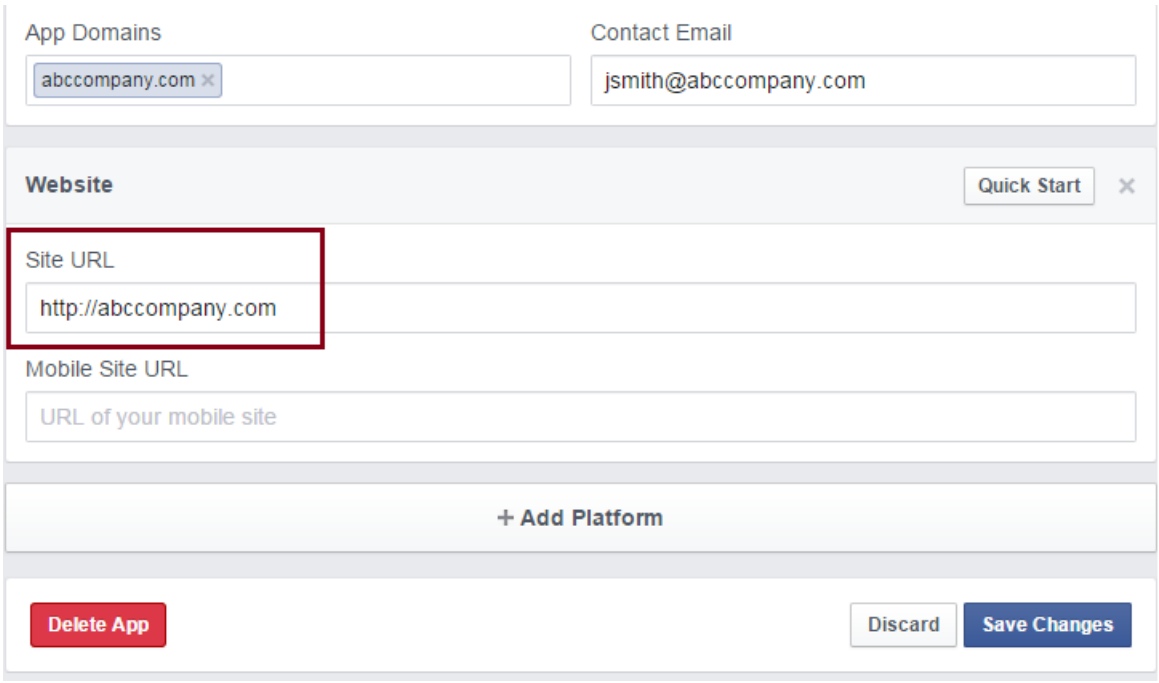
4. The Dashboard view opens and displays information about the new app including an App ID and an App Secret.



5. In the left panel, select **Settings**.
6. Enter in a valid domain name for the Extreme Access Control engines in the **App Domains** field in the right-panel **Basic** tab. For example, if the Access Control engine to which users are connecting is Access Controlengine.AbcCompany.com, enter "abccompany.com" in the **App Domain** field.



7. Enter a **Contact Email**.
8. Click **Add Platform**.
9. Select **Website** in the Add Platform options. The Platform window opens.

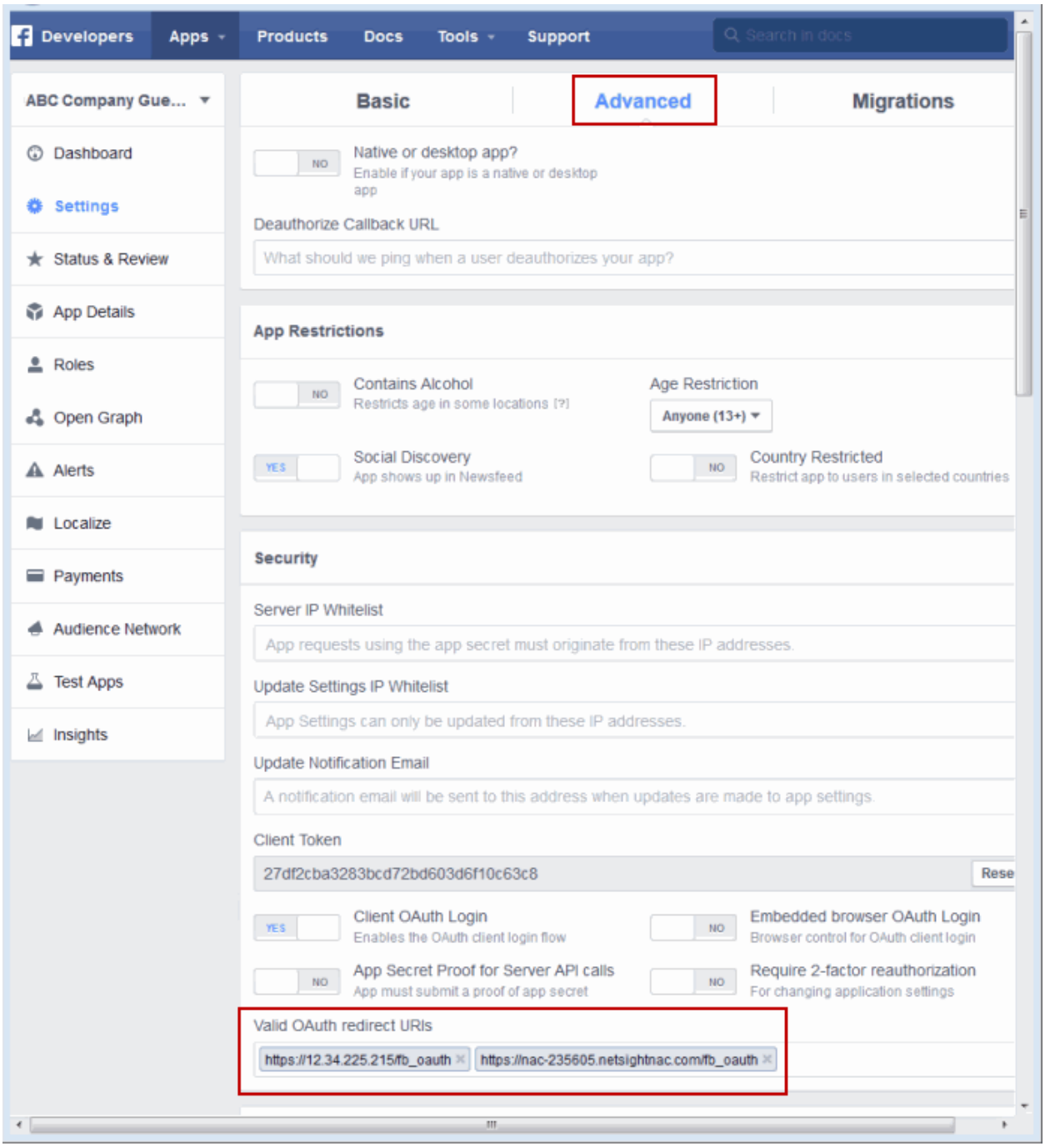


10. Enter the domain name you added in the **App Domain** field in step 5 in the **Site URL** field.
11. Click **Save Changes**.
12. In the **Advanced** tab, enter the Valid OAuth redirect URIs. A redirect URI is required to redirect the user back to the engine with an Access Token Management Center uses to access the user account and retrieve the user data. The Redirection URI should be in the following format:

    https://<Access ControlengineFQDN>/fb_oauth

    A Redirection URI must be added for each Access Control engine where end users can register via Facebook.

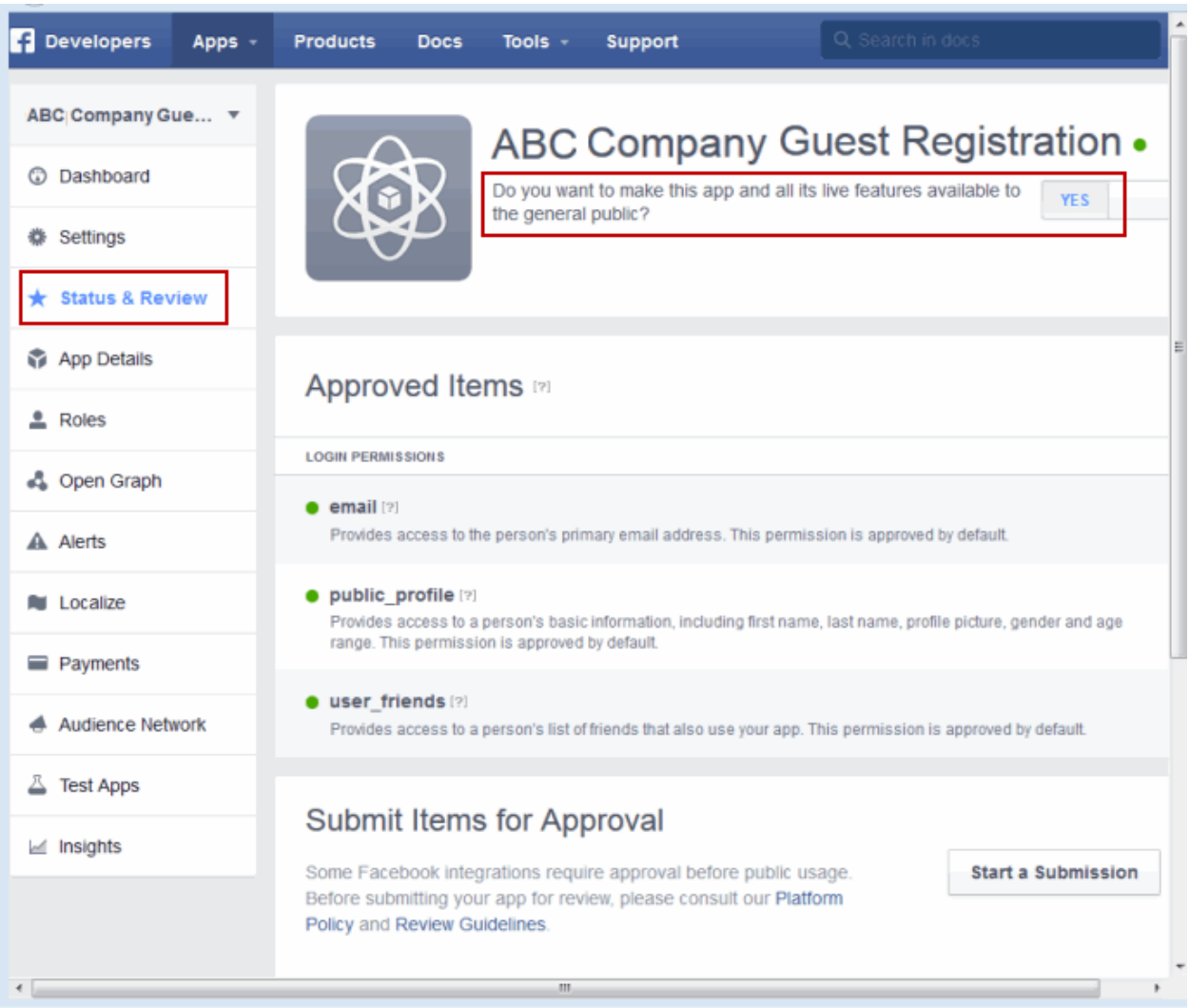
    Scroll down and click **Save Changes**.



13. In the left panel, select **Status & Review**. In the right-panel you see a top section with the question "Do you want to make this app and all its live features available to the general public?" Select **Yes** and confirm your selection.

    Under the Login Permissions section, you see 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.)

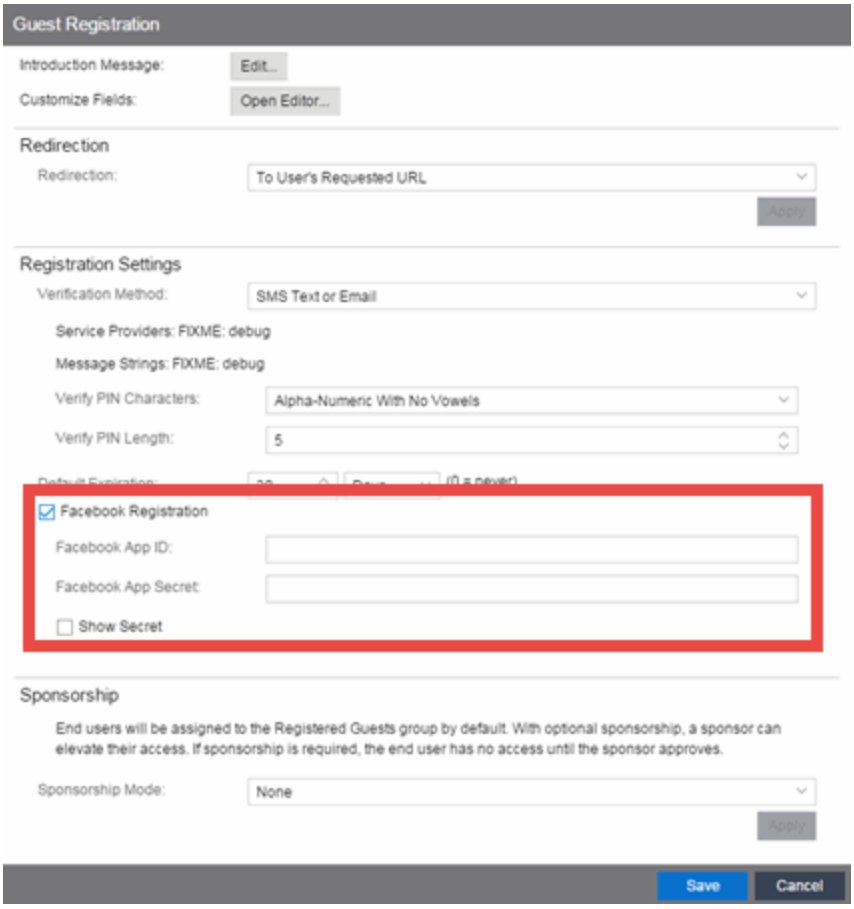


14. Your application is created and ready to use. You must now add the App ID and App Secret to your portal configuration.

Portal Configuration

The Application ID and Application Secret assigned during the creation of the Facebook application must be provided in the Portal Configuration in order for the entire process to complete properly.

1. Open the **Control** > **Access Control** tab.
2. In the left-panel tree, expand the Access Control Configurations > Portal tree and select Guest Registration.



3. In the Customize Fields section, 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**. You warnings messages are displayed 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 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 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.

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 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 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 7.0 (formerly NetSight), 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 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 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 Access Control folder in the tree to view all the different options you can set.

Instructions on setting the following Access Control options:

- Advanced Settings
- Assessment Server
- Data Persistence
- Display
- End-System Event Cache
- Enforce Warning Settings
- Features
- Notification Engine
- Policy Defaults
- Status Polling and Timeout

Advanced Settings

Use the Advanced Settings panel to configure advanced settings for Access Control. These settings apply to all users on all clients.

1. Select **Administration > Options** in Management Center. The Options window opens.
2. In the left-panel tree, expand the Access Control folder and select Advanced Settings.
3. Use the **Capacity** option configure the Management Center resources allocated to end-system and configuration processing services. The greater the number of end-systems and engines in your Access Control deployment, the more resources it requires.

- Low - For low performance shared systems.
- Low-Medium - For medium performance shared systems, or low performance dedicated systems
- Medium - For medium performance shared systems, or medium performance dedicated systems.
- Medium-High - For high performance shared systems, or medium performance dedicated systems.
- High - For high performance dedicated systems.
- Maximum - For extremely high performance dedicated systems.

4. Use the **Hybrid Mode** option to enable Hybrid Mode for Layer 2 Controllers. Hybrid Mode allows a Layer 2 Access Control Controller engine to act as a RADIUS proxy for switches, like a 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 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 IPv6 Support in the Management Center Configuration Considerations Help topic.
6. The **Enable Communication Channels for Appliance Groups** option allows you to create logical groupings of your 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. For more information and complete configuration instructions, see How to Configure Communication Channels.
7. 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 Controlengine 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. Access Control provides a default password you can change, if desired. However, if you change the password here, you need to change the password on the assessment agent adapter as well, or connection between the engine and assessment agent adapter is lost and assessments are not performed. For instructions, see How to Change the Assessment Agent Adapter Password.

1. Select **Administration > Options**. The Options window opens.
2. In the left-panel tree, expand the Access Control folder and select Assessment Server.
3. Specify the assessment agent adapter credentials.
4. 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 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 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 Management Center to generate an Access Control event when end-system information is modified.
7. In the **Health Result Persistence** section, specify how many health result (assessment results) summaries and details are saved and displayed in the End-Systems tab for each end-system. By default, the Data Persistence check saves the last 30 health result summaries for each end-system along with detailed information for the last five health result summaries per end-system.
   There are two additional options:
   - You can specify to only save the health result details for quarantined end-systems (with the exception of agent-based health result details, which are always saved for all end-systems).
   - You can specify to save duplicate health result summaries and detail. By default, duplicate health results obtained during a single scan interval are **not** saved. For example, if the assessment interval is one week, and an end-system is scanned five times during the week with identical assessment results each time, the duplicate health results are not saved (with the exception of administrative scan requests such as Force Reauth and Scan, which are always saved). This reduces the number of health results saved to the database. If you select this option, all duplicate results are saved.
8. Set the time you would like the Data Persistence Check to be performed each day.

9. In the **Transient End-Systems** section, configure the number of days to keep transient end-systems in the database before they are deleted as part of the nightly database cleanup task. The default value is 1 day. A value of 0 disables the deletion of transient end-systems. Transient end-systems are Unregistered end-systems and have not been seen for the specified number of days. End-systems are not deleted if they are part of an End-System group or there are MAC locks associated with them. Select the **Delete Rejected End-Systems** checkbox if you want end-systems in the Rejected state to be deleted as part of the cleanup. You can also delete transient end-systems using the Tools > End-System Operations > Data Persistence option.
10. 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:

- Options Window, Extreme Access Control Options

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 Access Control profile assigned to the matching Access Control rule and the end-system state.

In your Access Control profiles, each access policy is associated to a *policy mapping* that defines exactly how an end-system's traffic is handled when the access policy is applied.

A policy mapping specifies the policy role (created in the Policy tab) and other RADIUS attributes included as part of a RADIUS response to a switch. The RADIUS attributes required by the switch are defined in the 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 Access Control Controller engines and/or Access Control Gateway engines. In addition, if your network utilizes 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 Access Control Controllers:

If your network utilizes Access Control L2/L3 controller engines, the access policies specified in Access Control profiles are mapped to policy roles that are defined in a default policy configuration already configured on the controller. It is recommended that you review this default policy configuration using the Policy tab. To do this, you must create a policy domain in the Policy tab specifically for the Access Control Controller, assign the Access Control Controller to the domain, then import the policy configuration from the device into Policy tab. Review the policy roles and make any rule changes required for your environment. When you have finished modifying the policy configuration, you must enforce it back to the Access Control Controller.

For Access Control Gateway Appliances:

If your network utilizes Access Control Gateway engines, the access policies specified in Access Control profiles are mapped to policy roles that must be created and defined in the Policy tab and enforced to the policy-enabled switches in your network. If you have RFC 3580-enabled switches in your network, Extreme Management Center lets you associate your policy roles to a VLAN ID or VLAN Name using the Policy Mappings panel. This allows your 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 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 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 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 Access Control engine could attempt to scan the incorrect IP address. Be sure to take into account the amount of time required for an end-system to get a new IP address when setting the delay time value.

Setting Up Your Access Policies

Before you begin working with the Access Control tab, use these steps to define the policy mapping criteria (policy roles, corresponding VLAN IDs, etc.) available for selection for each access policy.

1. For each Access Control profile, create a worksheet listing the four Access Control policies. For each access policy, associate a policy role (created in the Policy tab), and the policy role's corresponding VLAN ID, if you are using RFC 3580-enabled switches in your network. For a description of each access policy, and some guidelines for creating corresponding policy roles, see the section on Access Policies in the Concepts file.

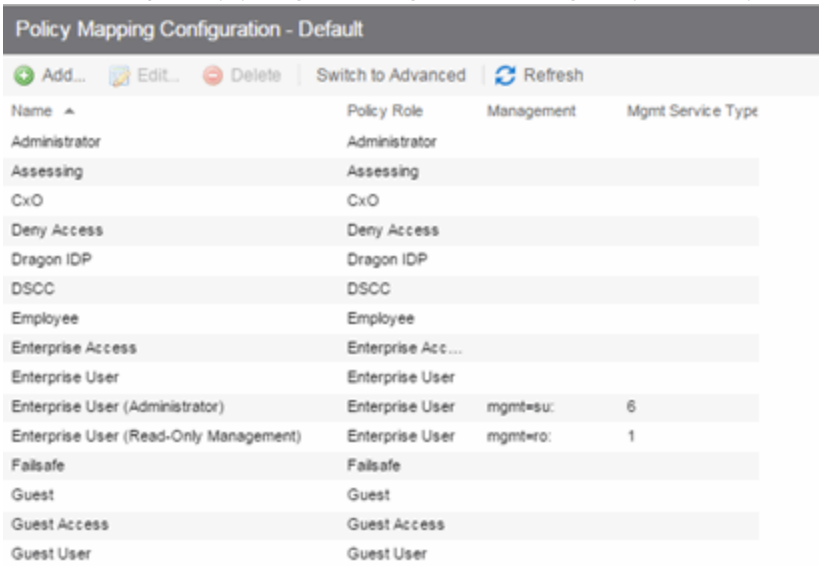
   NOTE: If your network uses Access Control Gateway engines with only RFC 3580-enabled switches, instead of listing policy roles, simply create a list of policy names that correspond to the VLANs you are using in your network. One tip is to use policy names that identify the corresponding VLAN name for ease of selection when you are creating your Access Control profiles.

   Here's an example of a worksheet for a Access Control profile that contains both policy-enabled and RFC 3580 switches:

Access Policy	Policy Role	VLAN ID
Accept Policy	Enterprise User	[2] Enterprise User VLAN
Quarantine Policy	Quarantine	[4] Quarantine VLAN
Failsafe Policy	Failsafe	[5] Failsafe VLAN
Assessment Policy	Assessing - Strict	[6] Assessing - Strict VLAN

2. For Access Control Controllers, use the Policy tab to verify that the policy configuration contains the required policy roles, and that the configuration has been enforced to the Access Control Controller. See the instructions above.
3. For Access Control Gateways, verify each policy role listed on your worksheet is created in 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 Access Control Configurations > Access Control Profiles > Policy Mappings left-panel option.

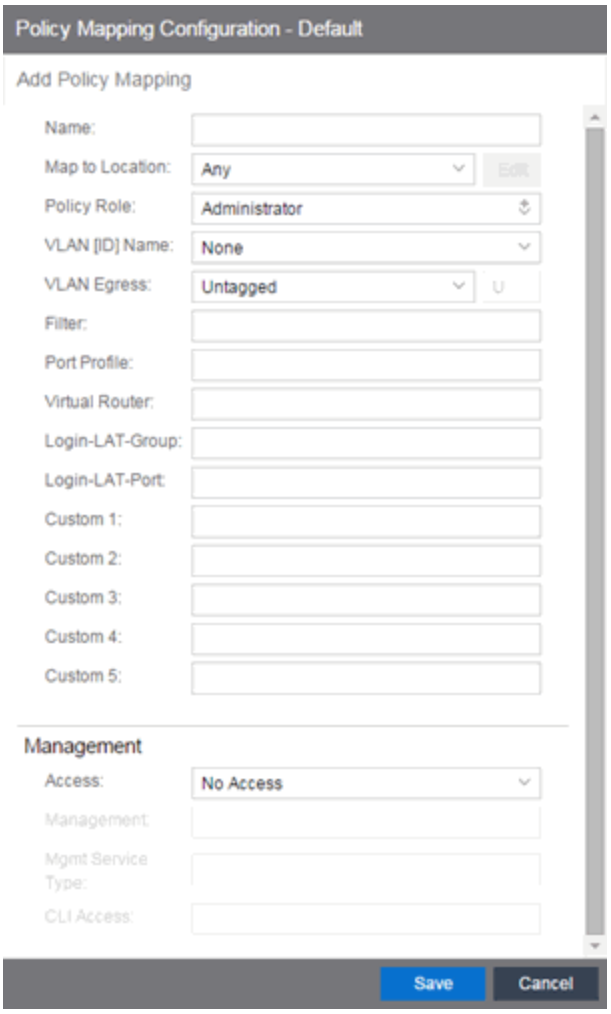
b. The Policy Mapping Configuration right-panel opens.



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.

   Access Control provides a list of default policy mappings you can use. Be aware if you use one of the default mappings, you still need to verify that the policy role specified in the mapping is part of your Access Control Controller policy configuration and/or is created and enforced to the policy-enabled switches in your network via the **Policy** tab.

d. To add a new policy mapping, click the **Add** button to open the Add Policy Mapping window.



For the new policy mapping, enter a mapping name and specify a policy role (created in the **Policy** tab) and other required RADIUS attributes included in the RADIUS response to a switch. 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 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 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 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 7 machine, they receive a lower level of network access.
- When an end user registers a Windows machine using its MAC address, another user cannot spoof that MAC address using a Linux system. (Device profiling does not resolve this issue in environments with dual boot machines.)
- If an end user exports a certificate from a corporate PC to an iPad and successfully authenticates with 802.1x, the iPad is not allowed full network access.

Device Profiling Use Case

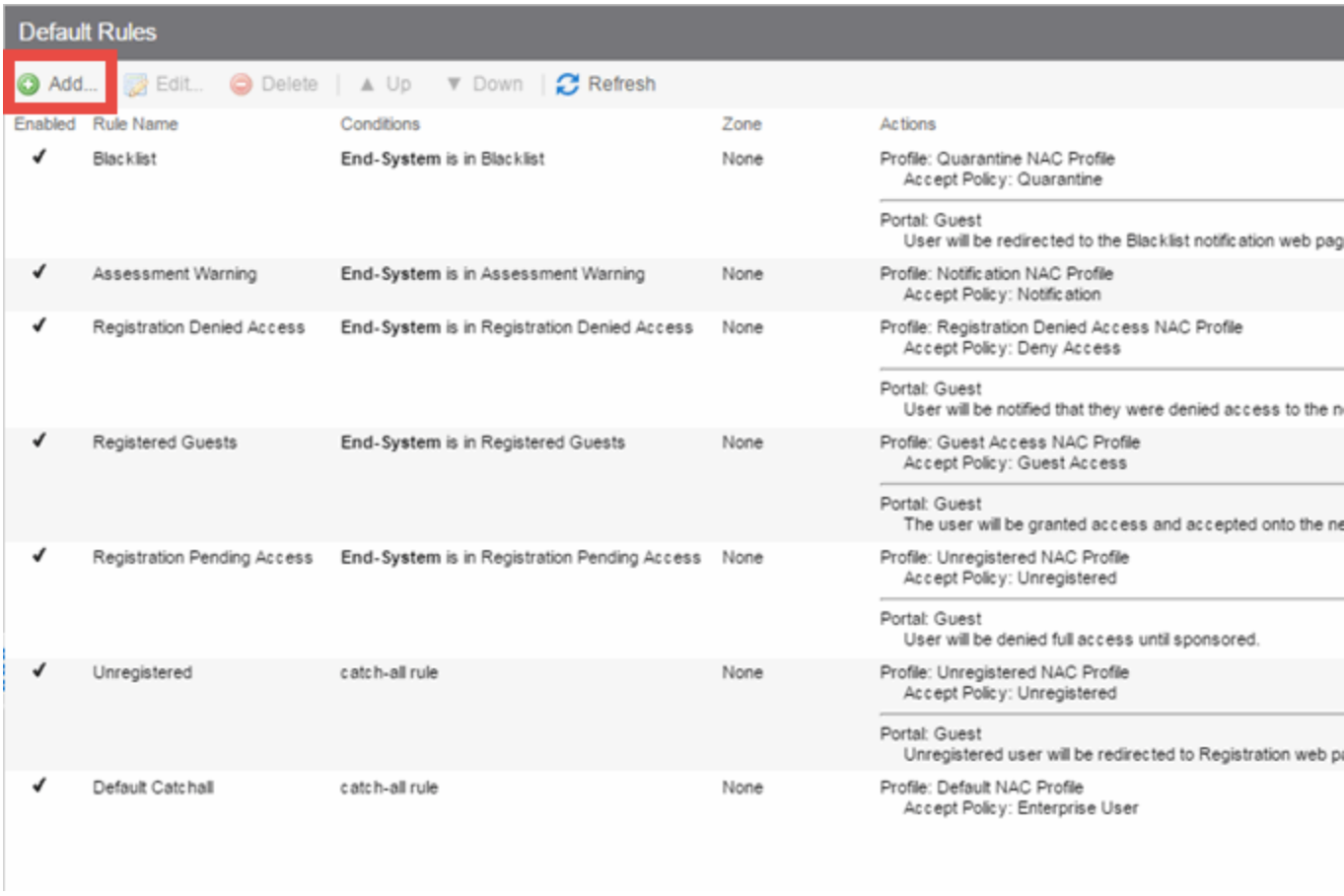
This section provides high-level instructions for configuring device type profiling for a sample use case. In this scenario, the network administrator has the following network access requirements:

- All Windows registered devices should be assigned the "Default Access Control Profile."
- All Windows 7 registered devices should be assigned the "Windows7 Profile."

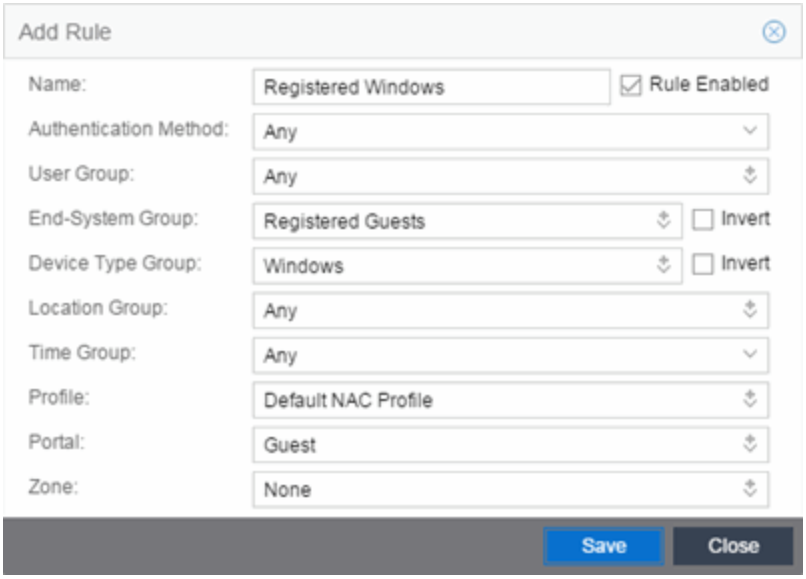
- All Linux registered devices should be assigned the "Default Access Control Profile." In addition, a new Linux version called SuperLinux needs to be added to the Linux family device type.
- All HP Printers should be assigned the "HP Printer Profile."

To do this, create four rules in your Access Control configuration that use device type as criteria for matching rules to end-systems authenticating to the network. The following instructions assume that you already created your profiles: Basic Profile, Windows7 Profile, and HP Printer Profile.

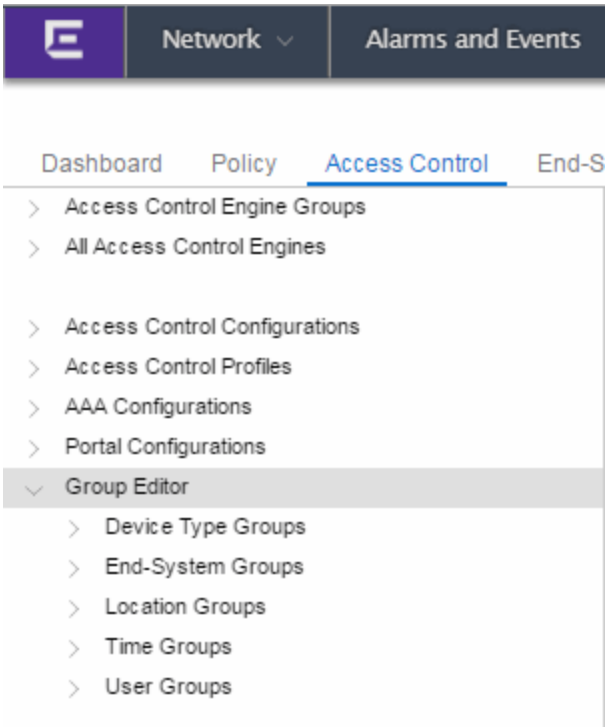
1. Expand the Default left-panel tree (Control > Extreme Access Control> Access Control Configurations > Default).
2. Select the Rules left-panel option and click the **Add** button in the right panel.



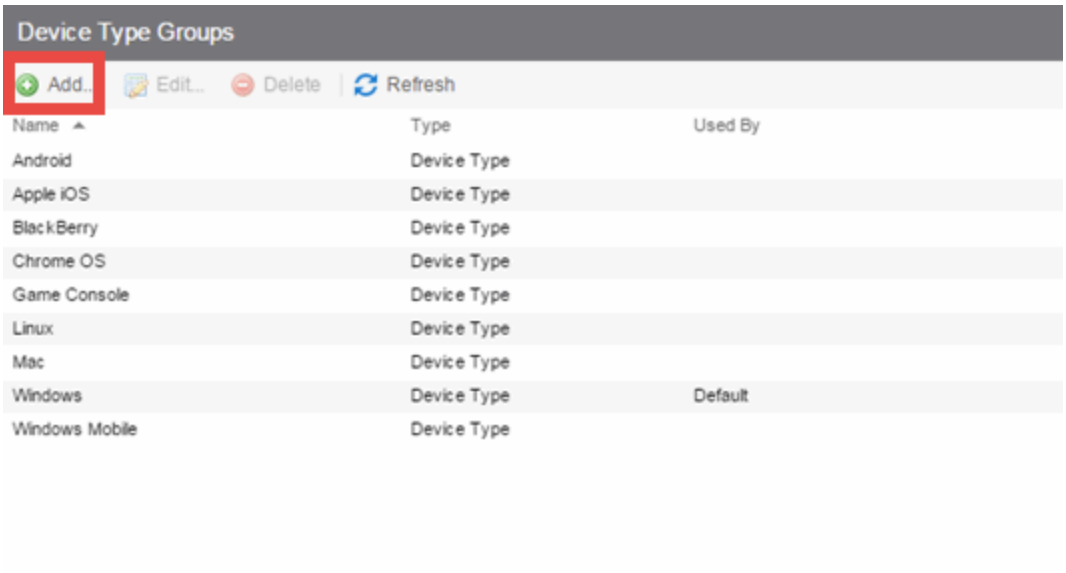
3. Create a rule that assigns the Default Access Control Profile to all Registered Guests using Windows devices as shown below.



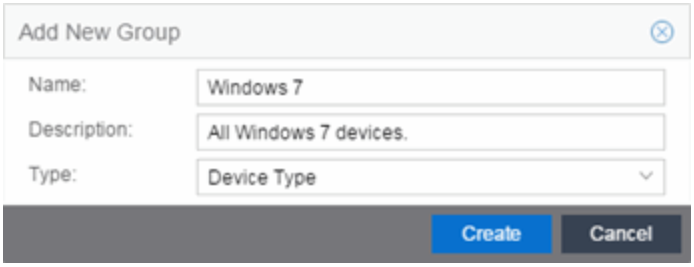
4. Create a rule that assigns the Windows7 Profile to all Windows 7 registered devices. To do this, you need to create a new Windows 7 device type group.
    a. From the Access Control Configurations left-panel tree, expand the Group Editor tree.



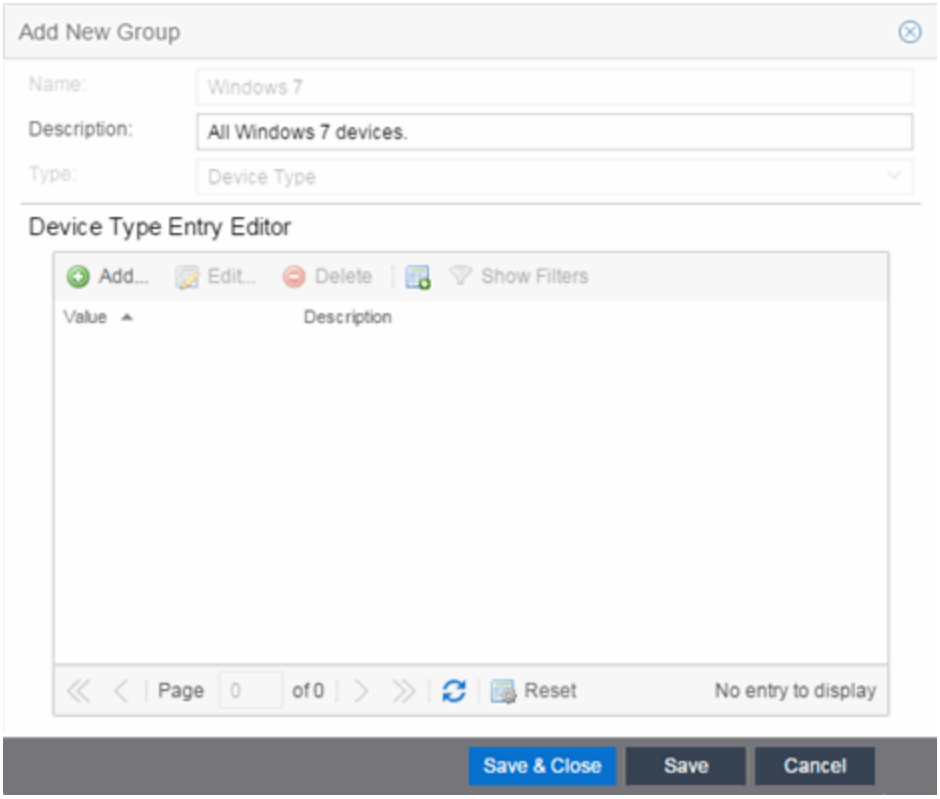
b. Select Device Type Groups and click the **Add** button in the right panel.



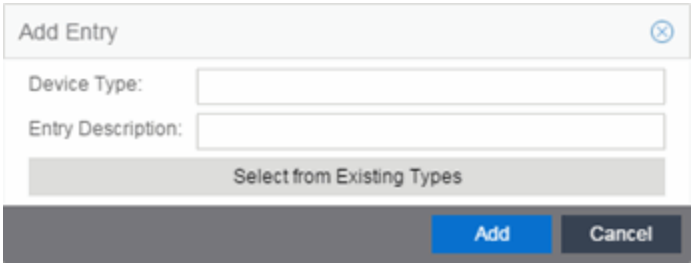
c. Create a new device type group with the name Windows 7.



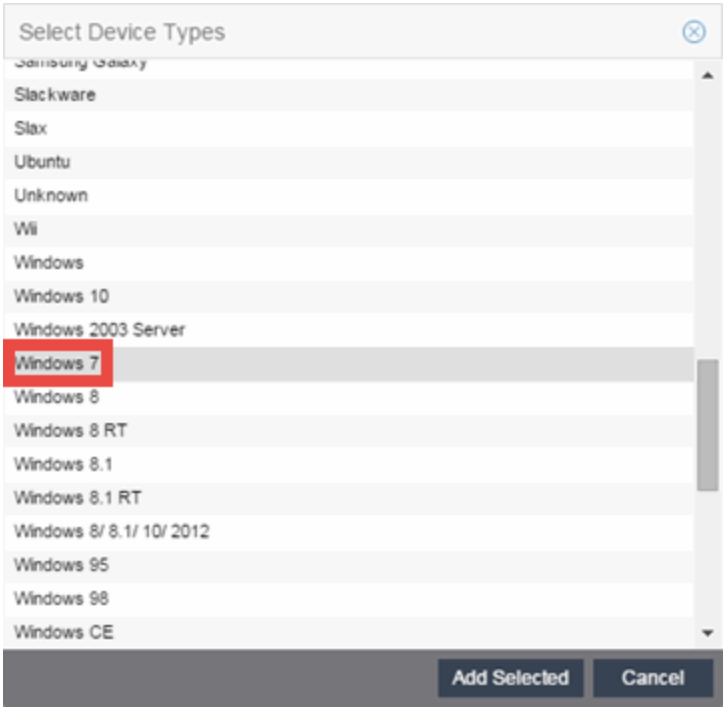
d. Click **Create**. The Device Type Entry Editor appears.



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 7.



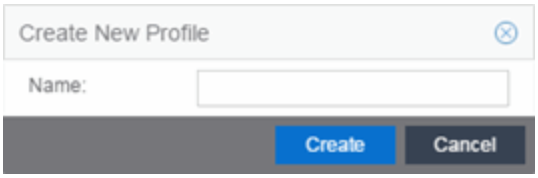
g. Click the **Add Selected** button.

h. Click the **Save & Close** button on the Add New Group window.

i. You can then create the rule.

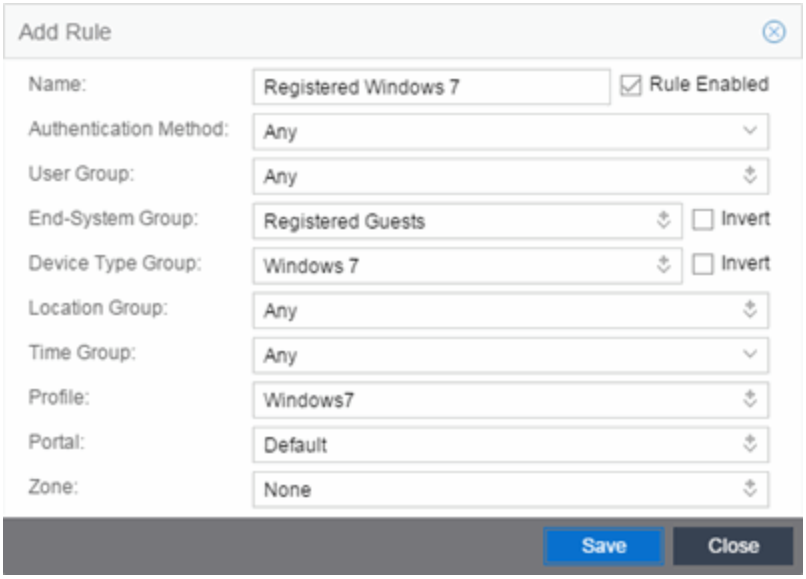
j. Select the Access Control Configurations > Default > Rules left-panel option and click the **Add** button in the right panel.

k. In the Profile drop-down menu, select **New**. The Create New Profile window appears.



l. Enter the name **Windows7** in the **Name** field and click the **Create** button.

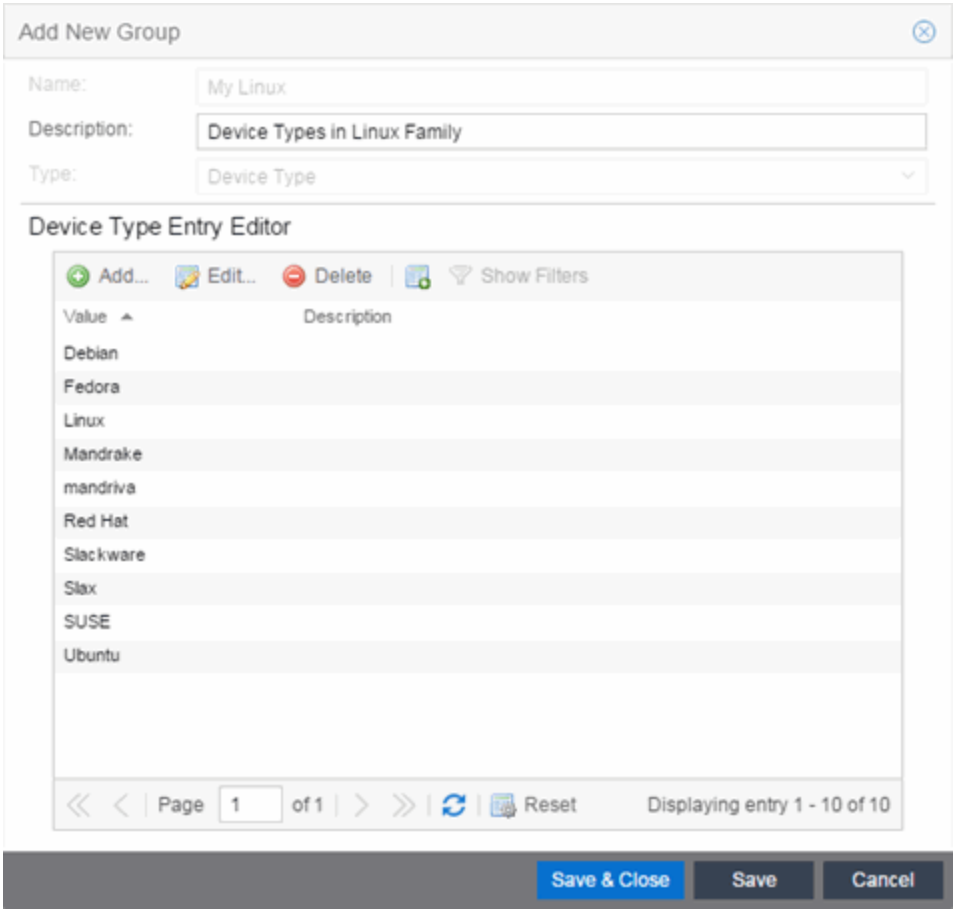
m. Configure the rule as shown in the screenshot below.



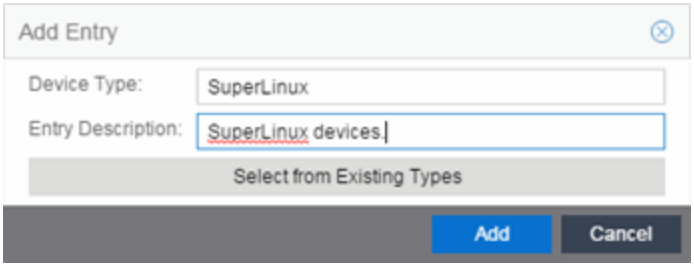
n. Click **Save**.

5. Create a rule that assigns the Default Access Control Profile to all Linux registered devices and add the SuperLinux version to the Linux family device type. To do this, you need to create a new Linux device type group that includes SuperLinux.

   a. Create the My Linux device type group to include the devices in the Linux device type group using the **Select from Existing Types** button in the Add Entry window as discussed in step 4f above.



b. Click the **Add** button and in the Add Entry window, create the **SuperLinux** Device Type as shown below.

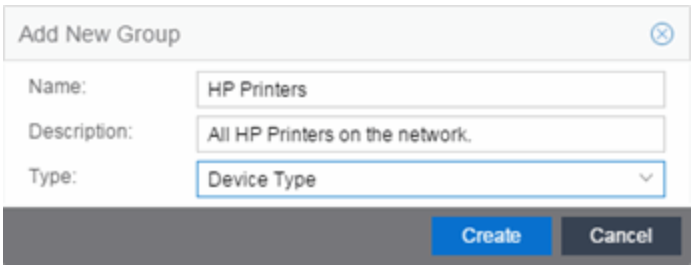


c. Click **Add** to save the SuperLinux device type to the My Linux device type group.

d. Click the **Save & Close** button on the Add New Group window.

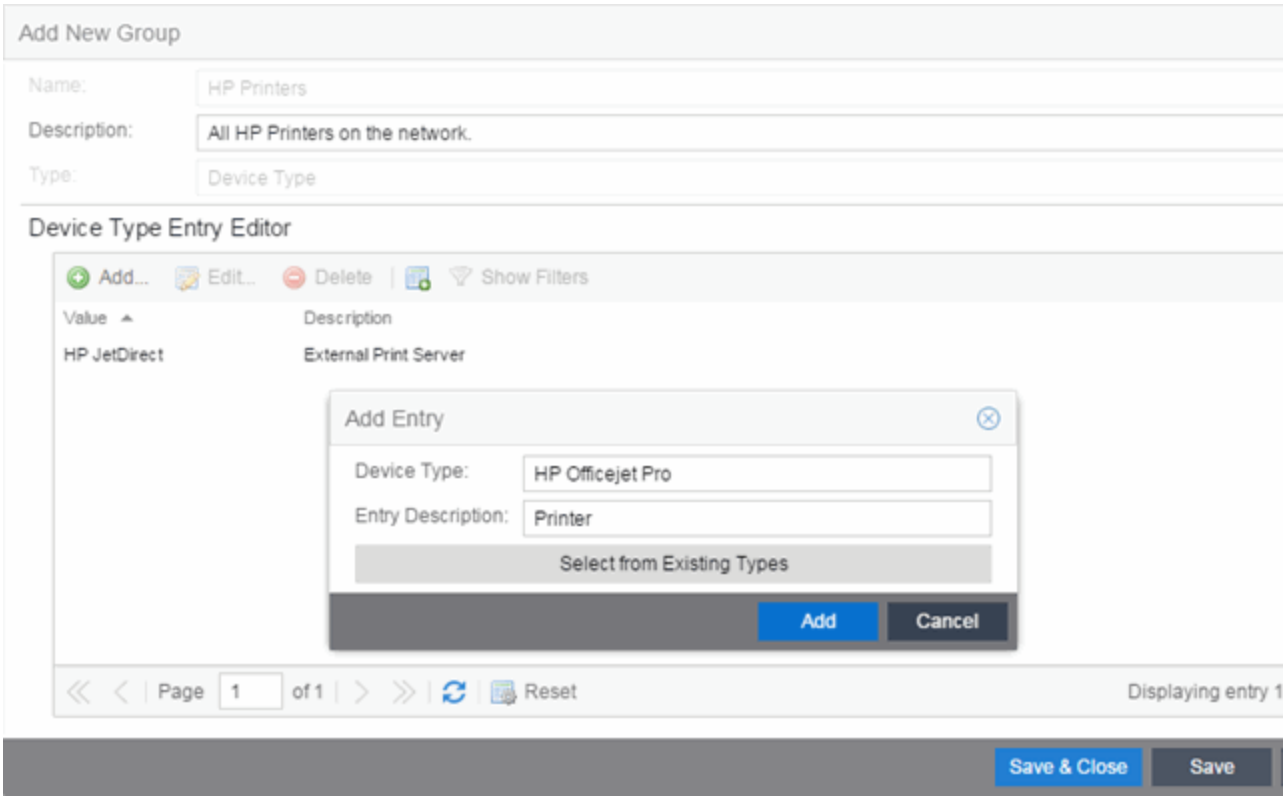
6. Create a rule that assigns the HP Printer Profile to all HP printers on the network. To do this, create a new HP Printers device type group.

a. Open the Add New Group window by clicking the **Add** button on the 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.



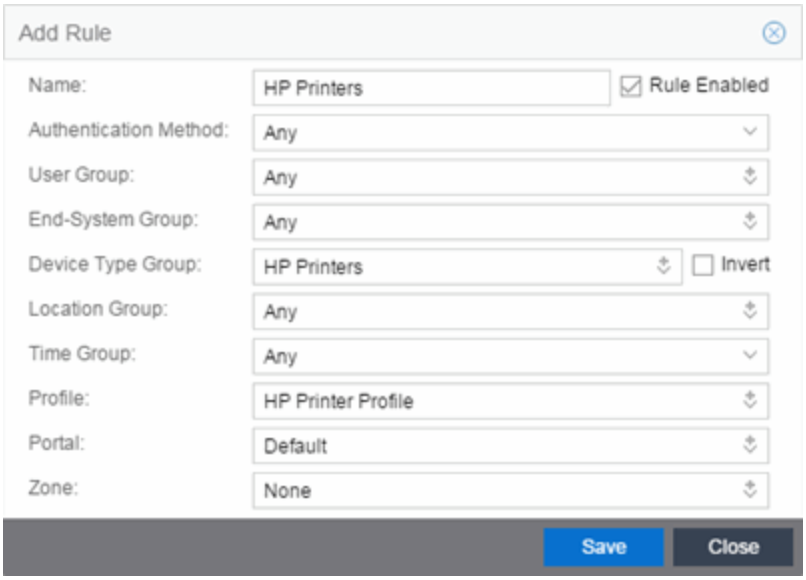
d. Click **Save & Close** to save the HP Printers group.

e. Select Rules in the left-panel tree (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 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

Analytics

The Analytics tab lets you view and customize Application Analytics reports and application flow data, as well as manage and configure your Application Analytics engines. Additionally, the Menu at the top of the screen provides links to additional information about your version of Extreme Management Center.

NOTE: Application Analytics reports and application flow data is not available unless a Application Analytics engine is configured and you are a member of an authorization group assigned the Management Center Application Analytics Read Access or Read/Write Access capability.

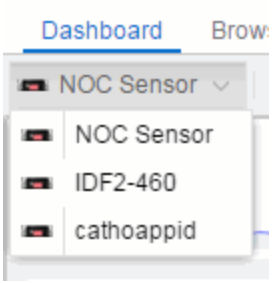
Viewing Application Analytics application data requires certain prerequisites. For additional information, see Getting Started with Application Analytics.

This Help topic provides information on the different reports available from the Analytics tab, as well as engine configuration information.

Dashboard

The Dashboard view 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. For many of the graphs, you can click on an item to view details.

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.

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, alternate values should be used.

Graph Descriptions

This section provides a description for each of the available graphs.

Overview

The Dashboard report contains an info bar and two summary graphs for top applications and application group usage. The info bar provides a selection of sparkline graphs showing different network statistics for the last 24 hours, with arrows that indicate trends compared to the previous reporting period.

- The **per hour** statistics show the average unique applications, clients, or servers seen per hour for the past 24 hours.
- The **total** statistics show the total bandwidth or flows reported for the past 24 hours.

The Network and Application graphs show the average reported response times for the last 24 hours. Rest your cursor on the graph to see a tooltip showing the response time including the time and date of the data sample. Clicking on a graph for which historical data is available displays the available historical data for the category, with options to change the reporting time period displayed.

The Top Application Groups report displays the top five applications for the last hour. Use the **Gear** button to change the start time for the report and whether the data is displayed as a pie chart, word cloud, tree map or bubble map. If you change the reporting start time, the data in the Dashboard info bar changes accordingly. Clicking an application link in the table to the right displays the list of clients using that application. Right-click on a client to open various reports, launch PortView, or search Management Center maps.

The Application Group Usage graph provides a longer view of application usage. Use the **Gear** button to change the start date and time and the number of days of data to display. You can also select whether to display bandwidth, flow, or client data in the graph. Use the arrows at the ends of the graph to quickly change the reporting period displayed. The table below the graph presents the individual bandwidth, flow, and client statistics for each group.

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** button 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 on the Info button ⓘ 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.

IP Reputation Dashboard

This report displays potential threat activity on your network 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. Additionally, each IP address classification has its own recommended course of action, listed below.

- CiArmy Top Attackers — The CiArmy reputation feed is a set of IP addresses tied to malicious activity defined by a collaborative network security effort backed by the Emerging Threats project. Any IP communications to addresses in this list from the local network are suspicious and may indicate that the local IP is involved in various activities such as command and control communications with the remote host. IP addresses classified as CiArmy Top Attackers require further investigation.
- Compromised Hosts Connecting Into the Network — IP addresses that match this classification are on a list of IP addresses maintained by the Emerging Threats project. This list consists of a set of IP addresses that appear to have been compromised by malware, individual actors, worms, botnets, or other means. When Application Analytics detects application flows that match an IP from the Compromised list, this is a likely indicator that systems in the local network are either under attack or have already been compromised (since the communications may be command and control directives emanating from the compromised host).
- Connections to Bad Hosts — IP addresses classified as Connections to Bad Hosts are known to function as command and control nodes for various botnets around the Internet. Any flows to or from such IP addresses have a high probability of being associated with botnet command and control traffic.
- Connections to Bad Hosts Based on Port — IP addresses flagged in this classification are known to function as command and control nodes for botnets based on the port number. For example, a botnet command and control node may be a legitimate webserver, which is not suspicious. However, if there are flows certain botnets are known to use specific ports on a node, these communications cause the IP address to be flagged in this classification.
- DShield Top Attackers — The DShield project is a distributed security analysis effort that collects logs, IDS/IPS events, and other data from volunteers around the Internet. This data is analyzed by DShield and a list of the top set of IP addresses that appear to be attacking other systems worldwide is provided by DShield. When application flows appear within Application Analytics that match any of the IP addresses from the DShield top attackers list, it is likely systems in the local network are being actively attacked.

- Tor Exit Node, Relay or Router — This reputation feed provides a listing of known Tor exit nodes, relays, and routers. Tor is a service that provides IP anonymity. It functions as a distributed set of systems on the Internet and builds sets of "virtual circuits" through this set of systems on behalf of users that do not want to reveal their local IP address to destination servers. Typically, Tor is used to mask web browsing communications, but other services can run over the Tor network. Matches against this reputation feed indicate Tor usage on the local network.

NOTE: IP addresses that match multiple classifications (e.g. an IP address is listed as both a CiArmy Top Attacker and a DShield Top Attacker) are only classified in the first category in which they match, not in additional categories.

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 Application Analytics locations linked to the Network tab map.

For information on configuring the 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 the 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 Dashboards present the response time in milliseconds of application data grouped by different criteria, selected from the dropdown menu. The data is displayed as a line graph, which is updated periodically. For additional information, see Response Time Dashboard.

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. For additional information, see Network Service Dashboard.

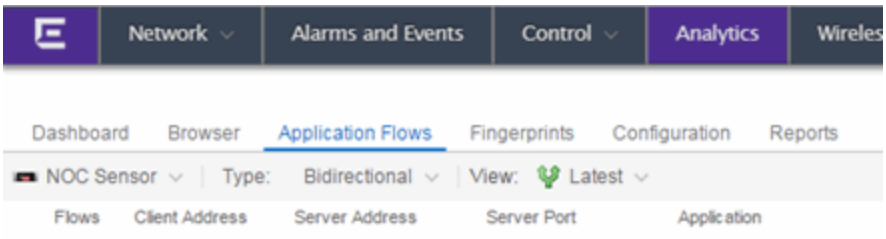
Browser

The Applications Browser lets you query information about recent network activity stored in the 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. For additional information, see Applications Browser.

Application Flows

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 TCP 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.

- Top N — These reports provide aggregated flow data for individual applications, clients, or servers, with results sorted based on bandwidth, number of flows, number of packets, or number of connections.
- Show All — Show all flows.
- Show Classified — Show only flows that have been classified by an application fingerprint.
- Show Unclassified — Show only flows that have not been 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.

Use the **Search** field at the top right of the table to search for a specific application, user name, or IP address. From the filtered search results, click a user name or IP address to launch PortView, which provides a detailed topology context for the user. Entering **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".

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. For additional information, see Create Policy Rule.
- Search 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.

Bidirectional Flows

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 how long the data has been collected, using X number of days, hh:mm:ss format.

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 **Gear** menu 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. For additional information, see Network Locations.

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.

Threat
: Indicates if the flow contains potential threat activity from IP addresses known to be suspicious. IP addresses can be considered suspicious for a variety of reasons. For additional information, see IP Reputation Dashboard.

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.

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.

Rx Packets
: The number of packets received for this flow.

Tx Bytes
: The number of bytes transmitted for this flow.

Rx Bytes
: The number of bytes received for this flow.

NetFlow Records
: The number of NetFlow records received in each flow.

Flow Source
: The IP address of the NetFlow 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.

Unidirectional Flows

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.

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 view shows how long the data has been collected, using X number of days, hh:mm:ss format.

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. Mouse 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. For additional information, see Network Locations.

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 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.

Bytes
The number of bytes in this flow.

NetFlow Records
The number of NetFlow records for this flow.

Flow Source
The IP address of the NetFlow 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.

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.

Report Features

The Application Flows table (bidirectional and unidirectional) includes the following features:

Search
The Search field 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.

Refresh Interval

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.

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.

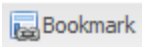
Interactive Tables

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 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.

CSV Export

Save report data to a CSV file to provide report data in table form.

Fingerprints

The **Fingerprints** view provides detailed information about fingerprints used by Application Analytics to identify application flows. A fingerprint is a description of a pattern of network traffic which can be used to identify an application. 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 Management Center server. When a fingerprint is changed, a flag is raised on the Application Analytics engine to show it needs enforcing.

There are two types of fingerprints: system fingerprints and custom fingerprints.

System fingerprints are provided by 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.

For additional information, see Add and Modify Fingerprints.

The **Fingerprints** view is divided into a left-panel tree and a table. 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 is a **Gear** menu  , where you can access various system and fingerprint actions. See below for a description of the menu options.

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 Hits and 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.

Gear Menu

Use the **Gear** menu  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 — For additional information, see Creating a Fingerprint.
- Delete Custom Fingerprint — For additional information, see Deleting a Custom Fingerprint.
- Fingerprint Definition — View the XML definition for a fingerprint.
- Enable/Disable Fingerprint — Enable or disable a fingerprint. When a fingerprint is enabled, it will be used to identify applications. When it is disabled, it will be ignored.
- Modify Fingerprint — Change a fingerprint's description. For additional information, see Modifying a Fingerprint.
- Reset Fingerprint Counters — Reset the Hits and Matches counters.

Column Definitions

Following are definitions for the table columns:

Application Name
: Name of the application this fingerprint detects. Click on an Application Name link to view client, flow, and usage information for that specific application.

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.

Hits
: The total number of times a hit has been recorded for this fingerprint for the selected engine. A hit is an occurrence of the Application Analytics engine matching a fingerprint in a flow. It may refine the application detected with other fingerprint hits on the same flow. This column is not displayed by default. You must display this column by clicking on a column heading drop-down arrow and selecting the Hits column option from the menu. See Notes below.

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:

- Hits and 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.
- A single hit, applied to one direction, may result in two matches, one in each direction.
- If you need to reset the Hits and Matches counters, use the **Reset Fingerprint Counters** option from the **Gear** menu  .

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.

Description

Description of the fingerprint.

Last Modified
: Date that the fingerprint was last modified.

Created
: Date that the fingerprint was created.

Configuration

The Configuration view provides detailed information on the Application Analytics engines you have configured. It also lets you add and enforce your engines, access enginereports and diagnostics, and configure network locations. You must be a member of an authorization group assigned the Management Center Application Analytics Read/Write Access capability to view the Configuration tab.

Adding an Engine

Use the following steps to add a Application Analytics engine to Management Center.

1. Select the Analytics tab in the Management Center and then select the Configuration view.
2. Select Overview in the left-panel tree.
3. Click on the Gear menu  and select Add Engine.
4. Enter the IP address of the management interface of the engine and a name for the engine.

   The engine is added to Management Center if it does not already exist.
5. Select the SNMPv3 profile to use for the engine.
6. Click OK. The engine is added to the engine list.
7. Enforce the engine.

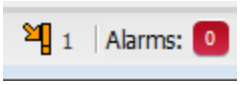
Enforcing an Engine

You need to enforce an engine whenever there are any changes made in Management Center that need to be sent to the Application Analytics engine. This includes changing system settings, changing engine settings, and changing fingerprints.

Use the following steps to enforce a Application Analytics engine.

1. Select the **Analytics** tab and then select the **Configuration** view.
2. Select **Overview** in the left-panel tree to display a list of configured engines. The orange Enforce icon is displayed above an engine that needs to be enforced.
3. Hover the mouse over the engine that needs to be enforced. Click on the yellow Enforce icon to the right of the engine to enforce the engine.
4. To enforce all engines, click on the **Gear** menu and select **Enforce All Engines**.

The orange Enforce icon is also displayed in the **Applications** view status bar along with the number of engines that need to be enforced. Mouse over the icon to see a tooltip that lists the engines that need to be enforced. Click the icon to enforce the engines.



Engine Administrative Options and Reports

Use the left panel in the Configuration view to access various engine administrative options and reports.

Overview

View a list of configured engines and their engine statistics. Access the following options from the **Gear** menu. For some of the options, you must first select an engine in the list.

- Add Engine — Adds a new Application Analytics engine to 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 Management Center.

Application Analytics Engines

View engine status information, configure web credentials, and configure advanced options for an individual engine. Selecting the engine name opens

- 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.
- Advanced Configuration — For additional information, see Application Analytics Engine Advanced Configuration.
    - Set privacy levels.
    - Enable Access Control Integration.
    - Add advanced configuration properties.
    - Enable sensor modules and sensor module logging.

Application Analytics System

Configure and manage components of the Application Analytics system.

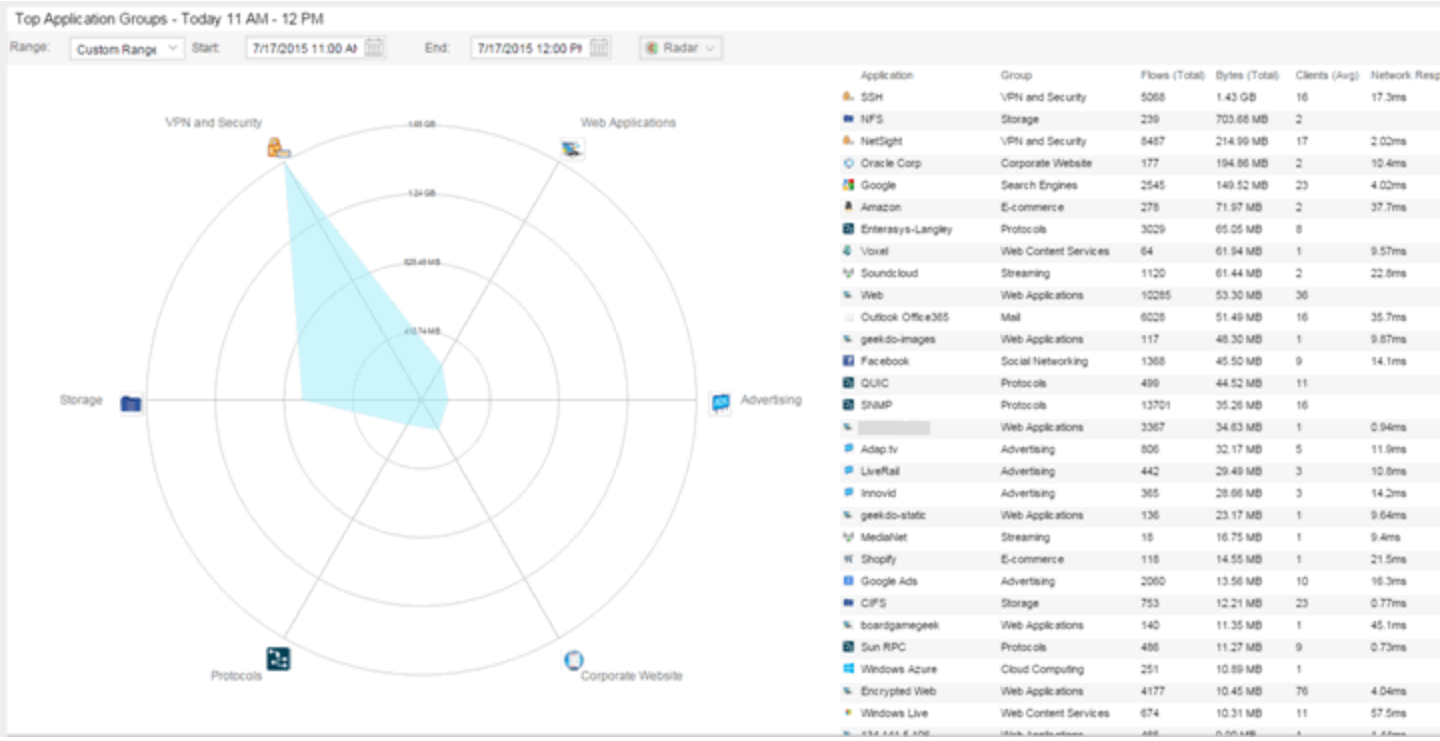
- Locations — Configure and manage network locations. For additional information, see Network Locations.
- Fingerprints — View a summary of the kinds of application fingerprints in use. Use the **Gear** menu  to access the following system fingerprint actions:
    - Update Fingerprints — Perform a manual one-time update of the fingerprint database. For additional information, see Updating Fingerprints.
    - Fingerprint Update Settings — Schedule fingerprint updates to be performed automatically on a daily or weekly basis. For additional information, see Updating Fingerprints.
- Licenses — Add an engine flow rate increase license. Click on Help Tips to read a description of the various sections.
- Advanced — Configure global options for the Application Analytics system.
- Status — View a collection of Application Analytics system statistics.

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.

In most of the reports, you can 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, alternate values should be used.

Report Descriptions

This section provides a description for each of the available reports.

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.

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.

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 for each network location.

Network Activity for a 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 for an 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 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. For additional information, see Network 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 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:

- **Start** — Select the start date and time.
- **Top N** — Select the number of clients displayed in the chart.
- **# 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 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:

- **Start** — Select the start date and time.
- **Top N** — Select the number of clients displayed in the chart.
- **# 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 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:

- Start — Select the start date and time.
- Top N — Select the number of clients displayed in the chart.
- # 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

For information on related Application Analytics topics:

- Getting Started with Application Analytics
- Add and Modify Fingerprints
- Custom Fingerprint Examples
- Network Locations

Getting Started with Application Analytics

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.

Application Analytics Access Requirements

Both the Application Analytics feature and the Analytics tab require the Management Center Advanced (NMS-ADV) license. Contact your sales representative for information on obtaining an Management Center Advanced license.

In order to view the Analytics tab, you must be a member of an authorization group that has been assigned the 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. For additional information, see How to Configure User Access to Extreme Management Center Applications.

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 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 Management Center and enforced via the Configuration view in the Analytics tab. For additional information, see Configuration.

Enable NetFlow Collection

Because the Analytics tab displays reports based on NetFlow data, you must enable NetFlow for your network devices that act as the NetFlow sensors, and enable flow collection for their device interfaces. For additional information, see How to Enable Flow Collection. You must also configure your NetFlow sensor devices to send their NetFlow information to the Application Analytics engine. In addition, the device interfaces you enable for flow collection must match the interfaces that are 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.

For additional information, see Network Locations.

Related Information

- Configuration - Analytics
- Network Locations

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 NetFlow 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 Management Center database. Management Center uses this data to provide reports that show how your network is being utilized.

To conserve space on your 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 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

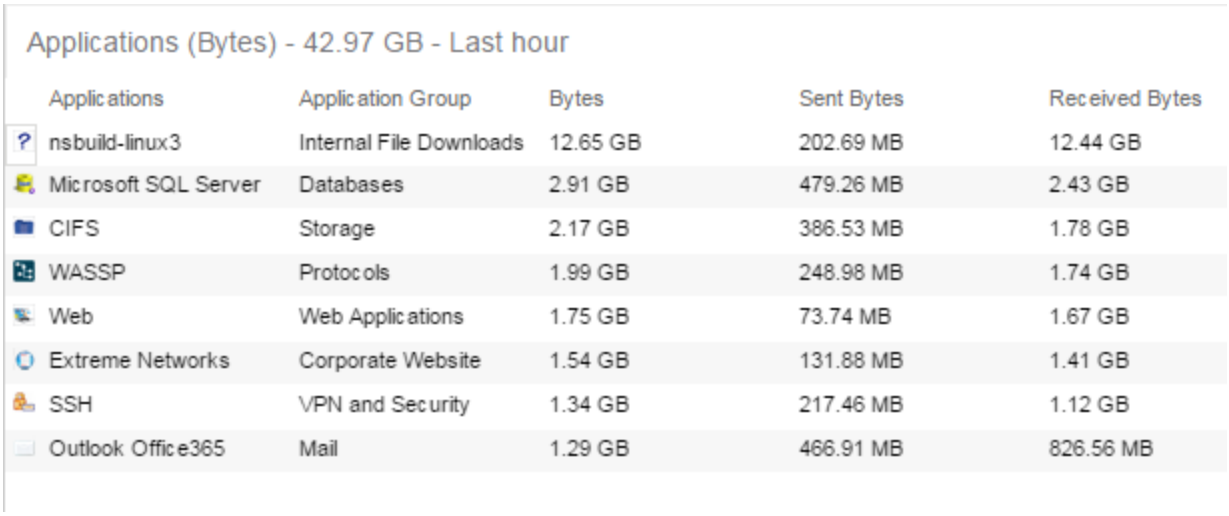
Flow data is collected on objects in your network called targets. Some targets are physical, such as clients and servers, and some are logical, such as applications.

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 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

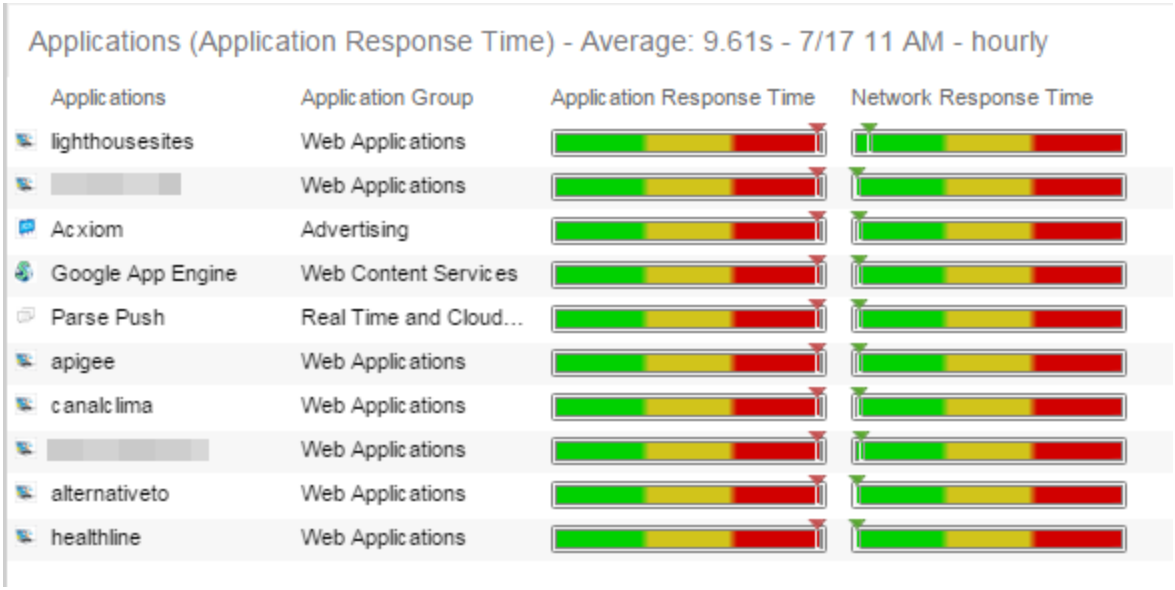
Collection statistics are quantitative data that can be collected for a target. This includes statistics directly reported in NetFlow records, such as bytes transferred, as well as information that can be derived indirectly, such as the number of unique clients seen using an application.

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.

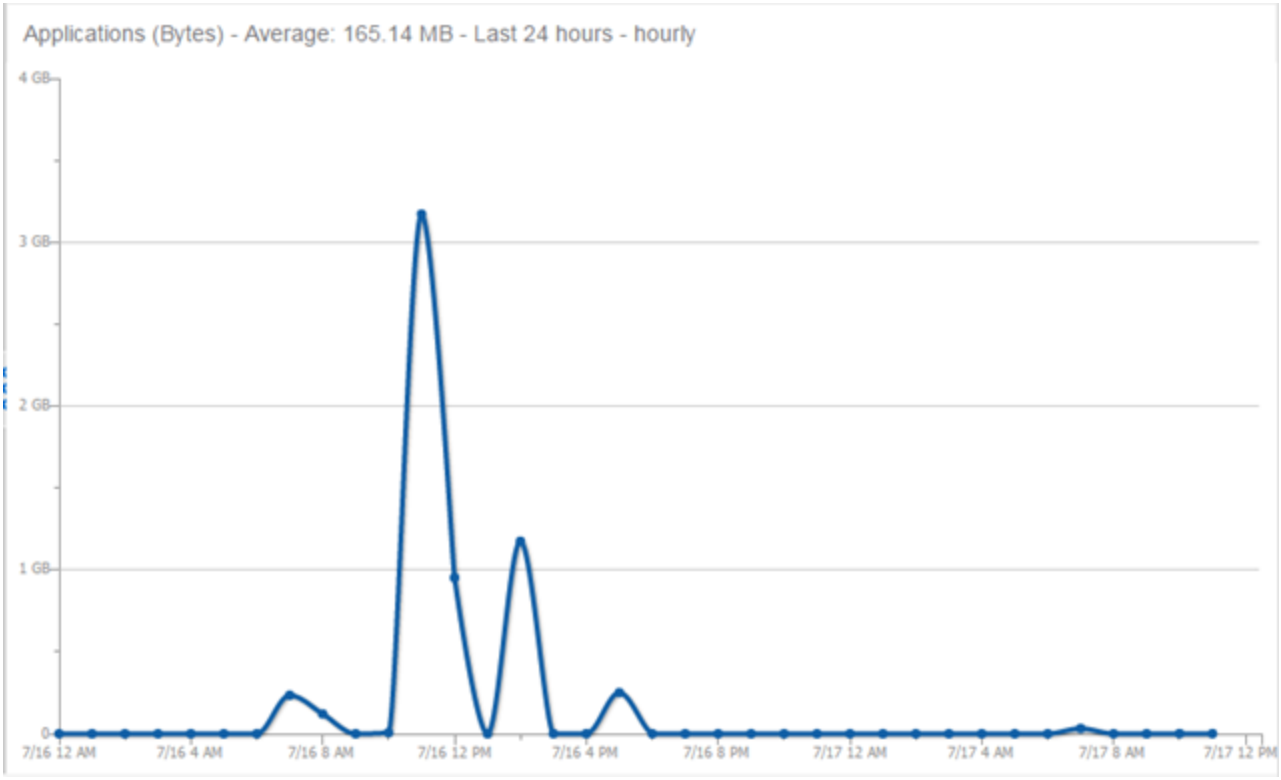


Collection Intervals

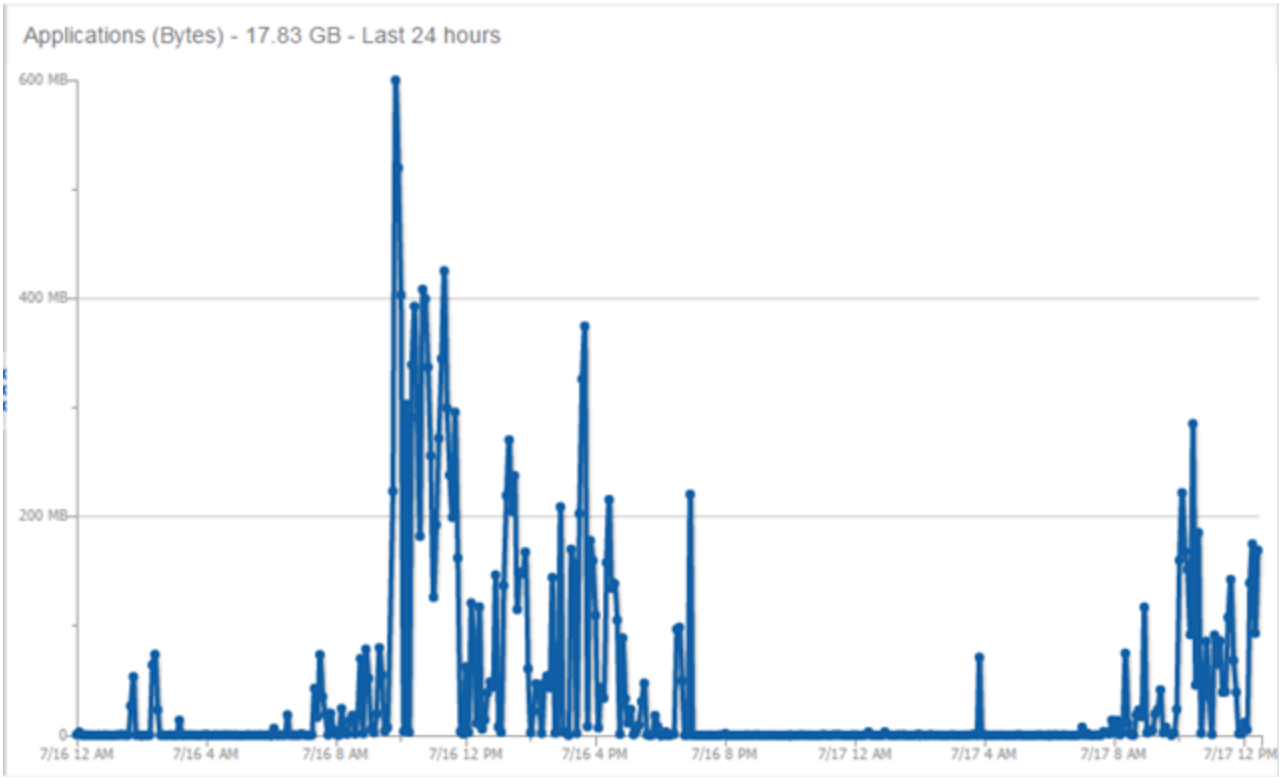
The Application Analytics engine collects and aggregates flow data for a period of time called an interval. At the end of the interval, the engine writes the totals to the Management Center database and a new interval begins, with new totals collected starting at zero.

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.

For additional information, see Network Locations.

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
Client		Bytes Received Bytes Transmitted Bytes Flows Receive Flows Transmit Flows Applications Network Response Time Application Response Time	All Flows

Target	Sub-Target	Bases	Traffic Used
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
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

Target	Sub-Target	Bases	Traffic Used
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 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 records and deep packet inspection.

NOTE: Most of these sources rely on Access Control data. If Access Control is part of your network configuration, then 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. For additional information, see Network Locations.

The following is a list of information that can obtained from different sources:

- Hostname — The client or server's hostname can be derived using Access Control. 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. 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 Access Control, if Access Control integration is enabled.
- Profile — The client's profile is derived from the Access Control profile assigned to the client end-system. Access Control integration must be enabled.
- Username — The client's username is derived from network packet inspection. The username can also be provided by Access Control, if 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 Access Control may provide the device family name of Windows.

Enabling Extreme Access Control Integration

If your network configuration includes Access Control, Access Control data can be integrated with flow data to provide additional information. Access Control integration is only useful if you are collecting flows for end-systems managed by Access Control.

When Access Control integration is enabled, if a client in a flow matches an end-system in Access Control, 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 Access Control profile.
- The detailed location in the flow is derived from end-system data.

If a server in a flow matches an end-system in Access Control, then:

- The server hostname in the flow is derived from the end-system.

To enable Access Control integration on the Application Analytics engine:

1. If the Access Control distributed end-system cache is not enabled on the 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 Management Center server. Click **OK**.
2. Enable Access Control Integration on each Application Analytics engine where you want to use Access Control 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 Access Control engines are using Communication Channels, you must select the **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

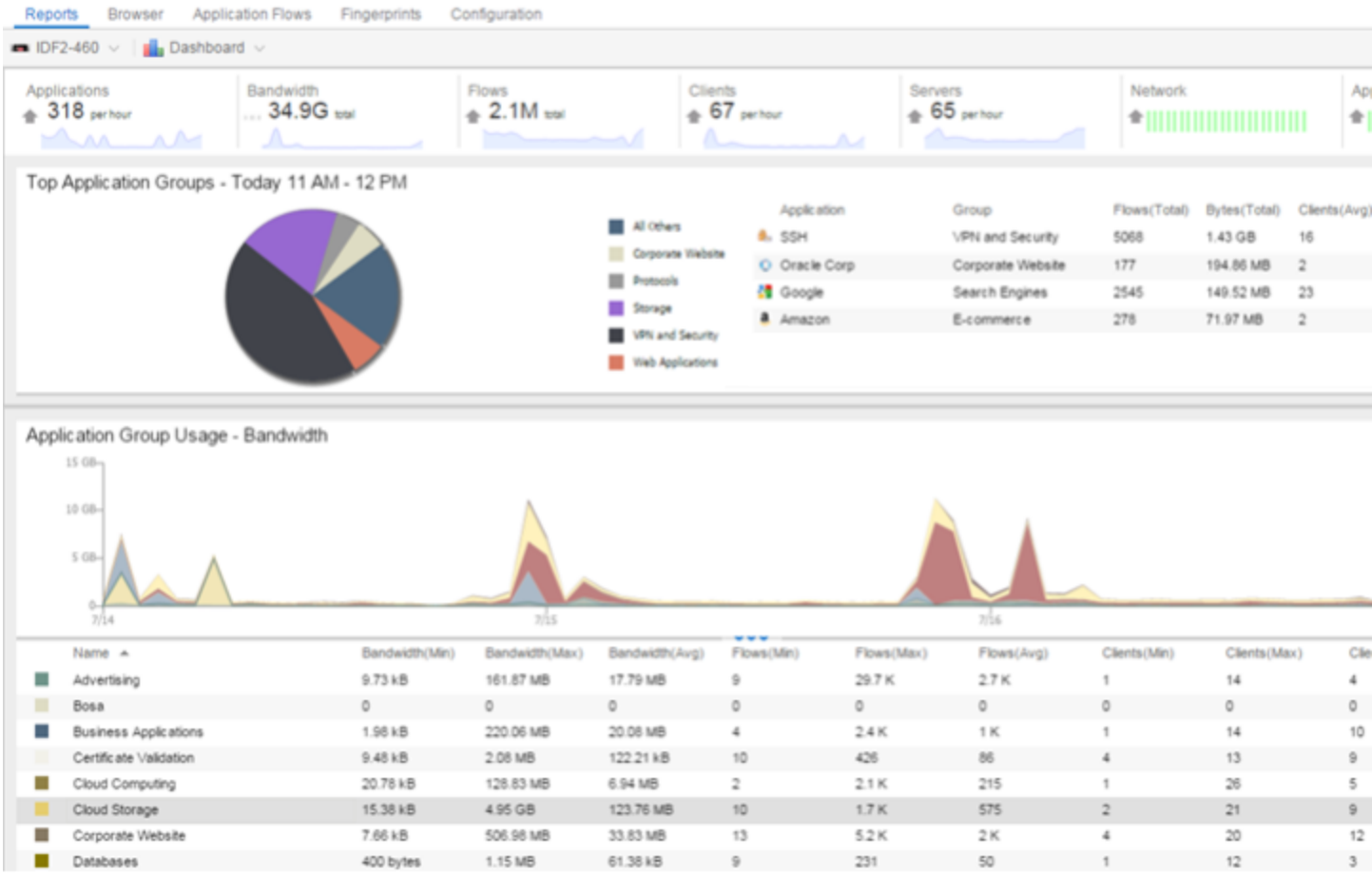
Data gathered from flow usage collection is the basis of many reports in the Management Center's **Analytics** tab. Once collection is enabled, these reports begin to exhibit data.

For additional information, see Analytics.

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.

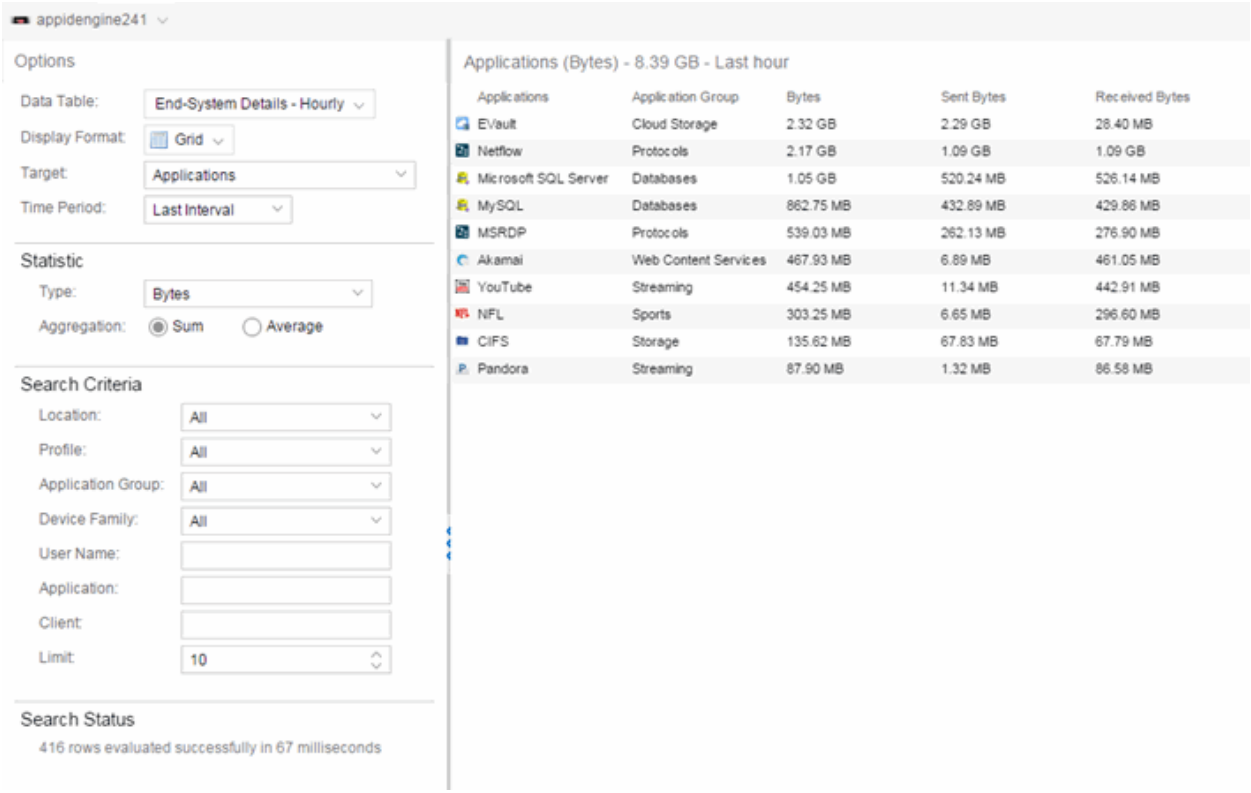
Note that data from different Application Analytics engines is maintained separately. If you have more than one Application Analytics engine, you need to select which engine to view, using the engine menu in the top-left corner.



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 Application Analytics
- Analytics
- Network Locations

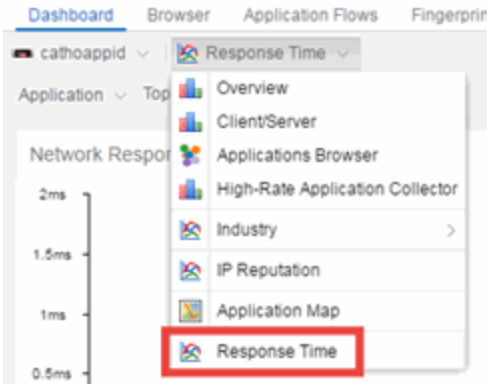
Application Analytics Response Time Dashboard

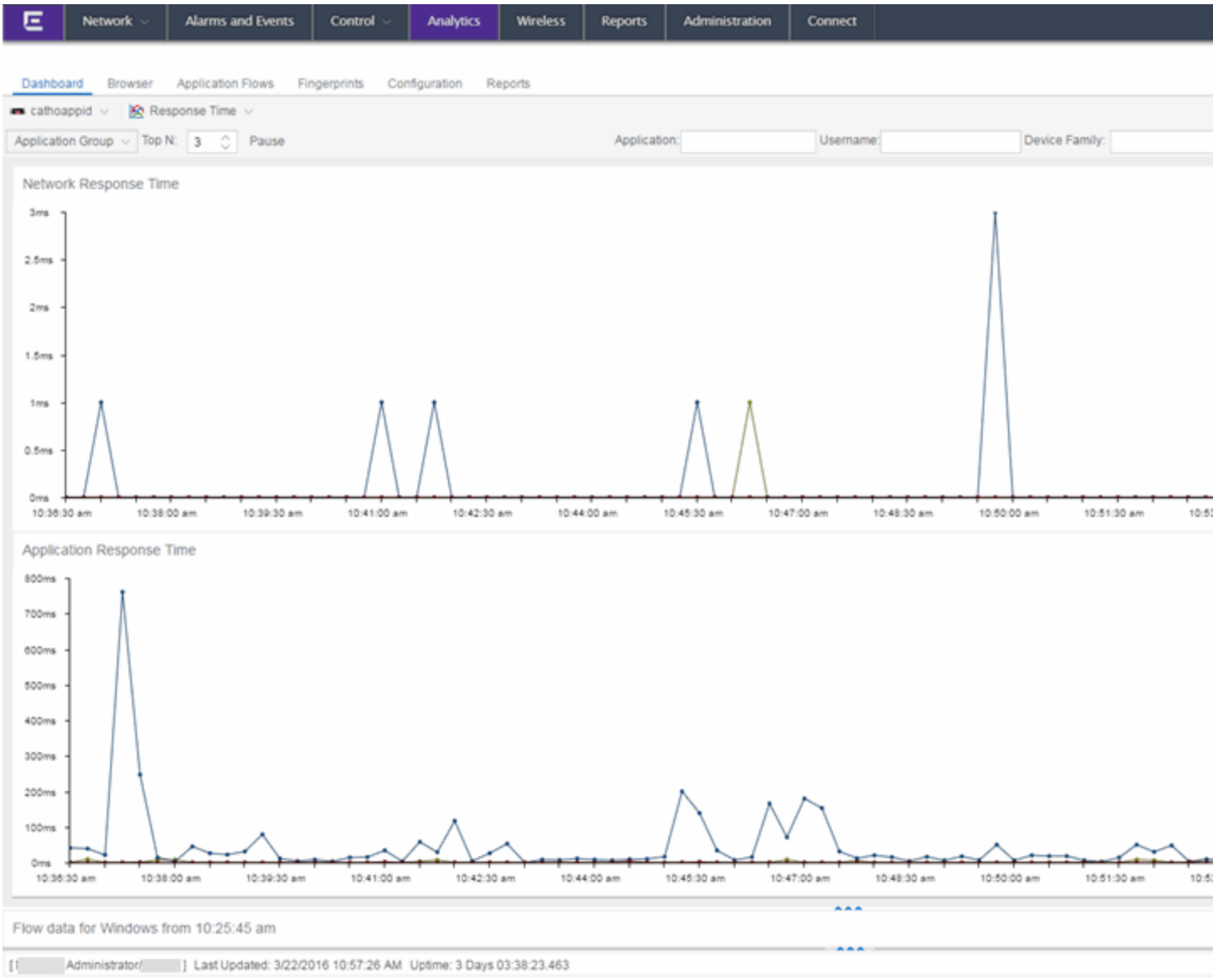
The Response Time Dashboard displays the network and application response time data for the slowest targets on your network based on response time for the last 20 minutes.

Extreme Management Center allows you to view response time data for a variety of targets, including application, device family, and username. For additional information, see Target.

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.

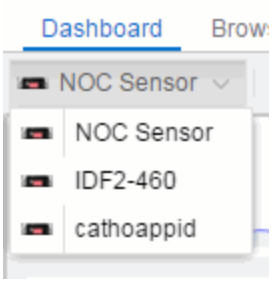




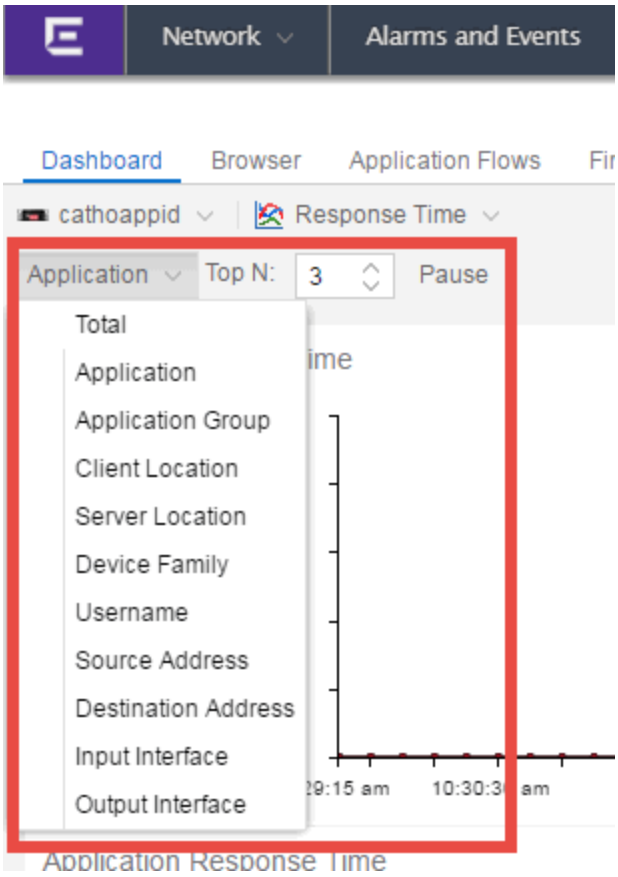
Overview

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.



Target

The **Target** drop-down menu allows you to group the data in the Response Time Dashboard by the following criteria:

- Total
- Application

- Application Group
- Client Location
- Server Location
- Device Family
- Username
- Source Address
- Destination Address
- Input Interface
- Output Interface

Top N

The **Top N** field allows you to limit the results in the graphs to display only the top results based on the number you enter.

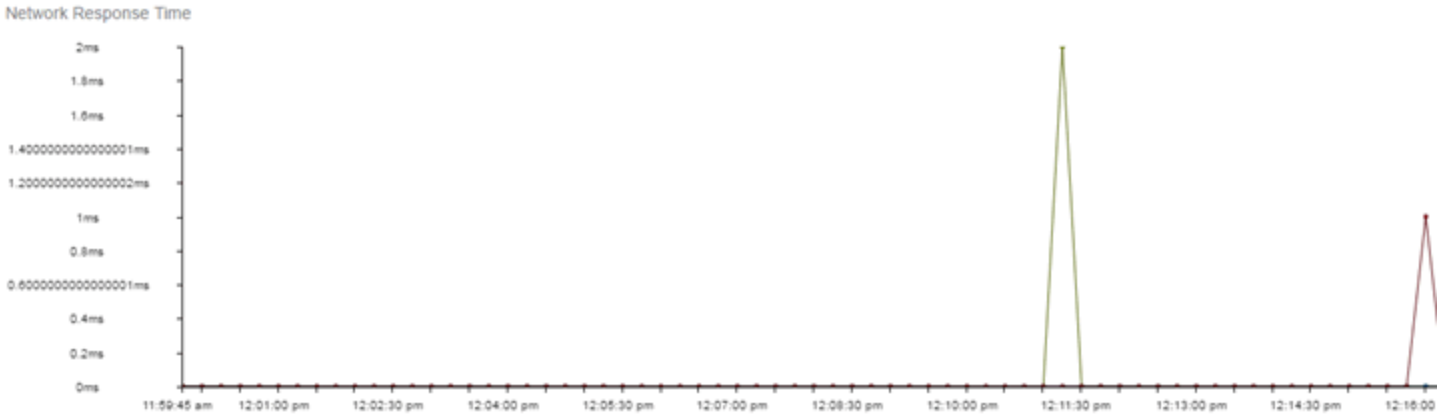
For example, you can configure the graphs to display the top 3 slowest applications by response time as shown in the above screenshot.

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 an 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. 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.



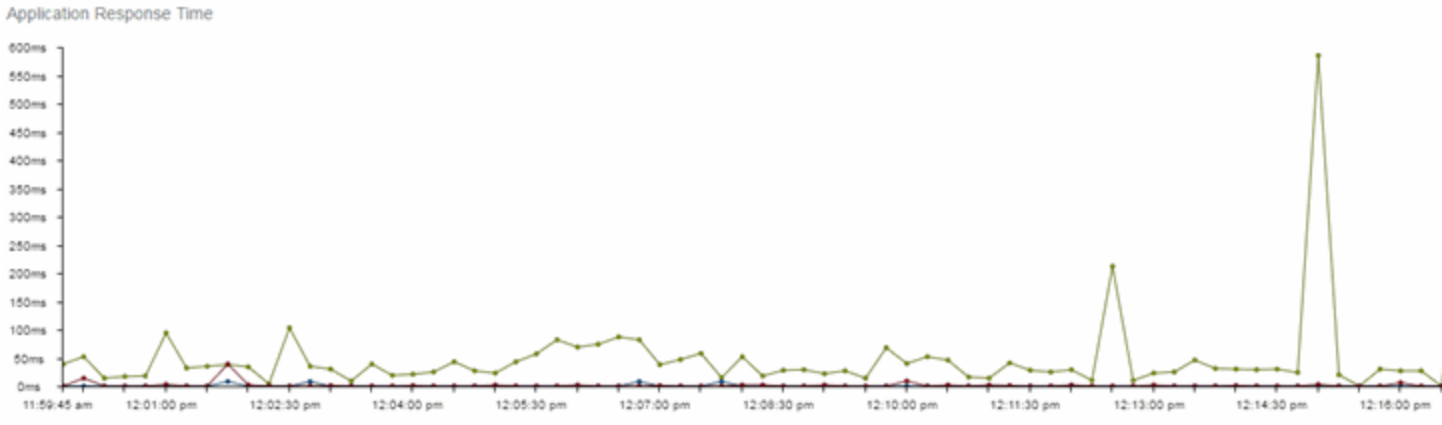
Hover over a point in the graph to see a pop-up with details about that application at that moment in time.

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. 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

For information on related Application Analytics topics:

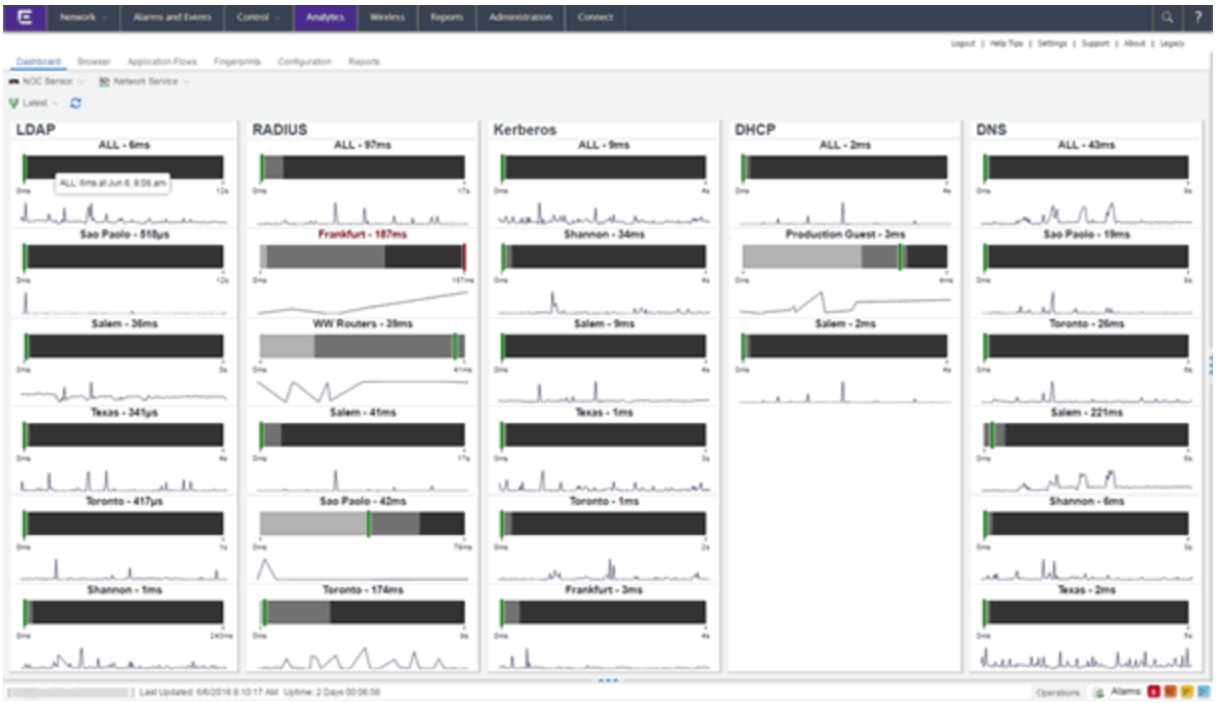
- Analytics
- Getting Started with Application Analytics
- Network Locations

Application Analytics Network Service Dashboard

The Network Service Dashboard displays the performance (in response time) on your network for the following network services:

- LDAP
- RADIUS
- Kerberos
- DHCP
- DNS

To access the Network Service Dashboard, open the Analytics > Dashboard tab and select Response Time in the dashboard drop-down menu.



Overview

The Network Service Dashboard contains two graphs for each network service, 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 ( ).

Use the **Date Range** drop-down menu (Latest) to indicate the date and time range for which data is displayed:

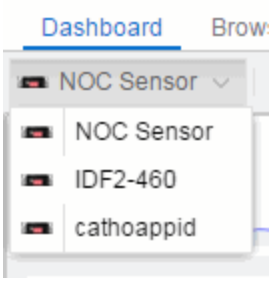
- **Latest** — Displays data for the current day and the previous seven days.
- **Custom** — Displays additional fields allowing you to indicate a **Start Date** and time and an **End Date** and time.

Using the dashboard, Extreme Management Center allows you to view the response time data for these services based on network locations you configure. Data in the dashboard is updated every minute.

Each column in the dashboard represents a service. The top row displays the average response time of all of the locations for that service, while the following rows indicate the top five worst performing locations for that service.

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.

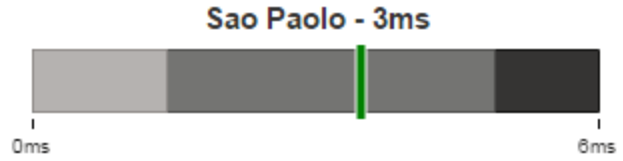
If you have multiple Application Analytics engines, use the **Engine** drop-down menu to select an engine to use as the source for the report data.



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 most recent response time for the network service as well as the date and time the measurement occurred.

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 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).

Hover over a point in the graph to display a pop-up with the date, time, and response time for that point.

This is the data set from which 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

For information on related Application Analytics topics:

- Analytics
- Getting Started with Application Analytics
- Network Locations

Applications Browser

The Applications 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 Management Center Analytics tab.

Viewing Application Analytics application data requires certain prerequisites. For additional information, see Getting Started with Application Analytics.

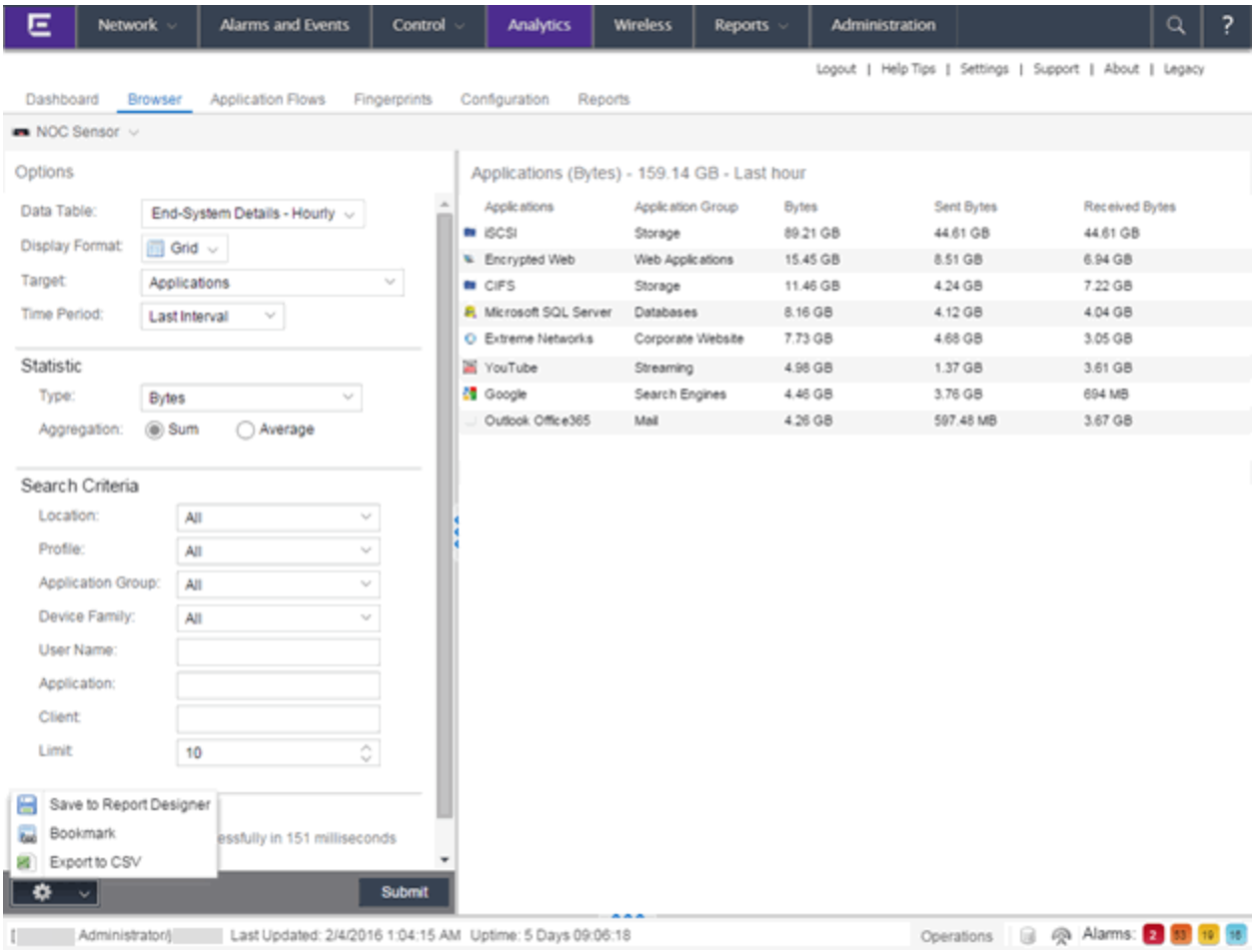
Overview

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 bookmark the report, save it to the Report Designer to use as a custom component, 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 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. 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 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 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 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.

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/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.
- 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. For additional information, see Network Locations.
- 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.
- Sent Bytes — The number of bytes sent by clients.
- 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. For additional information, see Network 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.
- 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 the Report

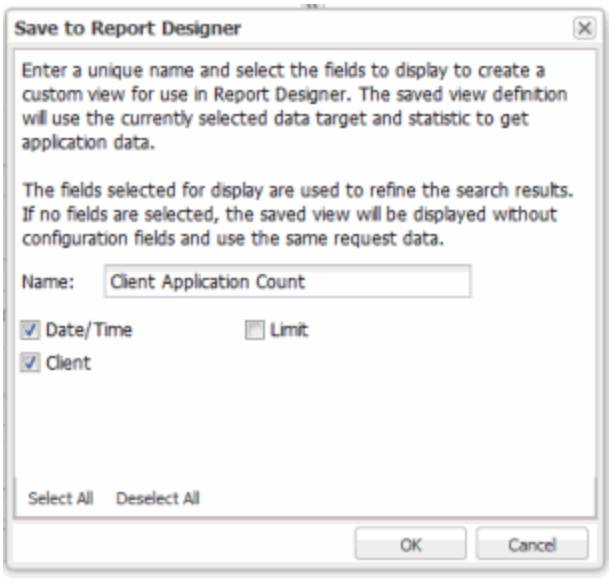
After you have generated a report, click the Gear menu in the lower left corner to save the options you have currently set. A new window opens for the current

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 to export the report data as a CSV file. The currently defined report opens in a spreadsheet, which can then be saved.

Related Information

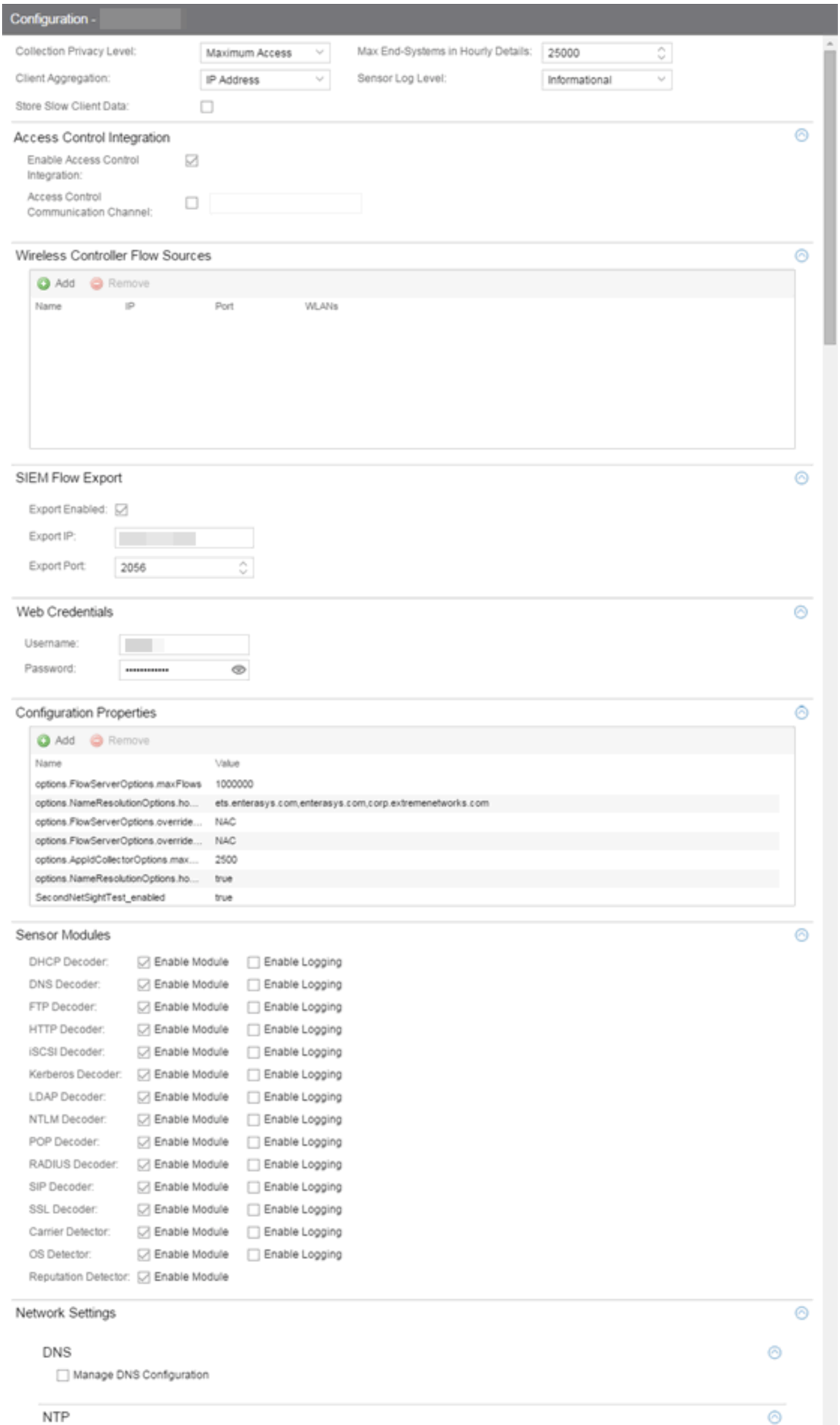
For information on related Application Analytics topics:

- Analytics
- Getting Started with Application Analytics
- Network Locations

Application Analytics Engine Advanced Configuration

The Advanced Configuration panel lets you configure advanced options for the selected Application Analytics engine. To access this panel, select the Configuration view in the Analytics tab in the Extreme Management Center. In the left-panel tree, expand an engine and select Configuration.

If you make any changes in this window, be sure to click Save and then enforce the engine.


Configuration -
Collection Privacy Level:
Maximum Access
Max End-Systems in Hourly Details:
25000
Client Aggregation:
IP Address
Sensor Log Level:
Informational
Store Slow Client Data:
Access Control Integration
Enable Access Control Integration:
Access Control Communication Channel:
Wireless Controller Flow Sources
Add
Remove
Name
IP
Port
WLANs
SIEM Flow Export
Export Enabled:
Export IP:
Export Port:
2056
Web Credentials
Username:
Password:
Configuration Properties
Add
Remove
Name
Value
options.FlowServerOptions.maxFlows
1000000
options.NameResolutionOptions.ho...
ets.enterasys.com,enterasys.com,corp.extremenetworks.com
options.FlowServerOptions.override...
NAC
options.FlowServerOptions.override...
NAC
options.AppIdCollectorOptions.max...
2500
options.NameResolutionOptions.ho...
true
SecondNetSightTest_enabled
true
Sensor Modules
DHCP Decoder:
DNS Decoder:
FTP Decoder:
HTTP Decoder:
iSCSI Decoder:
Kerberos Decoder:
LDAP Decoder:
NTLM Decoder:
POP Decoder:
RADIUS Decoder:
SIP Decoder:
SSL Decoder:
Carrier Detector:
OS Detector:
Reputation Detector:
Enable Module
Enable Logging
Network Settings
DNS
Manage DNS Configuration
NTP

Collection Privacy Levels

Collection privacy level settings restrict the amount of identifying information that is collected by the Application Analytics engine and displayed in the Application Information column of the Application Flows report. (Access this report from the **Analytics** tab. In the Application Flows report, hover over the Application Information column to view the collected information.) This information is also displayed in the Flow Summary window.

This allows you to protect the end user's identifying information from being viewed by IT staff with access to the Application Flows report. The default privacy level allows maximum access to the information. Increasing the privacy level allows you to restrict the information that is collected and displayed.

There are three privacy levels. For all three levels, passwords are **not** collected or displayed.

- Maximum Access — The Application Analytics engine collects both identifying information and sensitive information. The information displays in the Application Information column.
- Medium Privacy — The Application Analytics engine collects identifying information, but not sensitive information. Identifying information displays in the Application Information column.
- Maximum Privacy — The Application Analytics engine does not collect identifying information or sensitive information. Information does not display in the Application Information column.

Identifying information is data that identifies the end user, such as a username. The Application Analytics engine collects identifying information when the privacy level is set to Maximum Access or Medium Privacy.

Sensitive information is data an end user may not want to share, such as the caller ID or contact information from an end user's SIP voice call. The Application Analytics engine collects sensitive information when the privacy level is set to Maximum Access.

Client Aggregation

This field determines how client information is aggregated by the Application Analytics engine, either by **IP Address** or **MAC Address**.

Slow Client Data

Select Enabled in the drop-down menu to collect additional information about clients with poor response times by the Application Analytics engine.

Max End-Systems in Hourly Details

Enter the maximum number of client end-systems stored in the Management Center database for the Application Analytics engine. This ensures your client limit is not collected from one engine. Once the value set in this field is met, additional end-system data is not collected from the engine.

Sensor Log Levels

The Application Analytics sensor runs on the Application Analytics engine and inspects network traffic to identify applications and other information. The sensor log file records diagnostic information about sensor operations, which is useful for troubleshooting engine issues.

In the Configuration view, you can enable different levels of logging for the selected engine. Each logging level is inclusive of the levels above it. The five levels are:

- Informational
- Debug
- Verbose Debug
- Trace
- All

The sensor log level should be set to Informational unless you are troubleshooting an engine issue. When troubleshooting an issue, Extreme Networks Support may ask you to change the logging level to provide additional information.

To view the log file directly, log into the engine and navigate to the file /opt/appid/logs/appid.log.

You can also use the engine administration web page to view the sensor log. Access the web page using the following URL: https://<EngineIP or

hostname>:8443/Admin. The default user name and password is "admin/Extreme@pp." Once you have accessed the web page, navigate to the Log Files/Sensor Log page.

Access Control Integration

If your network configuration includes Access Control, Access Control data can be integrated with flow data to provide additional information. Access Control integration is only useful if you are collecting flows for end-systems managed by Access Control. For additional information, see Enabling Extreme Access Control Integration.

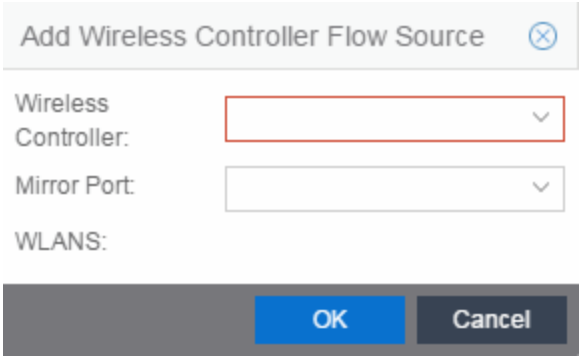
- To enable Access Control Integration for the engine, select the **Enable Access Control Integration** checkbox.
- If your Access Control engines are using Communication Channels, select the **Access Control Communication Channel** option and enter the channel name. The Application Analytics engine is only able to access end-systems in its channel.

Wireless Controller Flow Sources

This section displays the Wireless Controllers set up as flow sources in Application Analytics.

To add a Wireless Controller as a flow source:

1. Click the **Add** button.
   The Add Wireless Flow Source window opens.



2. Select a **Wireless Controller** from the drop-down menu.

NOTES: Only Wireless Controllers that support Application Analytics and have available L2 ports are listed.
Selecting a Wireless Controller set up as part of a controller pair automatically selects the paired Controller.

3. Select an available L2 port for mirroring in the Mirror Port drop-down menu.
4. Select a mirror port for the Paired Controller, if necessary.
5. Select the appropriate WLANs, if necessary.
6. Click OK.
7. Verify the L2 ports selected for mirroring are monitored by Application Analytics.

The configuration is complete.

To remove a Wireless Controller as a flow source, select a Controller in the Wireless Controller Flow Sources section of the window and click the Remove button.

Web Credentials

Enter a new Username and Password for web service requests between the Management Center server and the Application Analytics engine. Click the Show Password check box to display the Password field unencrypted.

NOTE: By default, the **Username** and **Password** are **admin** and **Extreme@pp**, respectively.

Configuration Properties

Use this section to add properties that provide a solution for a specific problem or task. These properties are supplied directly by Extreme Networks Support. Contact Extreme Networks Technical Support for guidance on using this section.

Sensor Modules

The Application Analytics sensor uses sensor modules to analyze different types of network traffic. For example, the HTTP decoder decodes HTTP traffic to

acquire data needed to match fingerprints against that traffic.

In most cases, it is best to leave the decoders and detectors enabled. For better sensor performance, you can disable decoders for traffic rarely seen on the network; however, doing so prevents some fingerprints from triggering.

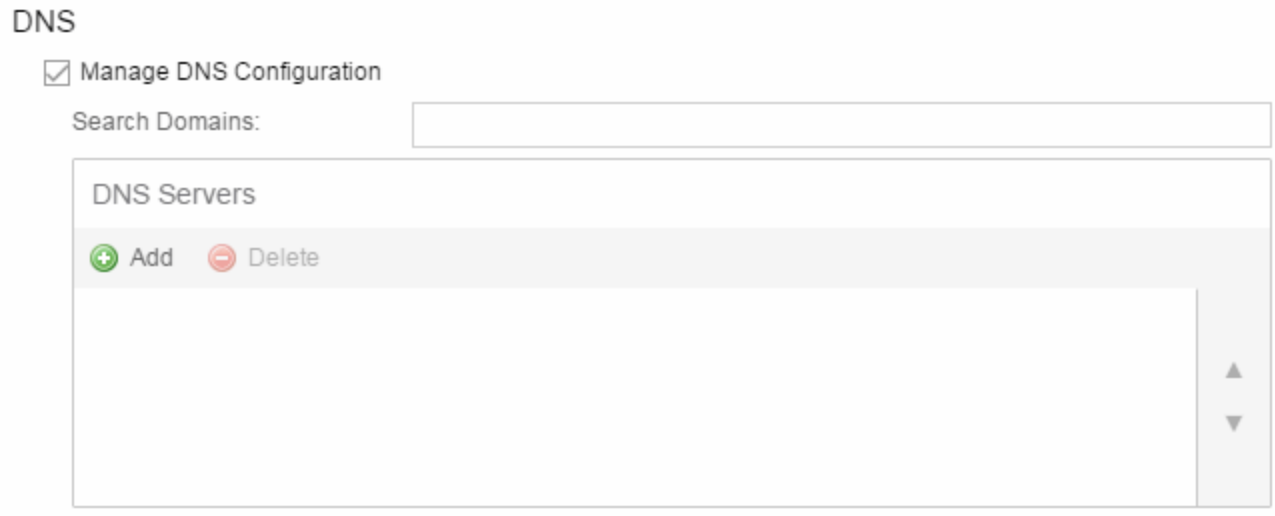
You can enable logging for any of the decoders and detectors for debugging purposes. As logging can impact disk space and performance, you should turn it on only for troubleshooting purposes. Do not enable logging during normal operation.

Network Settings

The Network Settings section of the window allows you to configure the network settings on an Application Analytics engine. Selecting a checkbox opens a new section from which you can configure the options for the setting. Click the Save button and the bottom of the panel to save your changes.

DNS

Select the Manage DNS Configuration checkbox to open the DNS Servers area. This allows you to enter a search domain or add or remove search domains and DNS server IP addresses.



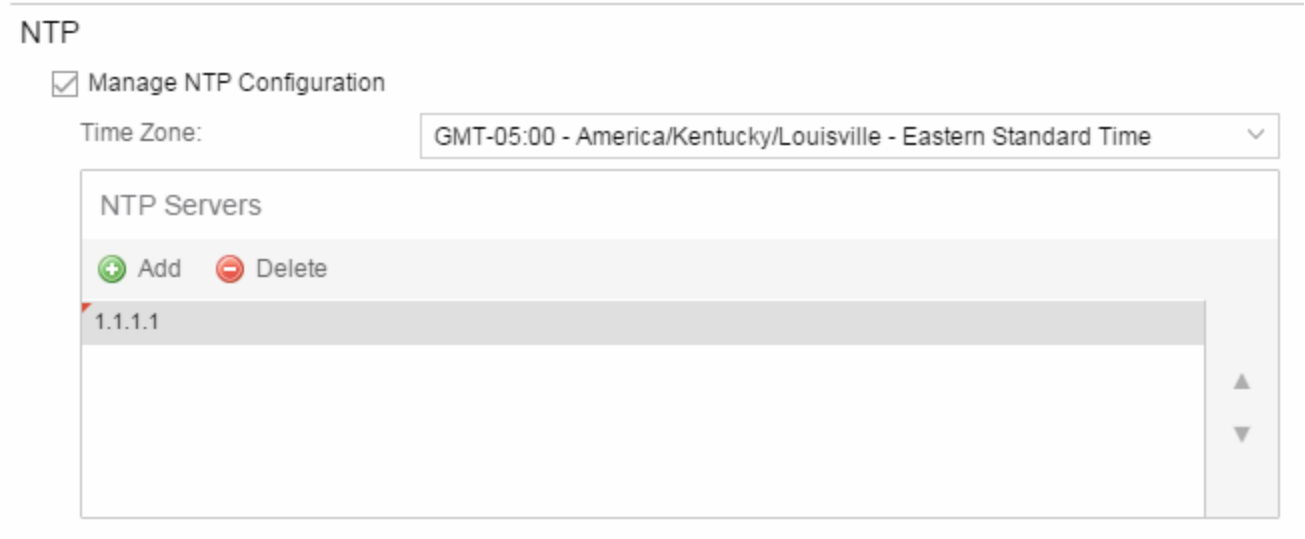
Search Domains
: A list of search domains used by the Application Analytics engine when doing lookups by hostname. When an attempt to resolve a hostname is

made, these domain suffixes are appended to the hostname of the device. For example, if someone does a ping to server1, Application Analytics 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 Application Analytics engine sends DNS lookups to for name resolution. The list is used by both hostname resolution and by the DNS proxy. Click the **Add** button to open a blank box in which you can enter an IP address. Select an IP address in the table and click the **Delete** button to remove an IP address. You can enter multiple servers for redundancy. Use the **Up** and **Down** arrows to list the servers in the order they should be used.

NTP

Select the **Manage NTP Configuration** checkbox to open the NTP (Network Time Protocol) Servers area. NTP configuration is important for protocols such as SNMPv3 and RFC3576 which incorporate playback protection. In addition, having accurate time configured on the Application Analytics engine is essential for event logging and troubleshooting.

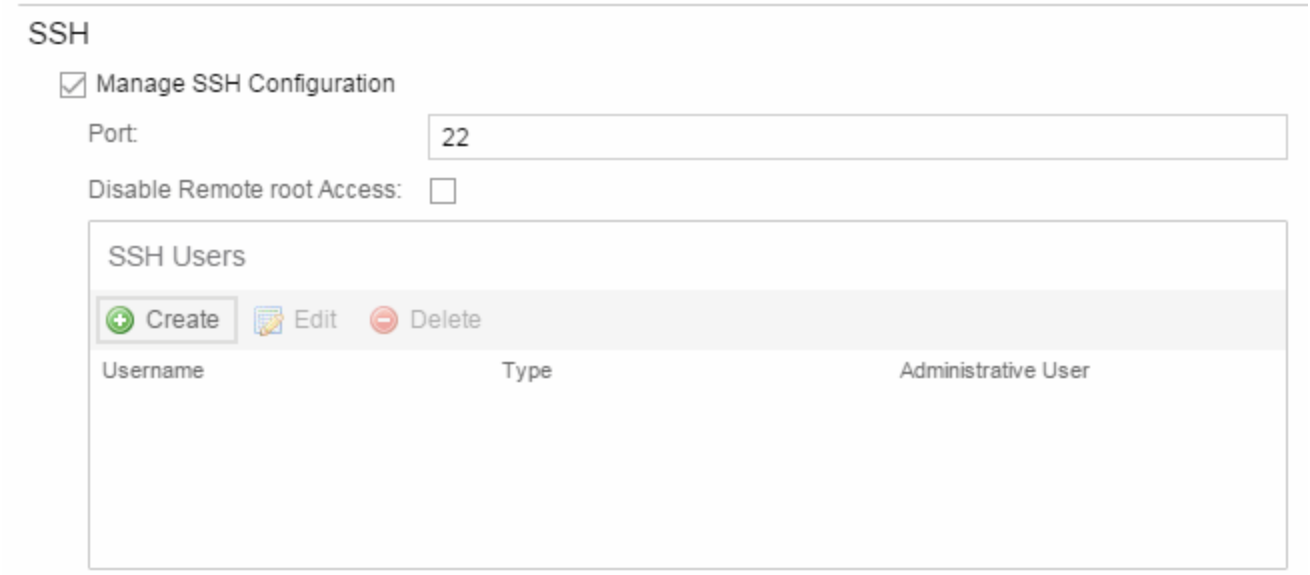


Time Zone
: Select the appropriate **Time Zone** from the drop-down menu to allow Application Analytics to manage date/time settings.

NTP Servers
: A list of NTP servers. You can enter multiple servers for redundancy. Click the **Add** button to open a blank box in which you can enter an IP address. Select an IP address in the table and click the **Delete** button to remove an IP address. Use the **Up** and **Down** arrows to list the servers in the order they should be used.

SSH

Select the **Manage SSH Configuration** checkbox to open the SSH Users area. SSH configuration provides additional security features for the Application Analytics engine.



Port
: The port field allows you to configure a custom port 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:

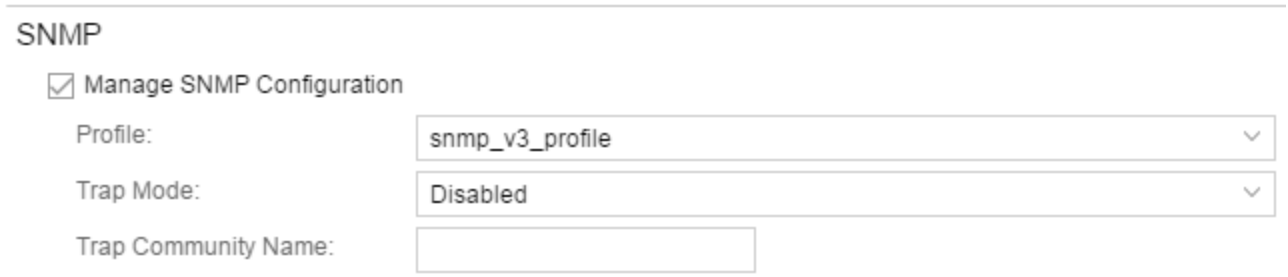
sshd[19735]: Accepted password for <username> from 10.20.30.40 port 36777 ssh2
su[19762]: + pts/2 <username>-root

Enabling this option does not disable root access via the console. Make sure that you don't disable root access unless you have configured RADIUS authentication or this disables remote access to the Application Analytics engine.

SSH Users
Use the toolbar buttons to create a list of users allowed to log in to the Application Analytics engine using SSH. Click the **Add** button to open a blank box in which you can enter an IP address. Select an IP address in the table and click the **Delete** button to remove an IP address. 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.

SNMP

The SNMP configuration section allows you to deploy SNMP credentials for the Application Analytics engine. The credentials can include different read/write credentials, for example, use "public" as the read credential and "private" as the write credential. In addition, basic host traps can be enabled from the Application Analytics 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 Application Analytics engine.

Trap Mode
Use the drop-down menu to set the trap mode.

Trap Community Name
: Enter the trap community name.

Related Information

For information on related Application Analytics topics:

- Analytics
- Enabling Extreme Access Control Integration

Wireless

The **Wireless** tab in Extreme Management Center (formerly NetSight) 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. Additionally, the Menu at the top of the screen provides links to additional information about your version of 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. 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 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

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.

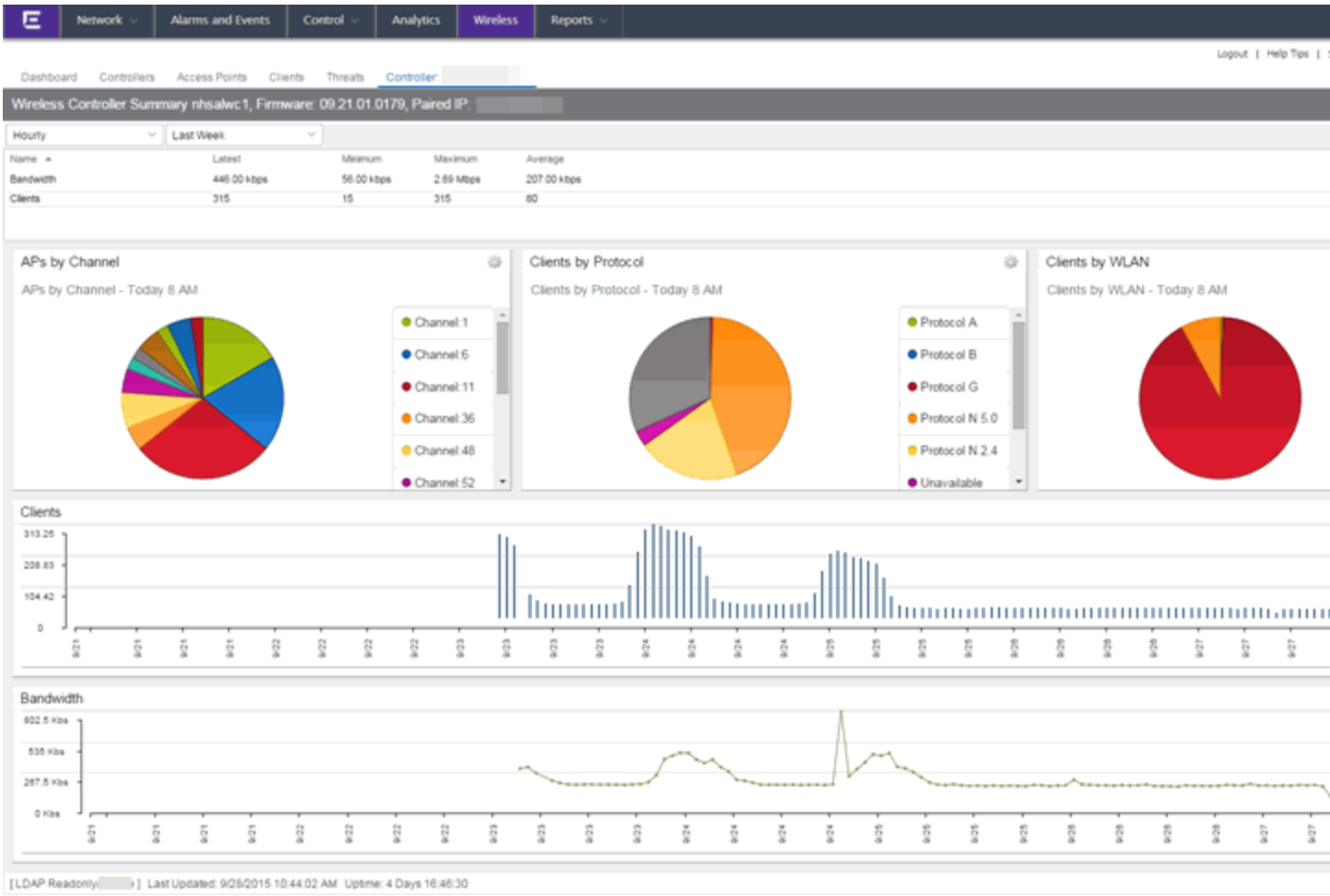
Select **Discover All Controllers** in the **Tools** menu at the bottom of the tree panel to perform a discover operation that looks for any configuration changes on your wireless controllers with device statistics collection enabled. In addition, you can select **Discover Controller** to rediscover 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 **Gear** menu 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 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

Select a client or client event in the report tables and use the **Gear** menu 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 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.

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

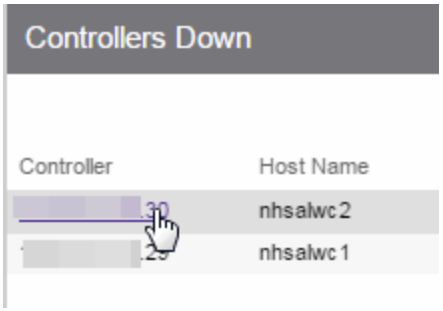
The **Reports** tab allows you to view information about the APs, controllers, and wireless traffic on your network. Available reports are accessible via the **Reports** drop-down menu at the top of the tab.

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.

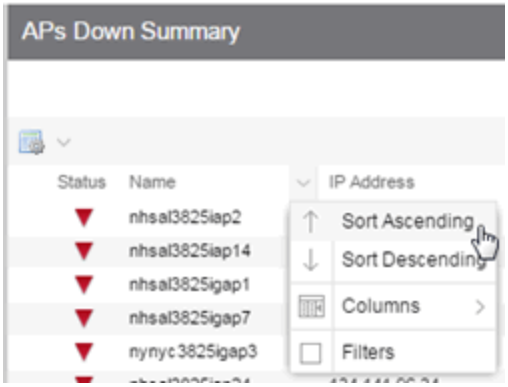
Report Features

Management Center reports include the following features (depending on the report selected):

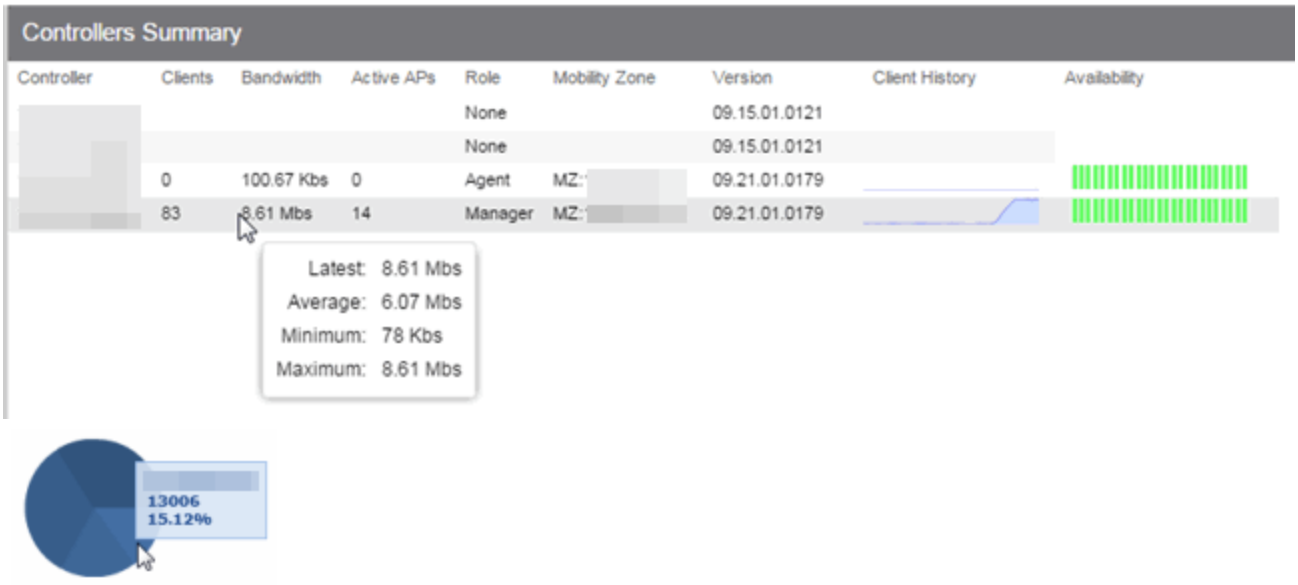
- **Drill-down for Details** — Link to summary reports containing more detailed information. For example, in the Controller Summary report, clicking on a controller shows a detailed report for that controller over time.



- 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 Management Center topics:

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

Extreme Management Center Reports

Extreme Management Center (formerly NetSight) Reports 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 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 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 at the top of the screen provides links to additional information about your version of 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 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 Management Center Suite-Wide Tools > Authorization Device Access.

To collect data in your 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:

- Access Control — Provides an overview of end-system connection information. You can also see these reports and others on the Control tab.
- Access Control Health — Provides reports on end-system assessment and state information. In the Risk Level pie chart, click on a pie section to open a filtered end-system grid for more detailed information about end-systems at that risk level.
- 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 Management Center engines, Linux systems, and Windows PCs. For more information, click the Info button ( ) 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 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 ⓘ 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.

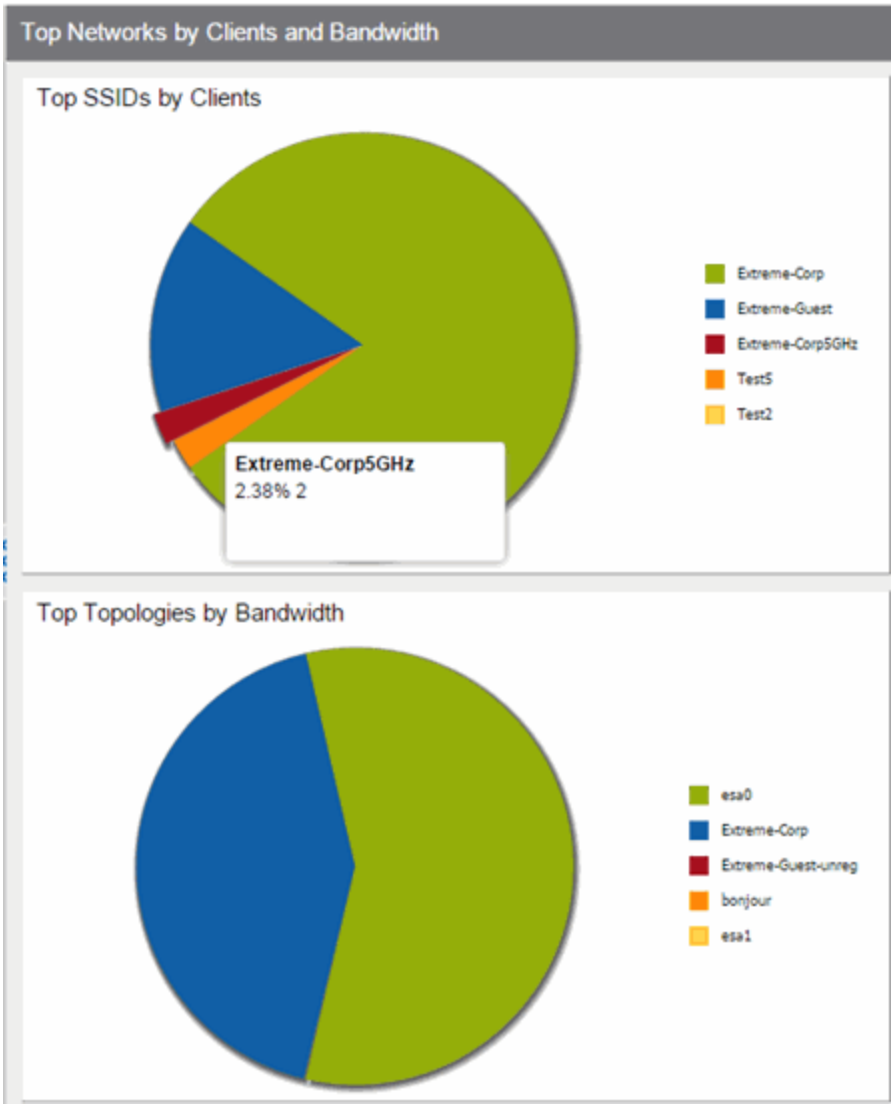
Once a report is created, it is available from the Reports tab.

For instructions on creating a custom report, see How to Use the Report Designer.

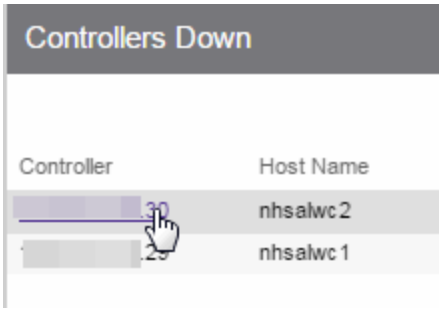
Report Features

Management Center reports include the following features (depending on the report selected):

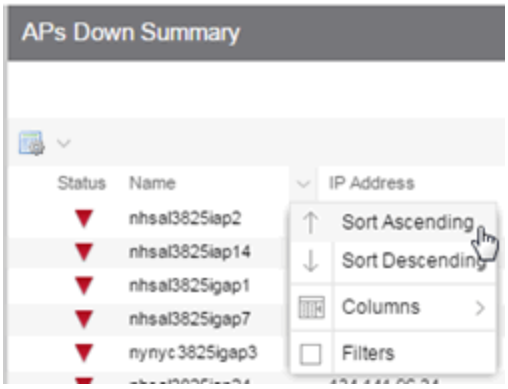
- Mouse Over for Info — Mouse over a pie section to display the name of the segment, the percentage represented by the segment and the number of elements. for some reports, clicking on a pie section opens a filtered end-systems grid for more detailed information.



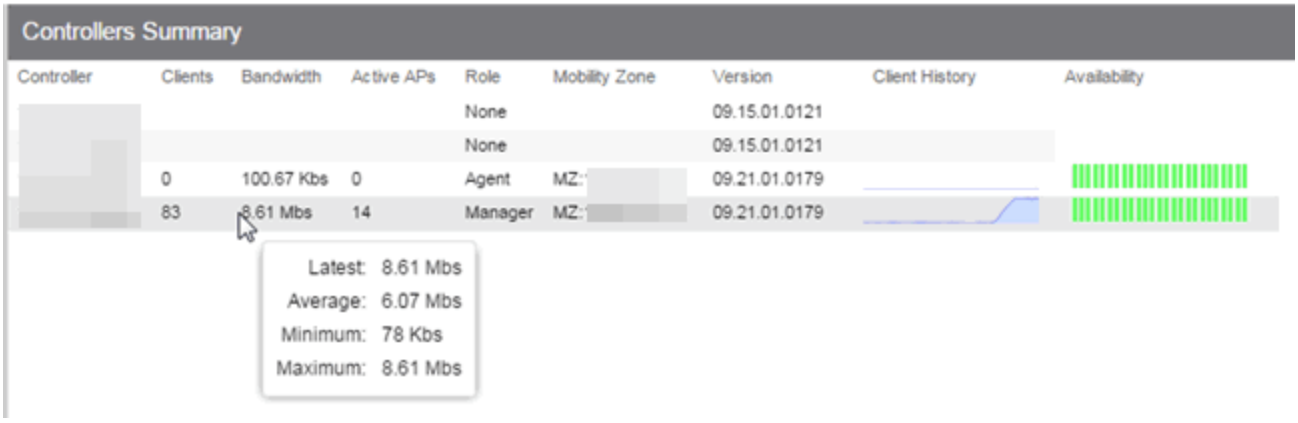
- Drill-down for Details — Link to summary reports containing more detailed information. For example, in the Controller Summary report, clicking on a controller shows a detailed report for that controller over time.



- 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

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 Management Center OneView > Access OneView and NetSight OneView > Access OneView Administration capabilities.

This Help topic provides the following information:

Creating a Report

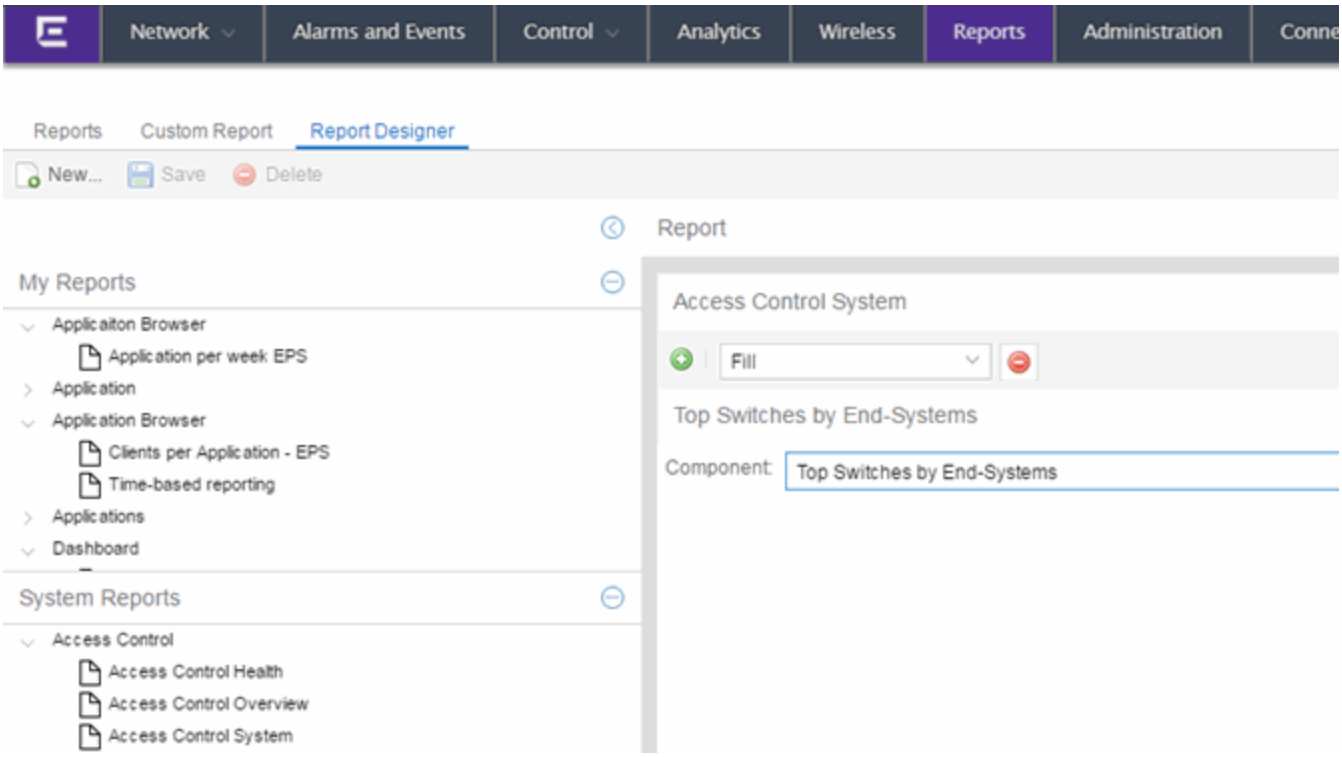
There are two ways to create a report. You can create a report by customizing an existing dashboard report (system report) or by creating a new report based on a selection of individual components.

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 Management Center where that report is used.

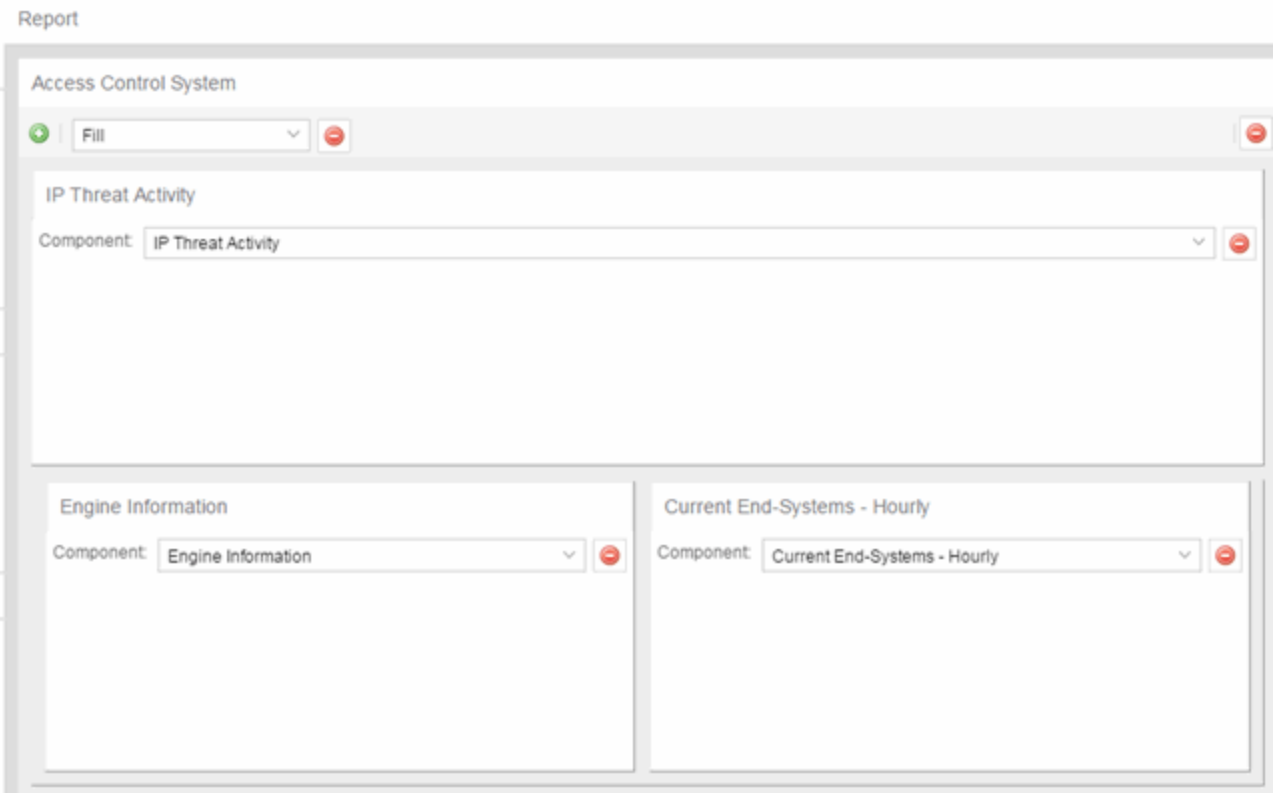
For example, you want to delete some of the dashboard panels and change some of the dashboard components in the Access Control System report.

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, Access Control > Access Control System report is selected. (Use the scroll bar to view the complete list of available reports.) The report becomes available to edit in the right panel.



3. Change the report:
   a. 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.



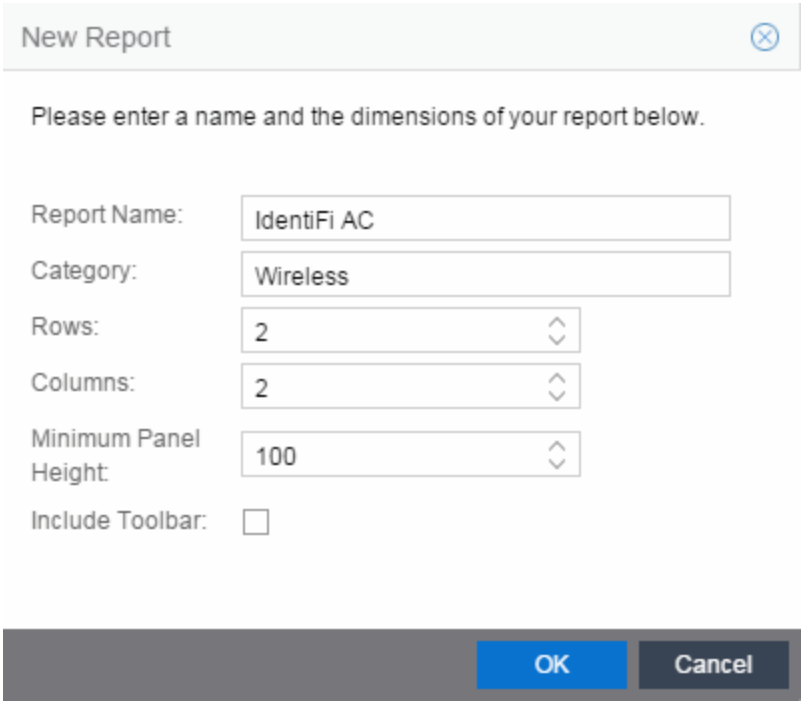
4. Once you have finished making changes to the report, click the **Save** button. The report is populated with data and displayed in a new tab as a way to preview the report. The name of the customized report is added to the My Reports section.

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.

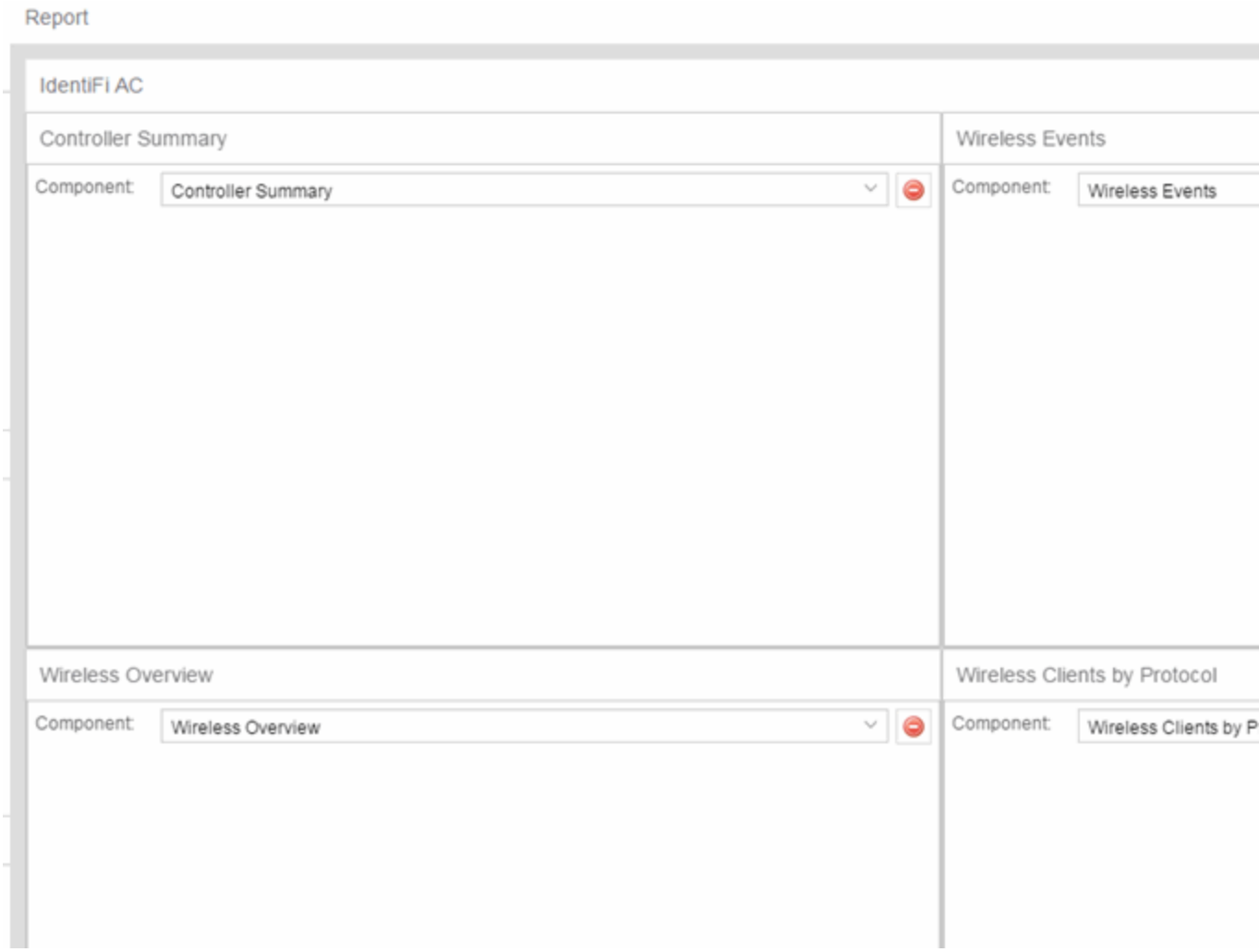
Create a New Report

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

Administration

Extreme Management Center's Administration tab provides diagnostic reports and tools to monitor, maintain, and troubleshoot the application and its components. There are six sub-tabs: Scheduler, Scripting, Profiles, Users, Options, and Diagnostics. For information about each tab, see each section below.

Additionally, the Menu at the top of the screen provides links to additional information about your version of Management Center (formerly NetSight).

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, see How to Configure User Access to Extreme Management Center applications and Extreme Management Center Access Requirements.

This Help topic provides information on the following sub-tabs:

- Scheduler
- Scripting
- Profiles
- Users
- Options
- Backup
- Diagnostics

Scheduler

Scheduler provides the ability to schedule automatic generation of a subset of available Extreme Management Center reports in PDF format. Report generation can be scheduled to occur on an hourly, daily, weekly, or monthly basis. When a report is generated, it is then automatically emailed to a specified recipient. For additional information, see How to Schedule a Task.

NOTE: For the email notification to work, configure your SMTP Email Server options. Click the **SMTP** button to open the SMTP E-Mail 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 with having to change the scheduled run times. This facilitates the testing of scheduled tasks.

Access the Scheduler event log from the Alarms and Events tab, which includes task execution events and errors.

Scripting

Scripting functionality is built in to Extreme Management Center and Management Center provides you with predefined scripts and allows you to create your own.

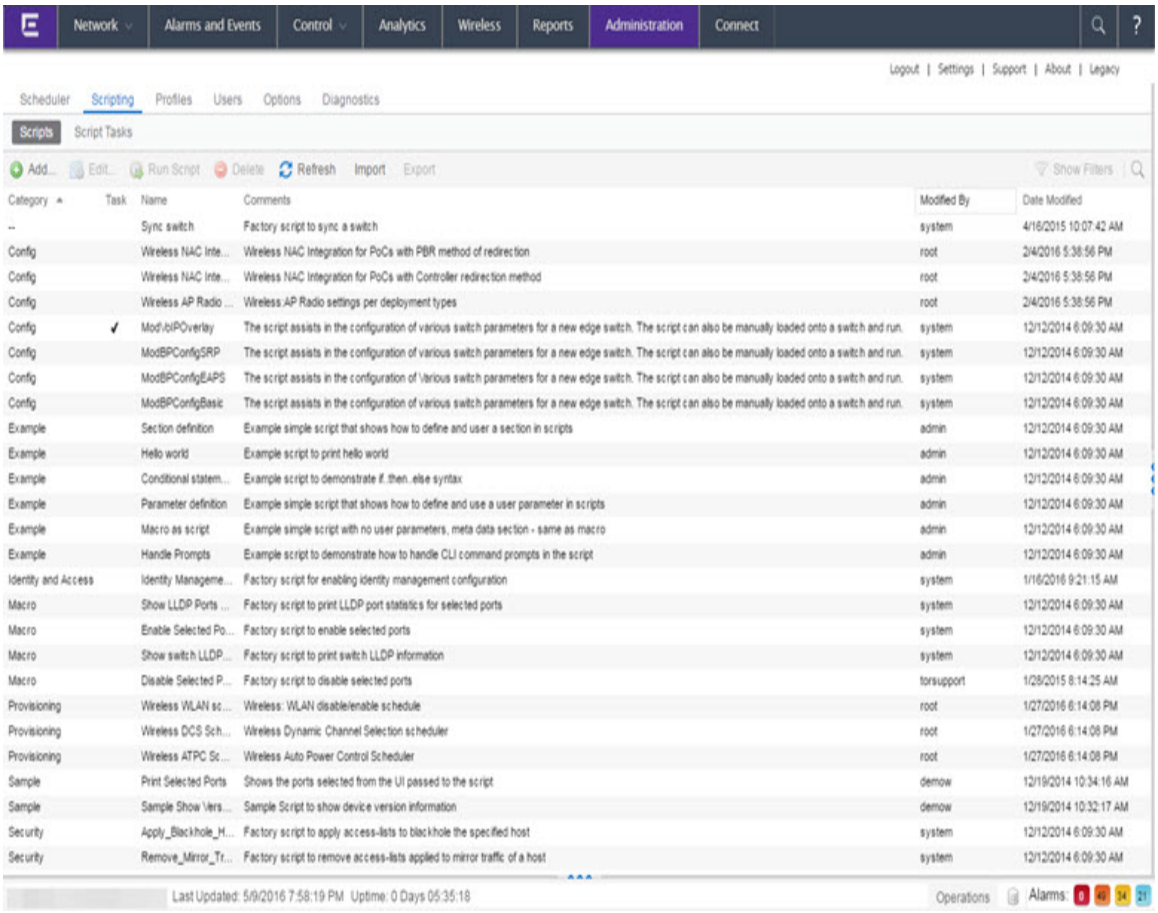
Extreme Management Center Script Overview

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.

Scripts tab

To display the scripts configured in Management Center, open **Administration > Scripting**. Click the **Scripts** subtab.



The **Scripts** tab contains the following information:

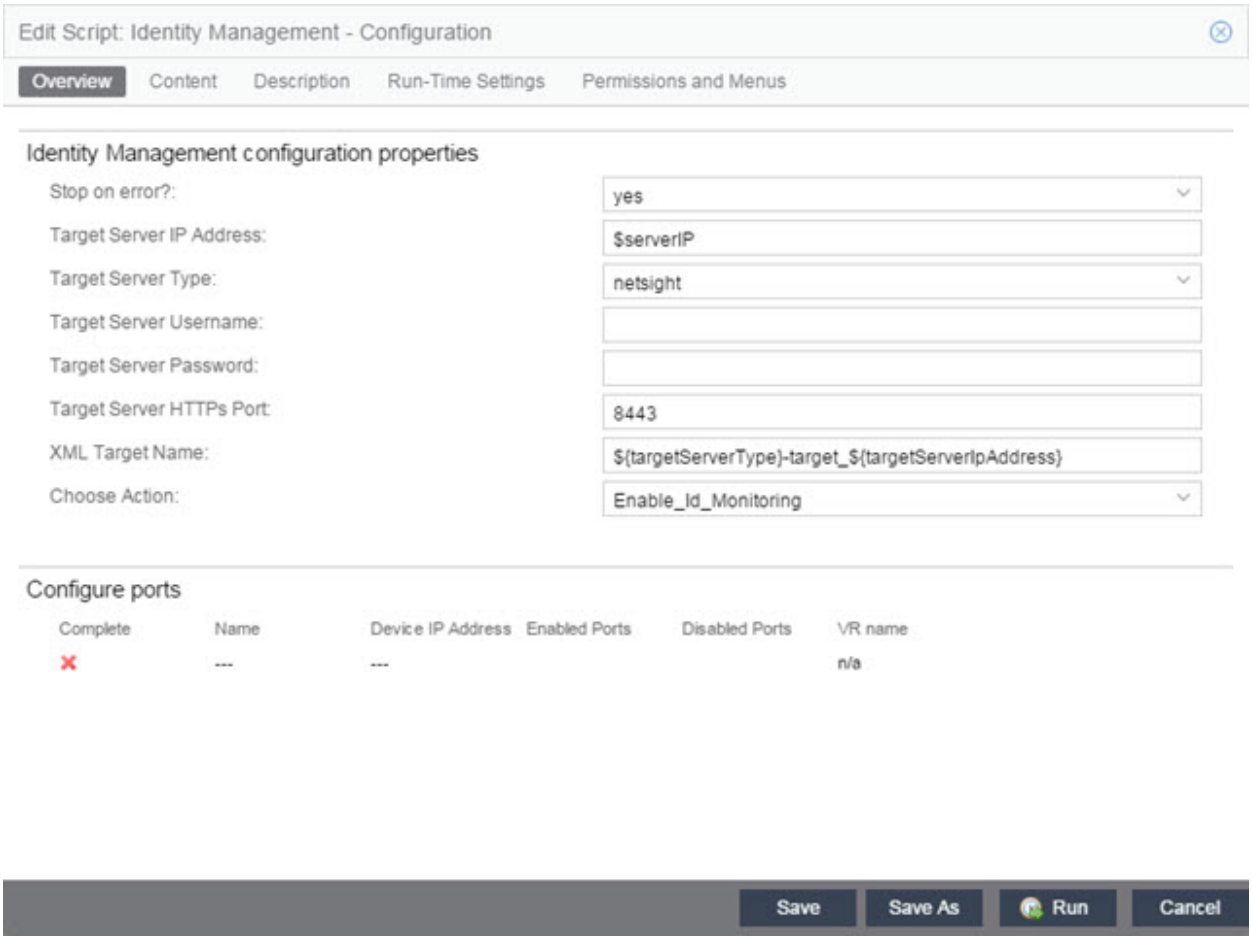
- **Category** — The script category, if configured.
- **Task** — Indicates whether the script is used in a scheduled task.
- **Name** — The name of the script.
- **Comments** — Comments or a description of the script.
- **Modified by** — Who last modified the script.
- **Date Modified** — When the script was last modified.

The **Script Tasks** tab contains the following information:

- **Scheduled** — Displays a checkmark, if this is a scheduled task.
- **Category** — The script category, if configured.
- **Name** — The name of the script task.
- **User Name** — Who created the script task.
- **Script Name** — The name of the script run by the script task.

- **Comment** — Comments or a description of the script task.
- **Date modified** — When the script was last modified.

Double-click a script to open the script editor dialog.



For additional information, see How to Create Scripts.

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, 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 that are required to be granted access.

For additional information, see Profiles tab.

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.

For additional information, see Users tab.

Options

Extreme Management Center options allow you to configure the behavior of Management Center. These options apply across all 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:

- Access Control Options
- Alarm Options
- Alarm/Event Logs and Table Options
- Compass Options
- Database Backup Options
- Extreme Management Center Server Health Options
- ExtremeNetworks.com Updates Options
- FlexView Options
- Inventory Manager Options
- Name Resolution Options

- NetFlow Options
- Network Monitor Cache Options
- OneView Options
- OneView Collector Options
- OneView Engine Options
- Policy Manager Options
- Port Monitor Options
- SMTP E-Mail Options
- SNMP Advanced Options
- Services for Extreme Management Center Server Options
- Status Polling Options
- Syslog Options
- TopN Collector Options
- Trap Options
- Web Server Options
- Wireless Manager Options

Backup

The Backup tab allows you to configure the URL and password for the database as well as perform database backup and restore operations. For additional information, see Backup.

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 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>/NetSight/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 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>/NetSight/appdata/logs/server.log file on the 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.
        - Log4j File Override — Sets the level to the level specified in the log4j.properties 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 Management Center reporting database. This allows you to reset 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

Related Information

For information on the other Management Center tabs:

- Alarms and Events
- Devices
- Reports
- Wireless

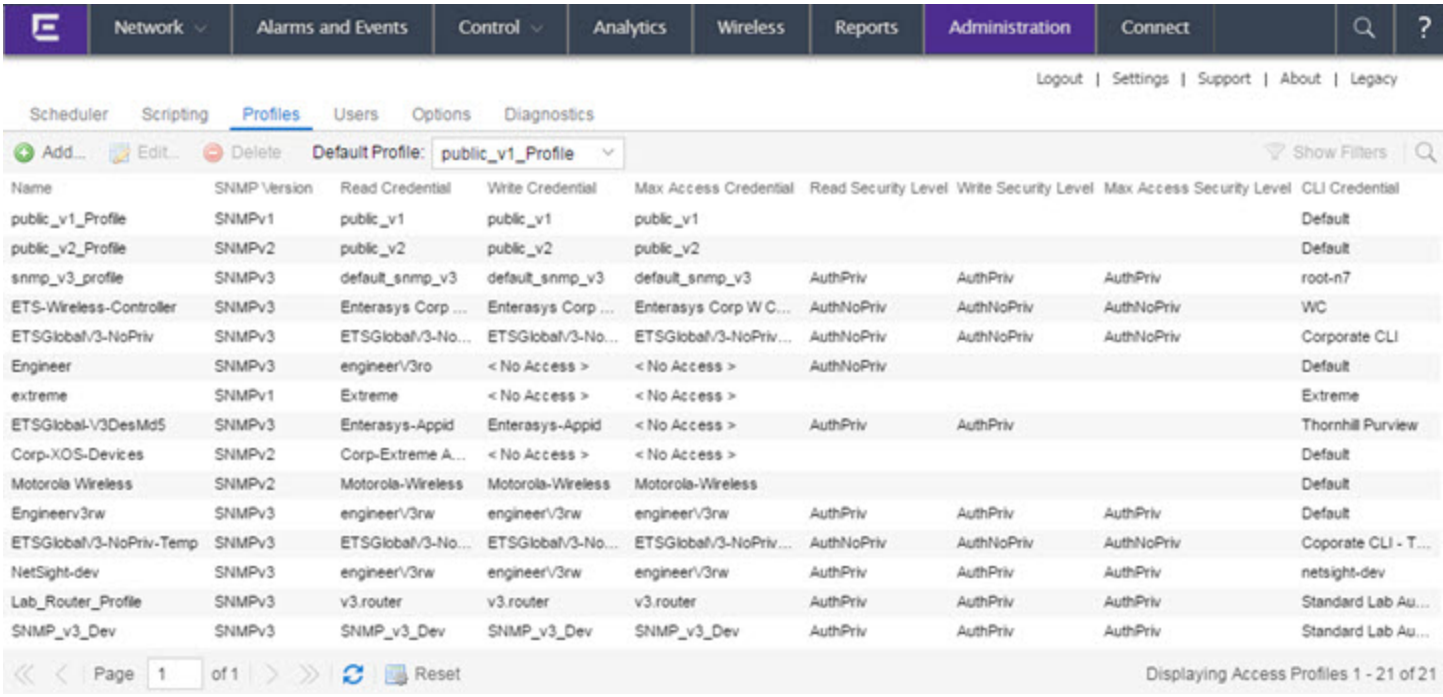
Profiles

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 command line interface (CLI).
- Profiles — Profiles are assigned to device models in the 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.

Name

This is the name assigned when the profile is created. The public_v1_Profile is automatically created during 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.

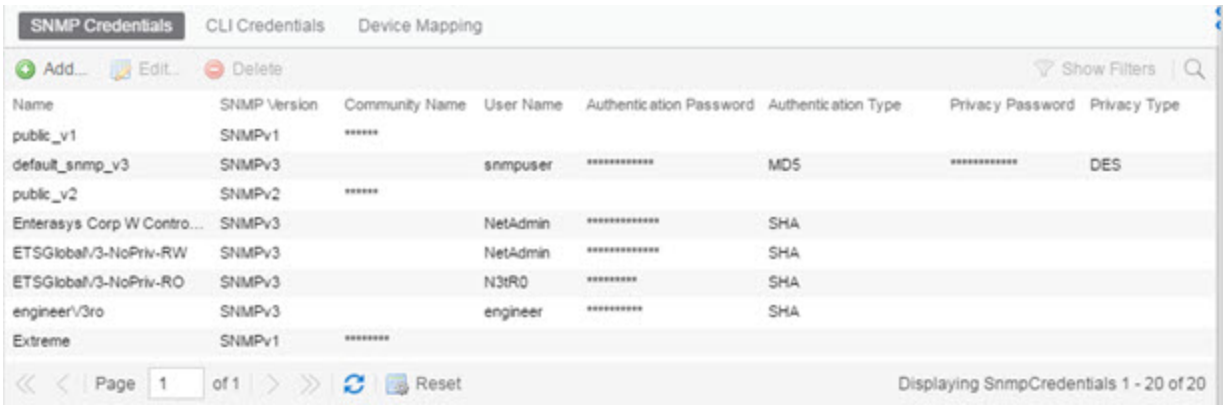
Add Button
: Opens the Add/Edit Profile window where you can select the SNMP version and define the profile name and passwords/community names used by the profile.

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.



Name
: This column lists names assigned to credentials created in the 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.

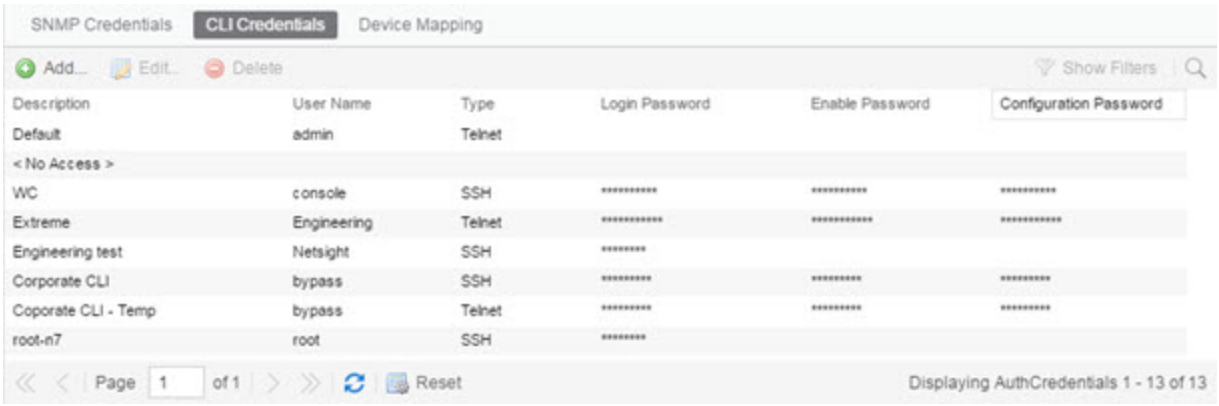
Add Button
: Opens the Add/Edit SNMP Credential window where you can define new SNMP credentials.

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.

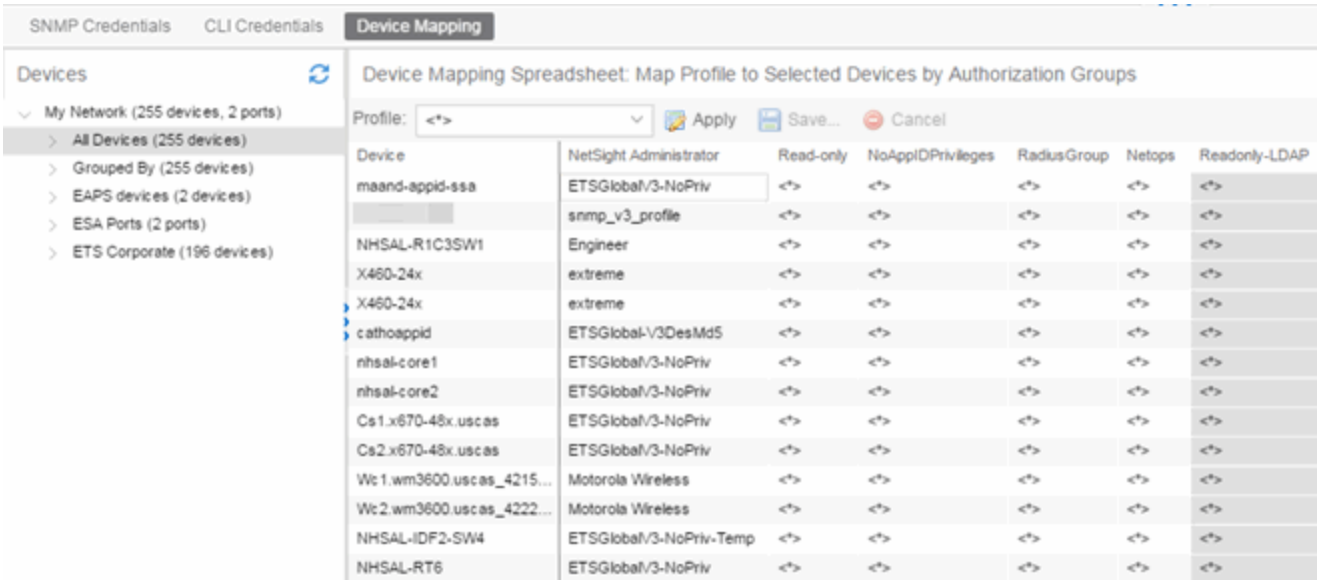
Add Button
: Opens the Add/Edit CLI Credential window where you can define a new CLI credential.

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.



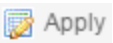
Device Tree

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 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 

Sets the profile selected in the **Profile** drop-down menu as the profile for the Authorization Groups selected in the table.

Save Button 

Saves your changes on the device or devices selected.

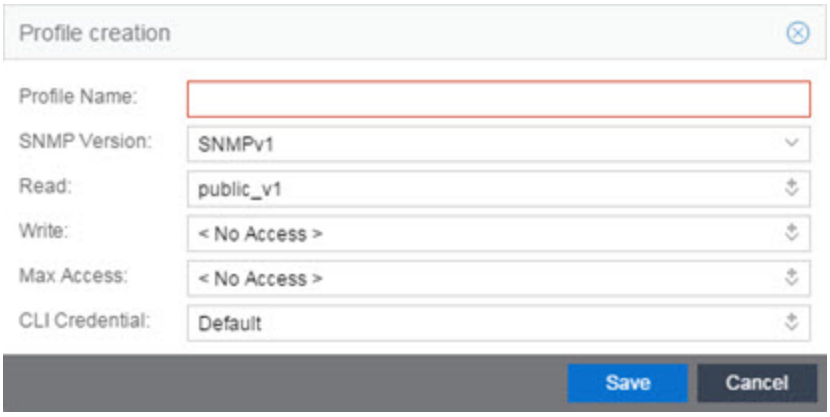
Cancel Button 

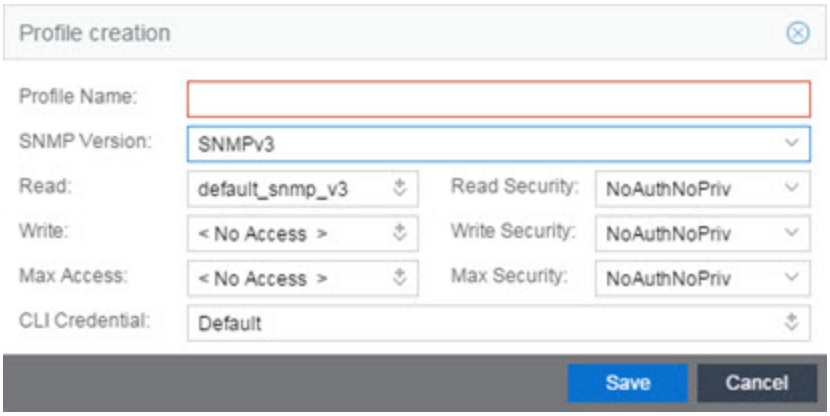
Discards your unsaved changes.

Add/Edit Profile Window

This window lets you select the SNMP and CLI Credentials for a new profile or modify the credentials for an existing profile.

NOTE: When configuring profiles for ExtremeWireless Controllers, ensure the controllers are discovered using an SNMPv2c or SNMPv3 profile. This profile must also 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:

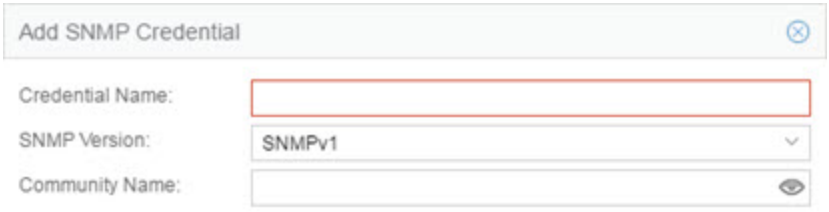
- AuthPriv — Highest security level requiring authentication and privacy (encrypted information).
- AuthNoPriv — Requires authentication, but unencrypted information.
- NoAuthNoPriv — Neither authentication nor privacy required.

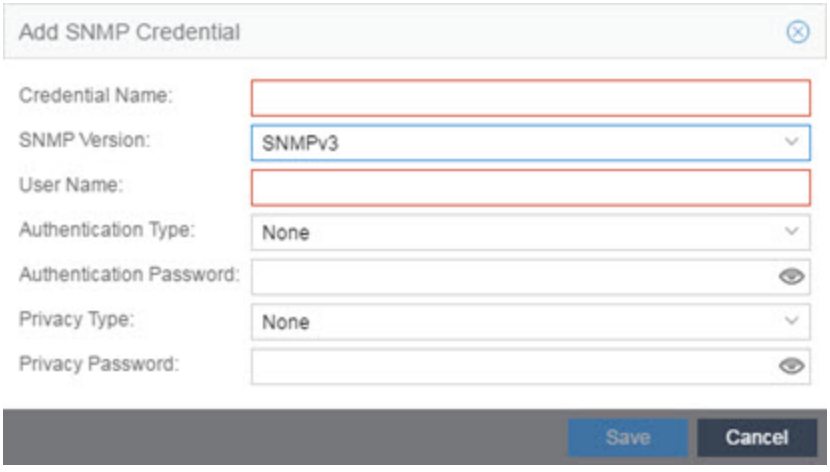
CLI Credential

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.

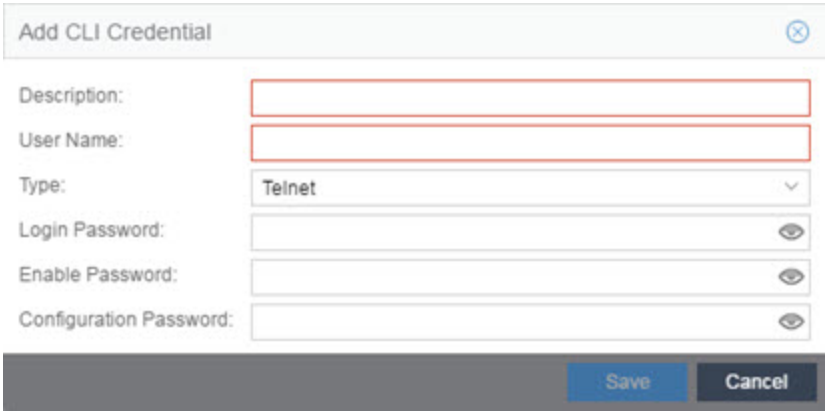
Privacy Type
: For SNMPv3 credentials, select DES or None from this drop-down menu.

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.

Eye icon
: When this icon is selected, passwords and community names appear as text. The default setting for this option is unselected and passwords and community names appear as a string of asterisks.

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.
- Enable — The password for entering Enable mode.
- Configuration — The password for entering Configure mode.

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.

Eye icon
: When this icon is selected, passwords and community names appear as text. The default setting for this option is unselected and passwords and community names appear as a string of asterisks.

Related Information

For information on related windows:

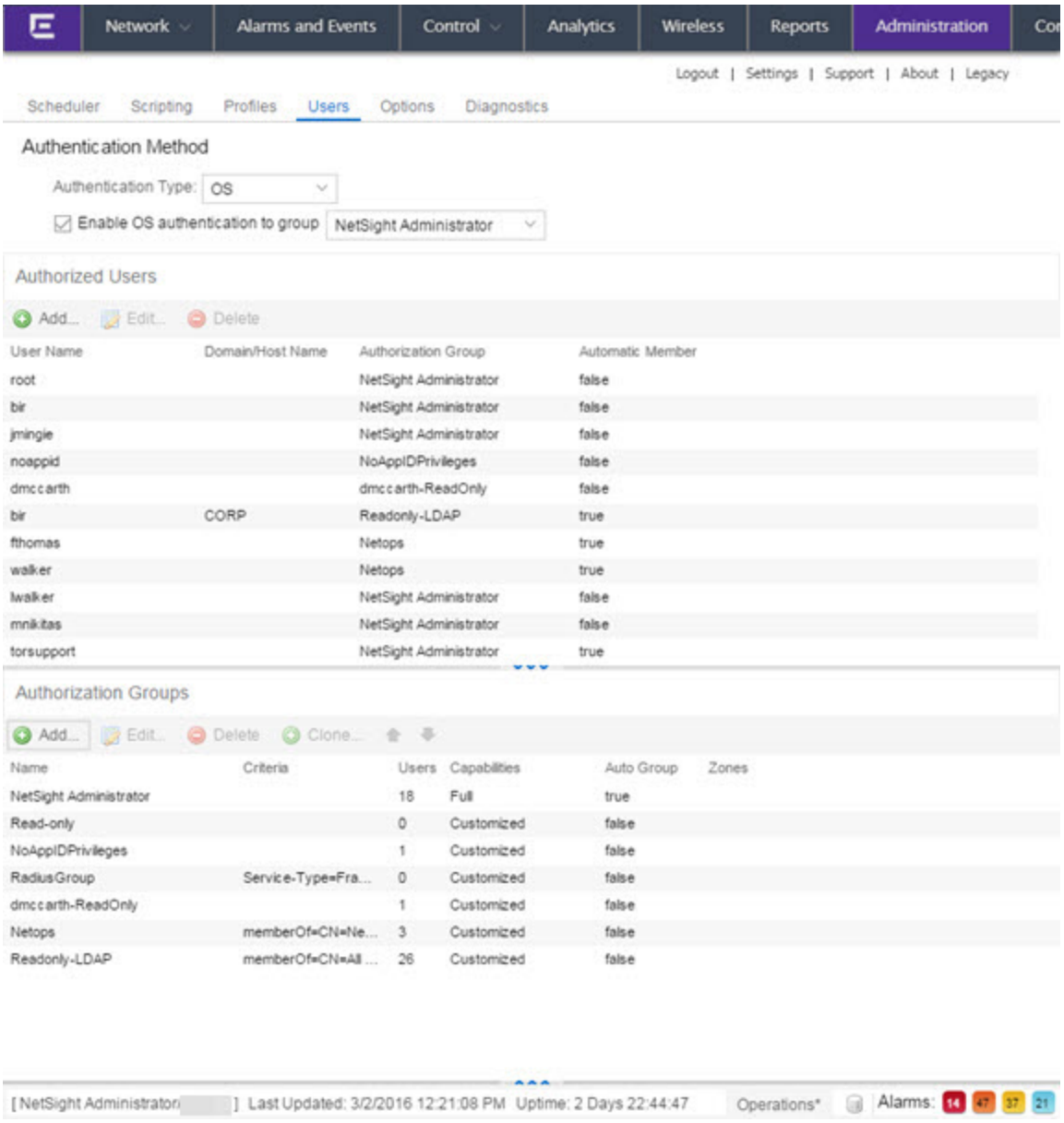
- Users/Groups Tab
- Site Tab

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 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.



Authentication Method

Use this section to configure the method used to authenticate users who are attempting to launch an Management Center client or access the Management Center database using the Management Center Server Administration web page.

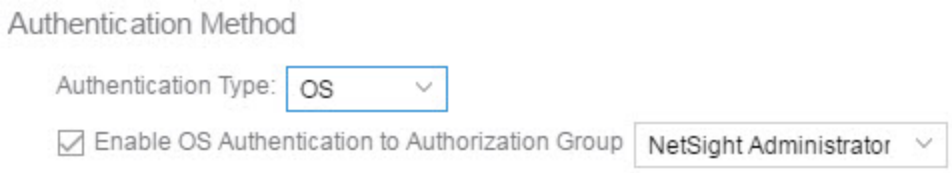
The following authentication methods are available:

- 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)

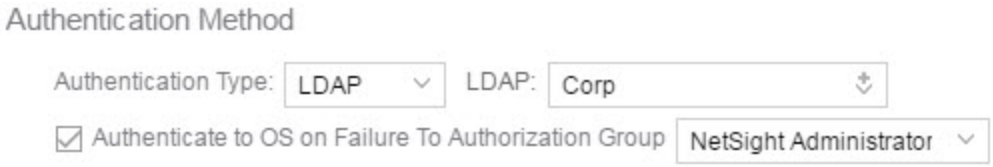
With this authentication method, the Management Center Server uses the underlying host operating system to authenticate users. Use the Authorized Users table to create a list of users allowed access and define their access capabilities.



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 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.

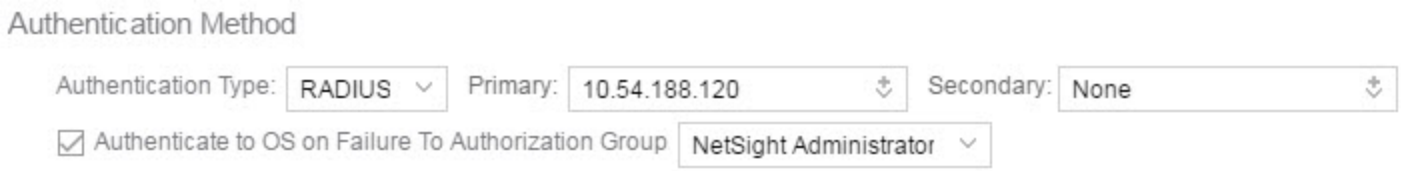
With LDAP Authentication, configure dynamic assignment of users to authorization groups based on the attributes associated with a user in Active Directory. For example, create an authorization group that matches everyone in a particular organization, department, or location. When a user authenticates, 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 Management Center Server uses the specified RADIUS servers to authenticate users.

NOTE: The RADIUS Authentication mode supports the PAP authentication type.



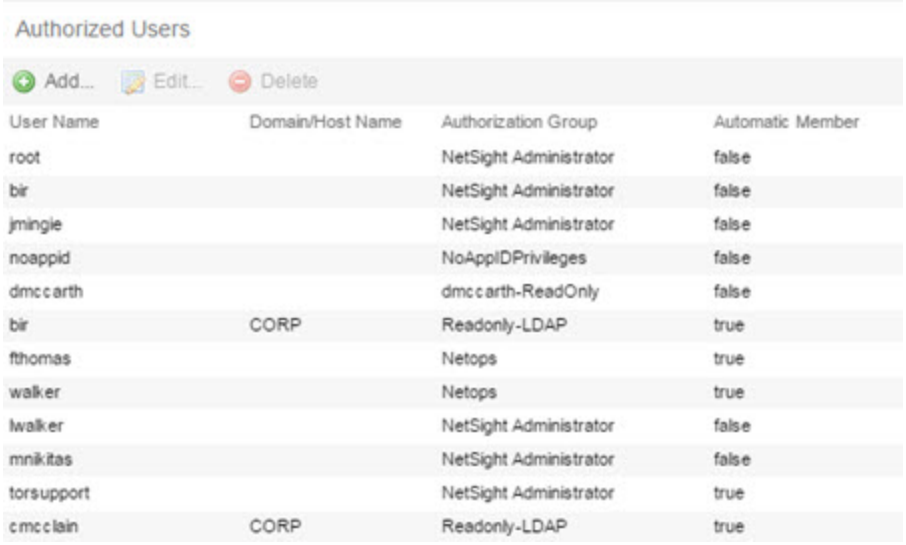
Use the drop-down menu to select the primary RADIUS server and backup RADIUS server (optional) on your network that you want to use to authenticate users. Use the New menu option to add a RADIUS server, or select Manage to manage your RADIUS servers.

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.

Authorized Users Table

This table lists all of the users who are currently authorized to access the 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.



User Name	Domain/Host Name	Authorization Group	Automatic Member
root		NetSight Administrator	false
bir		NetSight Administrator	false
jmingie		NetSight Administrator	false
noappid		NoAppIDPrivileges	false
dmccarth		dmccarth-ReadOnly	false
bir	CORP	Readonly-LDAP	true
fthomas		Netops	true
walker		Netops	true
lwalker		NetSight Administrator	false
mnikitas		NetSight Administrator	false
torsupport		NetSight Administrator	true
cmcclain	CORP	Readonly-LDAP	true

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 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.

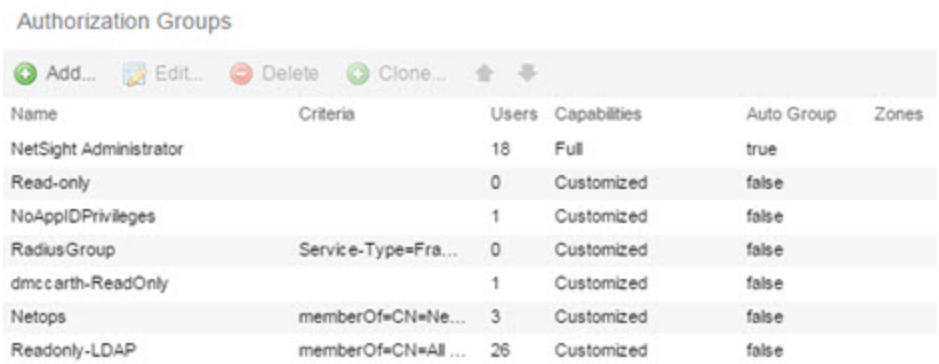
Add
: Opens the Add/Edit User window, which allows you to define the username, domain, and authorization group for a new authorized user.

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 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 that 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 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.

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).

Add
: Opens the Add/Edit Group window, which allows you to define the capabilities and settings for a new group.

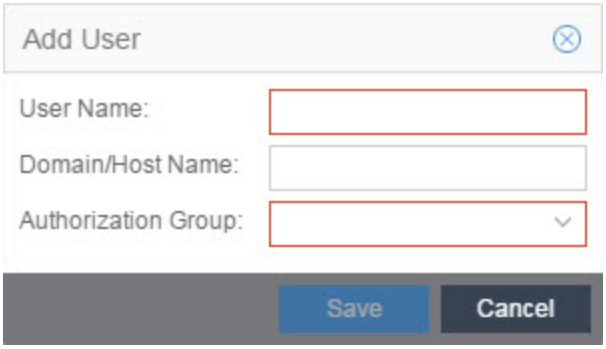
Edit
: Opens the Add/Edit Group window, which allows you to modify the capabilities and settings for a selected group.

Delete
: Removes the selected group from the Groups table.

Clone
: Duplicates the selected group from the Groups table and creates a new group with identical capabilities.

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 Management Center database.



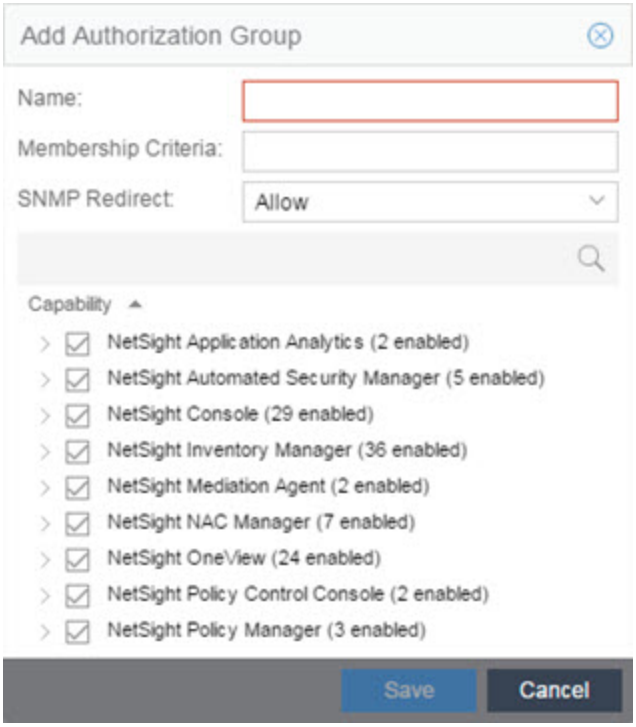
User Name
: The name used for this authorized user.

Domain/Host Name
: The user's domain/hostname used to authenticate to the 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: 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 Suite-wide Option setting for Client/Server SNMP Redirect.
- ALWAYS — Redirects all SNMP requests to the Management Center Server, regardless of the Suite-wide Option setting for Client/Server SNMP Redirect.
- NEVER — Never redirects SNMP requests to the Management Center Server, regardless of the Suite-wide Option 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

Access Control Options

These options apply only to the **Access Control** tab. In the **Options** tab (**Administration > Options**), the right-panel view changes depending on what you select in the left-panel tree. Expand the Access Control tree to view all the different available options.

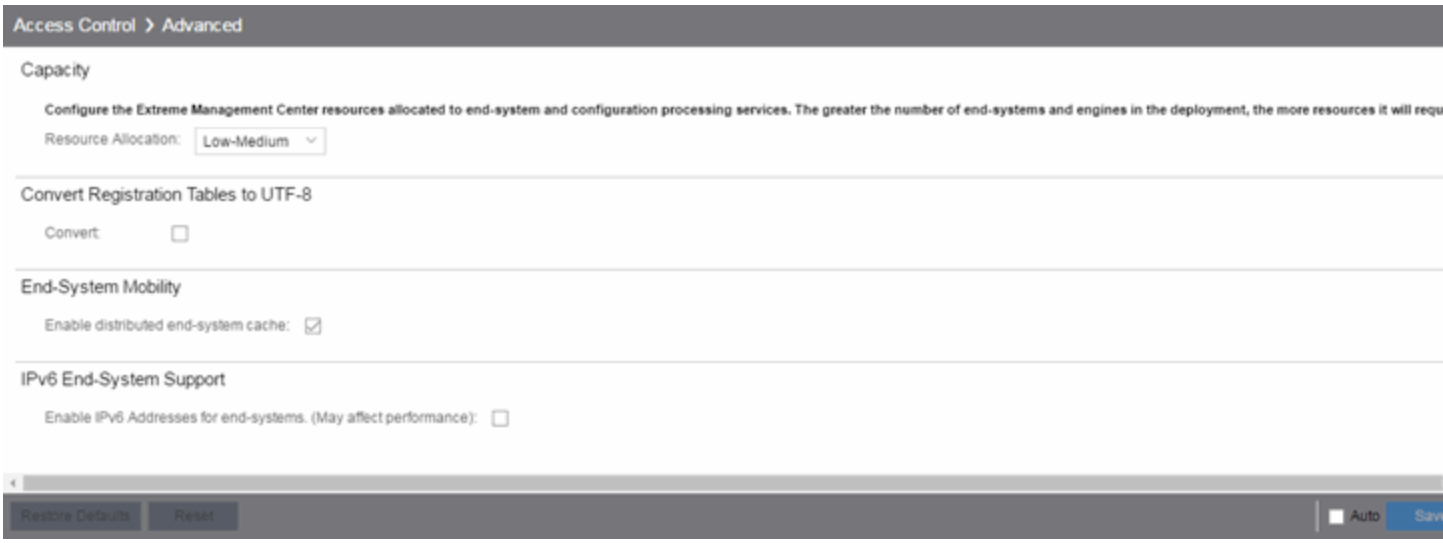
Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.

Information on the following Extreme Access Control options:

- Advanced Settings
- Assessment Server
- Data Persistence
- End-System Event Cache
- Enforce Warning Settings
- Features
- Notification Engine
- Policy Defaults
- Status Polling and Timeout

Advanced Settings

This Options view lets you configure advanced settings for the **Access Control** tab. These settings apply to all users.



Capacity

The 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 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.

Convert Registration Tables to UTF-8

Select the **Convert** checkbox to display registration tables in a readable format you can share.

IPv6 End-System Support

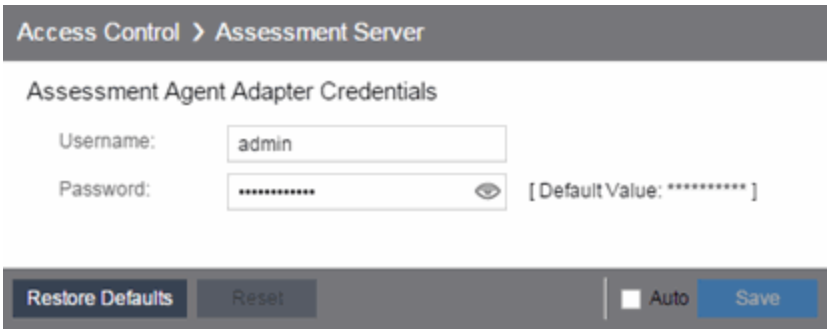
The **Enable IPv6 Addresses for end-systems** option allows Access Control to collect, report, and display IPv6 addresses for end-systems in the end-systems table. When this option is changed, you must enforce your engines before the new settings take effect. In addition, end-systems need to rediscover their IP addresses in order to reflect the change in the end-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 with only IPv6 addresses are not supported. End-system functionality support varies for IPv6 end-systems. For complete information, see IPv6 Support in the Management Center Configuration Considerations Help topic.

Assessment Server

These options let you provide assessment agent adapter credentials. The options apply to all users on all clients.



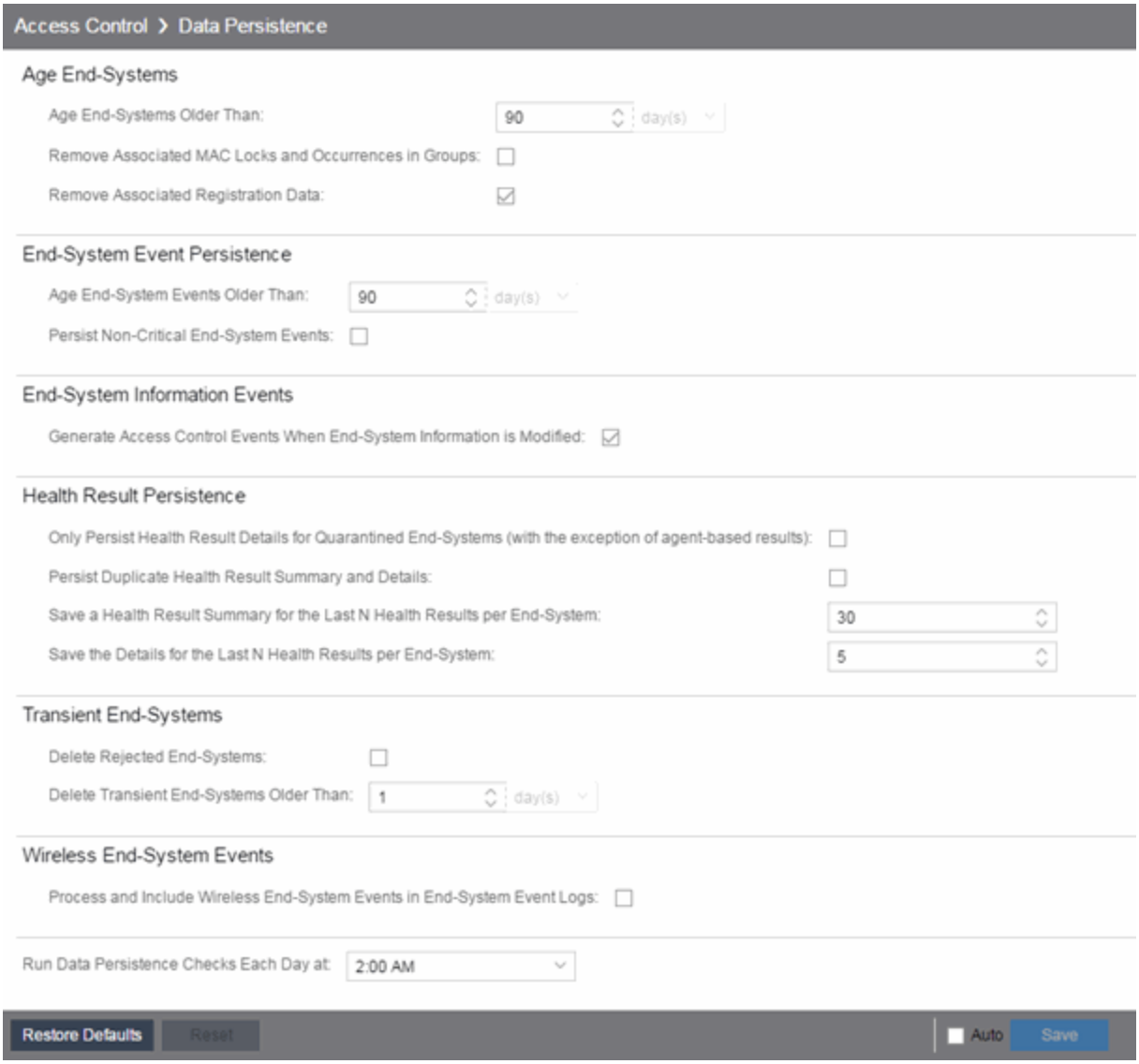
Assessment Agent Adapter Credentials

The password and username the Access Control engine uses when attempting to connect to network assessment servers, including Extreme Networks Agent-less, Nessus, or a third-party assessment server (an assessment server not supplied or supported by Management Center). The password is used by the assessment agent adapter (installed on the assessment server) to authenticate assessment server requests. Management Center provides a default password that can be changed, 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 is not performed. For additional information, see How to Change the Assessment Agent Adapter Password.

Data Persistence

This Options panel lets you customize how Extreme Access Control 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 view. These settings apply to all users on all clients.



Age End-Systems

Each day, when the Data Persistence check runs, it searches the database for end-systems for which Access Control did not receive an event in the number of days specified (90 days by default). It removes those end-systems from the End-System table in the End-Systems tab.

If you select the **Remove Associated MAC Locks and Occurrences in Groups** checkbox, the aging check also removes any MAC locks or group memberships associated with the end-systems being removed.

The **Remove Associated Registration Data** checkbox is selected by default, so that the aging check also removes any registration data associated with the end-systems being removed.

End-System Event Persistence

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).

End-System Information Events

Select the checkbox if you want Access Control to generate an event when end-system information is modified.

Health Result Persistence

This section lets you 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 results per end-system. Change these values, if necessary.

There are two additional options:

- 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).
- 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.

Transient End-Systems

This option lets you 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 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.

Select the **Delete Rejected End-Systems** checkbox if you want end-systems in the Rejected state to be deleted as part of the cleanup.

Wireless End-System Events

Select the checkbox if you want Management Center to generate an event when wireless end-system information is modified. This option is disabled by default.

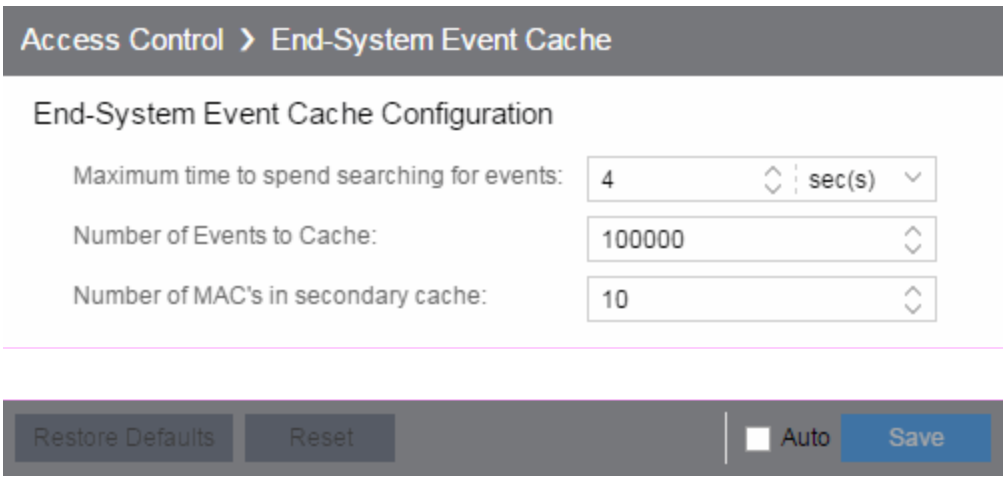
Run Data Persistence Checks Each Day at

Set the time that the Data Persistence Check is performed each day.

End-System Event Cache

End-system events are stored 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 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. These settings apply to all users on all clients.



Maximum Time to spend searching for events

This specifies the time 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 are not in the main cache.

Enforce Warning Settings

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 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.

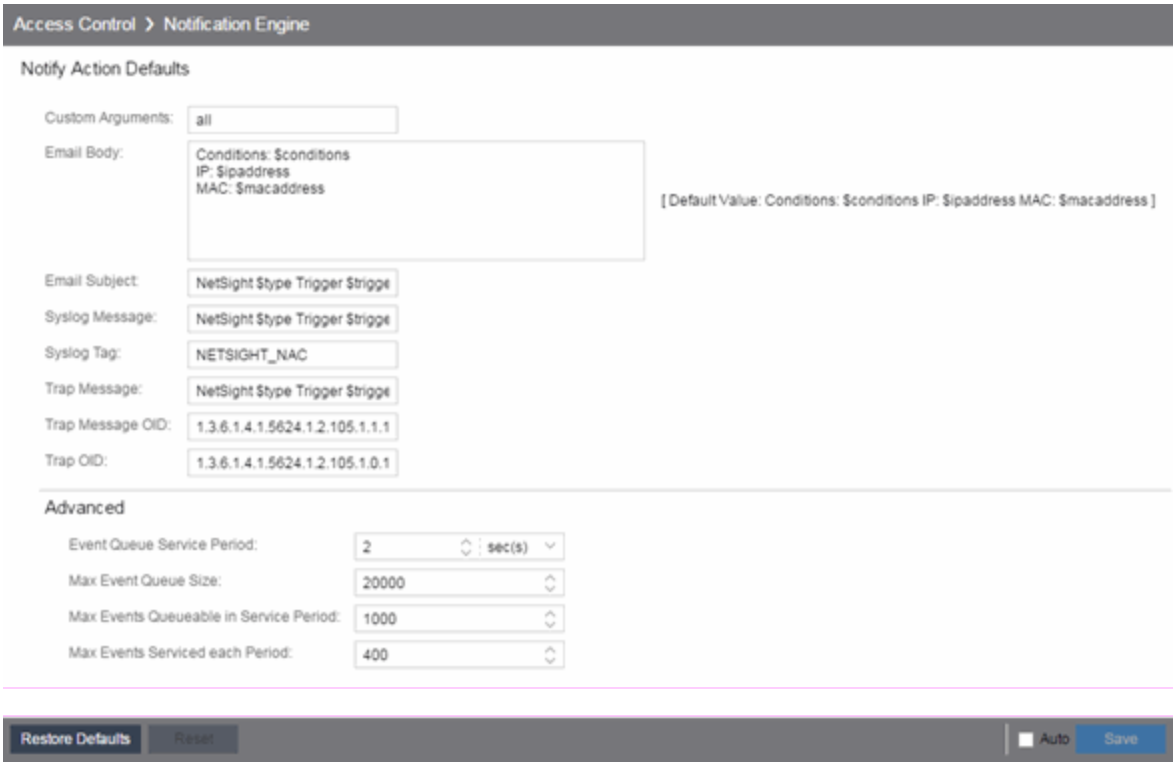
Select the checkbox in the Ignore column next to the warning message that you don't want displayed and click OK.

Features

This Options 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 Access Control windows.

Notification Engine

Selecting Notification Engine in the left panel of the Options tab provides the following view where you can define the default content contained in Access Control notification action messages. For example, with an email notification action, define the information contained in the email subject line and body. With a syslog or trap notification action, specify certain information contained in the syslog or trap message. These settings apply to all users.



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 Management Center Server, then use this field to enter the "all" option. Using the "all" option returns values for all the Access Control Notification keywords applicable to the notification type. The "all" option is the only valid option for this field. For additional information, see Keywords.

E-Mail Subject
: Defines the text and keyword values included in the e-mail subject line.

E-Mail Body
: Defines the text and keyword values included in the e-mail 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 (seconds)
: This controls 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.

Max Event Queue Size
: The maximum number of events that can be queued. By default, the dispatcher drops events after 5000 events are queued.

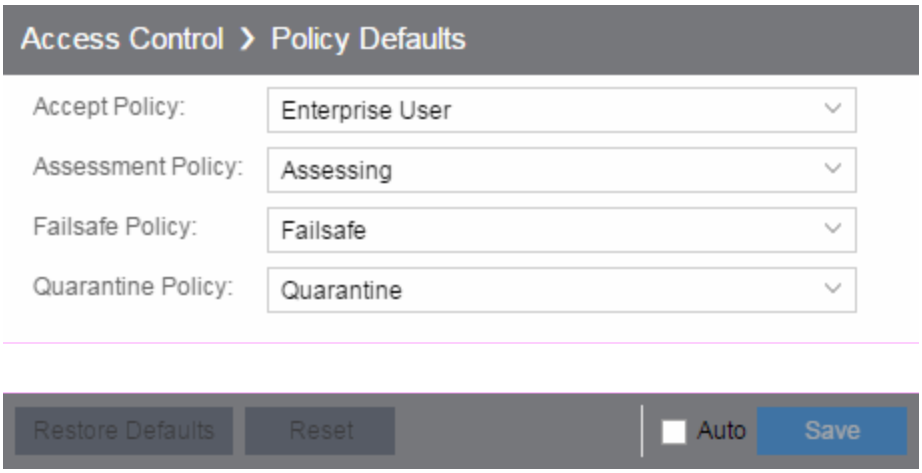
Max Events Queuable in Service Period (per second)
: This limits the rate that events can be added to the queue (not processed from the queue) and protects the event engine against a large amount of events arriving too quickly. If events arrive at a rate that exceeds this amount, they are discarded.

Max 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 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.

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 Access Control Gateway 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).

Failsafe Policy
: Select the default Failsafe policy. The 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 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 Access Control engines. These settings apply to all users on all clients.

Access Control Engine Enforce Timeout
: When enforcing to Access Control engines, this value specifies the amount of time Management Center waits for an enforce response from the engine

before determining the engine is not responding. During an enforce, a Extreme Access Control engine responds every second to report that the enforce operation is either in-progress or complete. Typically, you should not need to increase this timeout value, unless you are experiencing network delays that require a longer timeout value.

Access Control Inactivity Check

Enable a check to verify end-system Extreme Access Control activity is taking place on the network. If no end-system activity is detected, an Access Control Inactivity event is sent to the Events view. Use the Alarms and Events tab to configure custom alarm criteria based on the Access Control Inactivity event to create an alarm, if desired.

Status Polling

Length of Timeout — When communicating with Access Control engines for status polling, this value specifies the amount of time Management Center waits before determining contact failed. If Management Center does not receive a response from an engine in the defined amount of time, 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," Management Center is not be able to enforce a new configuration to it.

Polling Interval — Specifies the frequency Management Center polls the Access Control engines to determine engine status.

Related Information

For information on related tasks:

- How to Set Extreme Access Control Options

Alarm Options

Use this panel to set alarm settings.

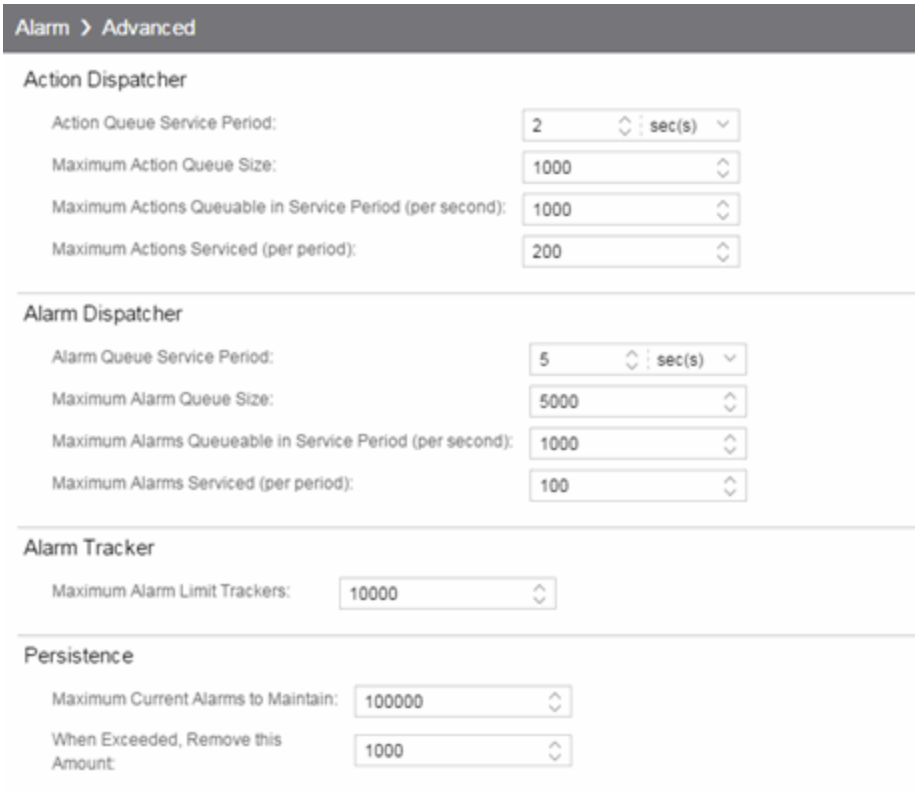
Changing a value from the system default causes a **Default Value** button to appear. Clicking this button changes the field back to the system default value.

Information on the following Alarm options:

- Advanced Settings
- Alarm Action Defaults
- Alarm History
- Consolidate Email
- Override Email

Advanced Settings

This Options 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 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 alarms/actions to process. The dispatcher runs once every service period. So by default, the dispatcher processes alarms/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 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, Management Center tracks whether the limit is exceeded and when to reset the count. This option sets the maximum number of alarms that 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 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.

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 certain information

you want contained in the syslog or trap message. These values are used unless they are overridden in an individual alarm.

Alarm Action Defaults Settings

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.

Following is a list of the most common keywords used. For additional information, see Keywords.

- $alarmName – the name of the alarm.
- $severity – the alarm severity.
- $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 Management Center to pass all variable values to the program as individual arguments.

E-Mail Body
: Defines the text included in the e-mail body.

E-Mail Subject
: Defines the text included in the e-mail 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.

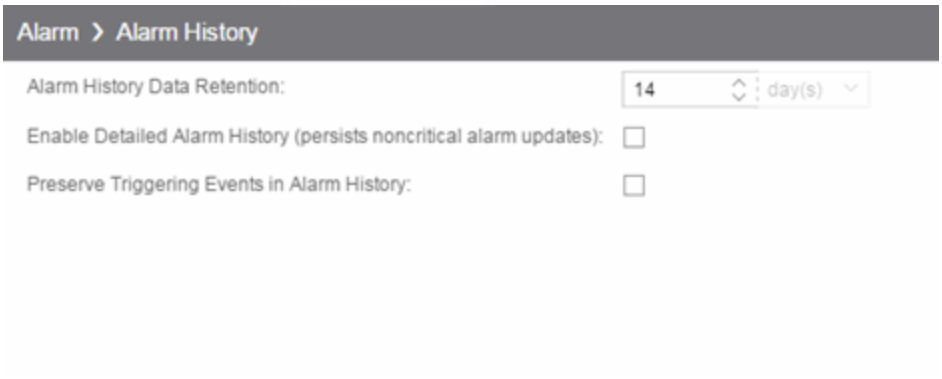
Trap Message
: The varbind sent in the trap.

Trap Message OID
: The OID of the varbind being sent that represents the message.

Trap OID
: The OID that defines the trap.

Alarm History Settings

Selecting Alarm History in the left panel of the Options panel provides the following view, where you can 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
: 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 is also recorded.

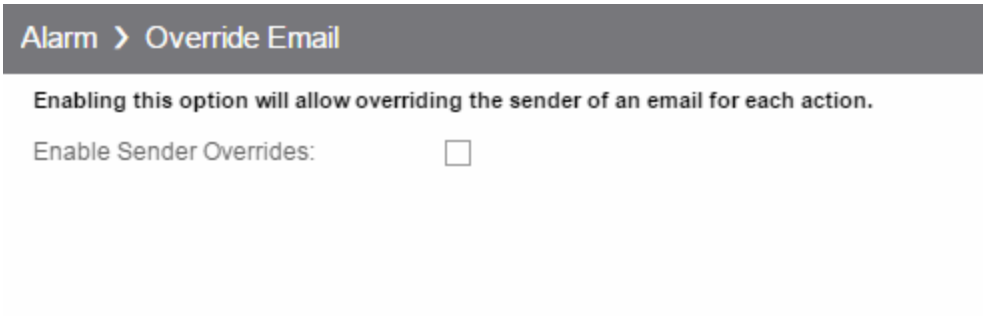
Preserve Triggering Events in Alarm History
: This option preserves alarm triggering events, so that any triggering events are stored with the alarm history record. This allows you to view the triggering event by clicking the View Trigger button in the Alarm History window.

Consolidate Email Settings

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
: The amount of time Extreme Management Center waits before sending an email of alarm actions when Select Enable Email Digest is selected.

Override Email Setting



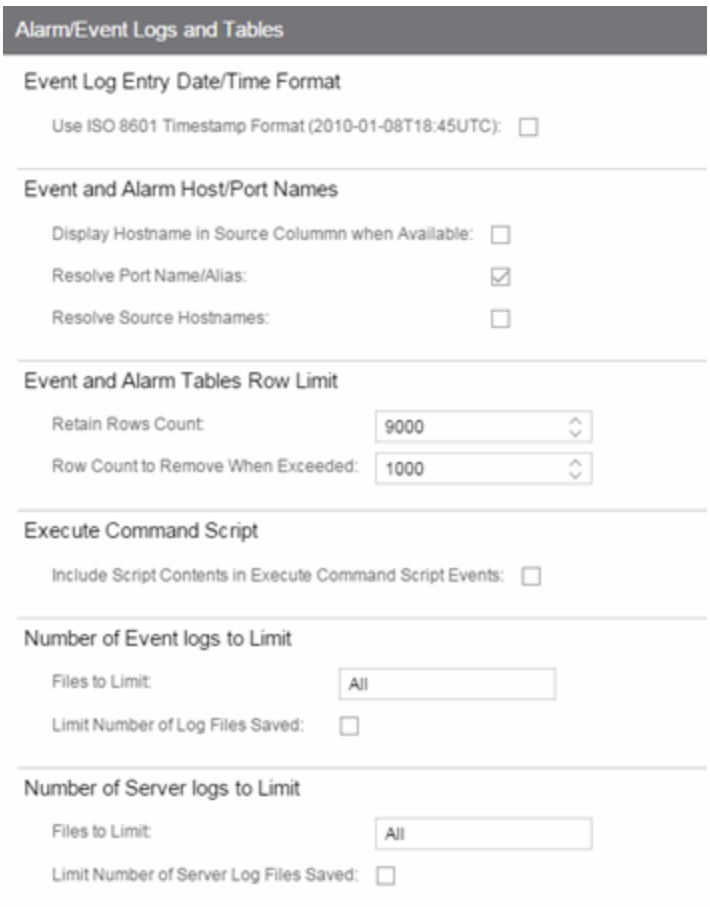
The Enable Sender Overrides option allows you to override the sender of an email for an alarm email action, including the ability to set the sender's password, if needed. Since alarms are typically sent out as email/text messages, this option allows IT staff to set different ring-tones based on the alarm

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.



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 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.

Event and Alarm Table Host/Port Names

These options let you configure host name and port name resolution, and display the device hostname in the Source column in alarm and event tables:

- Display Hostname in Source Column when Available — Select this option to display the host name in the source column in the Alarms tab in the Alarms and Events tab, if it's available in 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 Suite Name Resolution option.)
- Resolve Source Hostnames — Select this option to resolve hostnames 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.)

Event and Alarm Tables Row Limit

These settings determine the number of table rows displayed in all of the logs in the Alarms tab and the Events tab in 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 to the number of rows are reduced by the value specified in the Row Count to Remove When Exceeded field. Subsequent entries are retained until the Retain Rows Count value is exceeded and the row total is again reduced.

Execute Command Script

The Execute Command Script feature includes script contents in logged events, which is not secure if the script includes passwords. If this option is deselected (default), the script is removed from the logged event. Select this option to include script contents in Execute Command Script events.

Number of Event logs to Limit

This option limits the number of application log files saved to the `<install directory>\NetSight\appdata\logs` directory. It does not limit the number of Traps or Syslog logs saved. Specify one of the following options:

- Limit the 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 value of log files saved.

Number of Server logs to Limit

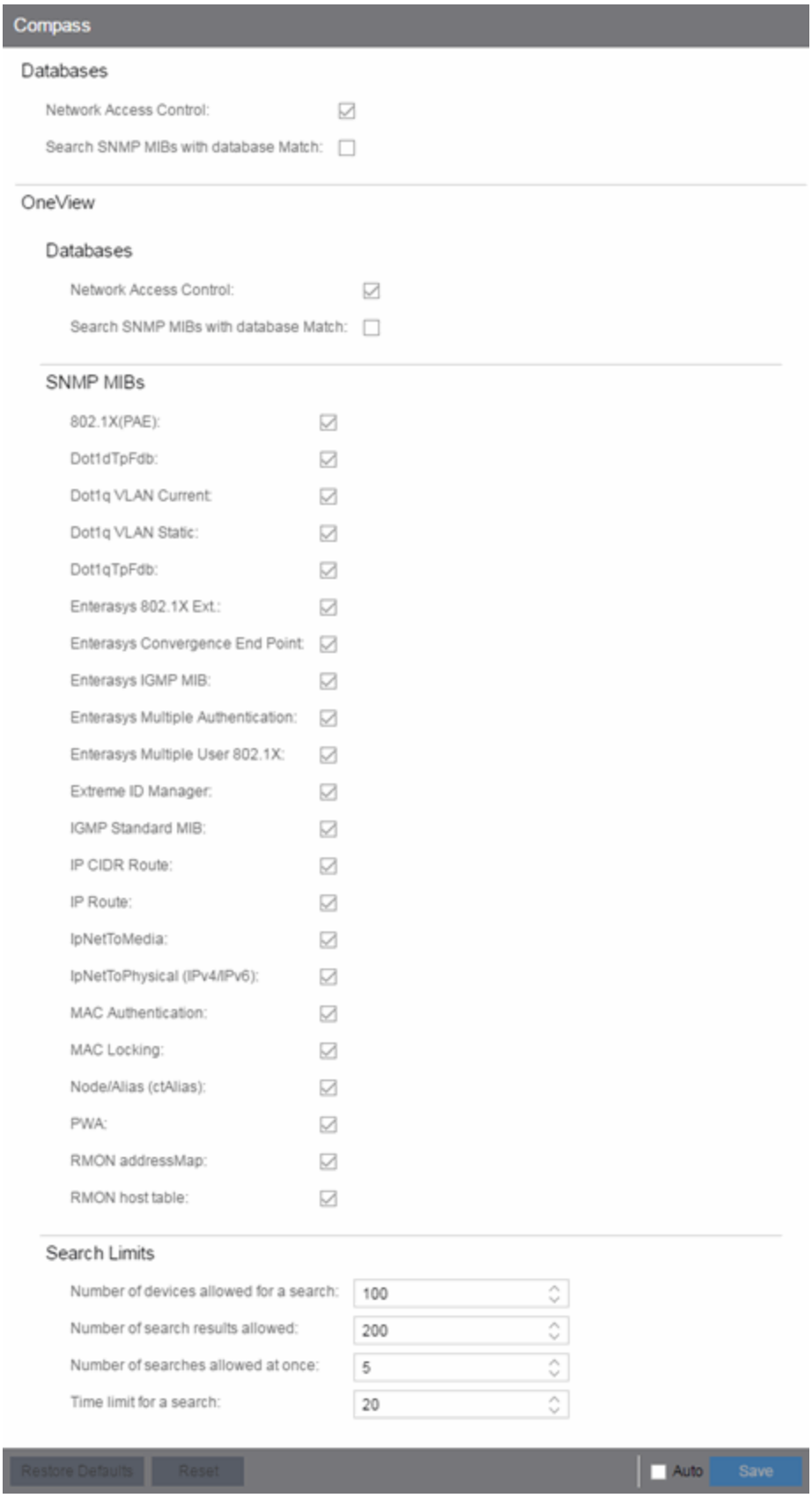
A new server log is created every day. This option limits the number of server log files that are saved to the `<install directory>\NetSight\appdata\logs` directory. Specify one of the following options:

- Limit the 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 value of server log files saved.

Compass Options

Selecting Compass in the left panel of the Options window 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.


Compass
Databases
Network Access Control:
Search SNMP MIBs with database Match:
OneView
Databases
Network Access Control:
Search SNMP MIBs with database Match:
SNMP MIBs
802.1X(PAE):
Dot1dTpFdb:
Dot1q VLAN Current:
Dot1q VLAN Static:
Dot1qTpFdb:
Enterasys 802.1X Ext.:
Enterasys Convergence End Point:
Enterasys IGMP MIB:
Enterasys Multiple Authentication:
Enterasys Multiple User 802.1X:
Extreme ID Manager:
IGMP Standard MIB:
IP CIDR Route:
IP Route:
IpNetToMedia:
IpNetToPhysical (IPv4/IPv6):
MAC Authentication:
MAC Locking:
Node/Alias (ctAlias):
PWA:
RMON addressMap:
RMON host table:
Search Limits
Number of devices allowed for a search:
100
Number of search results allowed:
200
Number of searches allowed at once:
5
Time limit for a search:
20
Restore Defaults
Reset
Auto
Save

Search Options

The boxes that are checked in this section determine which data sources are used with Compass searches. By default, Compass is configured to include the NAC Manager database (the Network Access Control checkbox) as well as various SNMP MIB objects when performing searches. For additional information, see MIB/Table Descriptions. 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 NAC Database, the SNMP MIBs are not searched unless the Search SNMP MIBs with database Match checkbox is also selected. If the "Network Access Control" checkbox is deselected, then the NAC Manager Database is not used to resolve IP address to MAC address.

OneView - These options are for the Compass search in Management Center. In addition to search options, they include search limit settings, which are used to help limit the 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 Management Center Compass searches that can be performed at one time.
- Time limit for a search. The maximum search time in seconds.

Related Information

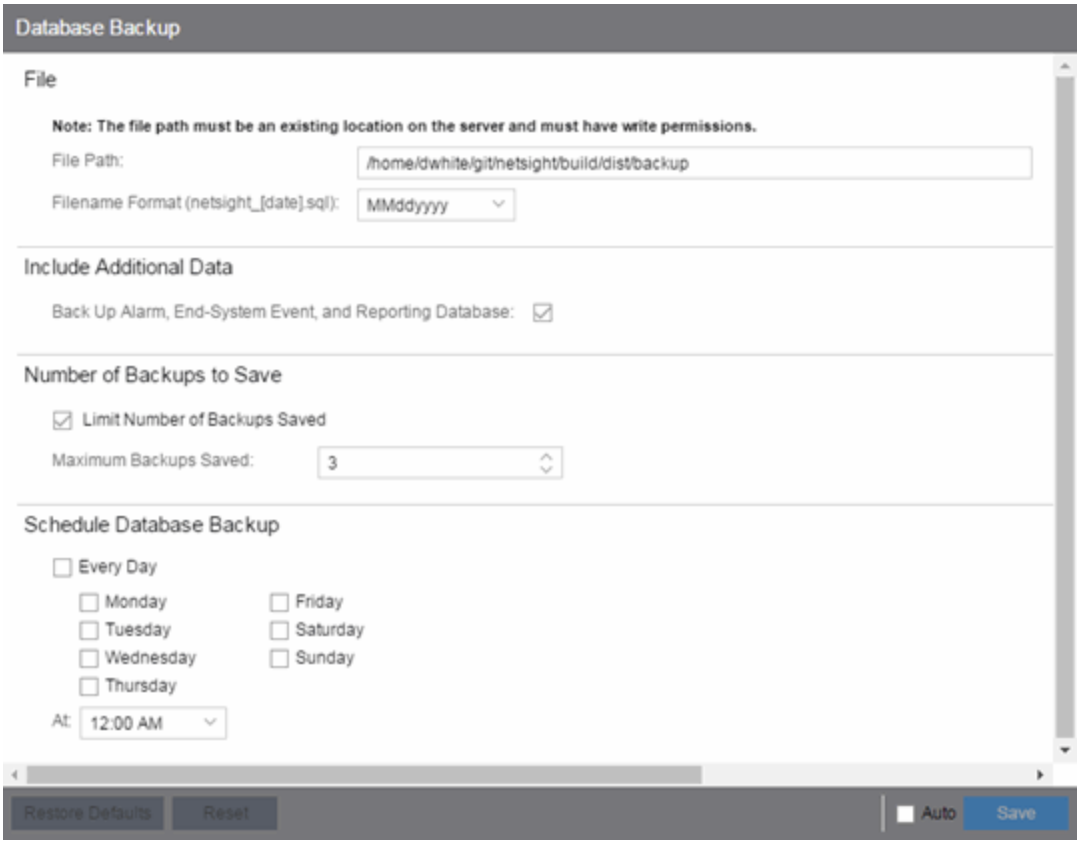
For information on related tasks:

- How to Set Extreme Access Control Options

Database Backup Options

Selecting Database Backup in the left panel of the Options window 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 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.



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.

You can also 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.

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.

The Backup Alarm and Reporting Database checkbox lets you enable and disable the automatic backup of alarm data and Management Center 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.

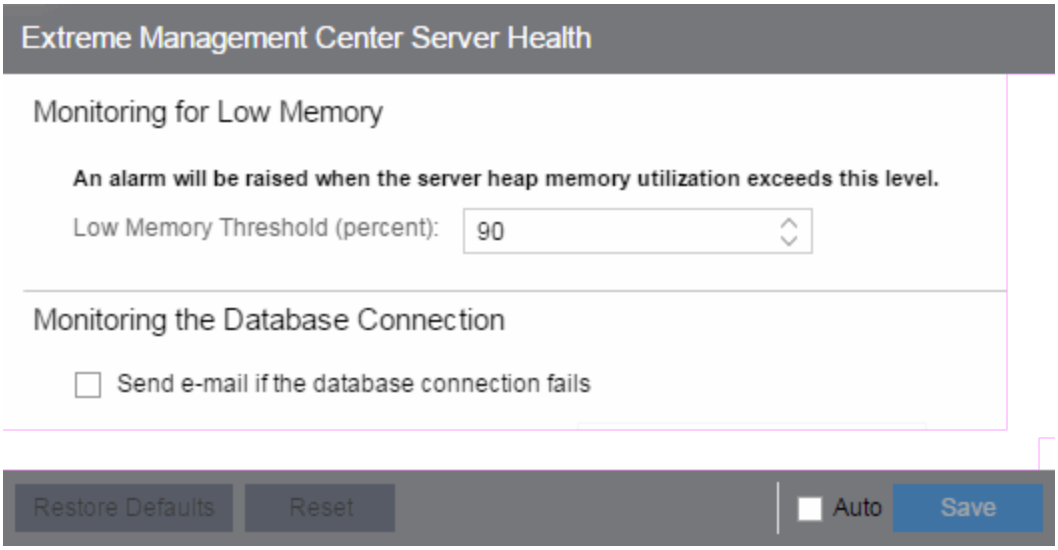
You can customize the date and time formats of backup files by selecting the option that formats the date -- day (DD), month (MM), and year (YYYY) -- according to your personal preference.

For additional information, see Tuning Database Backup Storage.

Extreme Management Center Server Health Options

Selecting Extreme Management Center Server Health in the left panel of the **Options** tab provides the following view, from which you can configure warnings to help monitor the 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.



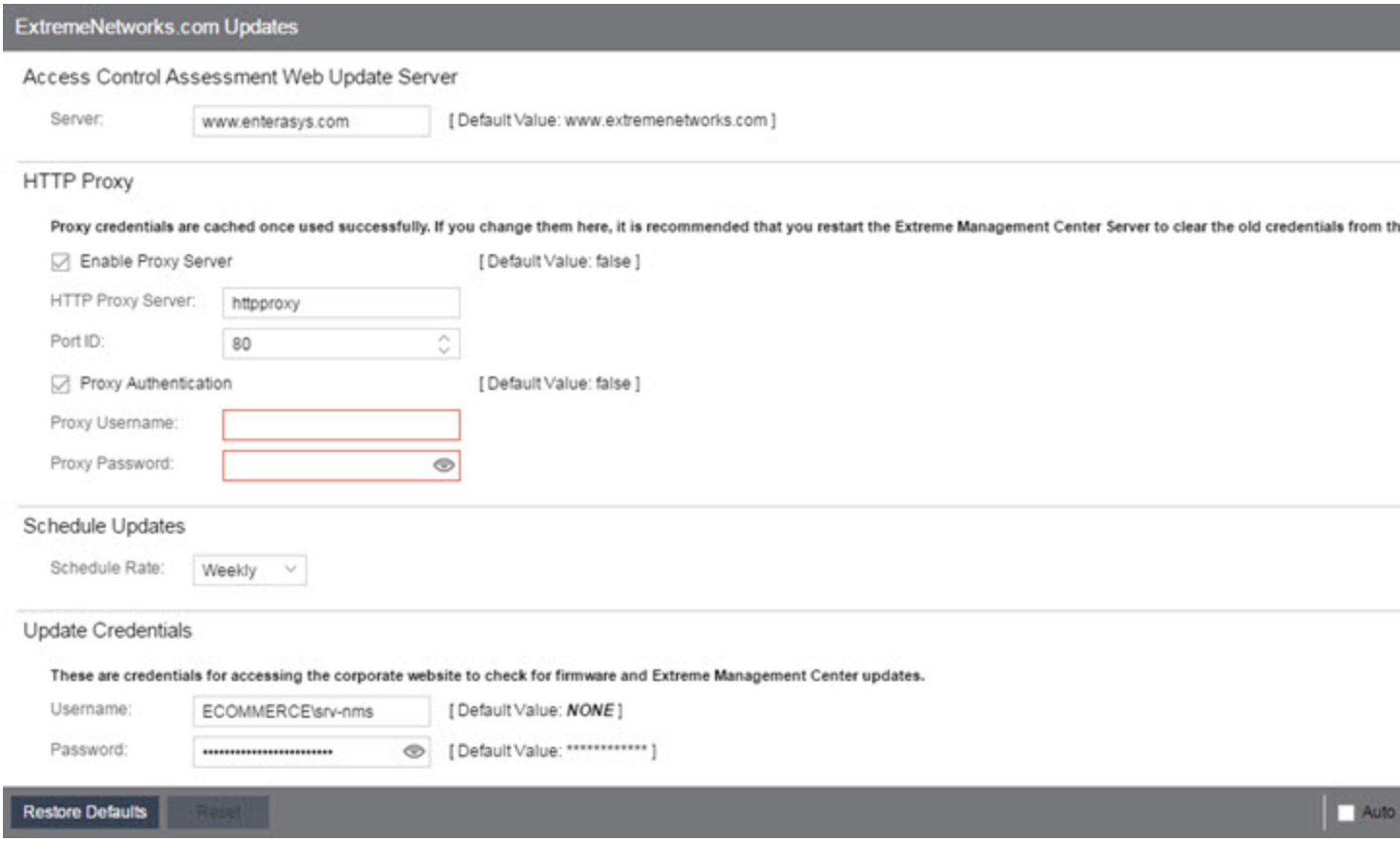
Low Memory Threshold (percent)
: Enter a percentage to specify the server heap memory utilization percentage above which an alarm is raised. If the memory utilization falls more than five percent below the threshold percentage, the alarm is automatically cleared.

Send e-mail if the database connection fails
: Select the checkbox and enter an email address to send an email notification if the Management Center database goes down and when the database comes back up.

ExtremeNetworks.com Updates Options

Selecting ExtremeNetworks.com Update 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.



Access Control Assessment Web Update Server

Displays the web update server used by Extreme Access Control to update Access Control assessment server software. This update operation pertains only to 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 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 a specific times to check for Management Center software updates. Use the drop-down menu to set the frequency (**Daily**, **Weekly**, **Disabled**) for checking for updates. If you select **Weekly**, use the drop-down menu to select the day of the week you perform the check and set the desired time. If you select **Daily**, set the desired time.

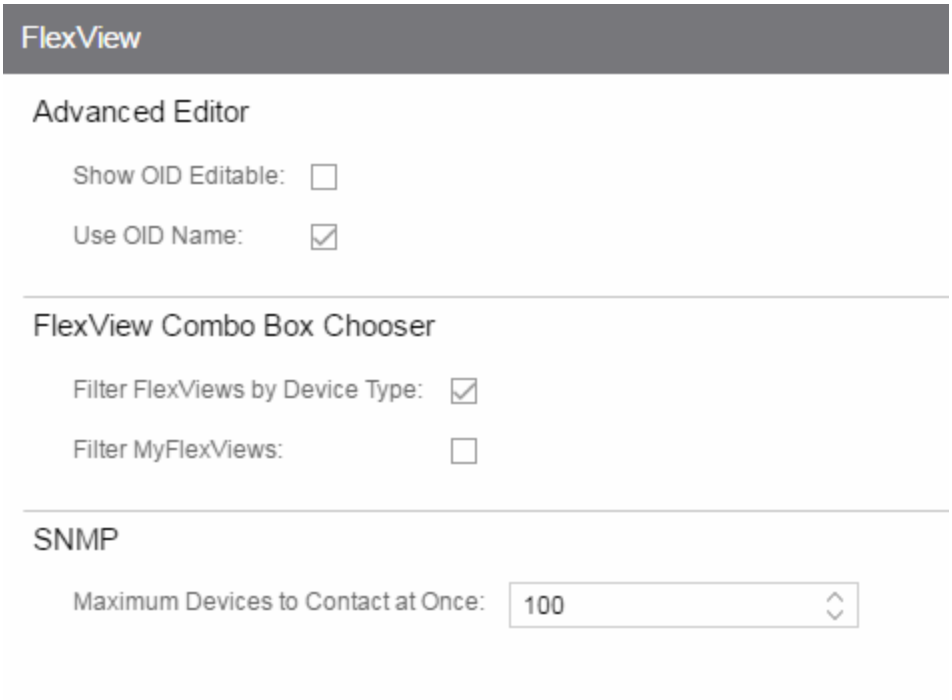
Update Credentials

Enter the credentials used to access the ExtremeNetworks.com website to obtain firmware and Management Center update information. You need to create an account at ExtremeNetworks.com and define a user name and password for the account, then enter the same credentials here.

FlexView Options

The default Maximum number of devices to contact at once setting indicates the maximum number of devices FlexView attempts to contact at once.

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 Editor

Show OID Editable
: Selecting the **Show OID Editable** option lets you create FlexViews with OID-based SNMP columns that are unique.

Use OID Name
: Selecting the **Use OID Name** option uses the OID name for the FlexView.

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.

SNMP

These status polling options pertain to devices whose poll type is set to SNMP.

Maximum number of devices to contact at once.
: The maximum number of IP addresses Management Center attempts to contact simultaneously.

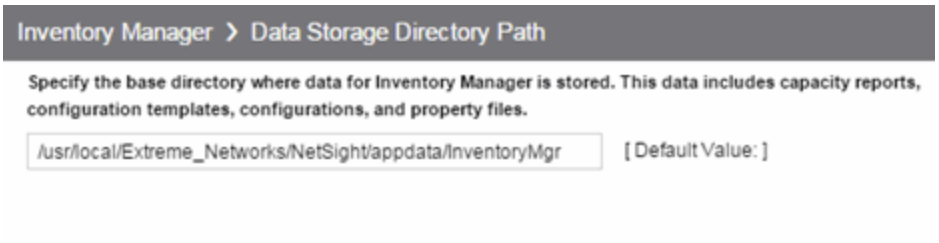
Inventory Manager Options

Selecting Inventory Manager in the left panel of the **Options** tab provides the following options, where you can schedule backups of Extreme Management Center data. An up-to-date data backup is an important component to ensuring that critical information pertaining to all 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.

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 Management Center can find them.



File Transfer Settings

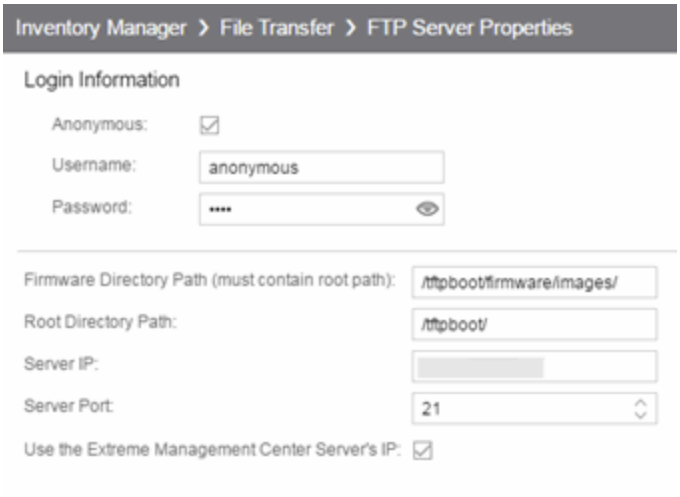
These options specify the FTP, TFTP, or SCP file transfer settings used when upgrading firmware.

Information on the following File Transfer Settings options:

- FTP Server Properties Settings
- TFTP Server Properties Settings
- SCP Server Properties Settings

FTP Server Properties Settings

Selecting FTP Server Properties in the left panel of the Options tab provides the following view, from which you can 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.



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. (The firmware images stored in the firmware directory are added to the left-panel Firmware tree when you perform a firmware discovery. 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.

Login Information

Anonymous

Select this checkbox if your FTP server is configured to accept Anonymous logins. Management Center automatically fills in the username and password fields.

Username/Password

Enter your username and password to access the FTP server. If you select the Eye icon, your password is hidden.

FTP Server Properties

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 to or read files from this directory and any of its subdirectories. The default root directory is the tftpboot directory 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:\ or D:\).
- **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\`

Server IP

Enter the IP address of the device where the FTP server resides. Only enter a value in this field if Use the NetSight Server's IP checkbox is not selected.

Server Port

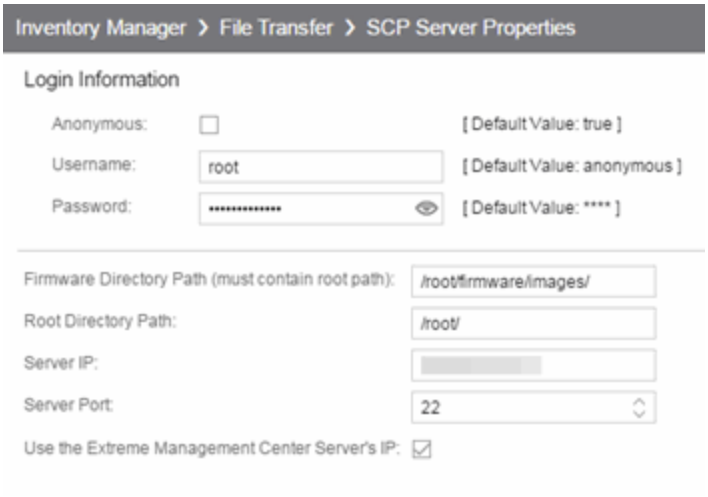
Specify the port number on which your FTP server is configured to run.

Use the Extreme Management Center Server's IP

Select this checkbox if your FTP server is on the same machine as the Management Center Server.

SCP Server Properties Settings

Selecting SCP Server Properties in the left panel of the **Options** tab provides the following view, where you can 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.



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. (The firmware images stored in the firmware directory are added to the left-panel Firmware tree when you perform a firmware discovery. 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.

Login Information

Anonymous

Select this checkbox if your SCP server is configured to accept Anonymous logins. Management Center automatically fills in the username and password fields.

Username/Password

Enter your username and password to access the SCP server. If you select the Eye icon, your password is hidden.

Root Directory Path

The root directory is the base directory to which the SCP server is allowed access. The SCP server is allowed to create files to or read files from this directory and any of its subdirectories. The default root directory is the tftpboot directory 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 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

  `\\yoursystemname\firmware\images`

SCP Server Properties

Server IP

Enter the IP address of the device where the SCP server resides. Only enter a value in this field if Use the NetSight Server's IP checkbox is not selected.

Server Port

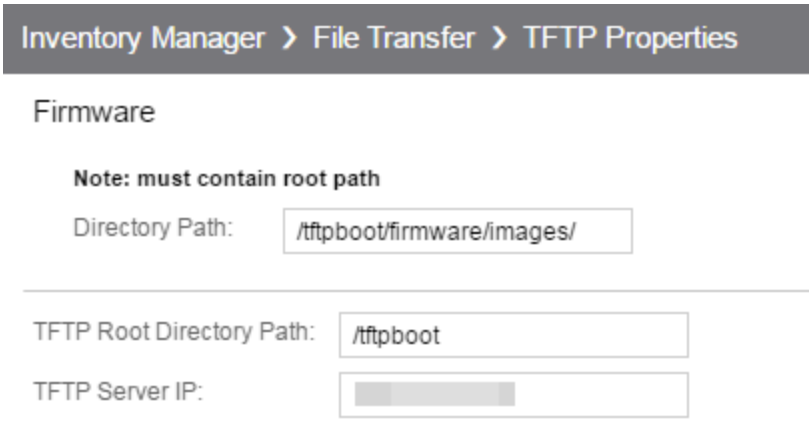
Specify the port number on which your SCP server is configured to run.

Use the Extreme Management Center Server's IP

Select this checkbox if your SCP server is on the same machine as the Management Center Server.

TFTP Properties Settings

Selecting TFTP Properties in the left panel of the Options tab provides the following view, where you can set TFTP server properties. This view displays the TFTP server IP address and root directory path specified in the Services for Extreme Management Center Server Options panel and lets you set the firmware directory path. These settings apply to all users.



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. (The firmware images stored in the firmware directory are added to the left-panel Firmware tree when you perform a firmware discovery. For additional information, see How to Upgrade Firmware.)

NOTE: **If you are using a TFTP server on a remote system,** use the Universal Naming Convention (UNC) when specifying the firmware 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 directory on the remote drive)

use

`\\yourservername\tftpboot\firmware\images\`

TFTP 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 to or read files from this

directory and any of its subdirectories. The default root directory is the tftpboot directory 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 an TFTP root directory, it must match the root directory entered here.
- If your TFTP server is **not** configured with an 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 an 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

  `\\yoursystemname\firmware\images`

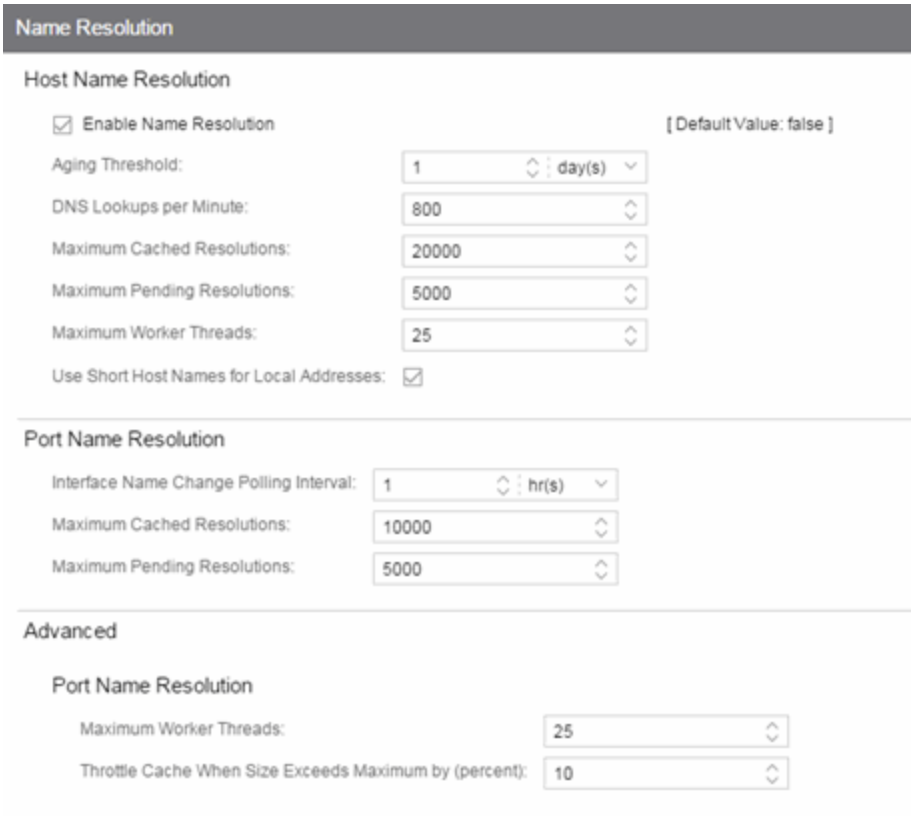
TFTP Server IP

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

Name Resolution Options

Selecting Name Resolution in the left panel of the **Options** tab displays 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/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.

DNS Lookups per Minute
: 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.

Maximum Cached Resolutions
: 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.

Maximum Pending Resolutions
: 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.

Maximum Worker Threads
: The maximum number of hostname 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 hostname resolution is enabled, and applies to Management Center only. When enabled, the hostname cache removes 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.

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 setting 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.

Advanced

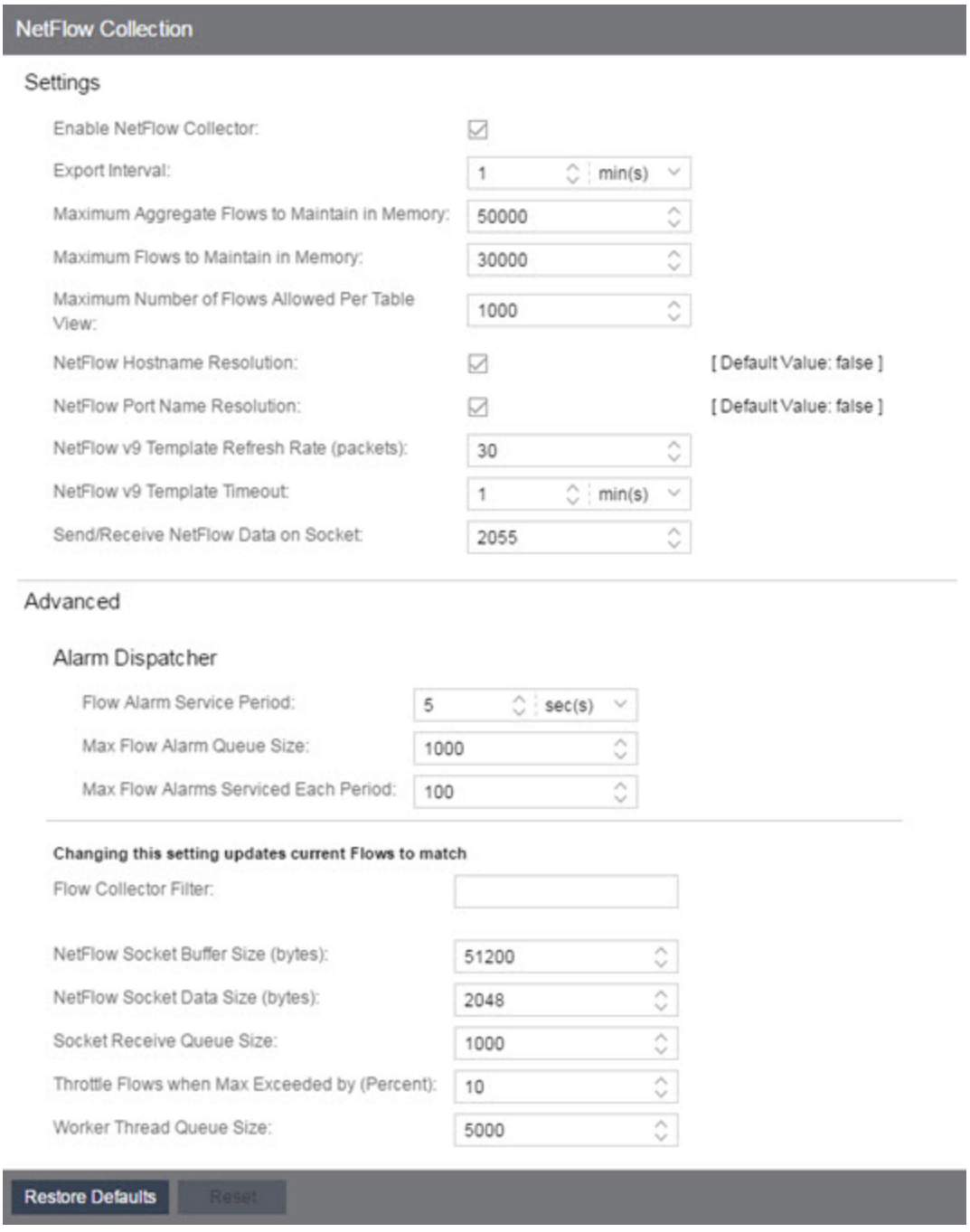
Maximum Worker Threads
: The maximum number of port name lookups that can be done at the same time. This number can be adjusted to control the amount of system resources used by port name resolution.

Throttle Cache When Size Exceeds Maximum by (percent)
: 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 Collection Options

Selecting NetFlow Collection in the left panel of the Options tab provides the following view where you can configure NetFlow flow collection 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.



Settings Section

Enable NetFlow Collector

Use this checkbox to enable/disable NetFlow packet processing on the Management Center server, allowing you to turn off NetFlow for

troubleshooting purposes. When NetFlow is enabled or disabled, a message is logged to the event log as well as the Management Center server log. When NetFlow is disabled, the Application Flows report on the Flows tab is cleared, however, the Flow Engine Summary on the Administration tab continues to show the statistics for previous flows.

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 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
: Indicates the maximum number of flowsdisplayed in NetFlow reports.

NetFlow Hostname 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 the Management Center Suite is enabled globally using the Management Center Suite-Wide Name Resolution option. The Suite-Wide option must 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 Suite Name Resolution option.)

NetFlow v9 Template Refresh Rate (packets)
: The number of export packets sent before the flow sensor retransmits a template to the collector when using NetFlow Version 9.

NetFlow v9 Template Timeout
: The number of minutes the flow sensor waits before retransmitting a template to the collector when using NetFlow Version 9.

Send/Receive NetFlow Data on Socket
: The port on the 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.

Advanced Section

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.

Max Flow Alarm Queue Size
: The maximum number of matched flows queued. By default, the dispatcher drops matched flows after 1000 matches are queued.

Max Flow Alarms Serviced Each Period
: The maximum number of matched flows pulled from the queue for processing each service period. By default, the dispatcher processes 100 matches every service period.

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 matching flows.

  Use this option if you want to use flow collection to look for specific results, and unrelated flows do not need to be processed. For example, only processing flows pertaining to a particular subnet.

NetFlow Socket Buffer Size (bytes)
: The buffer size (in bytes) set aside by the 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.

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).

Throttle Flows when Max 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).

Network Monitor Cache Options

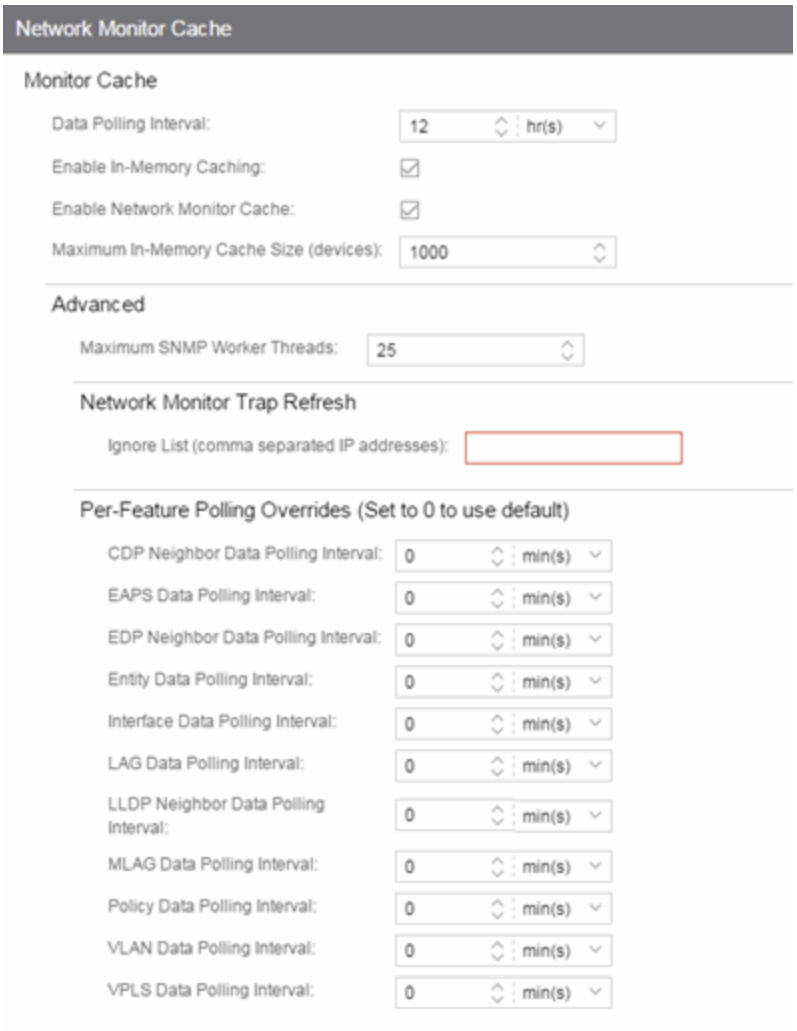
The network monitor cache stores information about the physical topology of a device, with additional emphasis on port information. Data is pulled from multiple places including slot and port details (Entity, ifTable), default role (Policy), neighbor link details (CDP, EDP, LLDP), Ethernet Automatic Protection Switching (EAPS), and Multi System Link Aggregation (MLAG).

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.



Data Polling Interval

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 increases background SNMP performed by the server.

Enable In-Memory Caching

Use this option to enable or disable the In-Memory Cache. To limit memory usage, disable the In-Memory Cache and configure the Device Cache rely directly on the database.

Enable Network Monitor Cache

Use this option to enable or disable the network monitor cache. Enabling the cache improves performance for Management Center views that request this information.

Maximum In-Memory Cache Size

The maximum number of devices whose data stored in the In-Memory Cache. This option lets you adjust the amount of memory the cache uses.

Advanced Settings

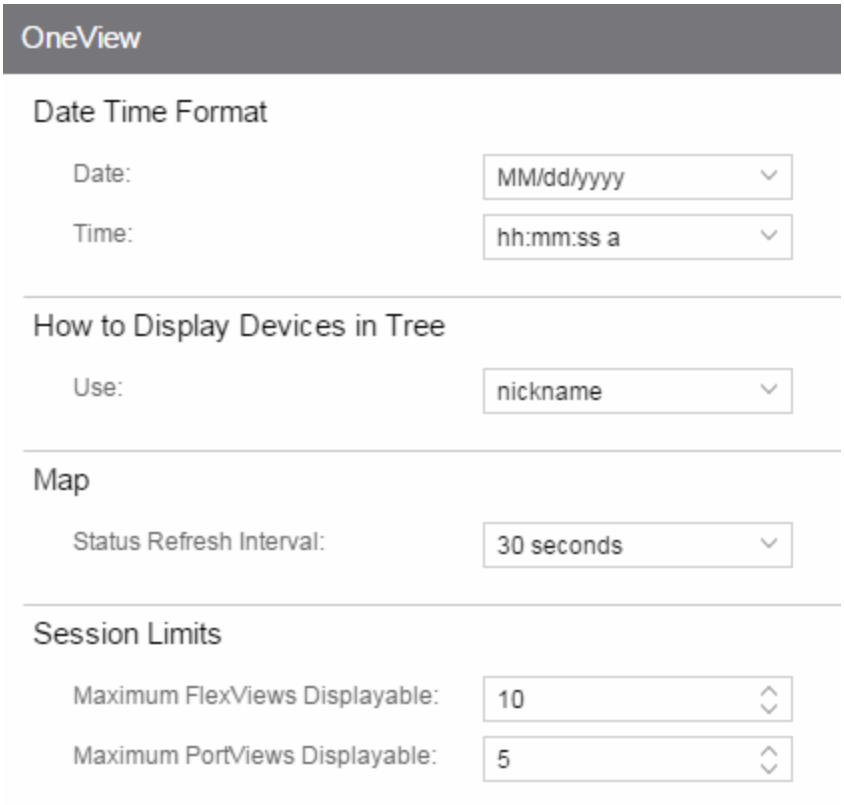
This section allows you to set network monitor cache advanced options.

- **Maximum number of SNMP worker threads.** 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 send SNMP queries in parallel.
- **Per-Feature polling overrides.** Allows you to set unique polling intervals for individual cache features polled more frequently. Set to 0 to use the interval set for the Data Polling Interval.

OneView Options

Selecting OneView in the left panel of the Options window provides the following view, where you can customize the date and time formats to your own personal preference. 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

Select how the date is formatted in 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

How to display devices in the device tree
: Select one of the following options:

  - IP — use the device's IP address.
  - systemName — use the administratively-assigned name of the device taken from the *sysName* MIB object.
  - nickname — use the user-defined nickname as defined in the Console Properties Tab (Device).

Map
: Select the interval that determines how often maps are automatically refreshed by Extreme Management Center. If None is selected, maps must be manually refreshed.

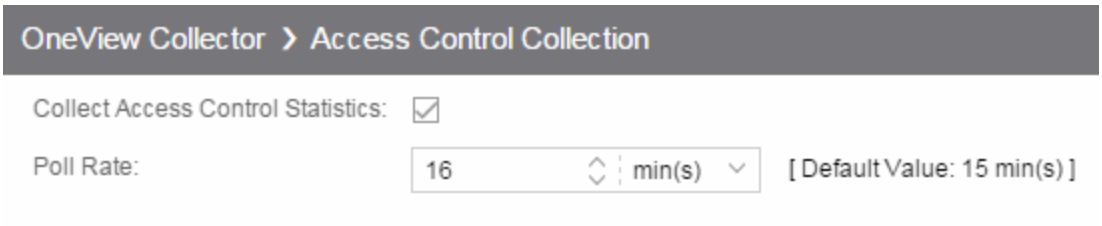
Session Limits
: Allows you to determine the maximum number of FlexViews and PortViews displayed per session.

OneView Collector Options

OneView Collector tree lets you access advanced device and interface collection settings for the OneView 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.

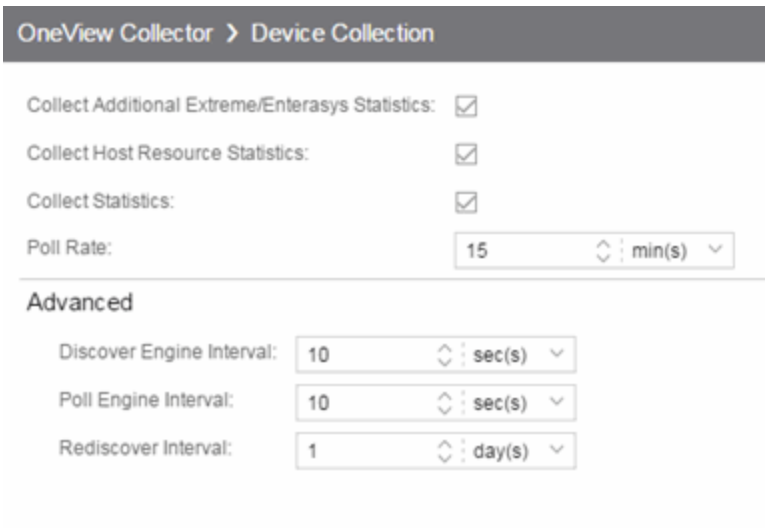
Access Control Collection



Collect Access Control Statistics
: Use this checkbox to enable or disable Extreme Access Control data collection.

Poll Rate
: The amount of time (in minutes) the data collector waits between polling Extreme Access Control engines.

Device Collection



Collect Additional Extreme/Enterasys Statistics
: Enables or disables Extreme or Enterasys switch resource statistics collection.

Collect Host Resource Statistics
: Enables or disables host resource statistics collection.

Collect Statistics
: Enables or disables additional statistics collection.

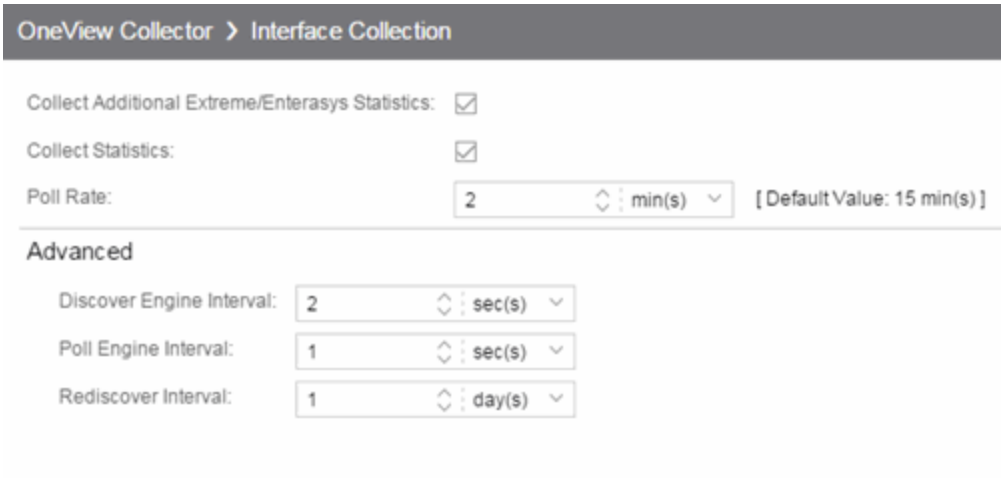
Poll Rate
: The amount of time the data collector waits between polling devices.

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 Max 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 Max 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 Additional Extreme/Enterasys Statistics
: Enables or disables Extreme or Enterasys switch resource statistics collection.

Collect Statistics
: Enables or disables additional statistics collection.

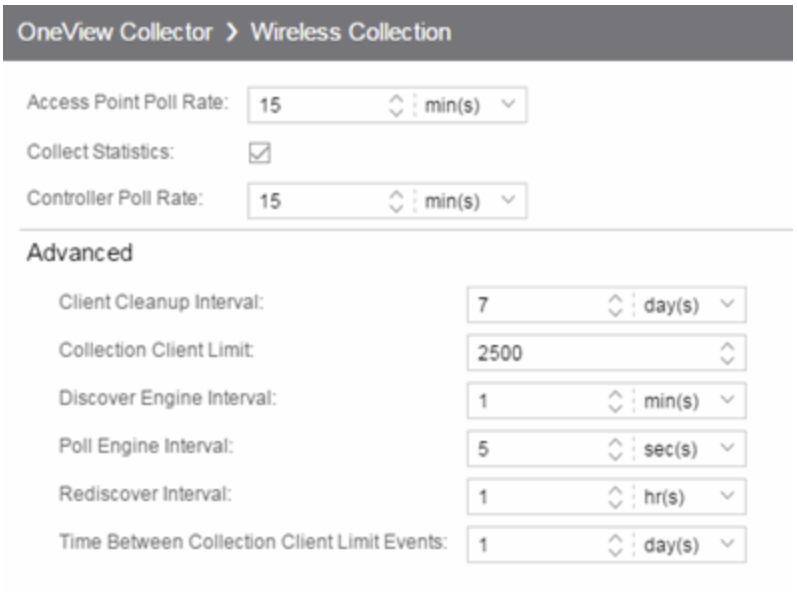
Poll Rate
: The amount of time the data collector waits between polling devices.

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 Max 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 Max 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



Access Point Poll Rate
: The amount of time (in minutes) the data collector waits between polling wireless access points.

Collect Statistics
: Use this checkbox to enable or disable wireless data collection.

Controller Poll Rate
: The amount of time (in minutes) 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.

Collection Client Limit
: The maximum number of wireless clients for which statistics are stored per collection interval. Valid values are 1 to 5000.

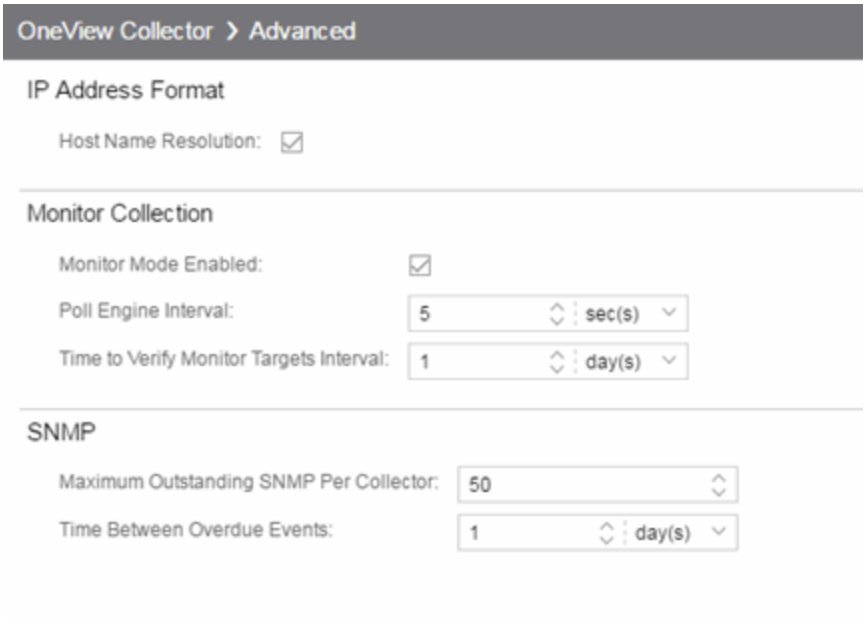
Discover Engine Interval
: This interval specifies the frequency the data collector performs discover operations on the collection targets. Discover operations are performed in blocks specified by the Max Outstanding SNMP per Collector value, with a new block scheduled according to the interval specified 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 Max 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.

Advanced Settings



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 Suite 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, seeEnable Report Data Collection.

Poll Engine Interval
: This interval specifies the frequency the data collector polls the collection targets. Polling is performed in blocks specified by the Max 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.

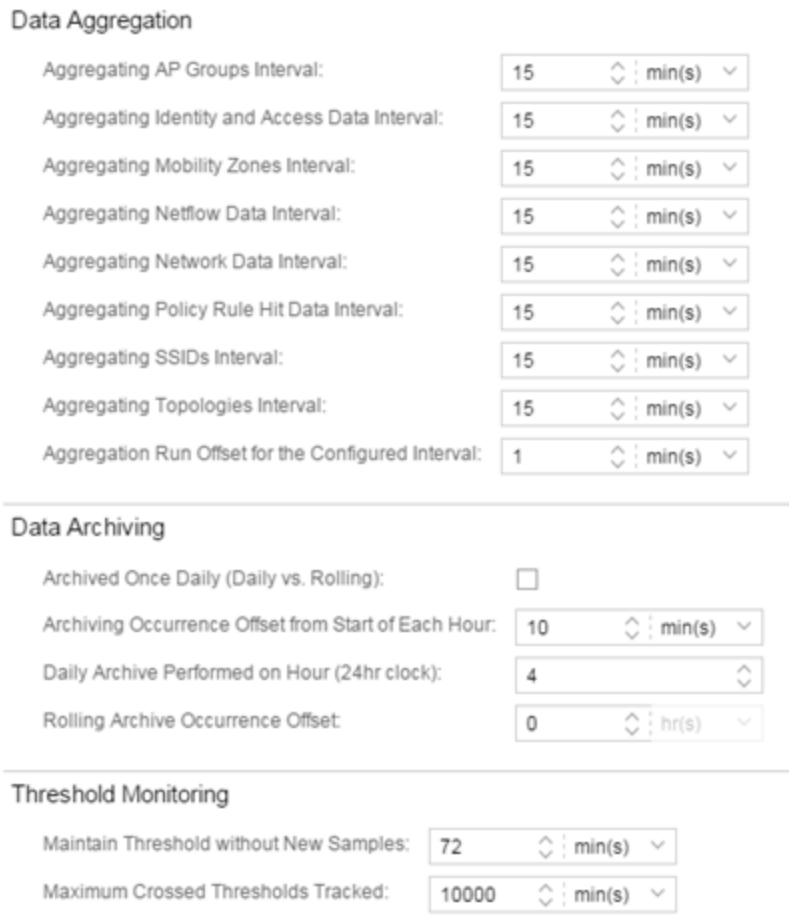
Time Between Overdue Events
: During a client cleanup, if a client is inactive for the amount of time specified here, then the client is aged out. Historical statistics already persisted are not removed.

OneView Engine Options

Selecting OneView Engine in the left panel of the **Administration** > **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 Settings



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 — If you want all the collection data (including the raw data, and the hourly, daily, weekly, and monthly data) archived once a day at a certain time, select the checkbox and specify the hour of day to perform the daily archive.
- 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, then 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

Server CPU Reporting

Extreme Management Center collects CPU usage statistics monitoring for the 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 Management Center database to provide data for the 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.

Policy Manager Options

These options apply only to the Policy Manager application. In the Administration > Options tab, the right-panel view changes depending on what you select in the left-panel tree. Expand the Policy Manager folder to view all the different options you can set.

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 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 class of service 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 option 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.

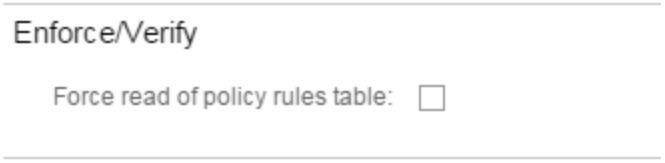
Role-Based Rate Limits/Transmit Queue Configuration
: Select this mode to configure role-based rate limits and transmit queues on devices. These rate limits are defined within a class of service and associated with a specific role via a rule action or as a role default. They are implemented based on the role assigned to a port. This mode also allows transmit queue behavior to be configured for the class of service. 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

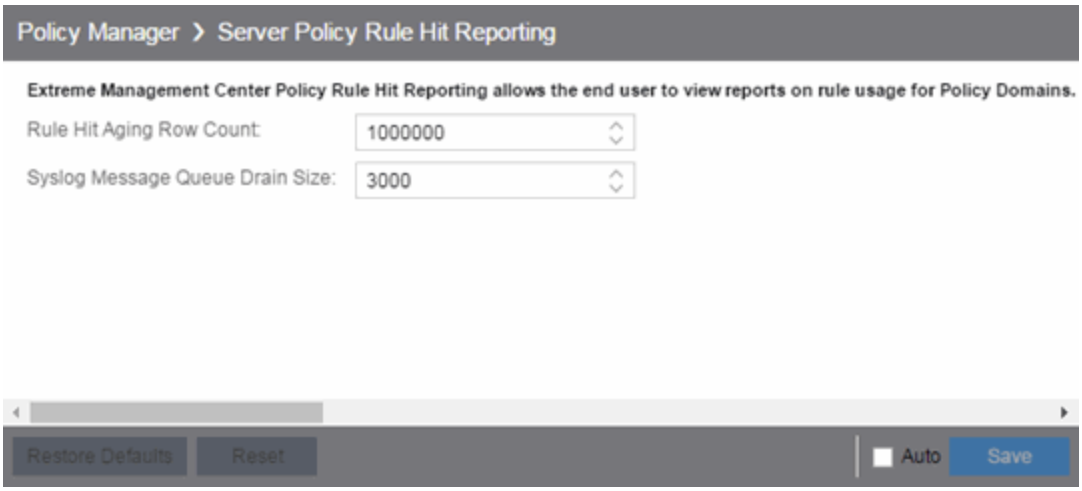


Force read of policy rules table

To improve performance time 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.

Server Policy Rule Hit Reporting

Server Policy Rule Hit Reporting allows you to configure the Policy Rule Hit Reporting feature. This feature allows you to view reports on rule usage for your policy domains. Access the reports from the View menu. To use rule hit reporting, rule accounting must be configured on the devices.



Rule Hit Aging Row Count

Once every 24 hours (based on when the server is started), the policy rule hit database table is trimmed to no more than the row count (number of entries) specified here. This prevents the table from getting too large. This setting is for all users.

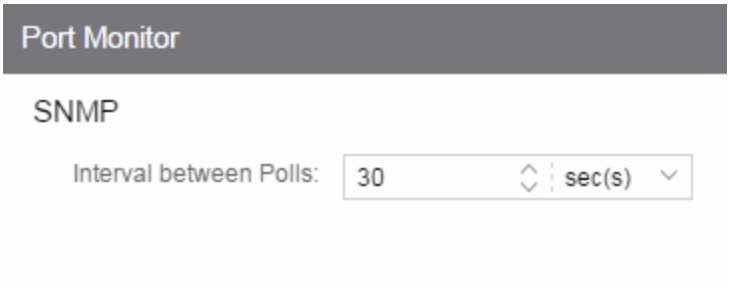
Syslog Message Queue Drain Size

Specifies the maximum number of rule hits written to the database by the reporting agent every two seconds. A message queue in the reporting agent stores all the rule hits from the syslog server. Every two seconds the queue is drained and the messages are written to the database. The Syslog message drain queue size limits the number of rule hits written to the database. This prevents the reporting agent from monopolizing the database in the case of a deny attack on the network, where many rule hits may be generated at one time. This setting applies to all users.

Port Monitor Options

Selecting Port Monitor in the left panel of the **Options** tab provides the following view where you can specify the Port Monitor display option. This applies to the current logged-in user.

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

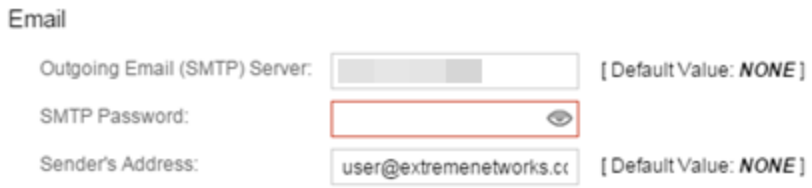


Interval between Polls
: The amount of time (in seconds) between polls of the device.

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 SMTP (Email) server used for outgoing messages.

SMTP Password
: The password for the user account entered in the Sender's Address field.

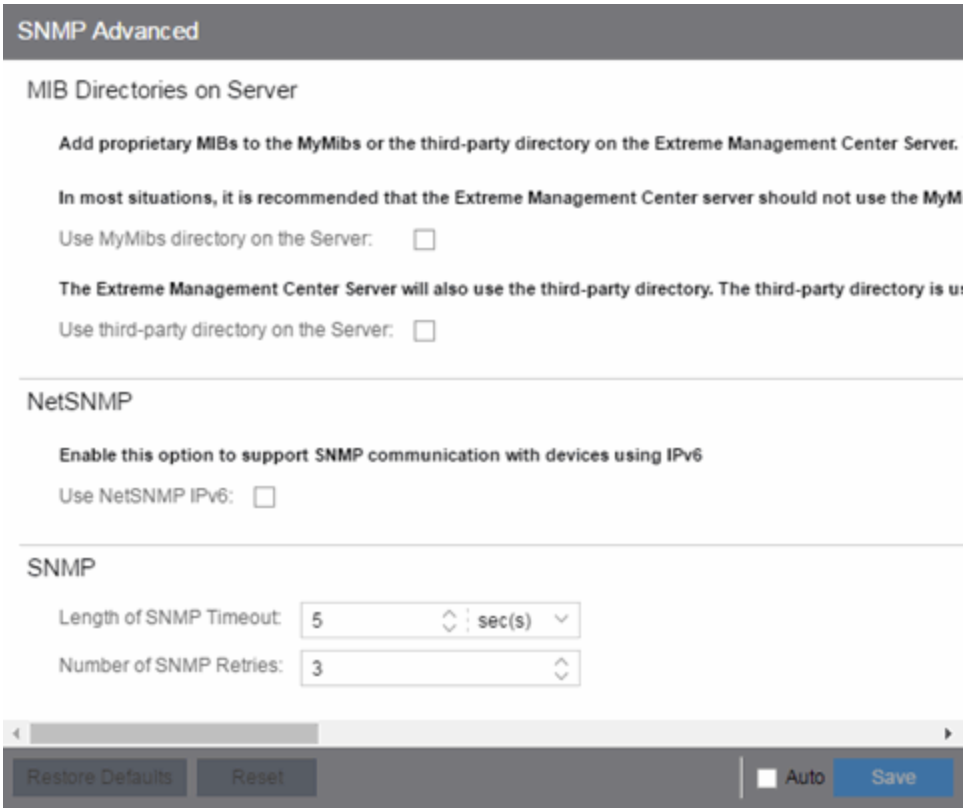
Eye Icon
: When selected, the password is shown in text. When unchecked, the password is shown as a string of asterisks.

Sender's Address
: The sender's address used to send outgoing email notification messages. Enter the address in a fully qualified format such as "sender's name@sender's domain."

SNMP Advanced Options

Selecting SNMP Advanced in the left panel of the Options window provides the following view, which allows you to configure the Extreme Management Center Server to use the MyMibs directory or thirdparty directory.

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.



Use MyMibs directory on the Server

Add proprietary MIBs to the MIB database on the Management Center Server in the MyMibs directory. This MIB information is then distributed to the Management Center remote clients. If you select this option, the Management Center Server also uses the MyMibs directory (e.g. the MIBs is included in the SNMP Server Stack).

Use third-party directory on the Server

The thirdparty directory is used for proprietary, client-based FlexViews and MIB Tools (Enterprise MIBs owned by other companies), not standard IETF or IEEE MIBs. If you select this option, the Management Center Server also uses the thirdparty directory.

CAUTION: Do **not** use the MyMibs or thirdparty directories unless it is required on your network as selecting this option may cause Management Center Server instability and undesirable consequences.

Use NetSNMP IPv6

The Use NetSNMP IPv6 option allows you to SNMP-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.

These options apply to all users. For these setting to take effect, the Management Center Server must be restarted.

Length of SNMP Timeout (in seconds)

The amount of time (in seconds) Management Center waits before re-trying to contact a device. The default setting is 5 seconds. The value for this setting must be between 3 and 60 seconds.

Override this value on a per-device basis in the Edit Device window by highlighting a device in the Devices table on the Network > Devices 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.

Number of SNMP Retries

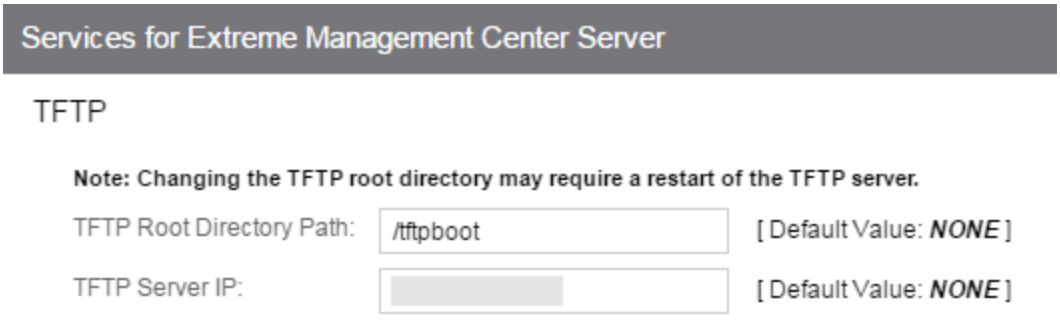
The number of attempts made to contact a device after an attempt at contact fails. The default setting is 3 retries, which means that Management Center retries a timed-out request three time after the initial attempt at contact is made, making a total of four attempts to contact a device. The value for this setting must be between 1 and 60 tries.

Override this value on a per-device basis in the Edit Device window by highlighting a device in the Devices table on the Network > Devices tab.

Services for Extreme Management Center Server Options

Selecting Services for Extreme Management Center Server in the left panel of the Options window provides the following view where you can specify your TFTP settings. 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.



TFTP Root Directory Path

You must specify a TFTP root directory, whether you are using the Management Center TFTP server or another TFTP server. The root directory is the base directory to which the TFTP server is allowed access. The TFTP server is allowed to create files to or read files from this directory and any of its subdirectories. Use the default root directory or enter a path to an alternate root directory in this field. Restart the TFTP server if you change the TFTP root directory.

NOTES: Changing the **TFTP Root Directory Path** may require a restart of the TFTP server.

If you are using a TFTP server other than the Management Center 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 // (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\`

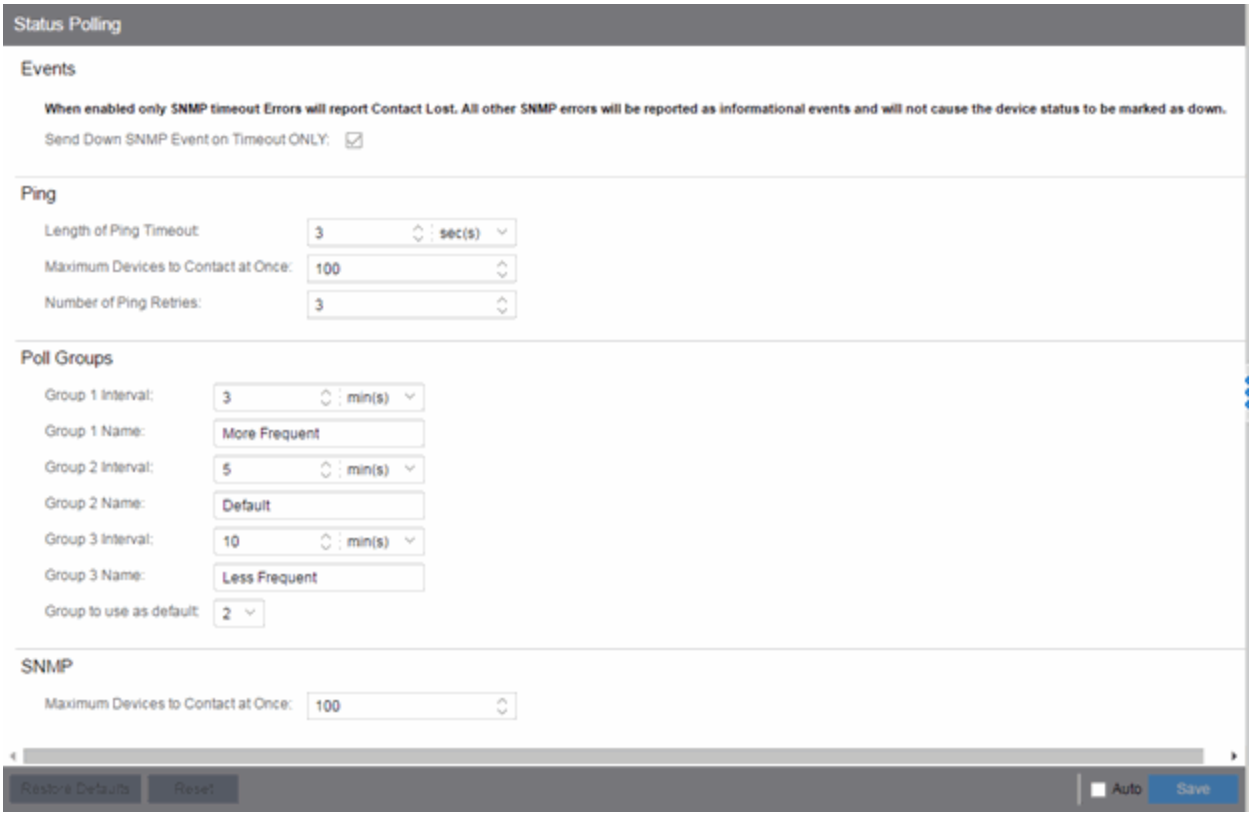
TFTP Server IP

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 here. This field accepts both IPv4 and IPv6 addresses.

Status Polling Options

Selecting Status Polling in the left panel of the **Options** tab provides the following view, where you can specify options for polling devices in the left-panel device tree. 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 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 Edit 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 this 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 does 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 (in seconds) Management Center waits before re-trying to ping a device. The default setting is 3 seconds. The maximum setting is 20 seconds.

Maximum Devices to Contact at Once
: The maximum number of IP addresses that Management Center attempts to contact simultaneously.

Number of Ping Retries
: The number of attempts made to ping a device. The default setting is 3 retries, which means Management Center retries a timed-out request three times, making a total of four attempts to contact a device.

Poll Groups

There are three poll groups that each define a unique poll frequency. The poll frequency for each group specifies the actual length of the poll cycle in seconds. The interval for individual poll groups can be set according to your network's needs using the guidelines below. Select one group as the default poll group. When a device is added to the 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 Edit Device window.

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 Devices to Contact at Once setting. This determines the maximum number of devices from each group polled at any given time. 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, Management Center 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 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 number of devices to contact at once) 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.

SNMP

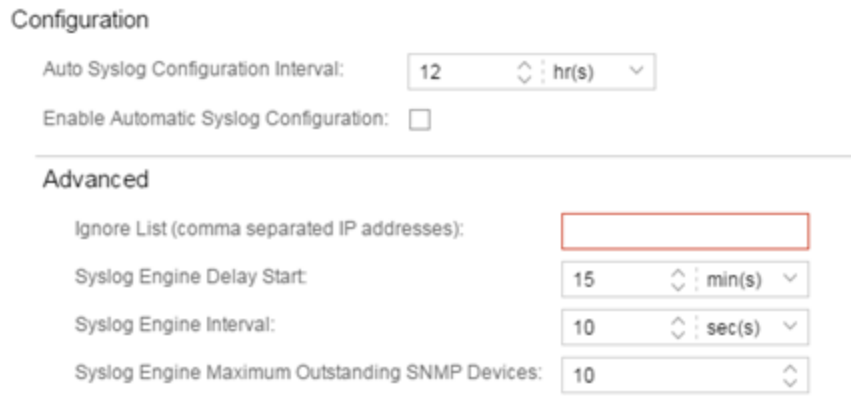
This status polling option pertains to devices whose poll type is set to SNMP.

Maximum Devices to Contact at Once
: The maximum number of IP addresses that Management Center attempts to contact simultaneously.

Syslog Options

Selecting Syslog in the **Administration** > **Options** tab opens the following view, which allows you to configure Extreme Management Center to automatically save information in the syslog.

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.



Auto Syslog Configuration Interval
: Enter the frequency with which Management Center automatically gathers information and posts it to the syslog.

Enable Automatic Syslog Configuration
: Select the checkbox to configure Management Center to automatically gather information and post it to the syslog.

Ignore List (comma separated IP addresses)
: Enter any IP addresses you do not want logged to the syslog automatically.

Syslog Engine Delay Start
: The amount of time Management Center waits before information in the syslog is aggregated and archived.

Syslog Engine Interval
: The amount of time between information in the syslog is aggregated and archived.

Syslog Engine Maximum Outstanding SNMP Devices
: The maximum number of outstanding SNMP devices archived by the syslog.

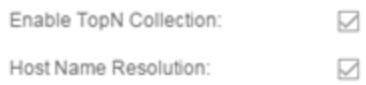
TopN Collector Options

The TopN Collector gathers the data used in TopN reports. It also collects the signal strength data reported by Wireless Controllers.

You can use this view to enable or disable TopN collection and host name resolution, and specify the number of days to maintain the TopN History. See below for more information on 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.

Collect TopN Data



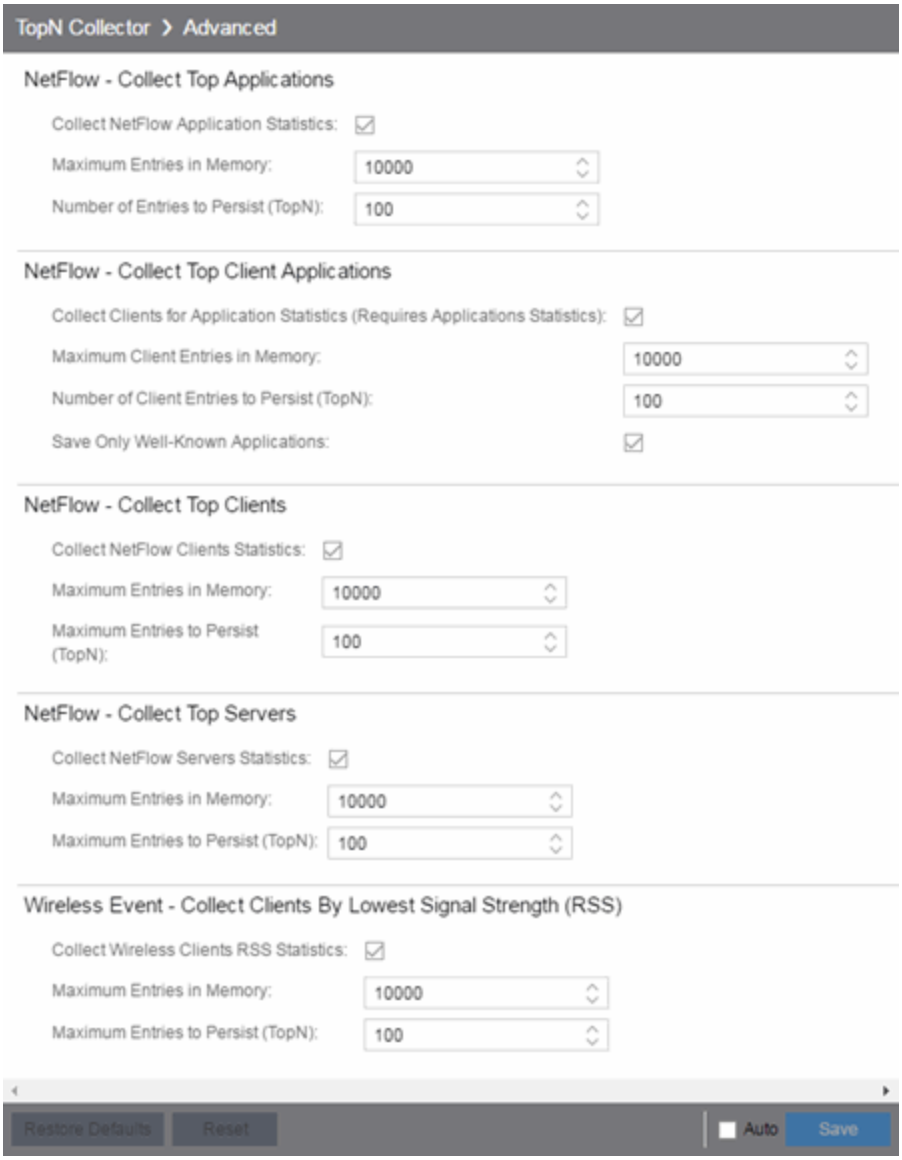
Enable TopN Collection
: This option allows you to enable and disable the TopN Collector. Changes to this option take place immediately.

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 Suite Name Resolution option.) Changes to this option take place immediately.

History

TopN History Data Retention
: This setting determines the number of days of 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.

Advanced



The TopN Collector collects the data used in TopN reports for applications, client applications, clients, and servers. It also collects the signal strength data reported by Wireless Controllers. 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.

You can use these advanced settings to enable and disable the collection of different TopN data. Enabling and disabling collection takes effect immediately.

You can specify the number of entries to save at the end of each hourly interval. You can also control the amount of memory used during the hour to collect information, by specifying a maximum number of entries. 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.

If you change the value for Number of Entries to Persist (TopN), the new value will be used for the next hourly calculation. For example, if you change the value at 3:05 or 3:55, the new value will be used for the 4:00 calculation.

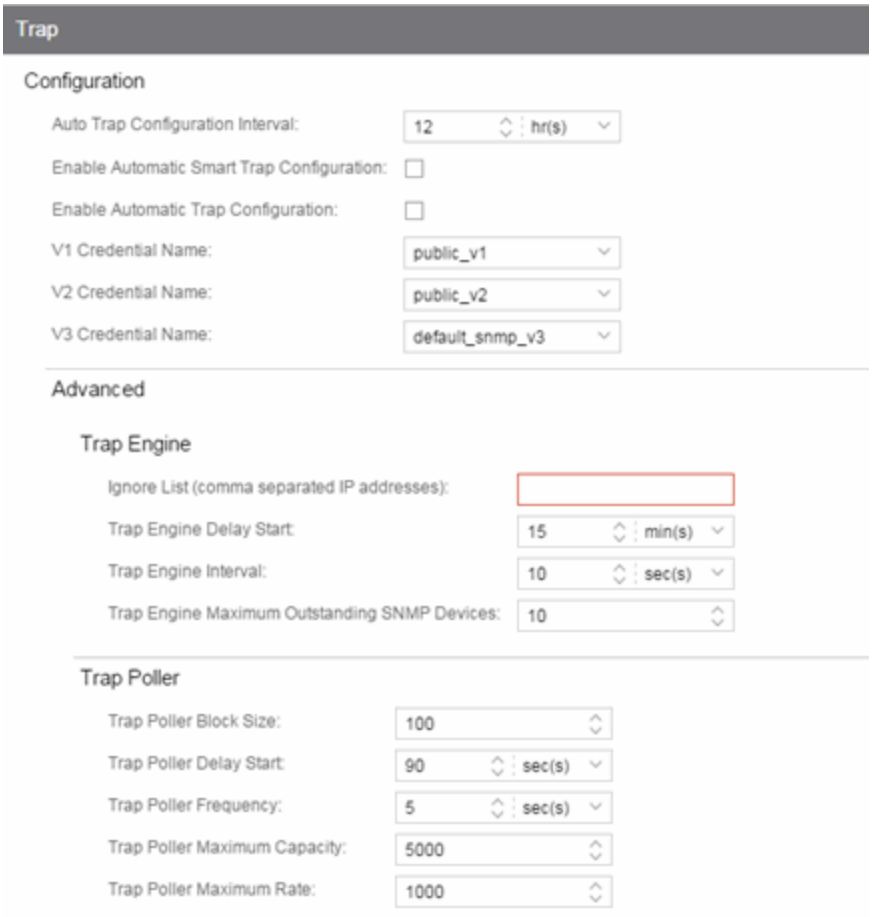
If you change the value for Maximum Number of Entries in Memory, the new value takes effect during the next hour of data collection. For example, if you change the value at 3:05 or 3:55, it takes effect during the hour that starts at 4:00 and ends at 5:00.

The default number of entries to persist is 100, with a minimum value of 5 and a maximum value of 1000. The default maximum number of entries in memory is 10000 with a minimum value of 1000 and a maximum value of 1,000,000.

Trap Options

Use this panel to set Trap Advanced Settings, Trap Poller Block Size, and configure IP addresses to ignore. This panel is accessible in the **Administration > Options** 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

Allows you 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.

Trap Engine

Use this section to enter a list of IP addresses that should be ignored by traps and to configure trap engine options.

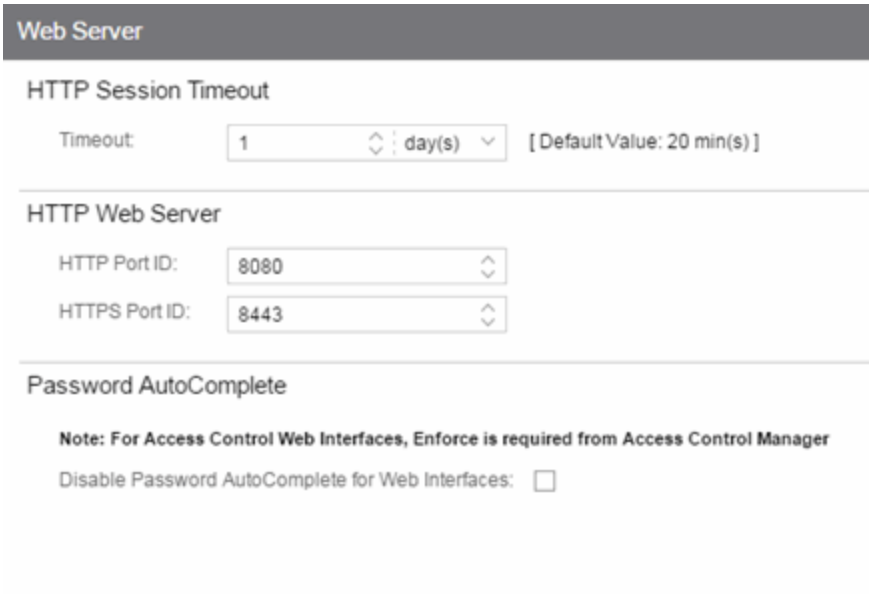
Trap Poller

Use this section to set advanced options for polling traps.

Web Server Options

Selecting Web Server in the left panel of the Administration > Options tab provides the following view where you can 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 Extreme Management Center client applications. By default, Management Center uses port ID 8080 (HTTP) and 8443 (HTTPS). If you change the port ID, you must restart the Management Center Server for the change to take effect.

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 Management Center web-based views.

HTTP Web Server

The HTTP Port ID and HTTPS Port ID fields let you specify the HTTP and HTTPS port ID for HTTP web server traffic, respectively.

Password AutoComplete

The Disable Password AutoComplete for Web Interfaces option lets you disable automatic password completion for users logging into Management Center web interfaces. Note that for Extreme Access Control

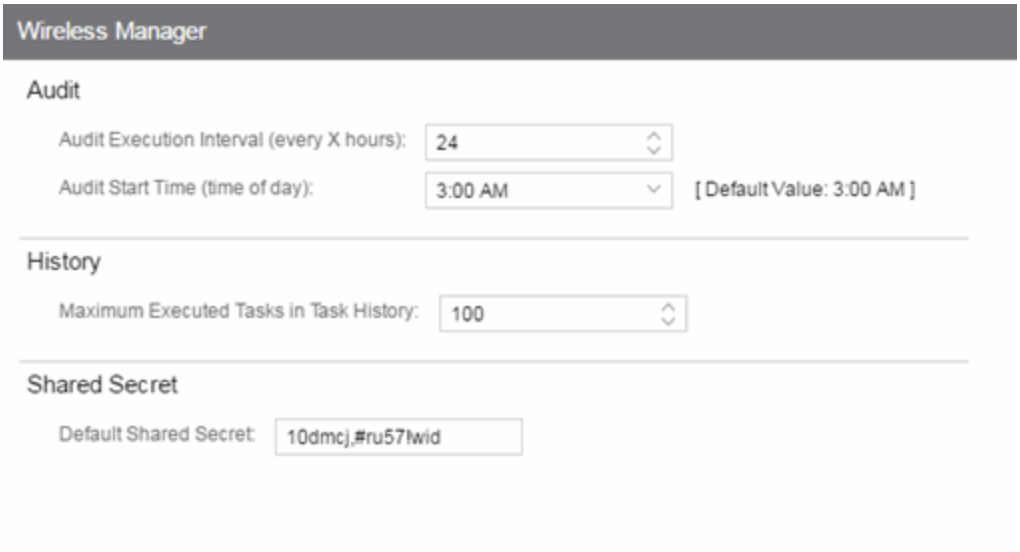
web interfaces, you must enforce from the Access Control tab for the option to take effect.

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 Administration > Options panel 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.



Audit

Wireless Manager audits controller configuration 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. Select the time of day when the audit starts in the Audit Start Time (time of day) field and the interval in hours between the start of successive audits using the Audit Execution Interval (every X hours) field. Auditing once every 24 hours is sufficient for most sites, but more frequent auditing can be enabled through this option.

History

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 will retain in its database. The default is 100 executed tasks retained, and the maximum is 500 tasks retained.

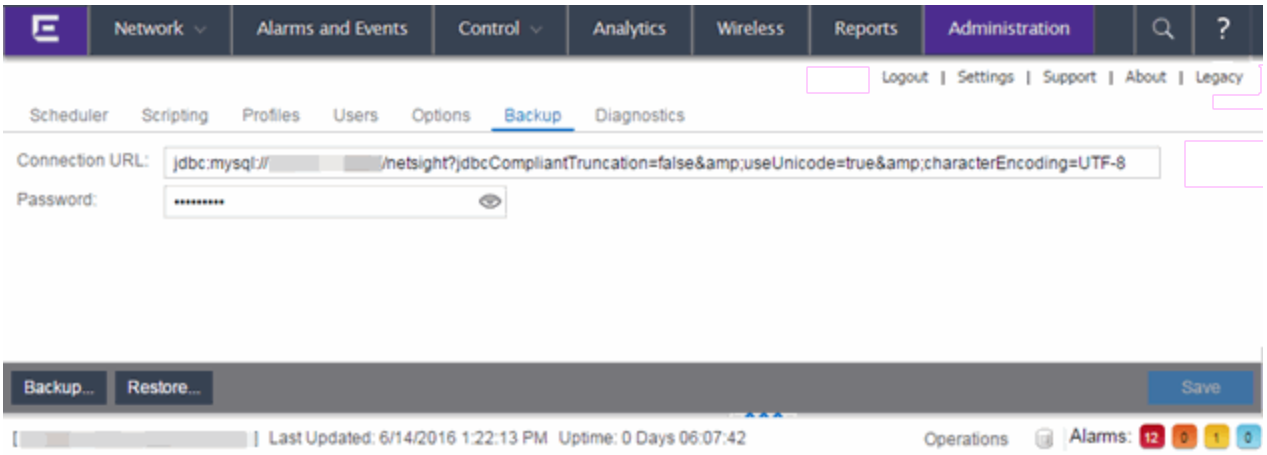
Shared Secret

When Extreme Management Center discovers a new controller, Wireless Manager attempts to authenticate with the controller using this shared secret. For proper functioning of Extreme Management Center, Wireless Manager, and Wireless Advanced Services, the controller must be configured with the same shared secret as Wireless Manager. Each controller can be configured with a different shared secret as long as Wireless Manager knows what it is. You can configure Shared Secrets on a per controller basis using Wireless Manager. Please refer to the Wireless Manager online Help for additional details.

Backup

This tab allows you to manage the password and connection URL for the database, and perform database backup and restore operations. You must be assigned the appropriate user capabilities to perform these functions.

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. Management Center then adds one generic user name (user = netsight) and password (password = enterasys). Change this password, since all customers who install Management Center know this generic password.



The values entered here are used by the Management Center Server when it connects to the database. The database is secured via a credential comprised of a user name and password (see the Important note above). This area lets you modify that password, and also view and modify the connection URL for the database.

Connection URL

Displays the URL the 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.

You must restart both the Management Center Server and client after you change the Connection URL.

Password
: Enter the password the Management Center uses when connecting to the database. The password is masked unless you select the Eye icon. You must restart both the Management Center Server and client after you change the database password.

Extreme Management Center Data Set Operations

This area lets you perform database backup and restore operations.

Backup Button
: Opens the Backup Database window where you can save the currently active database as a file. If the Management Center Server is local, you can specify a directory path where want the backup file stored. If the server is remote, the database is saved to the default database backup location.

Restore Button
: Opens the Restore Database window where you can restore the initial database or restore a saved database. Restoring an initial database removes all data elements from the database and populates the Management Center Administrator authorization group with the name of the logged-in user. Both functions cause all current client connections and operations in progress to be terminated. You must restart both the Management Center Server and the client following an initialize database operation. When restoring a database, if the server is remote, you only have access to databases in the default database backup directory.

NOTE: When restoring a saved database to a new 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 Management Center server.

- Changes to the default -Xmx memory settings in the <install directory>\NetSight\services\nsserver.cfg file need 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.

Related Information

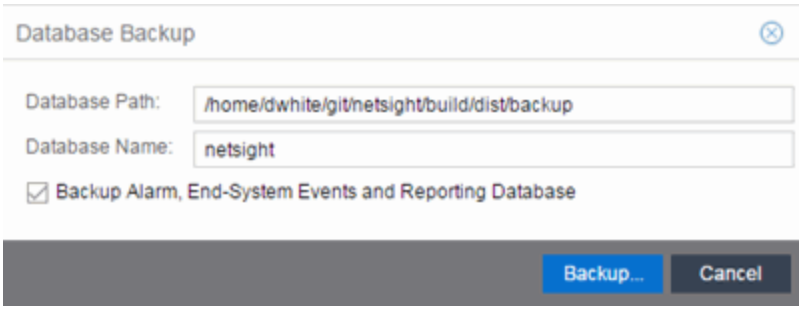
For information on related topics:

- Backup
- Restore

Database Backup

Use the Backup Database window to save the currently active database to a file on the Extreme Management Center (formerly NetSight) Server workstation. If the Management Center Server is local, you can specify a directory path in which to save the backup file. If the server is remote, the database is saved to the default database backup location. You can access this window by clicking the **Backup** button in the **Administration** > Backup tab.

NOTE: To schedule regular database backups, use the Database Backup option available from **Administration** > **Options** > **Database Backup**.



Database Path
: The default database backup location. If the Management Center Server is local, you can specify an alternate backup directory by entering a path to the directory, or using the **Browse** button to navigate to the directory. If the server is remote, the database is saved to the default database backup location.

Database Name
: Enter a name for the database backup file.

Backup Alarm, End System Event and Reporting Database
: The **Backup Alarm, End System Event and Reporting Database** checkbox lets you enable and disable backup of alarm, end-system event and reporting data as part of the backup operation. Because the database can be quite large, this allows you to control the amount of disk space used by the database backup operation.

Backup Button
: Starts the backup operation.

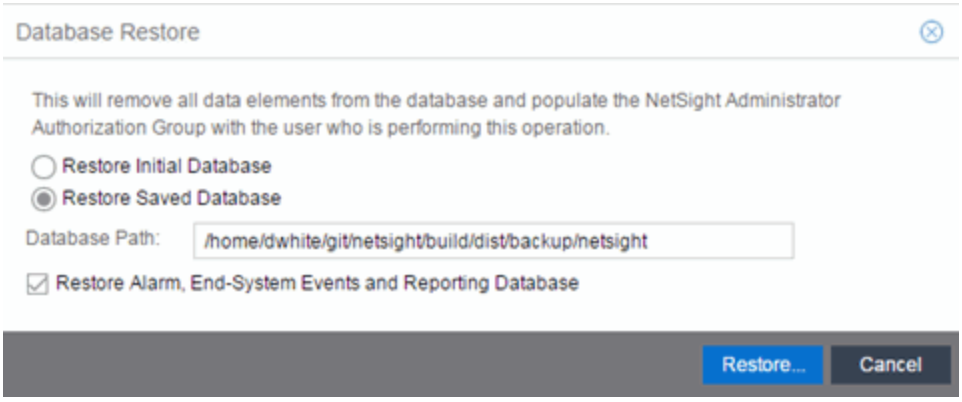
Related Information

For information on related topics:

- Backup
- Database Backup Options

Database Restore

Use the Restore Database window to restore the initial database or restore a saved database. Both functions cause all current client connections and operations in progress to be terminated. You can access this window by clicking the **Restore** button on the **Administration** > Backup tab.



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. You must restart both the Management Center Server and the client following an initialize database operation.

Restore Saved Database

Select this option and specify the path of the database you wish to restore. If the server is remote, you only have access to databases in the default database backup directory.

NOTE: When restoring a saved database to a new 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 Management Center server.

- Changes to the default -Xmx memory settings in the <install directory>\NetSight\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 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 Alarm, End System Event and Reporting Database
: The **Restore Alarm, End System Event and Reporting Database** checkbox lets you enable and disable restoring alarm, end-system event and reporting data as part of the restore operation. This option is only enabled if you have selected the **Restore Saved Database** option and the selected backup has a Management Center database included with it.

Restore Button
: Starts the restore operation.

Related Information

For information on related topics:

- Backup

Extreme Management Center Extreme Connect Overview

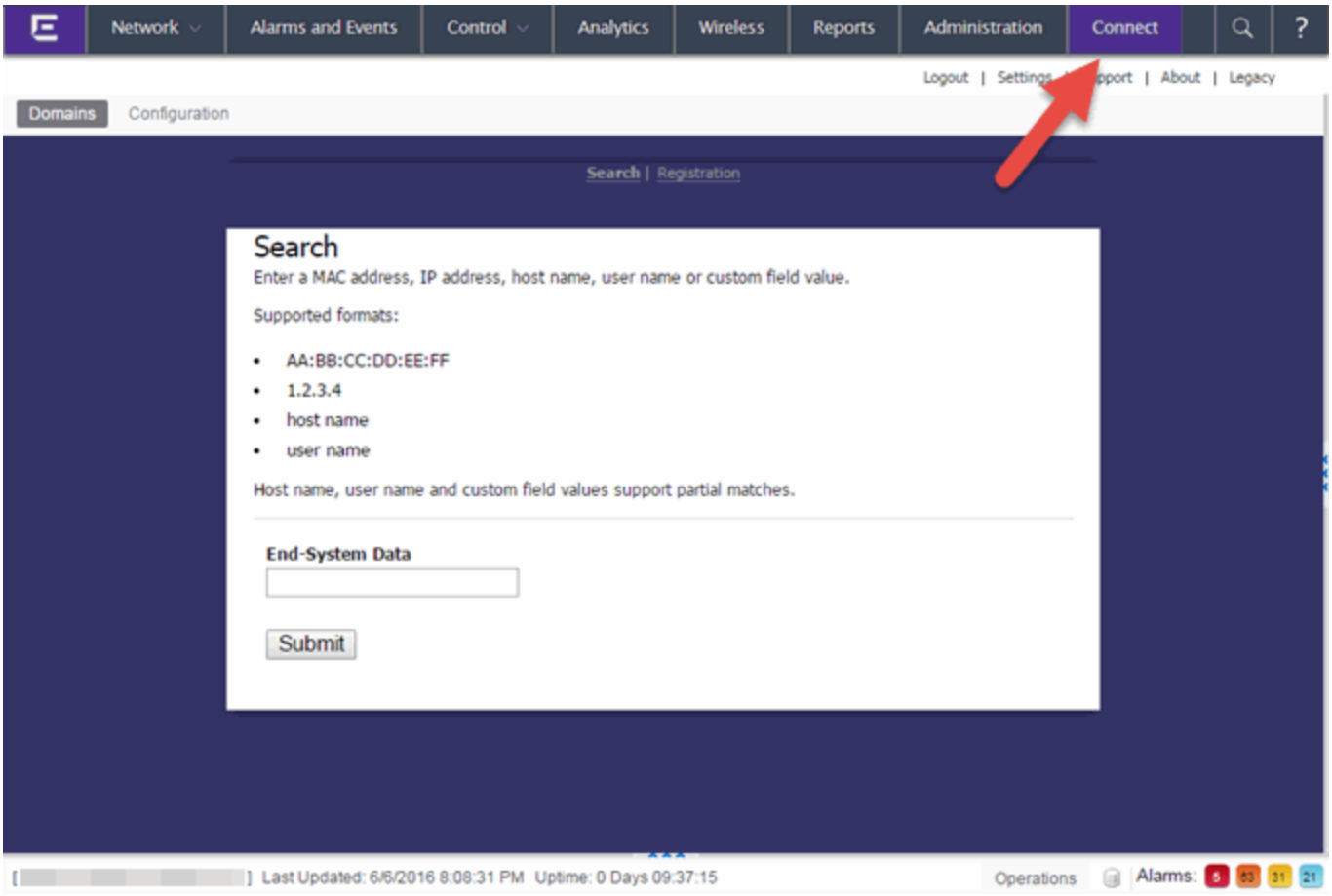
The Extreme Management Center **Connect** tab allows you to integrate third-party software with Management Center's Extreme Access Control solution.

Management Center's 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 Management Center.

To open the **Connect** tab, select **Connect** at the top of Management Center.

NOTE: Extreme Connect requires a 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 two sub-tabs:

- Domains — Allows you to search for a particular end-system in multiple versions of Management Center and returns information found using your third-party software. You can also add or remove MAC addresses from end-system groups.
- 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.

Additionally, the Menu at the top of the screen provides links to additional information about your version of Management Center.

Extreme Connect Requirements

The following outlines the system requirements for Extreme Connect:

- Management Center version 7.0
- Enough switches that support multi-user authentication and policy for the number of end-user sessions on the network.

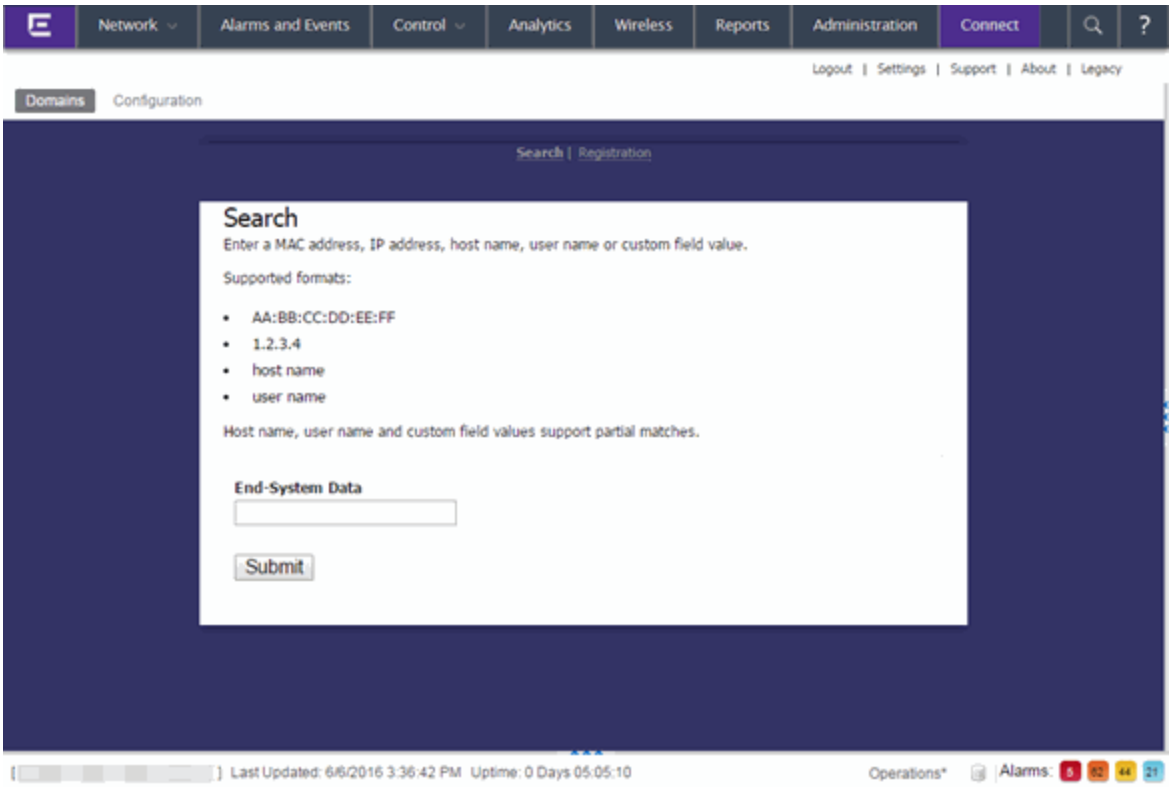
Related Information

For information on related tabs:

- Domains
- Configuration

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.



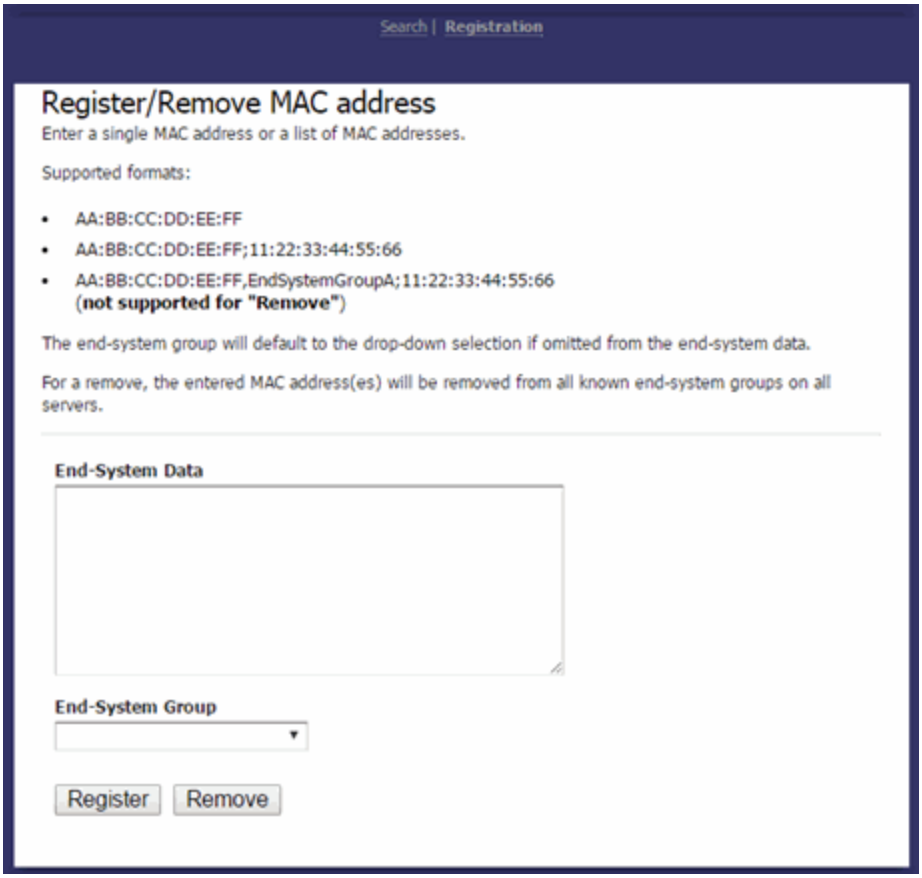
The **Domains** tab contains two sub-tabs:

- 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 — Allows you to search for an end-system across multiple versions of Management Center in all modules using the following criteria:
  - MAC address
  - IP address
  - Hostname
  - Username
  - Custom Field (user-defined value)

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 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 Management Center.

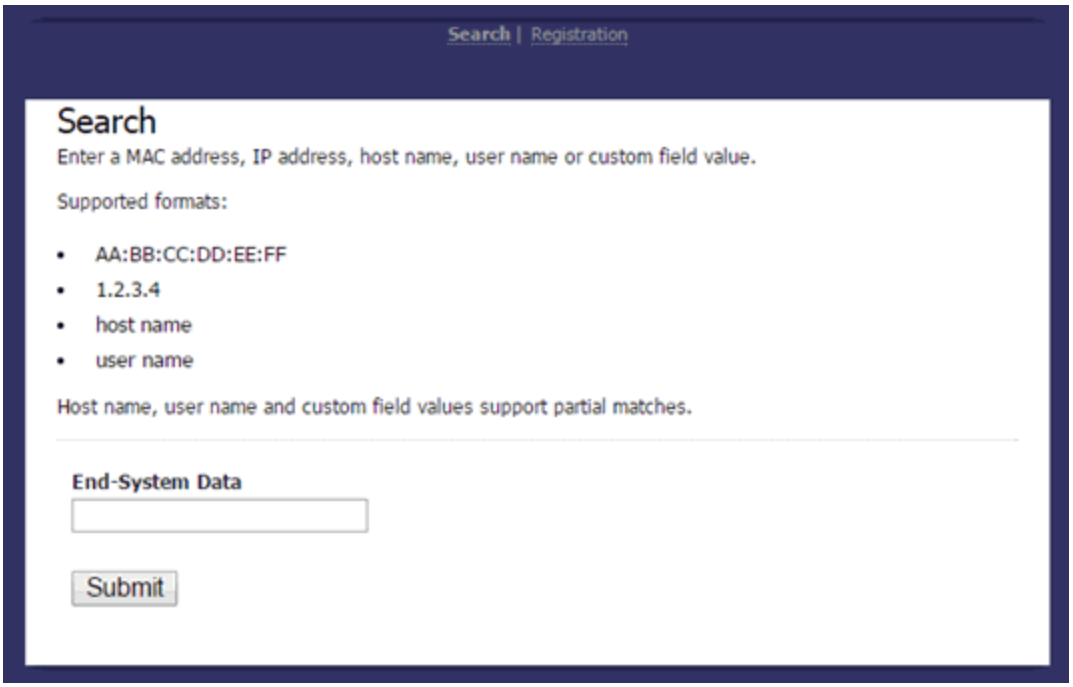
Register Button
: Click the **Register** button to add the end-system MAC addresses to the end-system group listed in the **End-System Data** field or selected in the **End-System Group** drop-down menu.

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 Access Control tab to configure network access rules for the end-systems in the group.

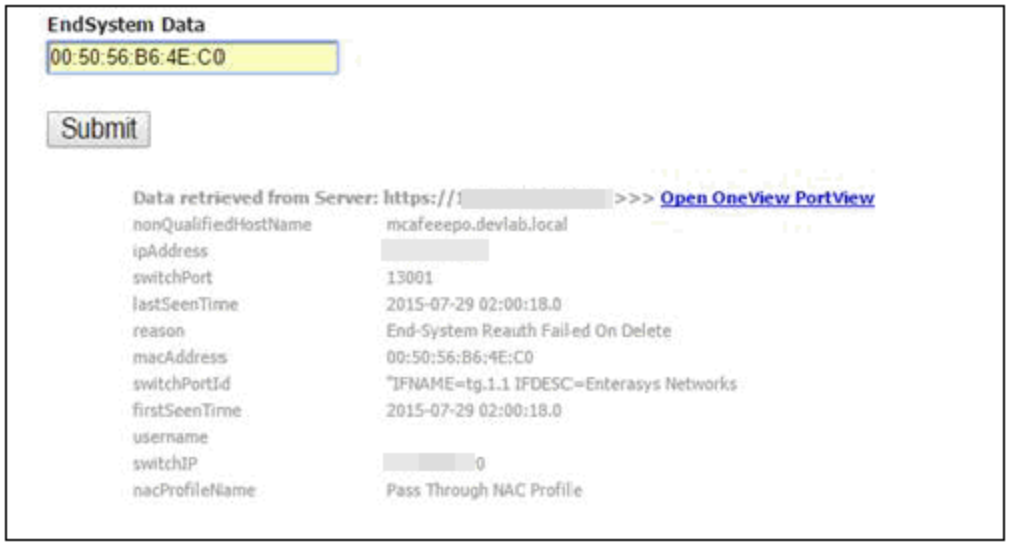
Search

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 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.



Related Information

For information on related tabs:

- Extreme Management Center Connect Overview
- Configuration

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.

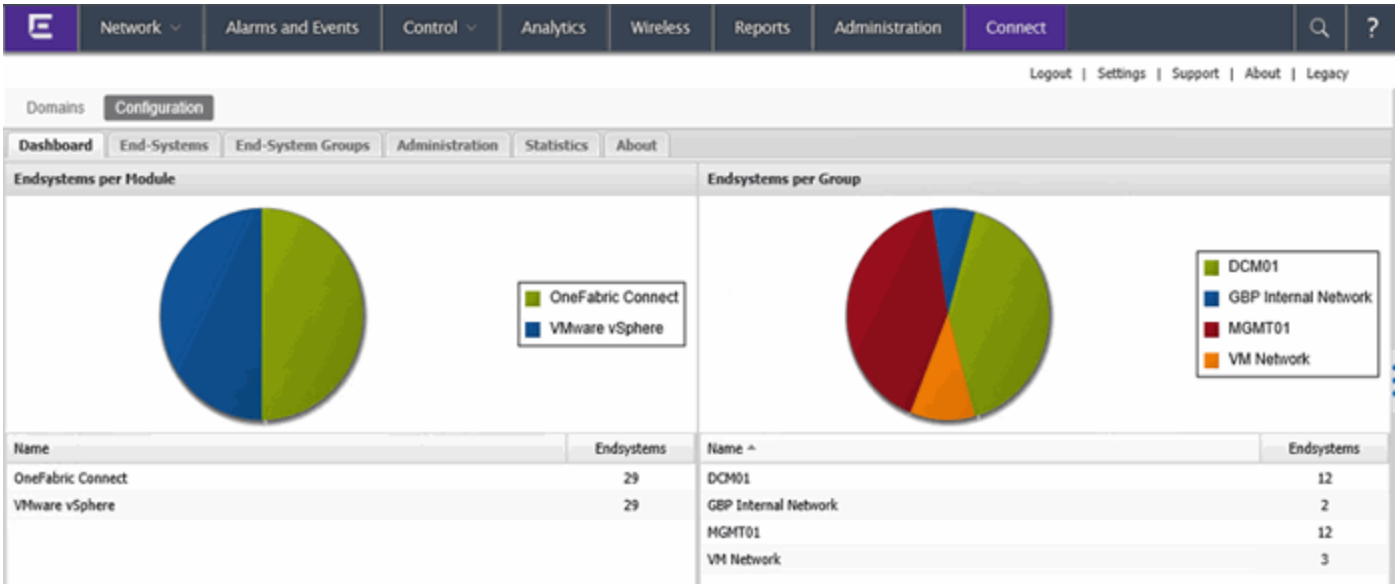
The **Configuration** tab contains the following sub-tabs, each providing information about end-systems:

- 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 Management Center communicates with each module and the behavior of the module within 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.

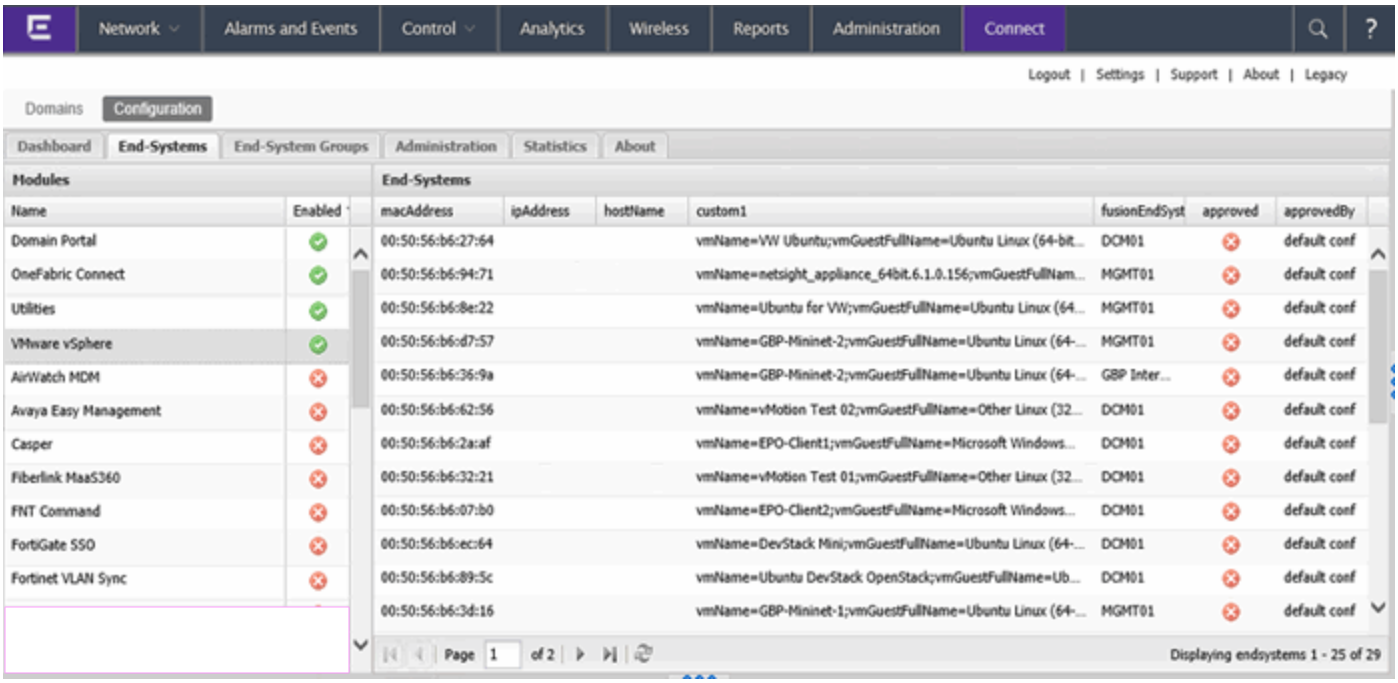
Dashboard

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:

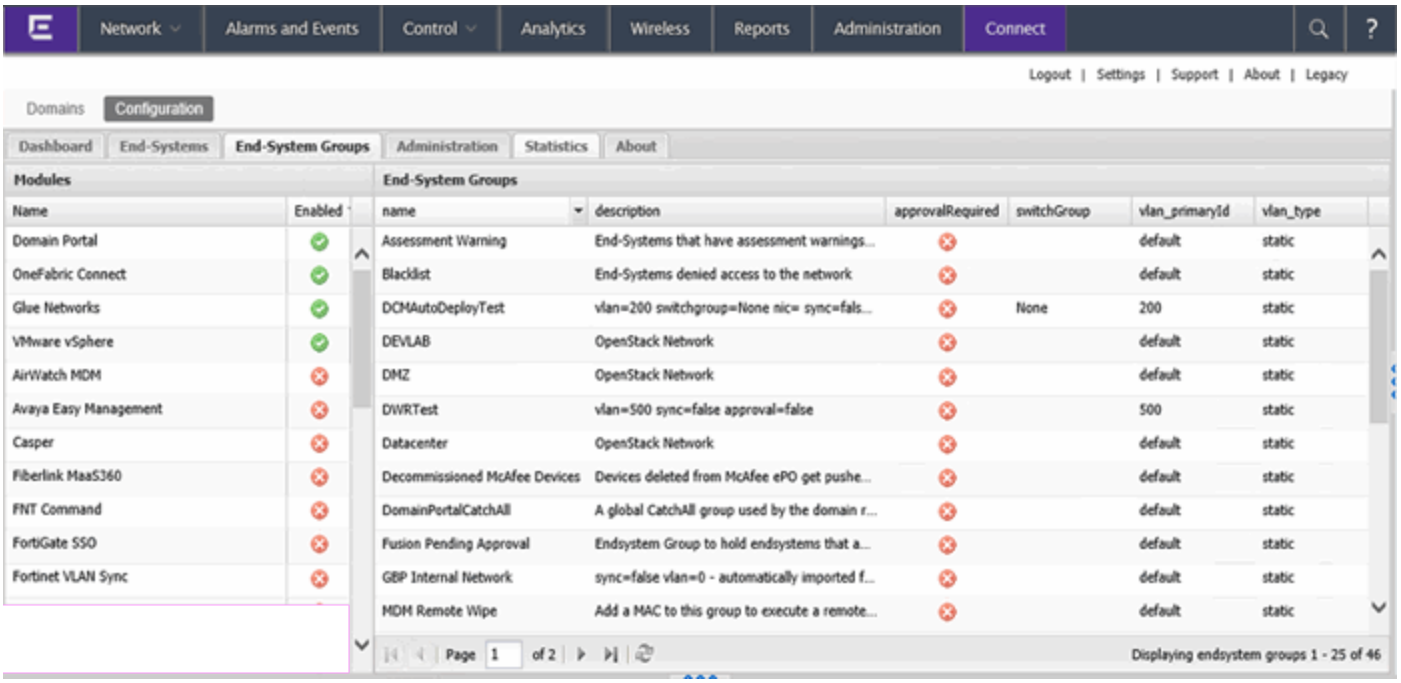
- Check icon (✓) — Module enabled on your network.
- X icon (✗) — Module not enabled on your network.

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

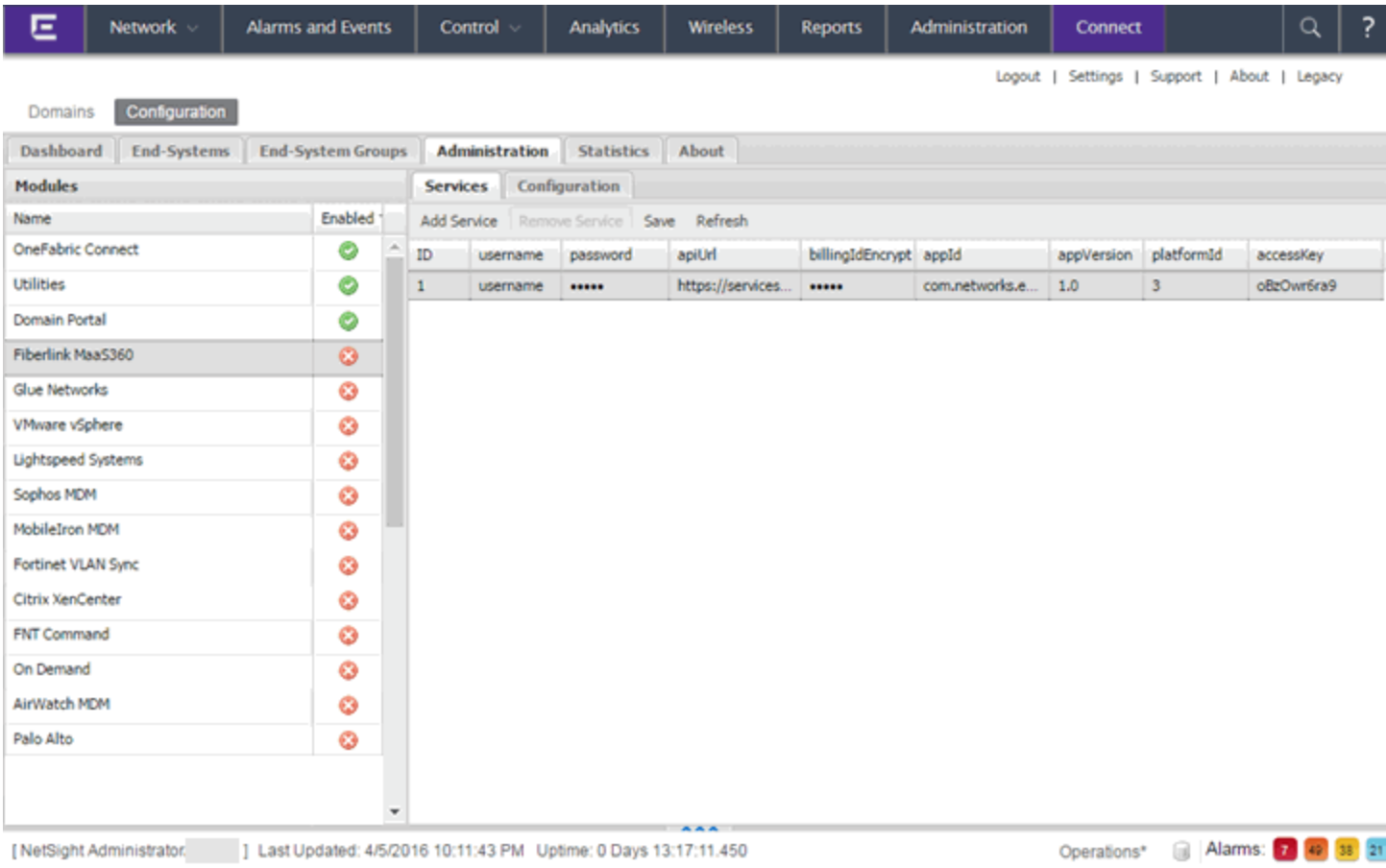
In the **Administration** tab, enter the information that details how Management Center connects to the module server and configure the module in Management Center.

The tab contains two sub-tabs:

- **Services** — A service outlines to 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 Management Center and how that information is presented.

Services

Access the **Services** tab to specify information detailing how 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.

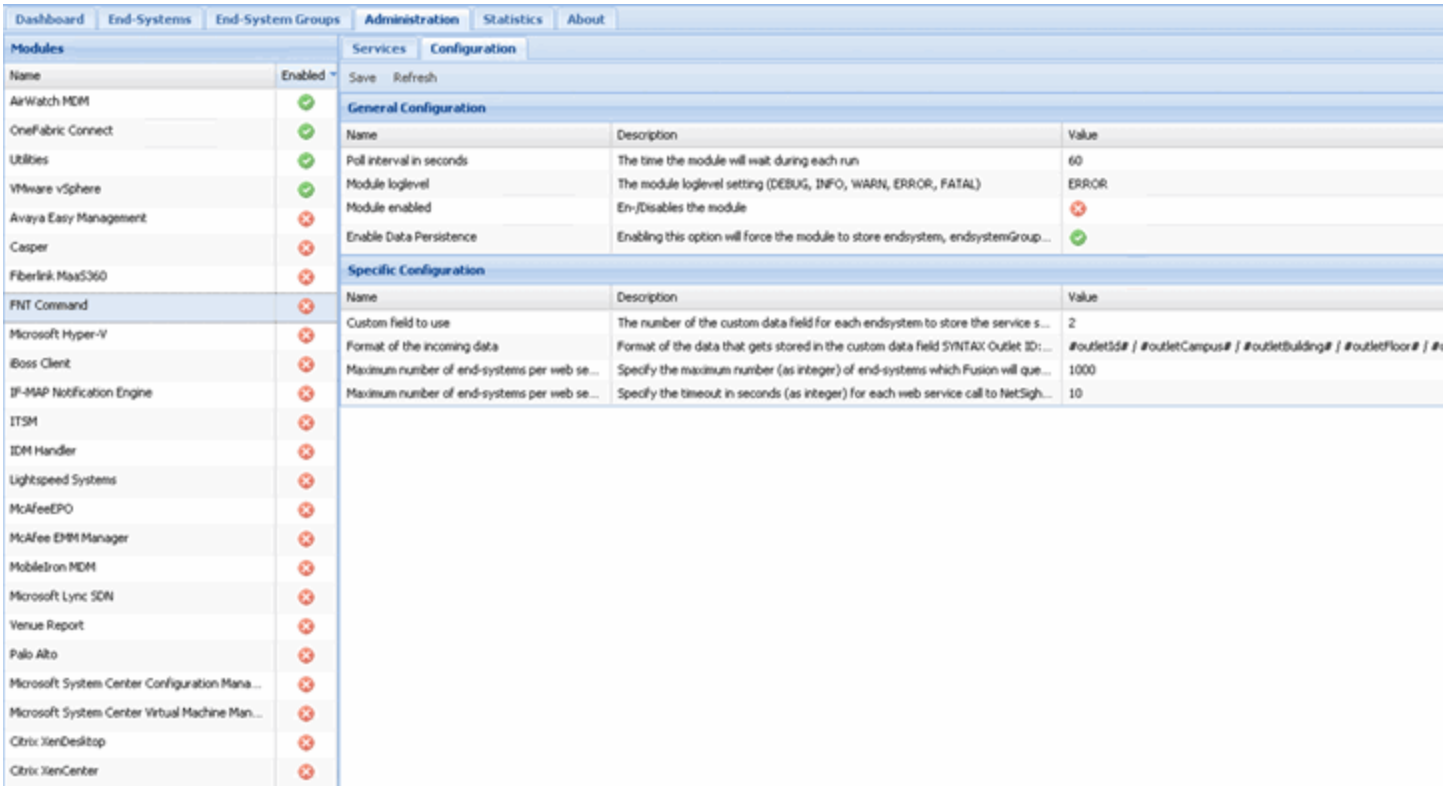
Save
Click the **Save** button to save any changes made to services in the Services table.

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 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 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.

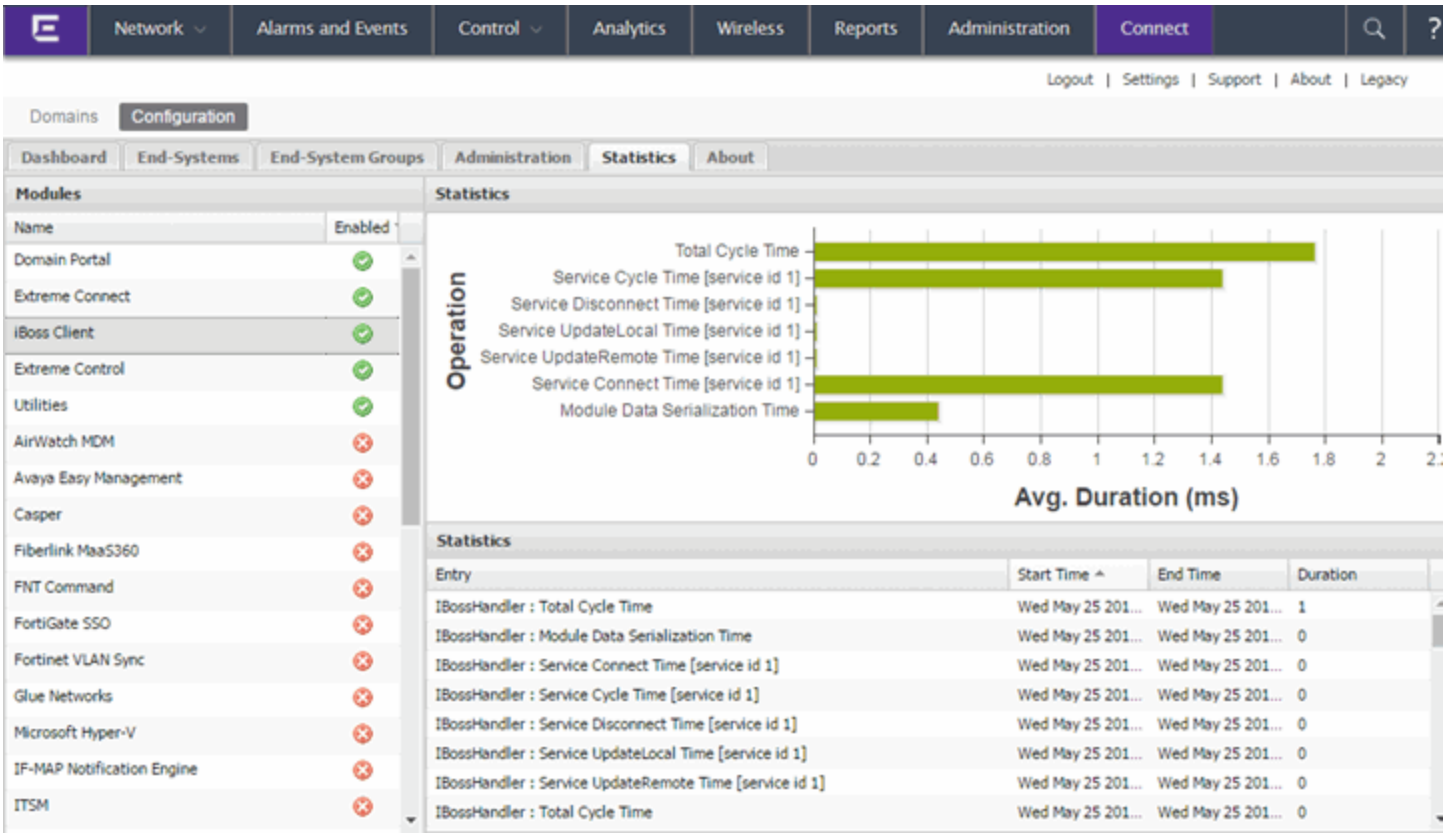
Description
: A brief description of the configuration and how it affects Management Center. This column cannot be edited.

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.

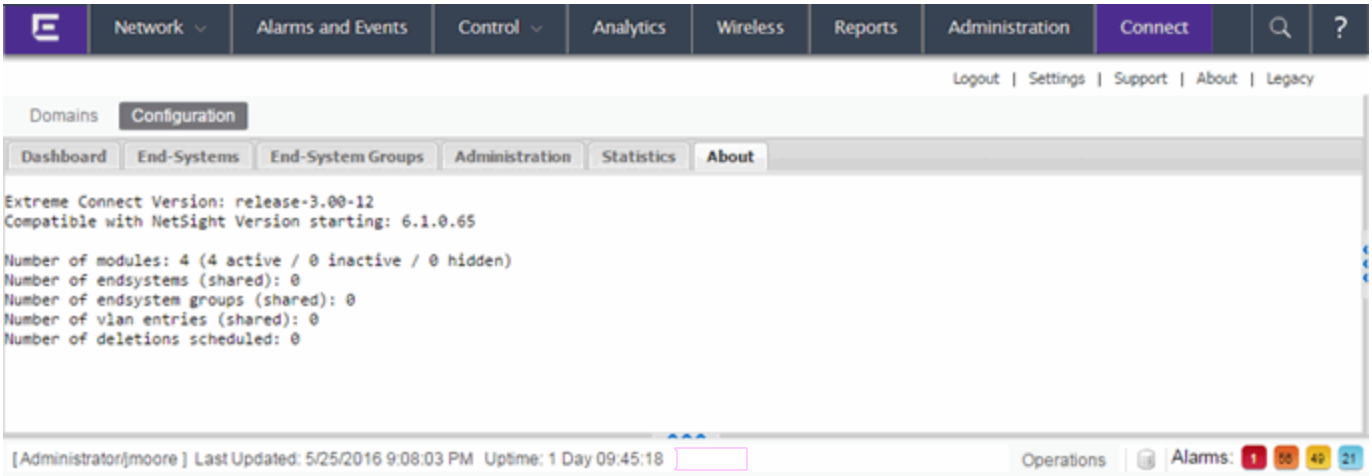
Right Panel

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 Center Extreme Connect Overview
- Domains

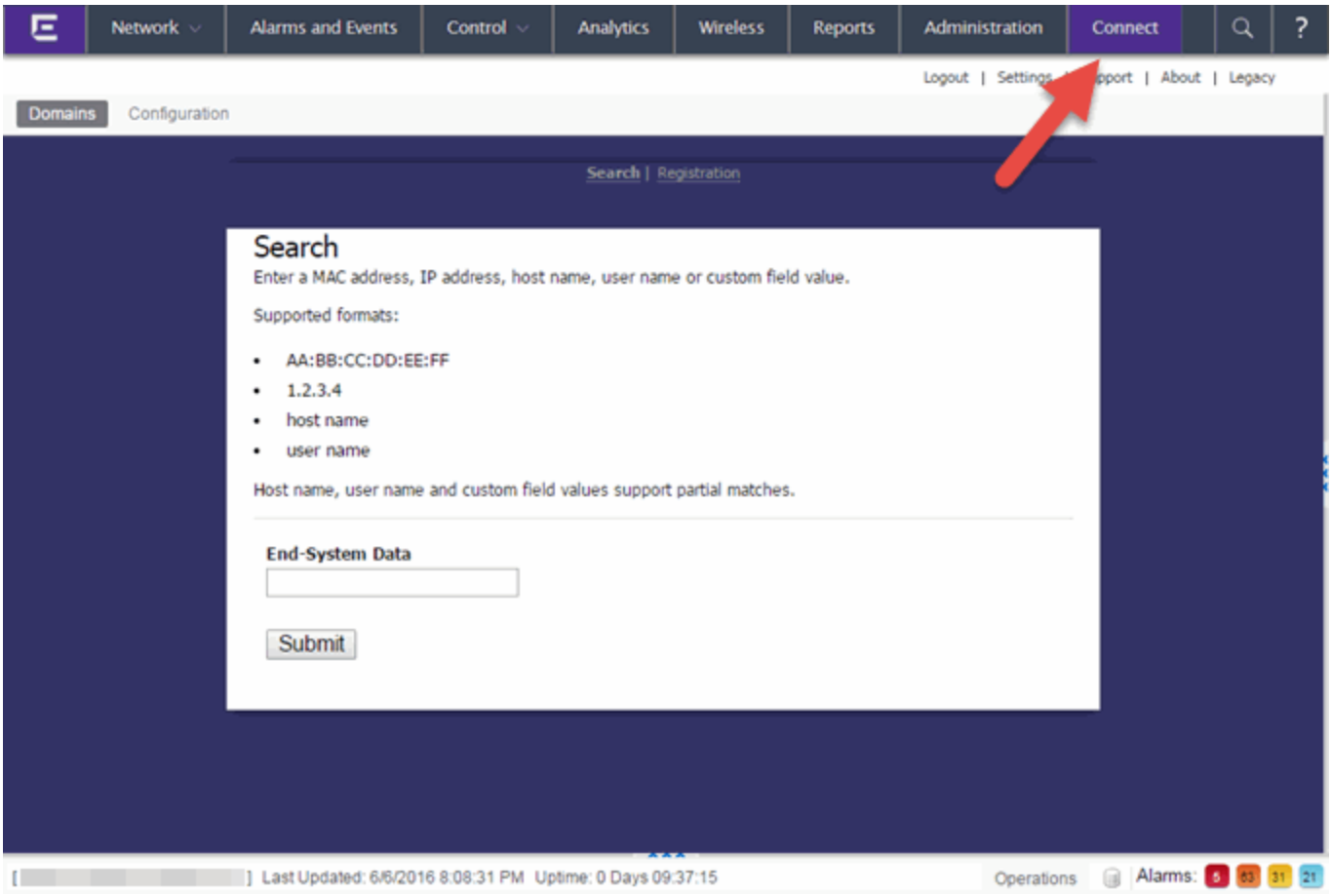
Connect Module Requirements

The Extreme Management Center (formerly NetSight) **Connect** tab allows you to integrate third-party software with Management Center's Extreme Access Control solution.

Management Center's 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. Management Center Connect bridges the gap between these tools and allows you to control your network configurations from within Management Center.

To open the **Connect** tab, select **Connect** at the top of 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 Management Center.

Extreme Connect Requirements

The following outlines the system requirements for Extreme Connect:

- 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

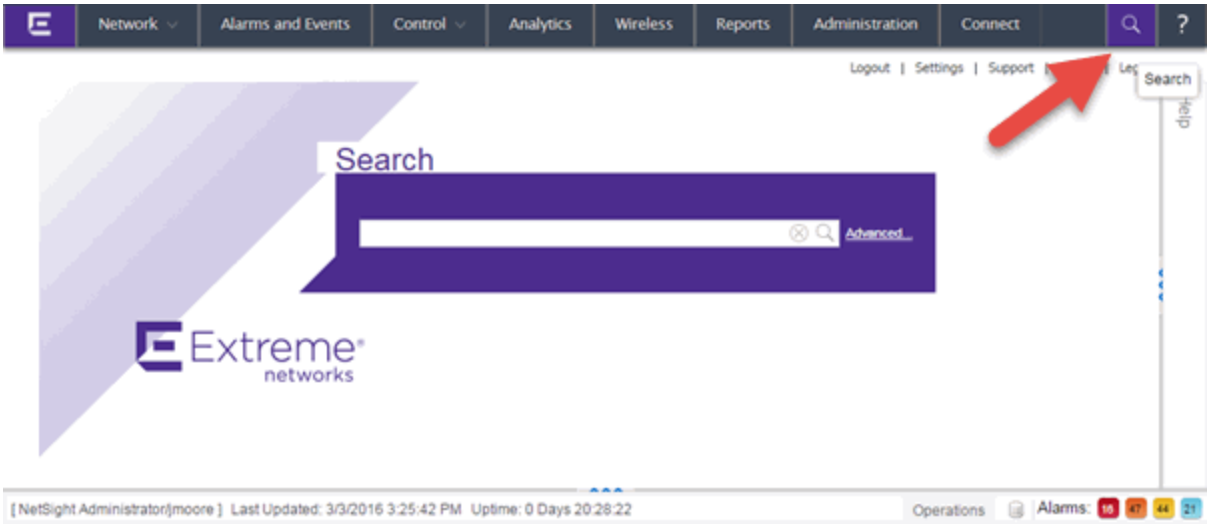
Extreme Management Center Search

The Extreme Management Center (formerly NetSight) Search is a powerful diagnostic tool for locating a network device or end-system you wish to troubleshoot by allowing you to display it in PortView. You can search by MAC address, IP address, or AP serial number, as well as Extreme Access Control end-system name, username, and registration custom field attributes. A device must be in the 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 a Access Control authenticated client.

In addition, there are two Advanced Search options, accessed from the Advanced link to the right of the **Search** field: searching in Compass and searching in Maps.

To view Management Center Search, 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.)

Management Center Search Field



This Help topic provides information on the following topics:

Using Extreme Management Center Search

In the **Search** 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** field. You can also search on AP serial numbers, and by 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 Management Center Search.

Search on 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** field.

Search on an Extreme Access Control Authenticated Client IP Address

You can also search on a 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** field.

Search on 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 OneView options (Administration > Options > OneView > 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.

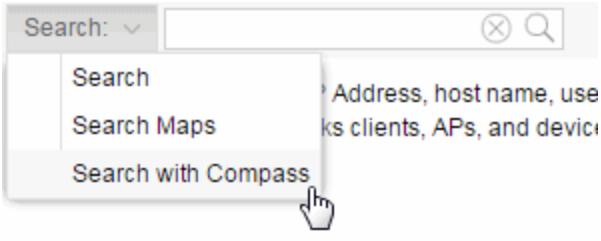
In the **Overview** (search results) tab, the device topology is displayed showing the relationships between a specific set of devices: Wireless Controller, Identity and Access Gateway, AP, switch, and client. The greatest number of devices displayed is five devices for a wireless client in an Access Control authenticated environment (six devices may be returned if the client is also connected via wire). The number of devices returned becomes smaller as you search for one of the five devices. For example, if you search for an AP instead of a client, four devices are returned. If you search for a Wireless Controller, Access Control Gateway, or switch, one device is returned.

Advanced Search Options

The Advanced Search, accessed from the Advanced link to the right of the **Search** 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 Extreme Management Center Maps Overview.
- **Search with Compass** — Provides additional fields, allowing you to refine your search. For more information, see Search with Compass.

Advanced Search Field and Menu Options



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 Management Center server resources used for the searches. For more information, see the Compass options section in the Management Center Help.

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

Compare Device Configurations in Extreme Management Center

You can compare archived device configurations in Management Center by using either the Network tab or the Archive Details Report available in the 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. For more information on authorization capabilities, see the Help topic "How to Configure User Access to Extreme Management Center Applications," located in Management Center Suite-Wide Tools > Authorization Device Access.

This Help topic provides the following information:

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 gear menu  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.

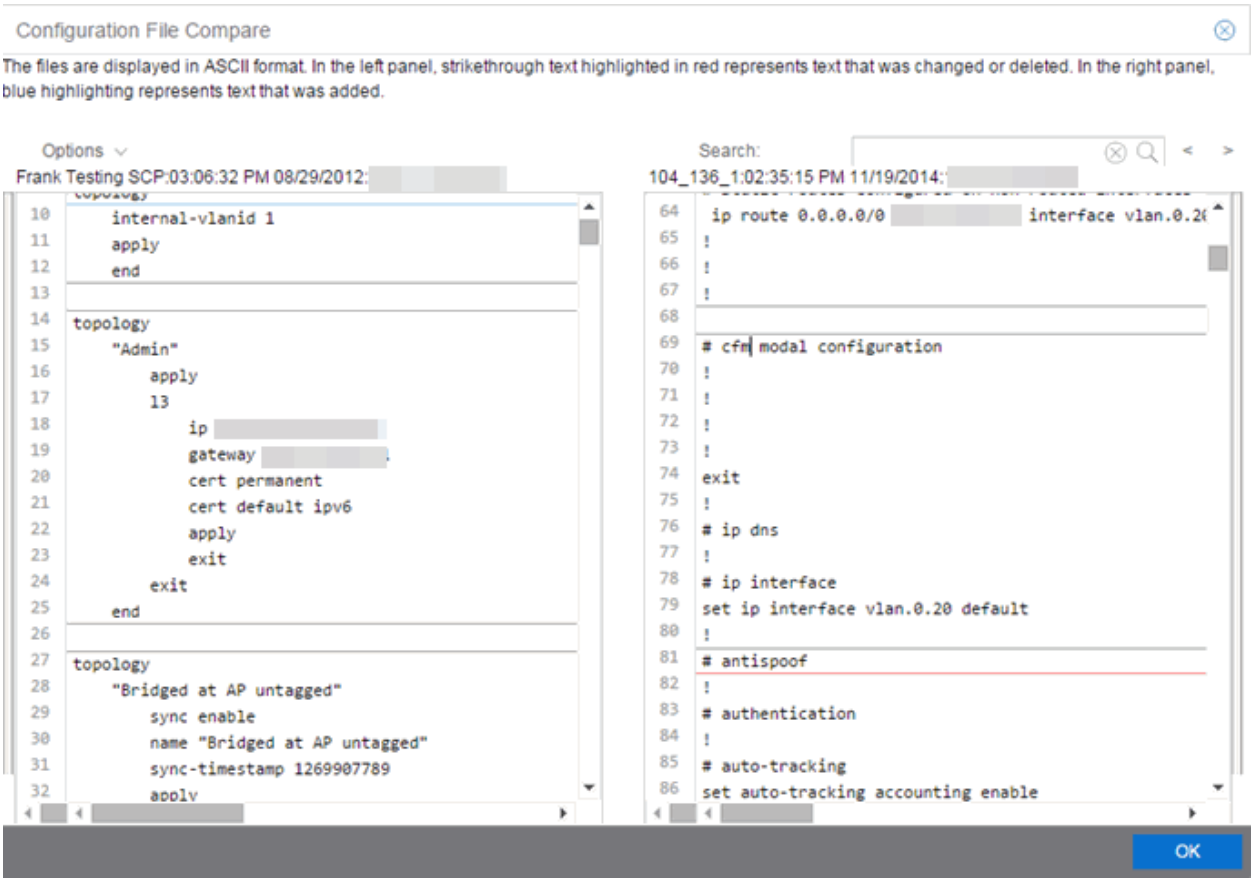
Select the Device > Device Archives report. Click on the Archive Details tab in the right panel and then click on the Archives by Device sub-tab.

The tab displays all the Inventory Manager 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 Management Center reports.

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

Requirements

Access Requirements

Access to DeviceView reports is determined by the user's membership in a 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 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 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.

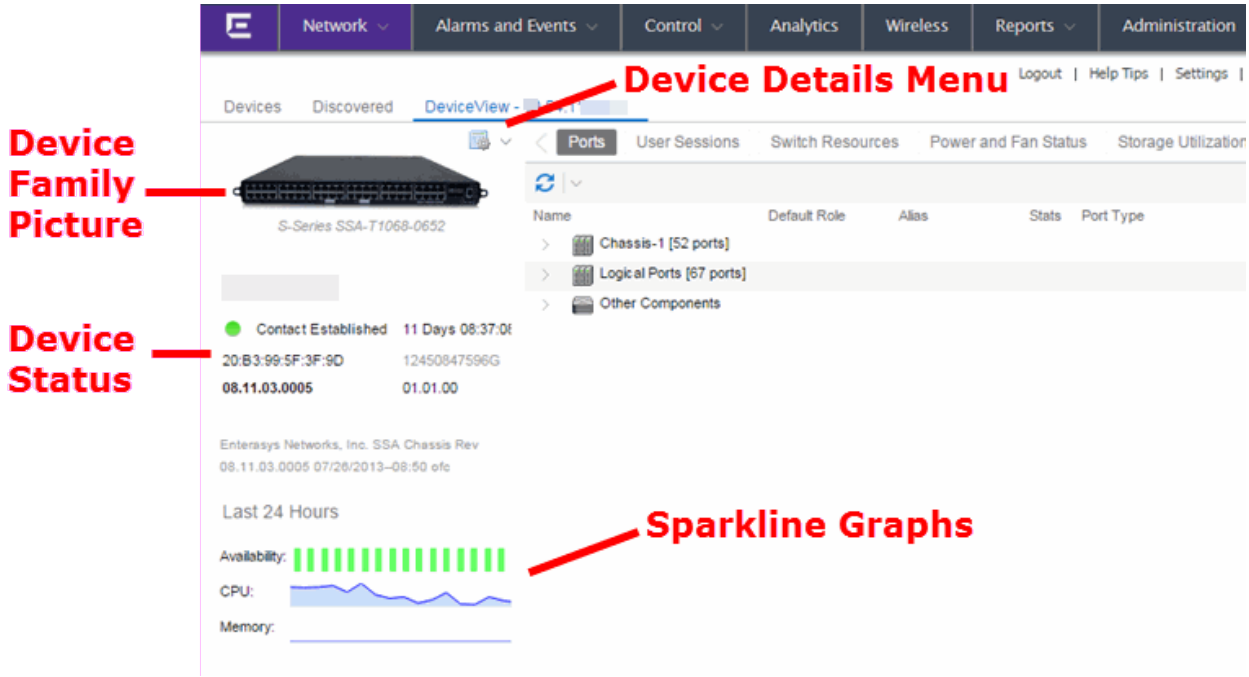
EOS Devices*	ExtremeXOS devices**	Wireless Controllers
Ports***	Ports***	Ports***
User Sessions	User Sessions	User Sessions
Switch Resources	Device and Module Information	Controller History
Power and Fan Status	Power and Fan Status	Active Access Points
Storage Utilization	Process Utilization	WLAN Services

EOS Devices*	ExtremeXOS devices**	Wireless Controllers
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.
****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 Gear menu in the upper right corner to access additional device reports.

Launching DeviceView

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

Launching from Management Center

Network Tab

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

1. Open the Network 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 Management Center.

Control Tab

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

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

Management Center Maps

Use the following steps to launch DeviceView from a map.

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

Launching from Console

You can launch DeviceView from Console using the following methods:

- In the Properties tab, right-click on a device and select View Device Details > DeviceView.
- In the left-panel tree, right-click on a device and select View Device Details > DeviceView.

Related Information

For information on related topics:

- Network Tab

ZTP+ Device Configuration in Extreme Management Center

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.

In Management Center, new devices are automatically discovered on the network the moment they are connected. ZTP+ enabled devices send information to 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 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.

NOTES: ZTP+ currently allows you to configure new Layer 2 access devices. Future releases will allow additional device types.

ZTP+ is currently only available on ExtremeXOS devices on which version 21.1 or newer is installed or on an Application Analytics appliance.

Pre-configuration

Before connecting your devices, you need to pre-configure the following:

- Select the Default Firmware Image Location
- Default Device Configuration in Extreme Management Center
- Switch/Appliance Settings

Select the Default Firmware Image Location

ZTP+ devices automatically update using the most recent firmware image version detected on the system.

NOTE: Application Analytics engines do not support firmware image downgrades via ZTP+.

For the device to recognize a new version is available, the firmware image must be saved in a directory you specify in Management Center.

To configure the file transfer location:

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.

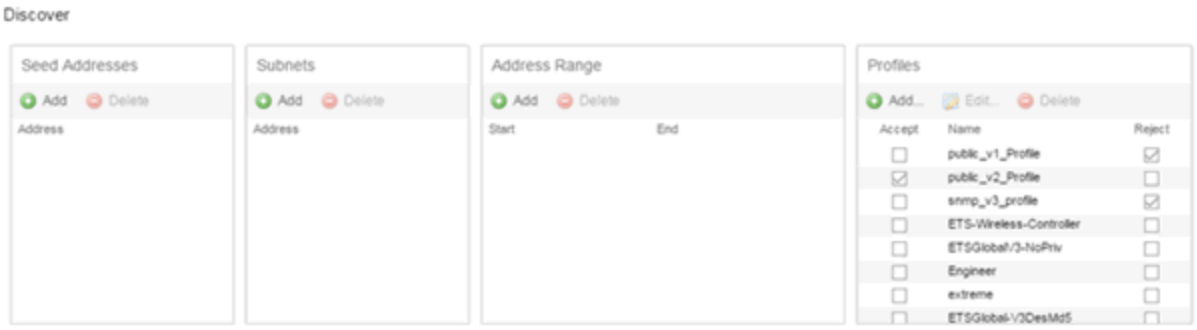
   Your device automatically updates with this firmware image when it restarts and is logged in the Event log with a **Category** of **Inventory**.

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.

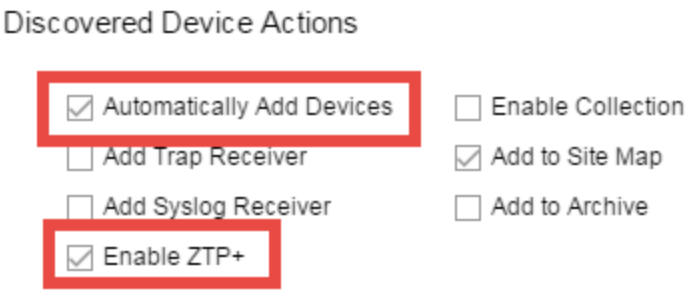
Default Device Configuration in Extreme Management Center

Before connecting your devices, you can configure the default settings that Management Center applies to all devices you add to the network. This is accomplished using the **Site** tab. For information about each of the fields in the **Site** tab, see the **Site** tab help topic.

1. Access the **Network** > **Devices** tab in 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 profiles you want the devices on your network to **Accept** or **Reject** using the **Profiles** list in the Discover section of the tab.
   Create new profiles by clicking the **Add** button. For additional information about profiles, see the **Profiles** tab help topic.



5. 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 Management Center.



6. Enter the **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.
7. 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**.
8. Click **Save**.

   The default configuration for this site is complete and any devices you discover with this site selected use this criteria.

Switch/Appliance Settings

In order for the switch or appliance to communicate to the Management Center server:

- The DHCP Server needs to return a DNS Server and Domain Name to the ZTP+ device.

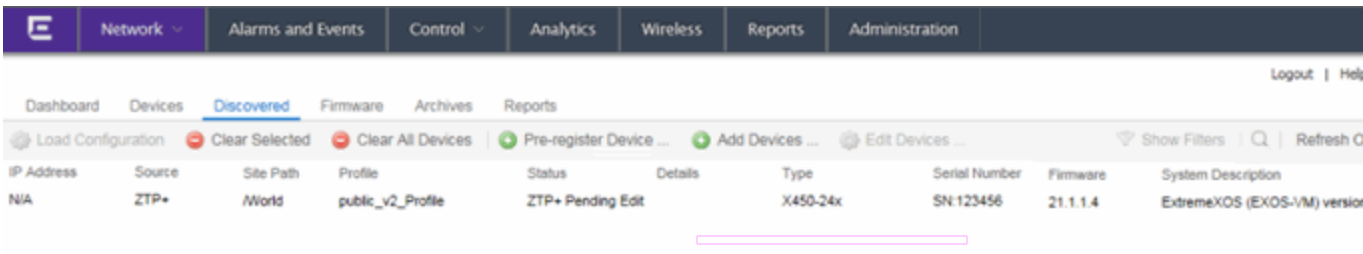
- The DNS Server needs to map the name **extremecontrol.<*domain-name*>** to the IP address of the Management Center server.

Once the Management Center and ZTP+ device are pre-configured, you can add the site definition to the Management Center database.

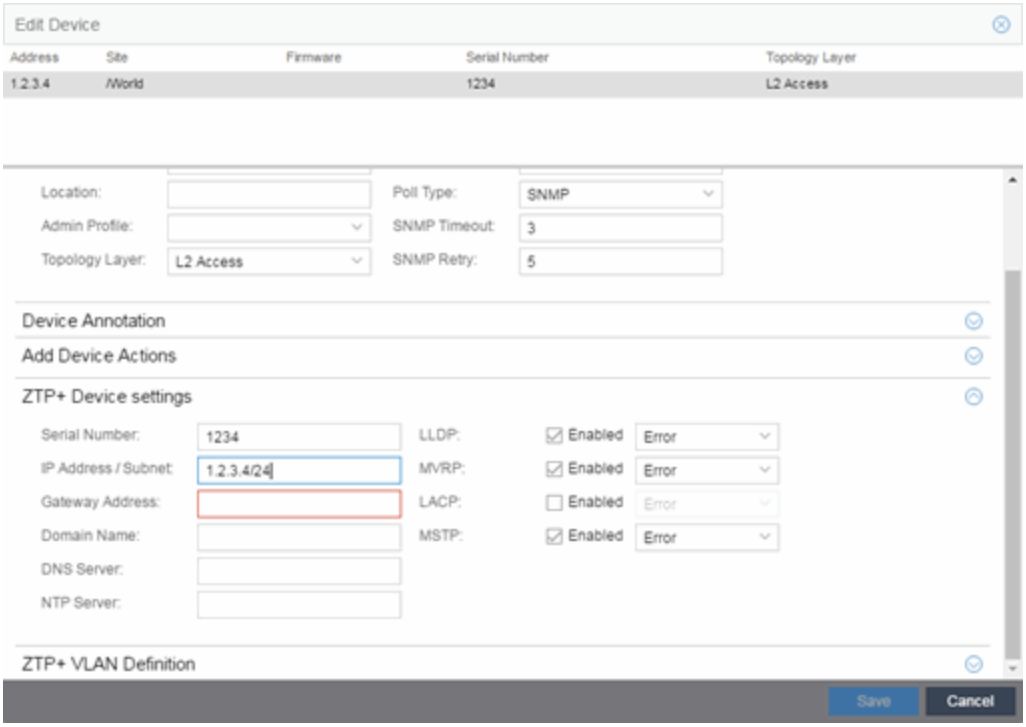
Adding the Device to the Extreme Management Center Database

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 Management Center database, you can connect the device and add it to Management Center.

1. Connect the device to your network.
   ZTP+ enabled devices communicate with Management Center securely via an HTTPS connection and transmits information to Management Center, including the serial number, firmware version, MAC address, operating system, and port information. 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. For more information, see the Firmware tab help topic.
2. Open the **Network** > **Discovered** tab in 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 Management Center server. For more information about the **Discovered** tab, see the Discovered tab help topic.



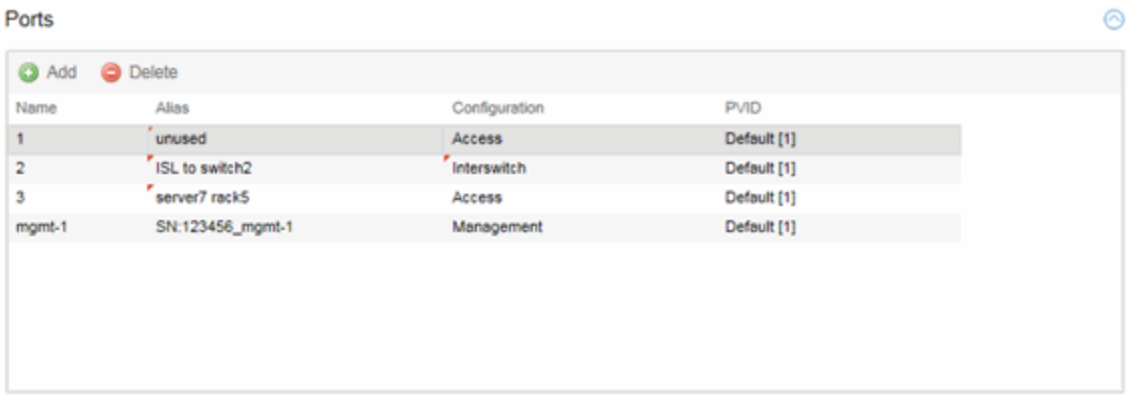
3. Select the device and click the **Edit Devices** button.
   The Edit Devices window opens.



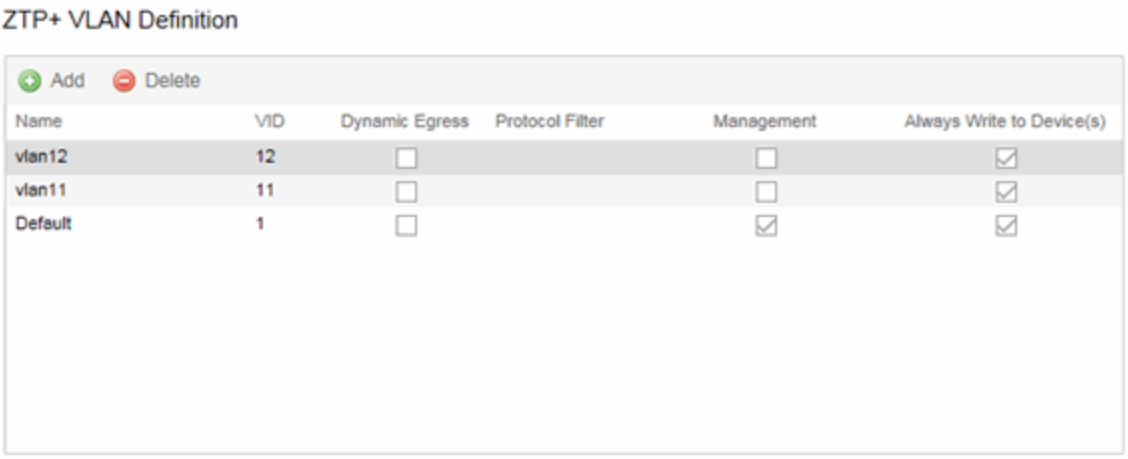
4. Open the ZTP+ Device settings section by clicking the heading.
5. Enter an IP address and subnet in the IP Address/Subnet field.

NOTE: Management Center allows you to enter the IP address in either IPv4 of IPv6 format.

6. Enter the Gateway Address.
7. Open the Ports section of the window by clicking the section heading. The Ports section opens, displaying the ports transmitted by the device to Management Center when connected to the network.



8. 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 **Name** by which the port is known.
   b. Enter the port **Alias**.
   c. 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 Management Center.
   d. Enter a VLAN ID for the port in the **PVID** field.
9. 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.



10. Add any device-specific VLANs to those already included in the list by clicking the **Add** button.
11. Change any incorrect fields in the Device, Device Annotation, or Discovered Device Actions sections.
    For additional information, see the Edit Device window help topic.

12. Click the Save button at the bottom of the window.
The device is added to the 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 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.

Related Information

For information on related topics:

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

ZTP+ Device Configuration in Extreme Management Center

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.

In Management Center, new devices are automatically discovered on the network the moment they are connected. ZTP+ enabled devices send information to 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 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.

NOTES: ZTP+ currently allows you to configure new Layer 2 access devices. Future releases will allow additional device types.

ZTP+ is currently only available on ExtremeXOS devices on which version 21.1 or newer is installed or on an Application Analytics appliance.

Pre-configuration

Before connecting your devices, you need to pre-configure the following:

- Select the Default Firmware Image Location
- Default Device Configuration in Extreme Management Center
- Switch/Appliance Settings

Select the Default Firmware Image Location

ZTP+ devices automatically update using the most recent firmware image version detected on the system.

NOTE: Application Analytics engines do not support firmware image downgrades via ZTP+.

For the device to recognize a new version is available, the firmware image must be saved in a directory you specify in Management Center.

To configure the file transfer location:

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.

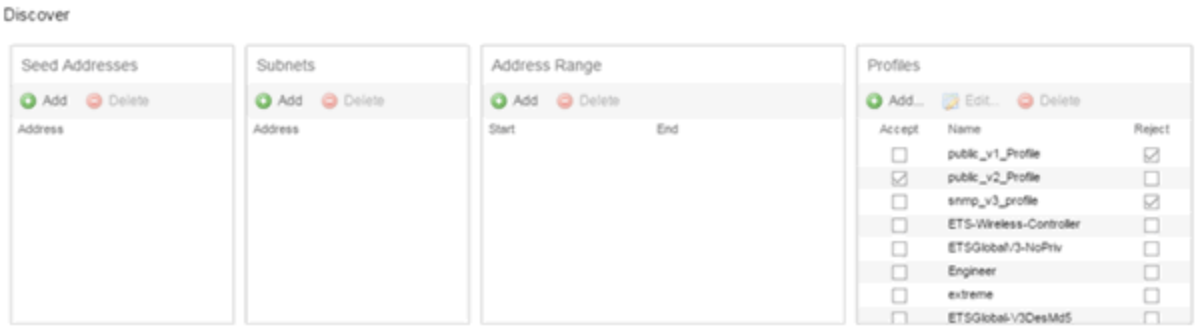
   Your device automatically updates with this firmware image when it restarts and is logged in the Event log with a **Category** of **Inventory**.

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.

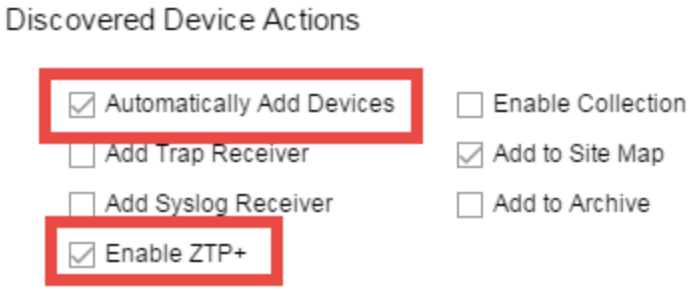
Default Device Configuration in Extreme Management Center

Before connecting your devices, you can configure the default settings that Management Center applies to all devices you add to the network. This is accomplished using the **Site** tab. For information about each of the fields in the **Site** tab, see the Site tab help topic.

1. Access the **Network** > **Devices** tab in 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 profiles you want the devices on your network to **Accept** or **Reject** using the **Profiles** list in the Discover section of the tab.
   Create new profiles by clicking the **Add** button. For additional information about profiles, see the Profiles tab help topic.



5. 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 Management Center.



6. Enter the 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.
7. 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.
8. Click Save.

   The default configuration for this site is complete and any devices you discover with this site selected use this criteria.

Switch/Appliance Settings

In order for the switch or appliance to communicate to the Management Center server:

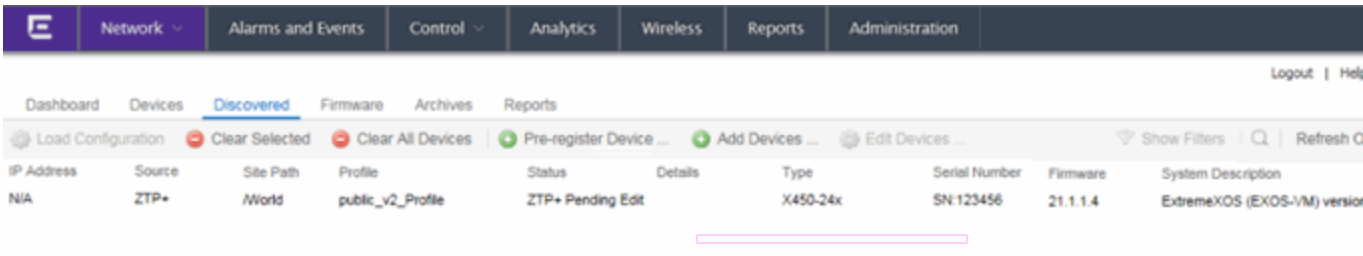
- The DHCP Server needs to return a DNS Server and Domain Name to the ZTP+ device.
- The DNS Server needs to map the name **extremecontrol.<*domain-name*>** to the IP address of the Management Center server.

Once the Management Center and ZTP+ device are pre-configured, you can add the site definition to the Management Center database.

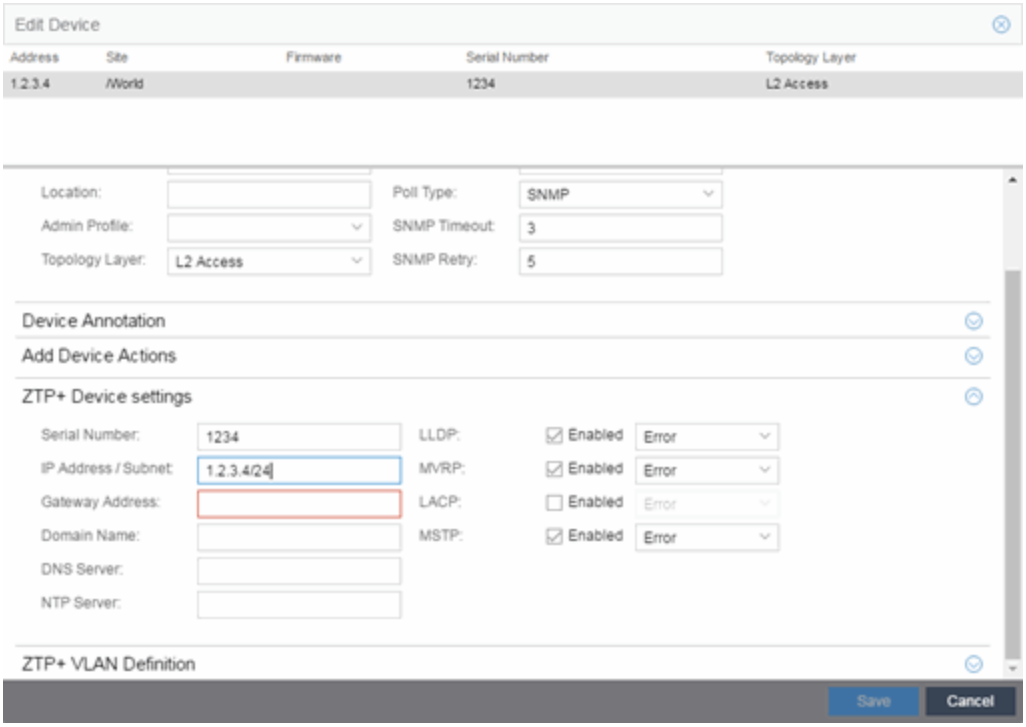
Adding the Device to the Extreme Management Center Database

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 Management Center database, you can connect the device and add it to Management Center.

1. Connect the device to your network.
   ZTP+ enabled devices communicate with Management Center securely via an HTTPS connection and transmits information to Management Center, including the serial number, firmware version, MAC address, operating system, and port information. 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. For more information, see the Firmware tab help topic.
2. Open the **Network** > **Discovered** tab in 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 Management Center server. For more information about the **Discovered** tab, see the Discovered tab help topic.



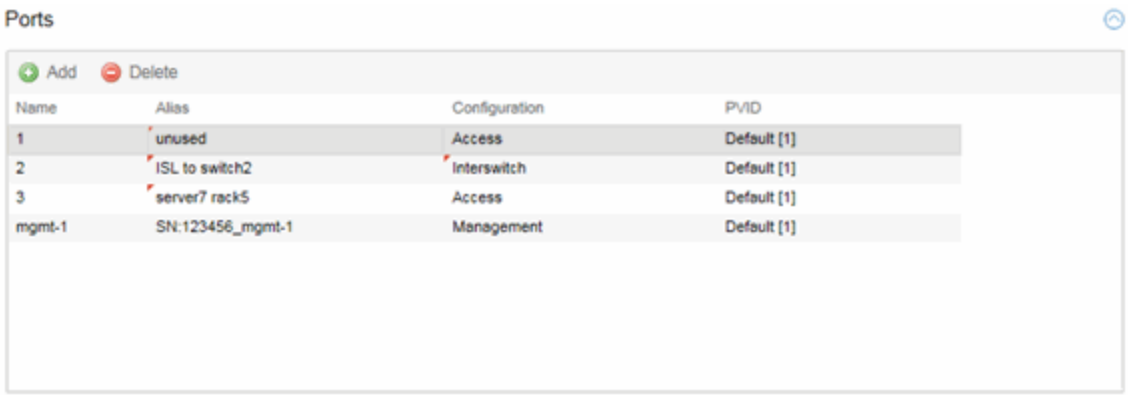
3. Select the device and click the **Edit Devices** button.
   The Edit Devices window opens.



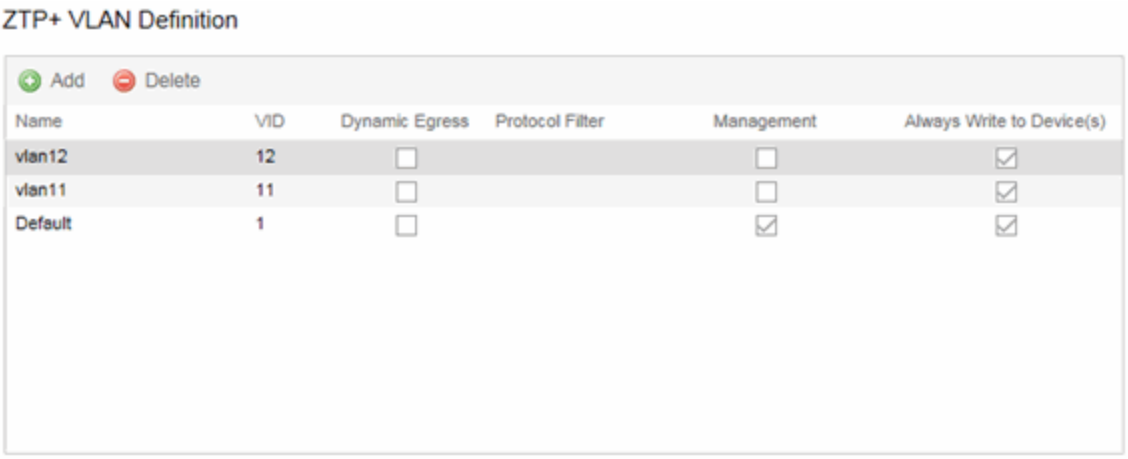
4. Open the ZTP+ Device settings section by clicking the heading.
5. Enter an IP address and subnet in the IP Address/Subnet field.

NOTE: Management Center allows you to enter the IP address in either IPv4 of IPv6 format.

6. Enter the Gateway Address.
7. Open the Ports section of the window by clicking the section heading. The Ports section opens, displaying the ports transmitted by the device to Management Center when connected to the network.



8. 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 **Name** by which the port is known.
   b. Enter the port **Alias**.
   c. 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 Management Center.
   d. Enter a VLAN ID for the port in the **PVID** field.
9. 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.



10. Add any device-specific VLANs to those already included in the list by clicking the **Add** button.
11. Change any incorrect fields in the Device, Device Annotation, or Discovered Device Actions sections.
    For additional information, see the Edit Device window help topic.

12. Click the Save button at the bottom of the window.
The device is added to the 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 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.

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 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 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 Management Center license (NMS) or Management Center Advanced license (NMS-ADV) to view PortView reports. (Contact your sales representative for information on obtaining 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 Access Control Dashboard end-system events table filtered to display all events for the end-system based on the MAC address. Health Results — Displays risk information for the selected end-system.	Switch must have Access Control authentication enabled.
Map	Displays the map containing the device to which the end-system is connected.	
Sessions	The tabs within the report contain the following information: Interface History — Historical interface utilization and availability. Client History — Historical statistics for wired or wireless clients. End-System Events — View the Access Control Dashboard end-system events table filtered to display all events for the end-system based on the MAC address. NetFlow — NetFlow data for the selected port.	Requires active interface statistics collection. Client statistics collection must be enabled. Switch must have Access Control authentication enabled. The switch must support NetFlow and flow collection must be enabled on the port.

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 a 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 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 > Access Control > OneView End-Systems Read Access or NetSight OneView > Access Control > OneView End-Systems Read/Write Access

Launching PortView

You can launch PortView from a variety of locations in Management Center, as well as the legacy java applications Console and NAC Manager. By default, you can have five active PortView searches displayed in Management Center at one time. You can change this display limit in the Maximum PortViews Displayable field in OneView options (Administration > Options > OneView > 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 Management Center

Management Center Search Tab

The primary launch point for PortView is from 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 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.

Management Center Interface Summary FlexView

Use the following steps to launch PortView from a 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 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.

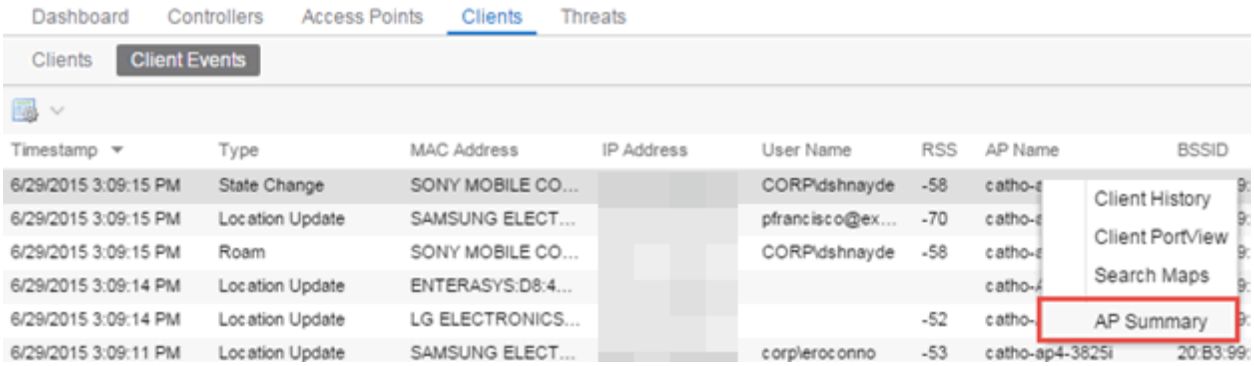
In addition to capturing network traffic for analysis in Wireshark, the AP also collects RF information. The RADIOTAP header format delivers RF information. You must use Wireshark 1.6 or later to read the full RADIOTAP header information. For troubleshooting features like TxBF/STBC, you can enable capturing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

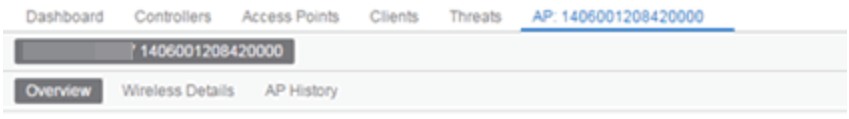
Configure and Use Real Capture

Use the following steps to configure and use the Real Capture feature.

1. Launch 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.

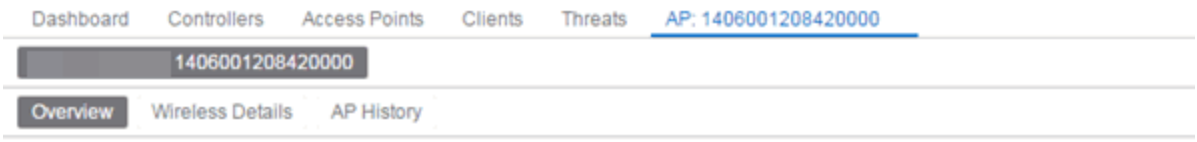


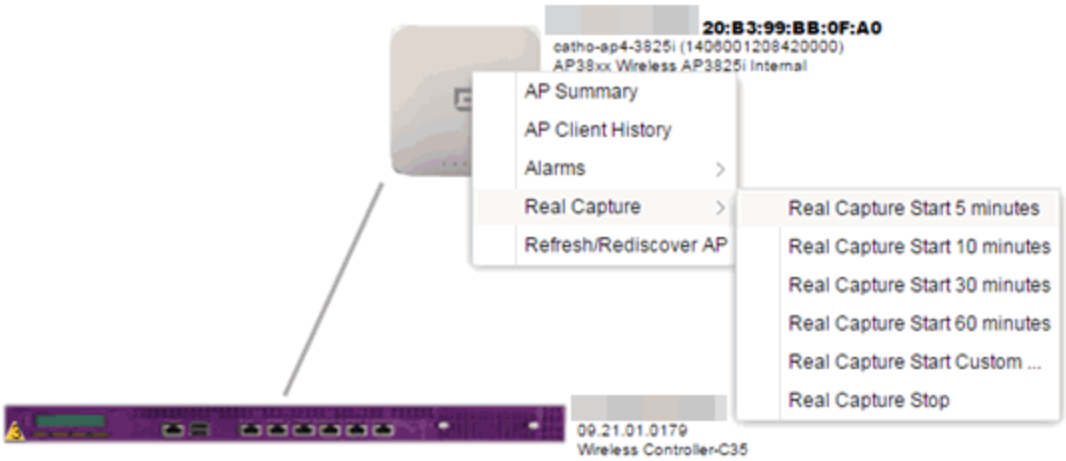
    b. The AP PortView opens.



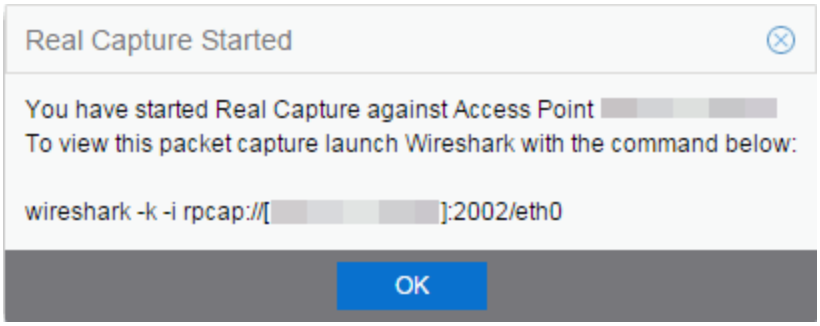
NOTE: You can also launch PortView for the AP using the **Search** tab. Open the **Search** tab, enter the search criteria (MAC, IP, hostname, or AP serial number) and press **Enter** to display the AP PortView.

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.



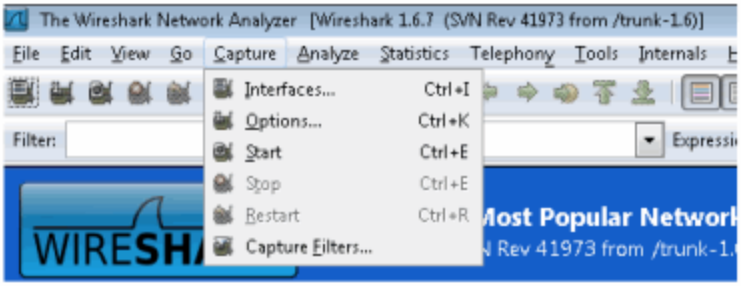


4. A message appears to inform you Real Capture has started, and provides a CLI command you can use on a client on which Wireshark is installed, to launch Wireshark against the AP and view the captured traffic.

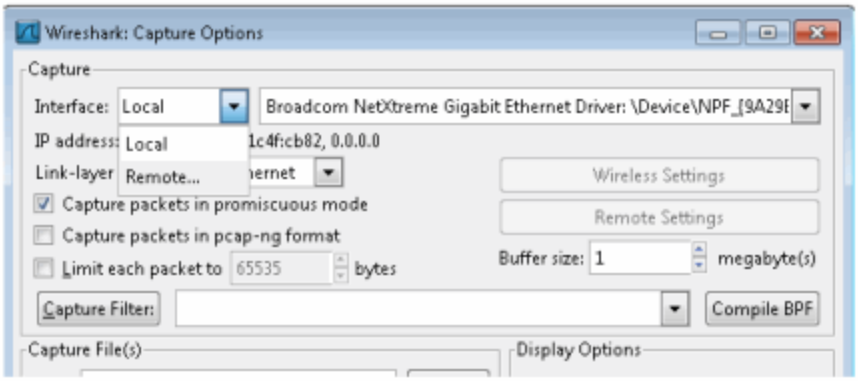


5. You can also access the captured traffic in Wireshark using the following steps:

   a. In Wireshark, select **Capture** > **Options** from the menu bar.

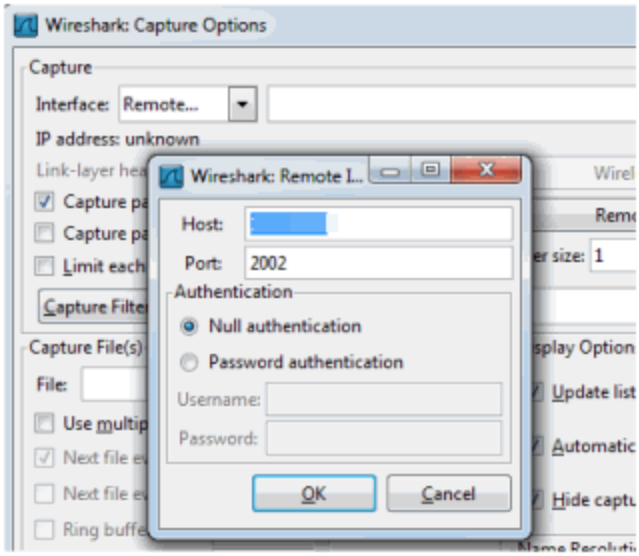


   b. In the Capture Options window, set the **Interface** value to **Remote**.

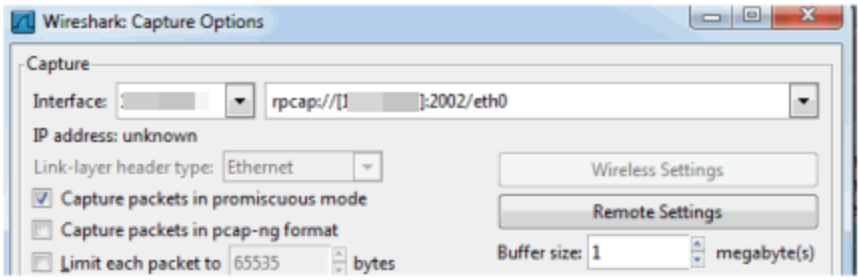


   c. The Remote Interface window appears. Enter the AP's IP address in the **Host** field, and the port number (2002 or 2003) in the **Port** field (you can see this information in the CLI command message described in step 4). In the Authentication section, select **Null authentication**.

Click **OK**.



d. Wireshark adds the command information to the Capture options.

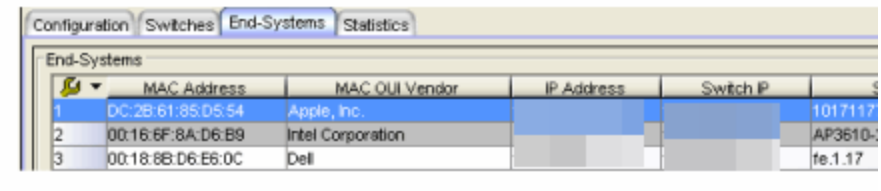


e. Click **OK** in the Capture Options window to begin viewing the captured traffic in Wireshark. When you have the data you need, you can stop the capture and save it to a file for further diagnosis and troubleshooting.

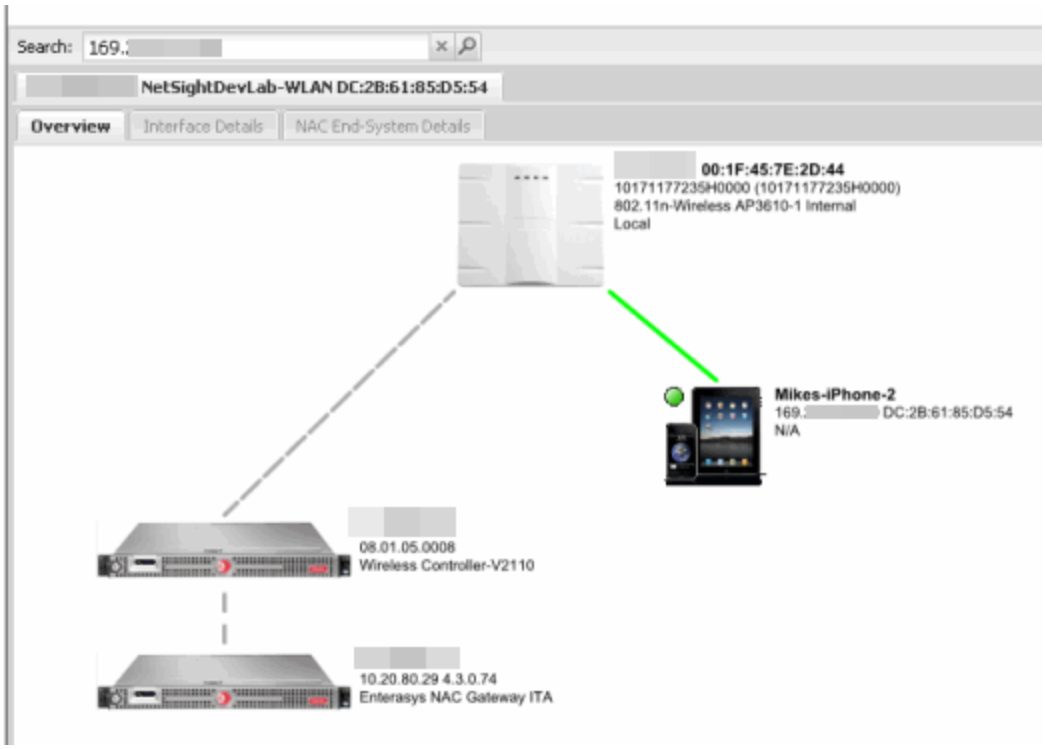
Real Capture Example

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

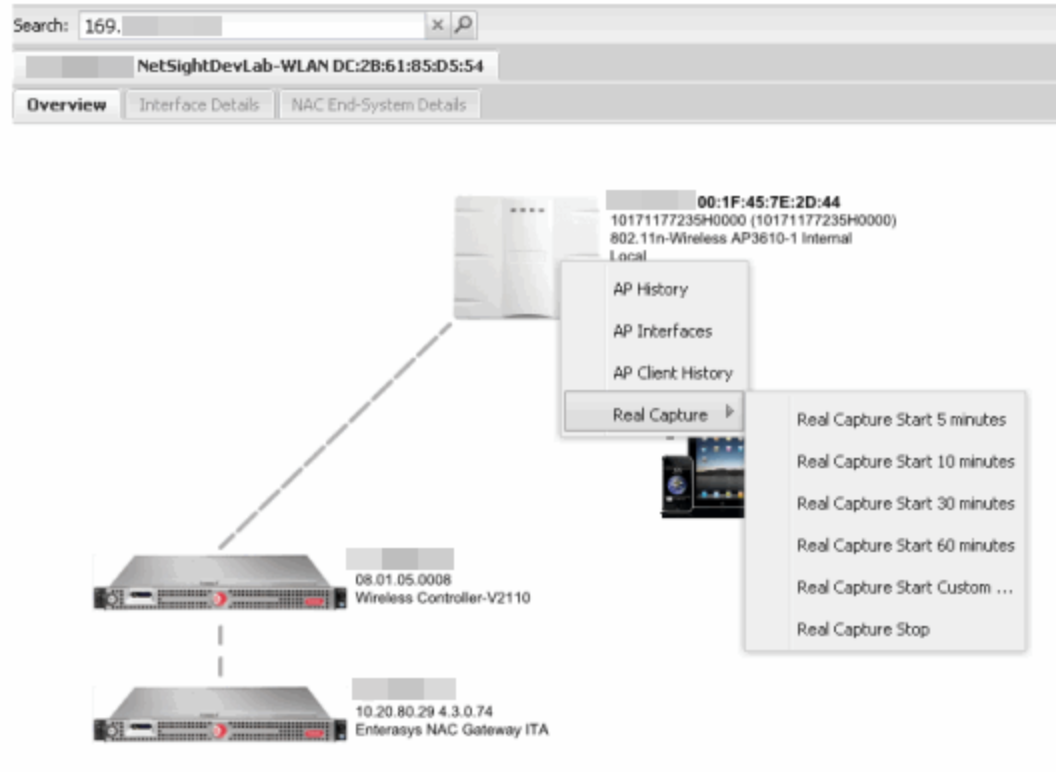
The problem starts when an end-system in NAC Manager is not able to obtain an IP address.



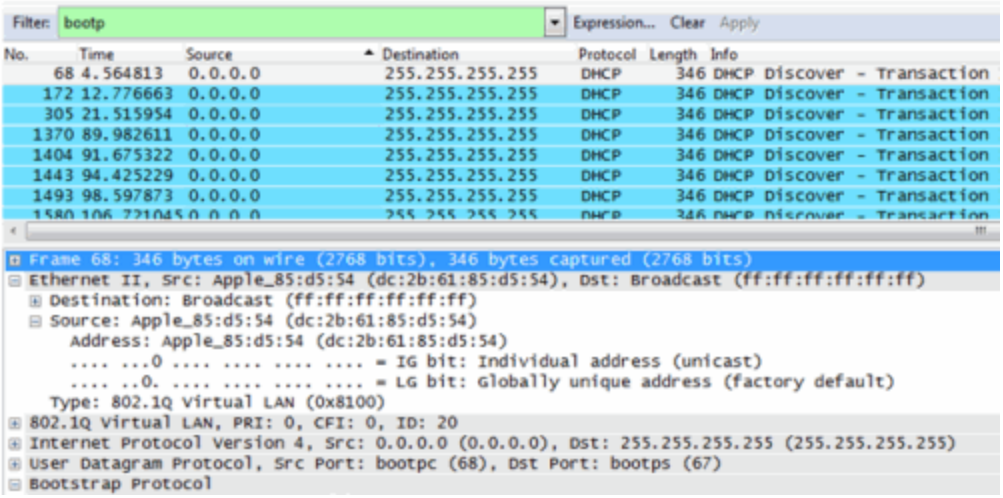
A search is performed on the 169.x.x.x IP address.



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 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.

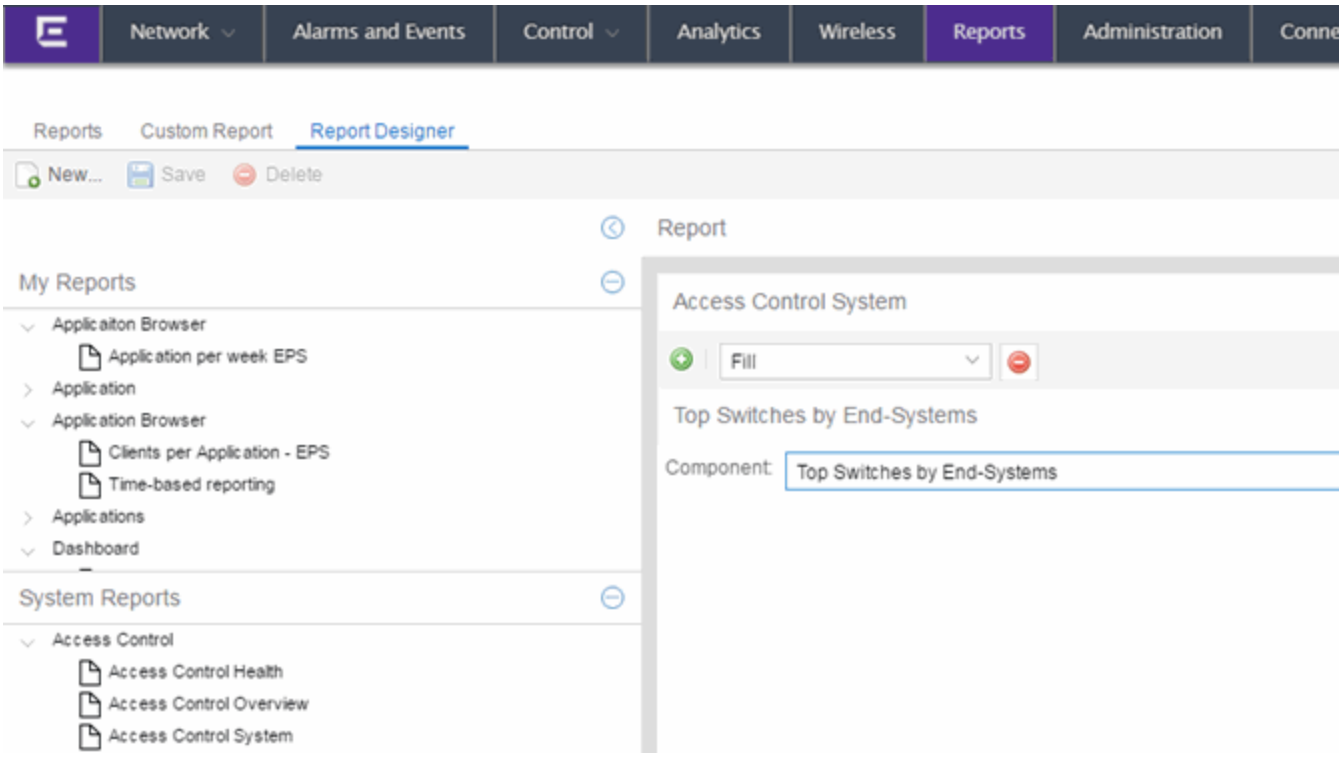
Customize a System Report

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 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 Access Control System report.

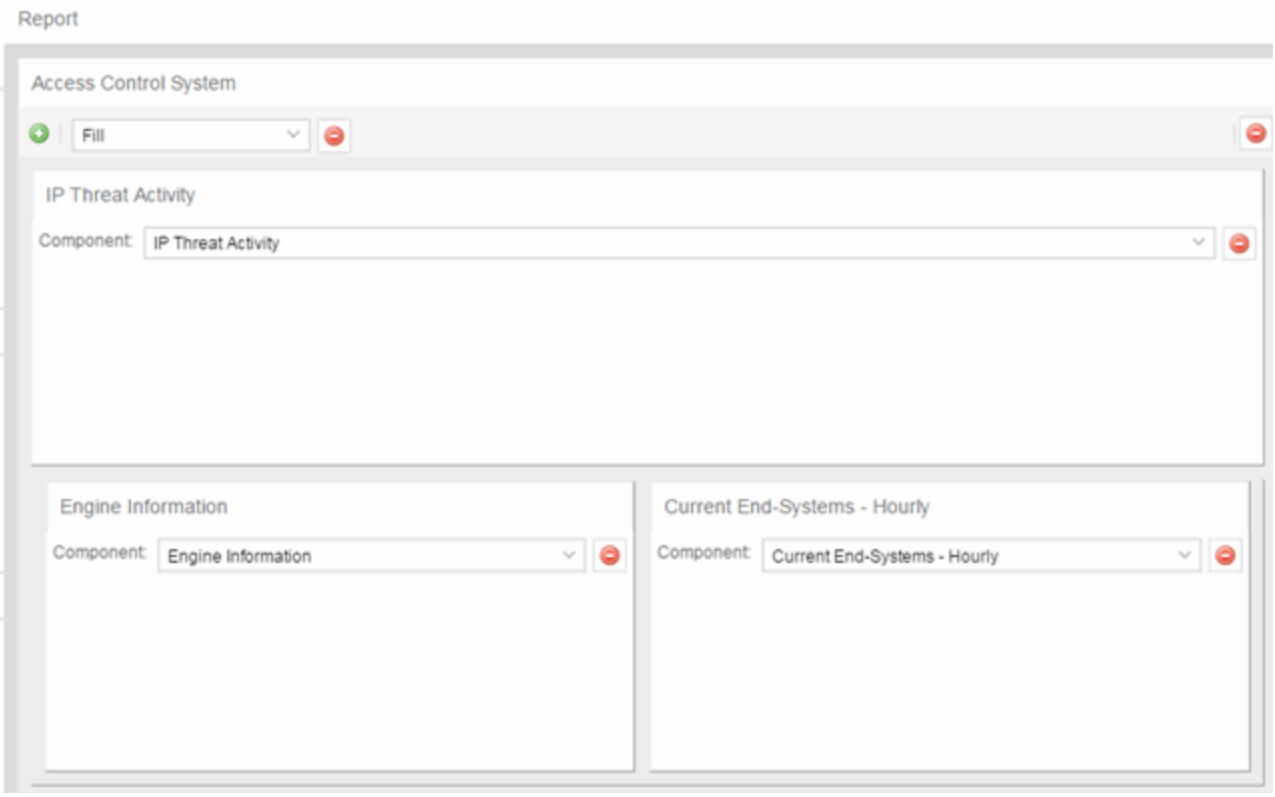
1. Select the **Reports** tab in Extreme Management Center and then select the **Report Designer**.
2. Select the system report you want to customize in the System Reports section. In the example below, Access Control > Access Control System

report is selected. (Use the scroll bar to view the complete list of available reports.) The report becomes available to edit in the right panel.



3. Change the report:
   a. 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.



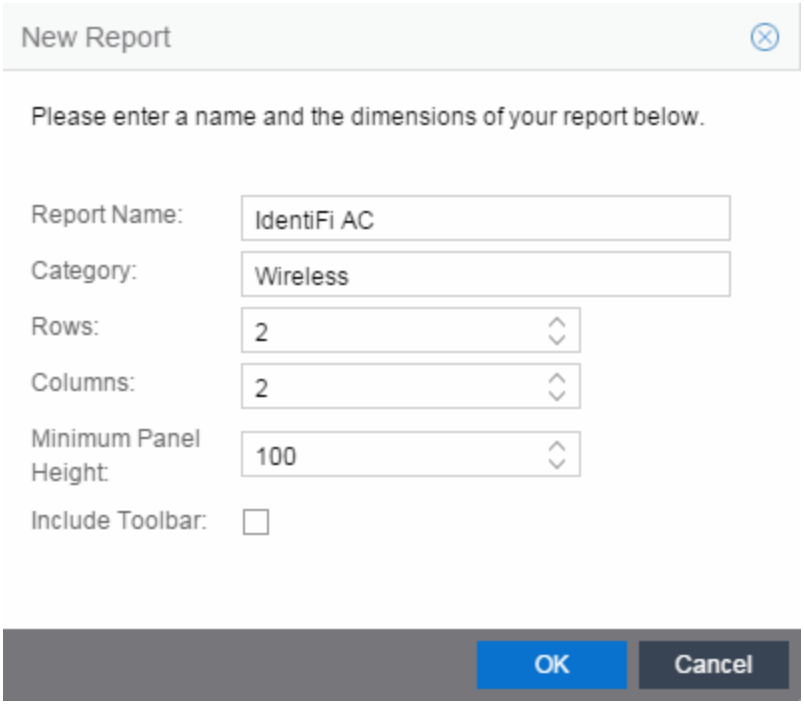
4. Once you have finished making changes to the report, click the **Save** button. The report is populated with data and displayed in a new tab as a way to preview the report. The name of the customized report is added to the My Reports section.

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.

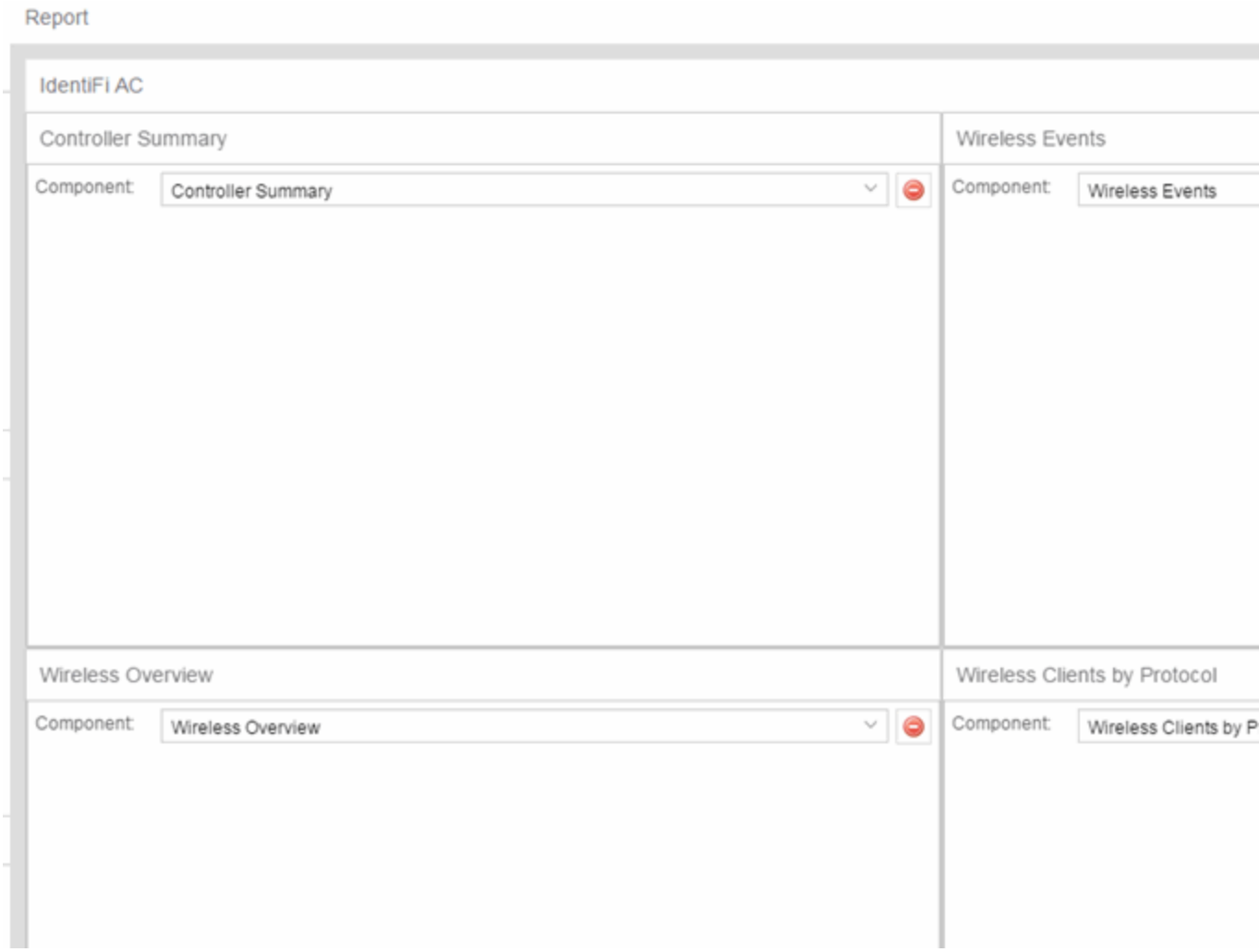
Create a New Report

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

Restore Device Configuration in Extreme Management Center

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. For more information on authorization capabilities, see the Help topic "How to Configure User Access to Extreme Management Center Applications" located in Management Center Suite-Wide Tools > Authorization Device Access.

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 Mgmt tab in Inventory Manager. 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://extranet.extremenetworks.com/downloads/ or from the **Download** icon in the Firmware Mgmt tab's Details View.

1. Place your new firmware in your firmware directory. Inventory Manager uses the default tftpboot\firmware\images directory for storing your firmware.
2. In the left-panel **Firmware Mgmt** tab, select **View > Refresh** from the menu bar. (You can also use the Refresh icon in the right-panel Details Views.) Inventory Manager automatically adds your new firmware to the appropriate firmware groups in the left-panel Firmware Mgmt tree.

The new firmware version is available when configuring the device in 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 in Inventory Manager.

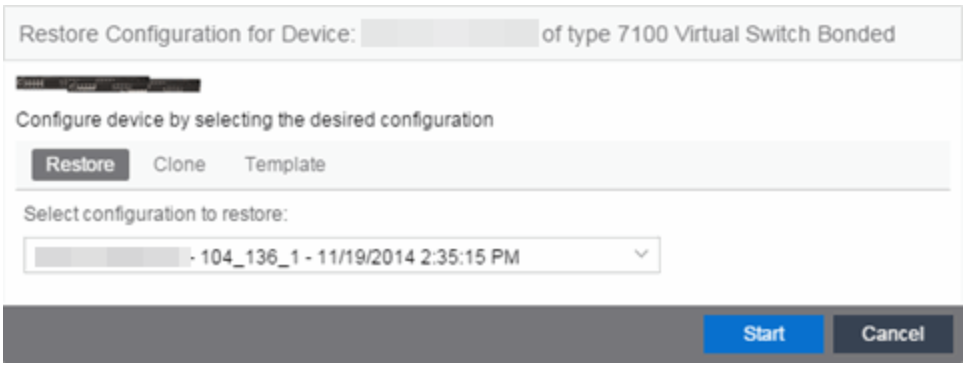
Cloning a device configuration is useful when you want to use the exact same configuration on another device. If you are cloning a device configuration, you must have an existing configuration for that device archived in Inventory Manager. For more information, refer to "How to Archive" in the Inventory Manager Help.

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 in Inventory Manager to use as the source configuration for a device. For information, refer to "Creating a Configuration Template" in the Inventory Manager Help.

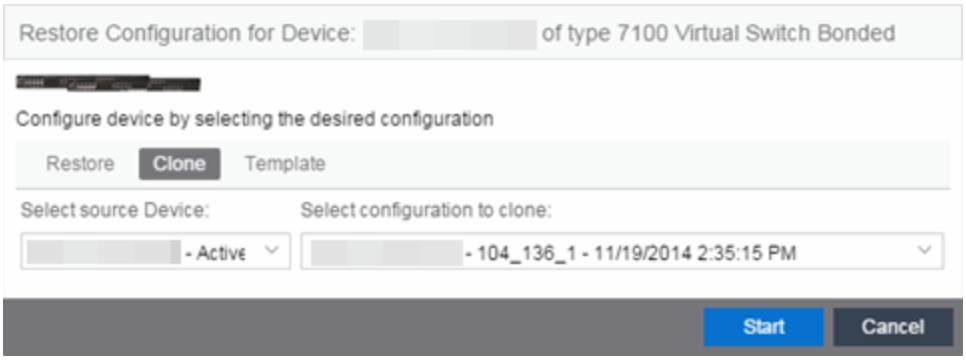
Cloning a Device Configuration

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 Management Center. On the **Network** tab, right-click on the active device and select **Configuration/Firmware > Restore Configuration**. The Restore Configuration window opens.



2. Select the **Clone** tab.



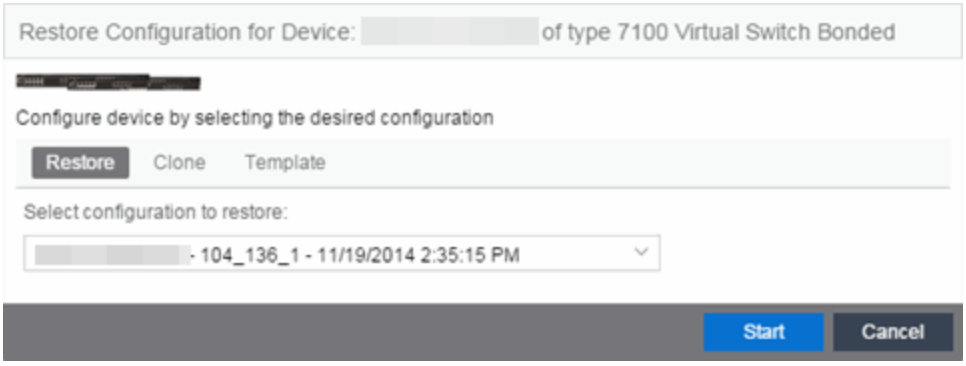
3. If desired, select a new version of firmware to download to the device. (You must add the new firmware version to Inventory Manager. For more information; see "Device Firmware".)
4. Select the Device option as the Configuration Source.
5. Select the source device for the configuration. The selected 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 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 Management Center.

Related Information

For information on related topics:

- Network tab
- New Device Configuration in Extreme Management Center

How to Create Scripts

This chapter describes the scripting functionality built in to Extreme Management Center, and how to use Management Center to create scripts.

Extreme Management Center Script Overview

Management Center scripts are files containing CLI commands, control structures, and data manipulation functions. 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.

Create 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.

Management Center scripts are similar to ExtremeXOS scripts in that they are collections of ExtremeXOS CLI commands and control structures. Management Center scripts add some additional commands specific to Management Center.

In general, Management Center scripts support syntax and constructs from the following sources:

- ExtremeXOS CLI commands — ExtremeXOS CLI commands in a 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 Management Center scripts. See "CLI Scripting" in the *ExtremeXOS User Guide* for more information on ExtremeXOS script functionality and syntax.
- The Tcl scripting language version 8.1. For general information about the Tcl scripting language, see www.tcl.tk.

  For a list of the Tcl commands supported in Management Center scripts, see "Tcl Support in Management Center Scripts".

  Syntax and constructs from these sources work seamlessly within 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.

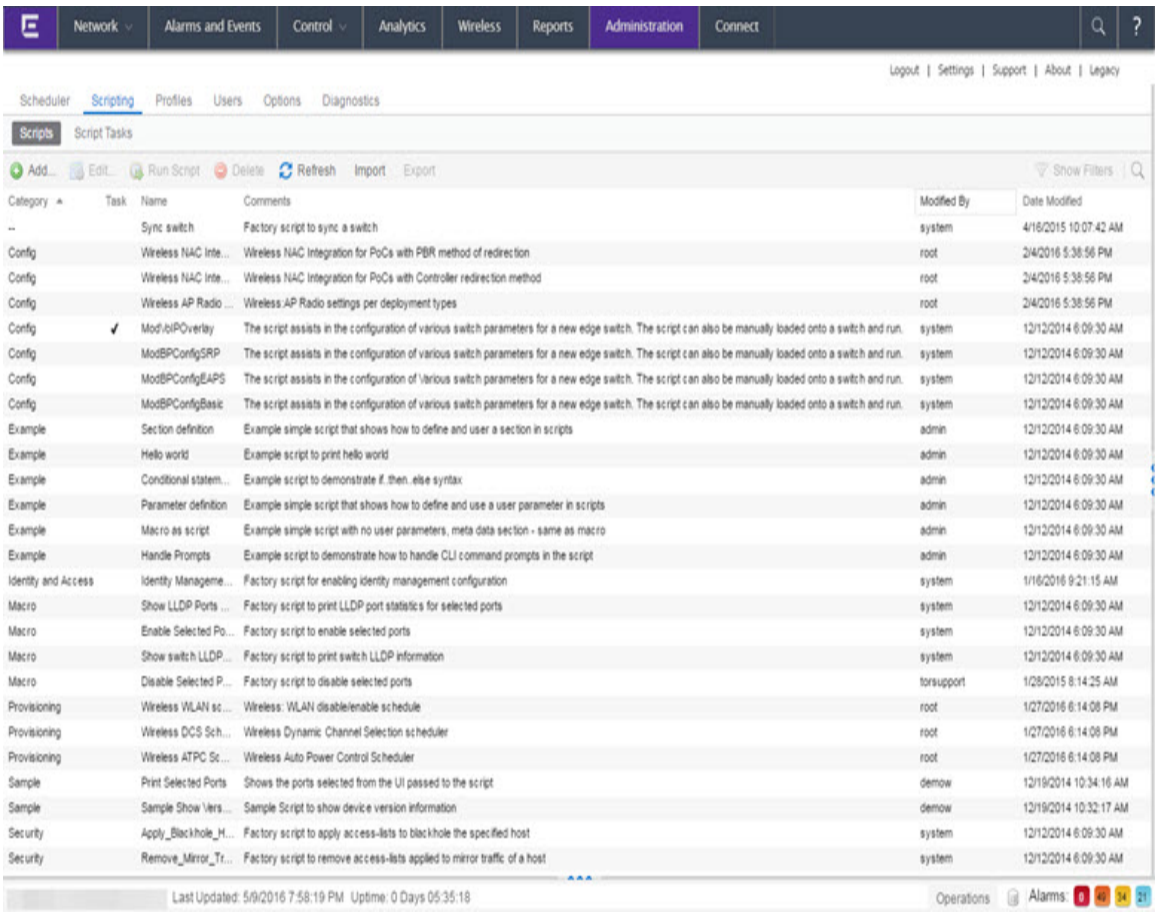
Bundled Extreme Management CenterScripts

Management Center includes a number of sample scripts you can use as templates for your own Management Center scripts. These scripts perform such tasks as enable/disable ports, apply ACLs, reset engines, and configure VLANs.

The sample scripts included with Management Center are available to users with an Administrator role. The XML source files for the scripts are located at *<NetSight_install_dir>*`\appdata\scripting\bundled_scripts`.

The Extreme Management Center Script Interface

To display the scripts configured in Management Center, select the **Administration > Scripting**. Click the **Scripts** subtab.



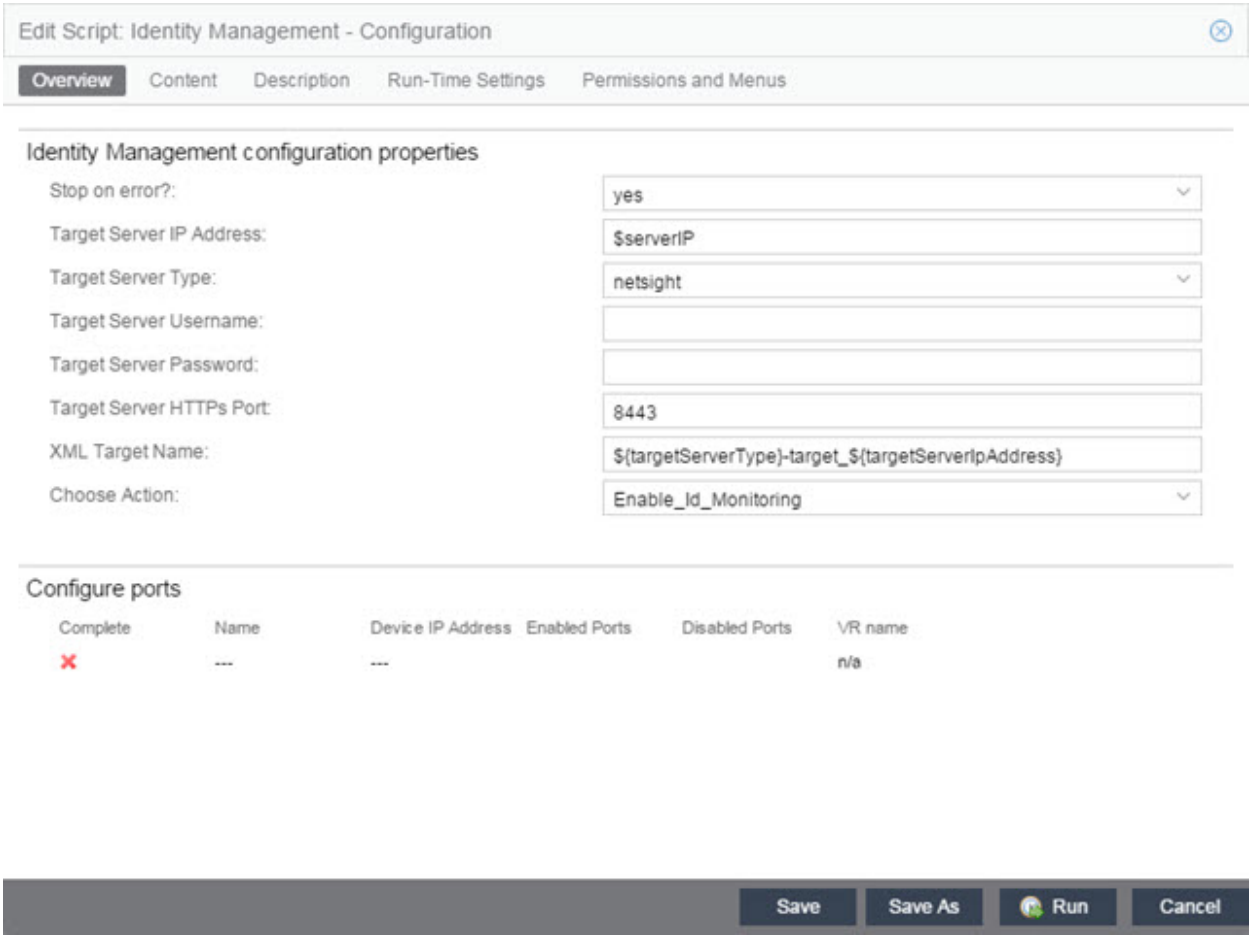
The **Scripts** tab contains the following information:

- Category — The script category, if configured.
- Task — Indicates whether the script is used in a scheduled task.
- Name — The name of the script.
- Comments — Comments or a description of the script.
- Modified by — Who last modified the script.
- Date Modified — When the script was last modified.

The Script Tasks tab contains the following information:

- Scheduled — Displays a checkmark, if this is a scheduled task.
- Category — The script category, if configured.
- Name — The name of the script task.
- User Name — Who created the script task.
- Script Name — The name of the script run by the script task.
- Comment — Comments or a description of the script task.
- Date modified — When the script was last modified.

Double-click a script to open the script editor dialog.



The Management Center script editor allows you to add content to a script, set values for parameters, specify run-time settings, and indicate the Management Center users that can run the script.

The following tabs appear in the Management Center Script Editor window:

- Overview — Displays fields to enter script parameters. The contents of this tab is 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 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 Management Center interface, such as on a menu or in a shortcut menu.

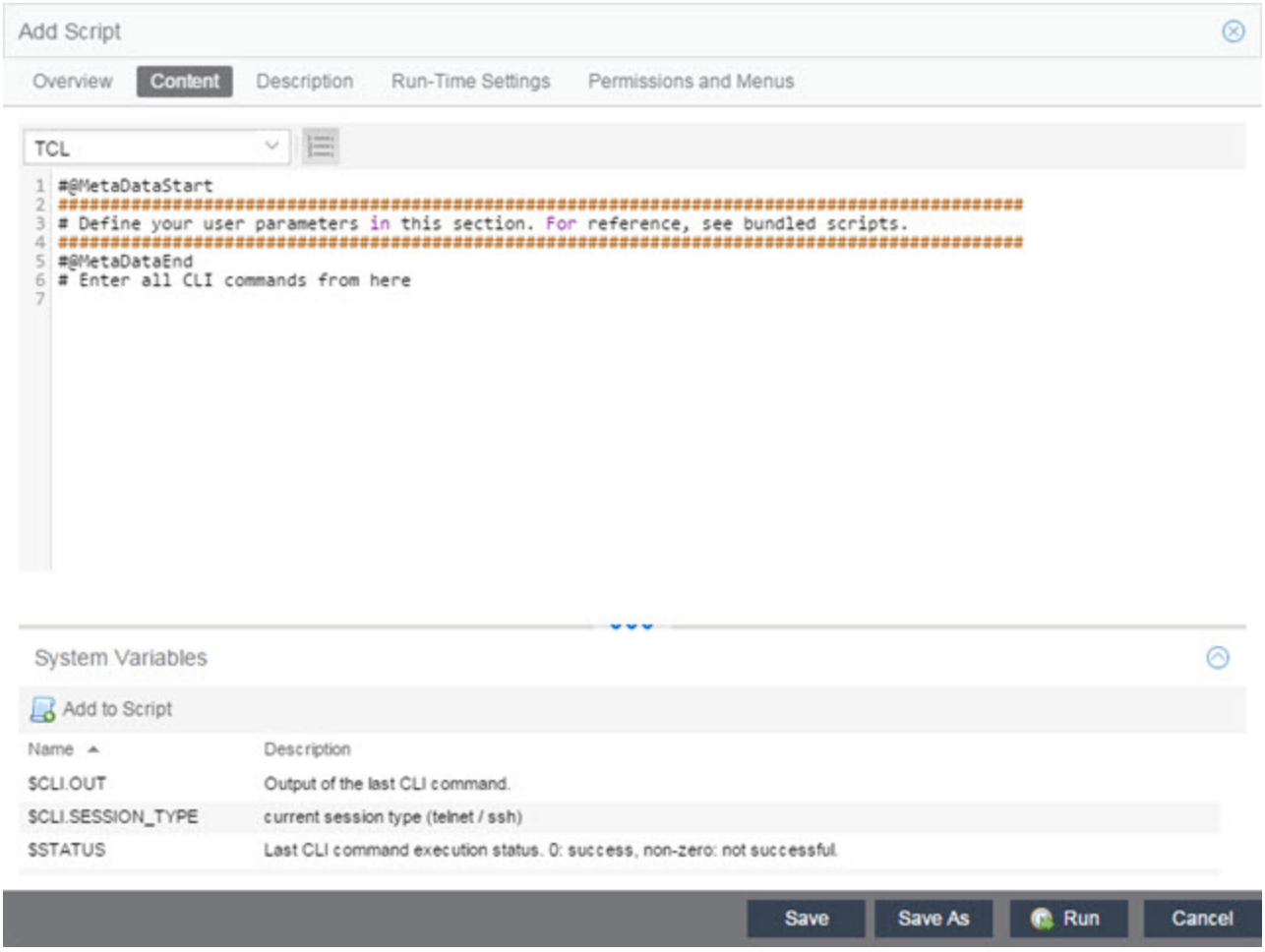
Managing Extreme Management Center Scripts

With scripting, you can:

- Create a Extreme Management Center script.
- Specify run-time settings for a script.
- Specify permissions and menu locations within Extreme Management Center for a script.
- Import scripts.
- Export scripts.
- Edit scripts.
- Delete scripts.
- Run a script on one or more managed devices, with device-specific parameters.
- View script results.
- Configure script tasks.

Adding a New Extreme Management Center Script

1. On the **Scripting** tab, click **Scripts**.
2. Click the **Add** button. The Add Script dialog box appears.

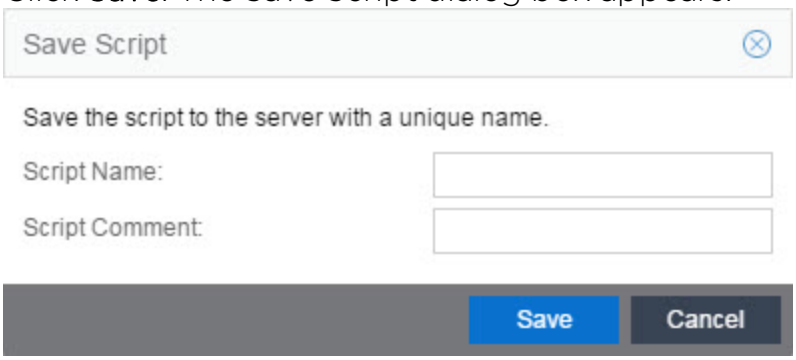


By default, a new script you create in Management Center contains a metadata section, where you can enter a script description and define script sections and metadata that appears on the Overview tab. For more information about metadata, see Metadata Tags.

3. 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.
4. Place variable definition statements in the metadata section (between `#@MetaDataStart` and `#@MetaDataEnd` tags). Variables can be defined by entering values in the Overview tab. A list of system variables appears under System Variables. To add a variable to the script select the variable and double-click or click Add to Script.
5. Enter ExtremeXOS 12.1 and later CLI scripting commands, Tcl commands, and constructs after the metadata section of the script. For information

about what can appear in a Management Center script, see Management Center Script Reference.

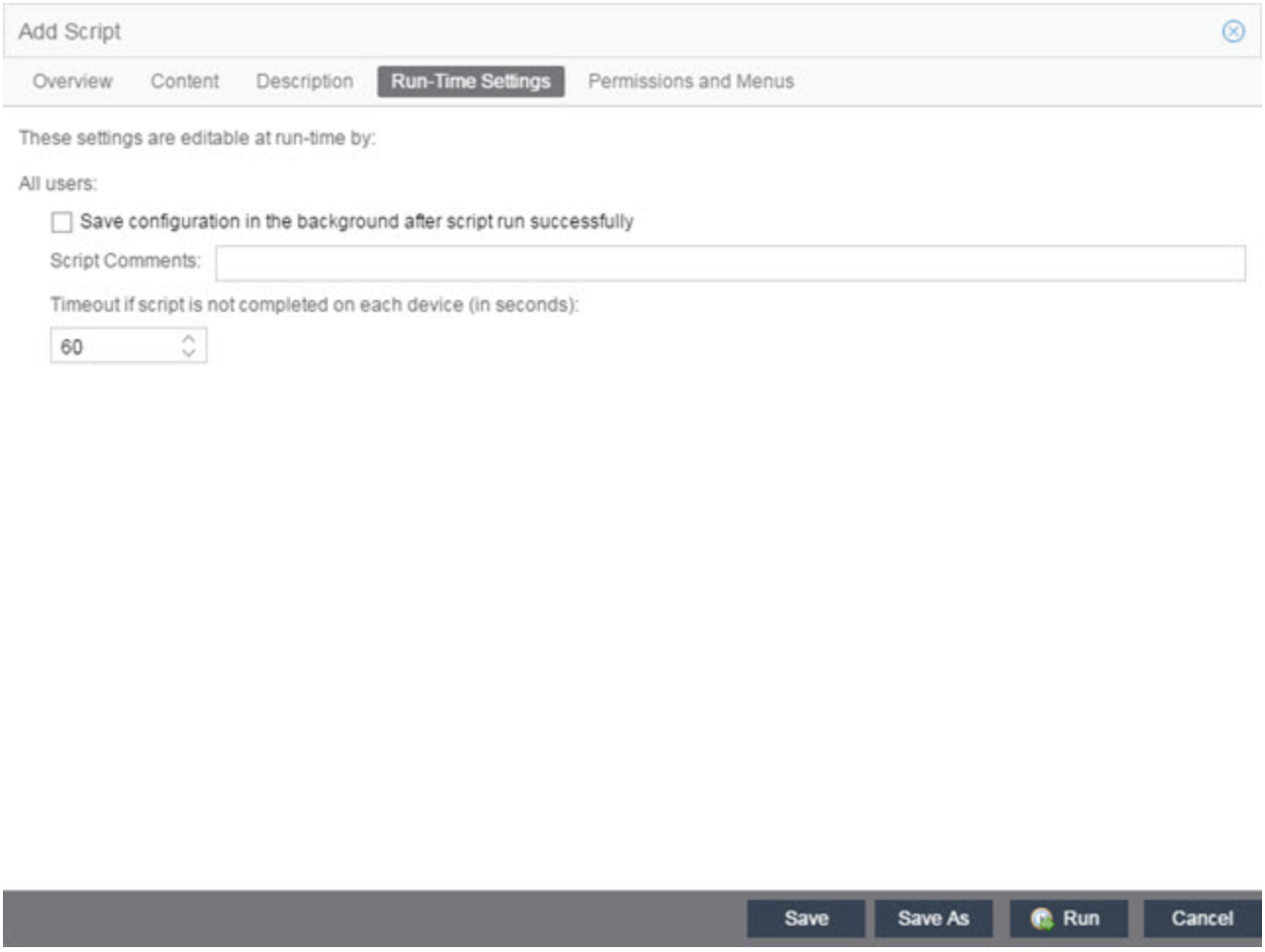
6. If you want to specify run-time settings, click the **Run-Time Settings** tab and make changes as need. For additional information, see Specifying Run-Time Settings for a Script.
7. To specify which Management Center user roles have permission to run the script, and whether or not, and where, the script appears in the menu or in a shortcut menus, click the **Permissions And Menus** tab, and make changes as needed. For additional information, see Specifying Permissions and Run Locations for Scripts.
8. Click **Save**. The Save Script dialog box appears.



9. Type a name for the script file in the **Script Name** box and, if desired, a comment about the script in the **Script Comment** field.
10. Click **Save**.
11. Click **Run** to run the script now or **Cancel** to run the script at a later time.

Specifying Run-Time Settings for a Script

To specify the run-time settings for a script, click the **Run-Time Settings** tab.



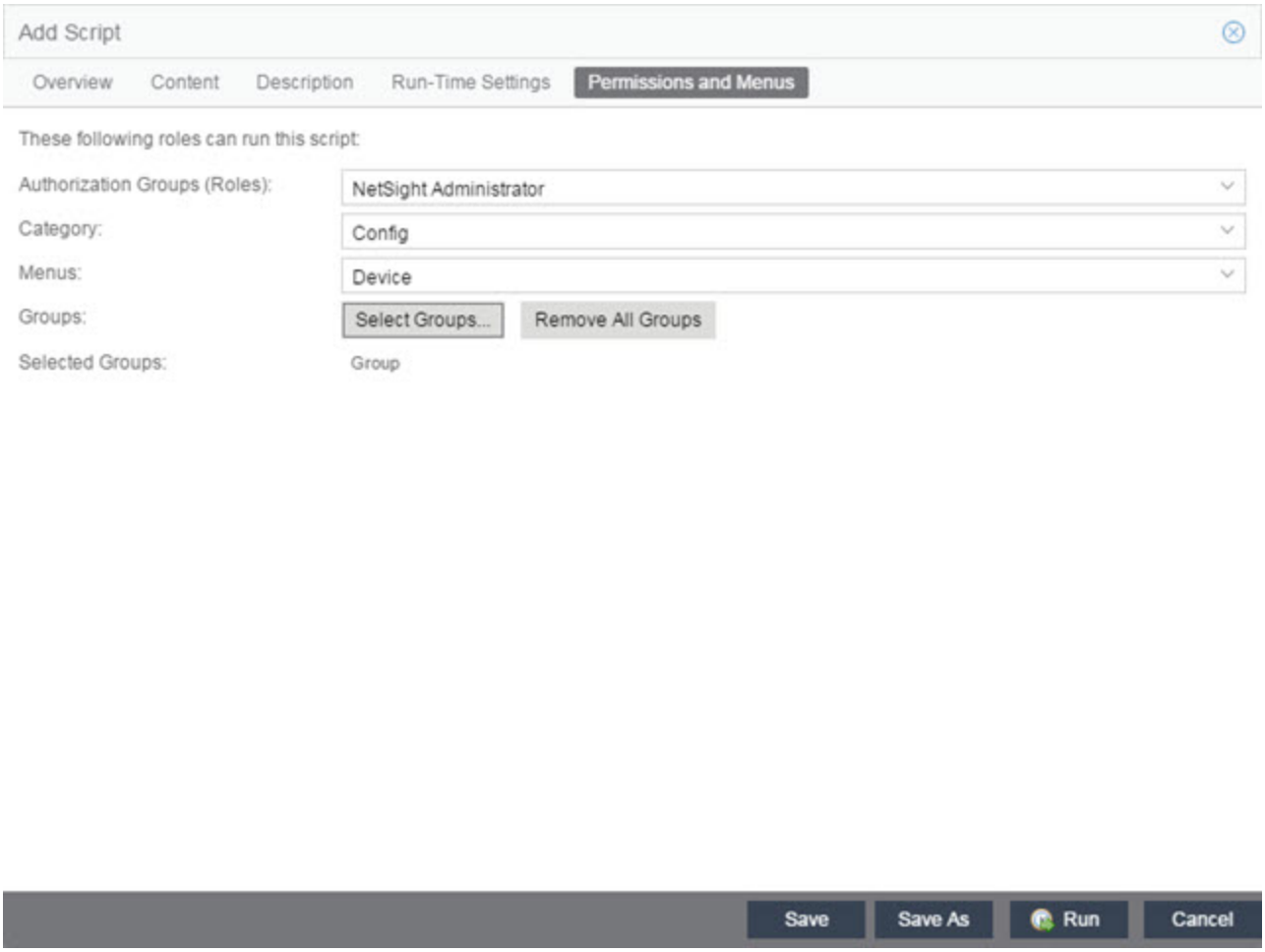
Use this tab to specify the following settings:

- Save configuration in the background after script run successfully — When selected, the configuration on the device or port is saved after the script is run successfully.
- Timeout occurs if a device does not respond within the amount of time entered (in seconds) — Use to set a maximum amount of time for the script to run on each device or port (in seconds). This timeout value applies to each device or port independently.

Specifying Permissions and Run Locations for Scripts

Specify which 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 menus.

To set permissions and menu locations for the script, click the **Permissions and Menus** tab.



- Specify the Management Center user roles able to see and run the script. Select the check boxes for the roles you wish to enable.
- Set whether or, and where, the script appears in on the menu and in shortcut menus in the given locations.

Running a Script

From the Network tab

1. Right-click the device in the Devices table or in the Device Groups left-hand panel.
2. Select a script in the Scripts menu. The Run Script window opens.

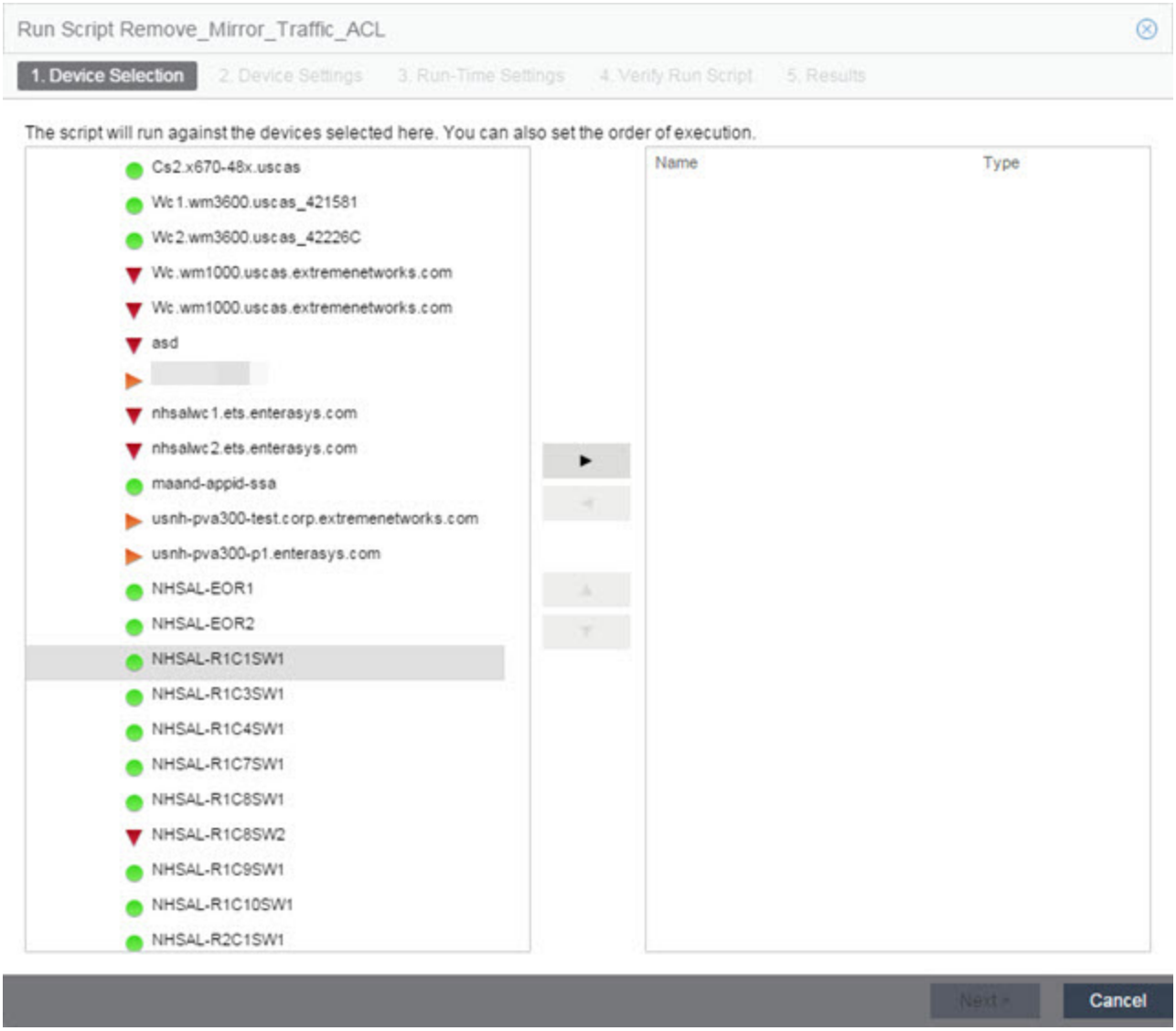
3. On the **Device Selection** tab, select the device or devices against which you want to run the script. Use the arrows to add/remove device and to control the order of the selected devices.
4. Click **Next**.
5. On the **Overview** tab of the **Device Settings** tab, set the configuration properties 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**.
7. On the **Run-Time Settings** tab, set the run-time settings for the script. For additional information, see Specifying Run-Time Settings for a Script.
    - Save configuration in the background after script run successfully — When selected, the configuration on the device is saved after the script is run successfully.
    - 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 a task — Select to run the script now and not save this 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. For additional information, 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. For additional information, see Creating Script Tasks.
8. Click **Next**. The **Verify Run Script** tab opens.
9. 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**.

From the Administration tab

1. In the Scripting tab, 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 box.
3. Select the script by clicking its row and then click Run Script. The Run Script window opens.

NOTE: Be sure to select only one script. The **Run Script** 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 device 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, set the run-time settings for the script. For additional information, see Specifying Run-Time Settings for a Script.

    - Save configuration in the background after script run successfully — When selected, the configuration on the device is saved after the

script is run successfully.

- 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 a task — Select to run the script now and not save this 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. For additional information, 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. For additional information, see Creating Script Tasks.

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**.

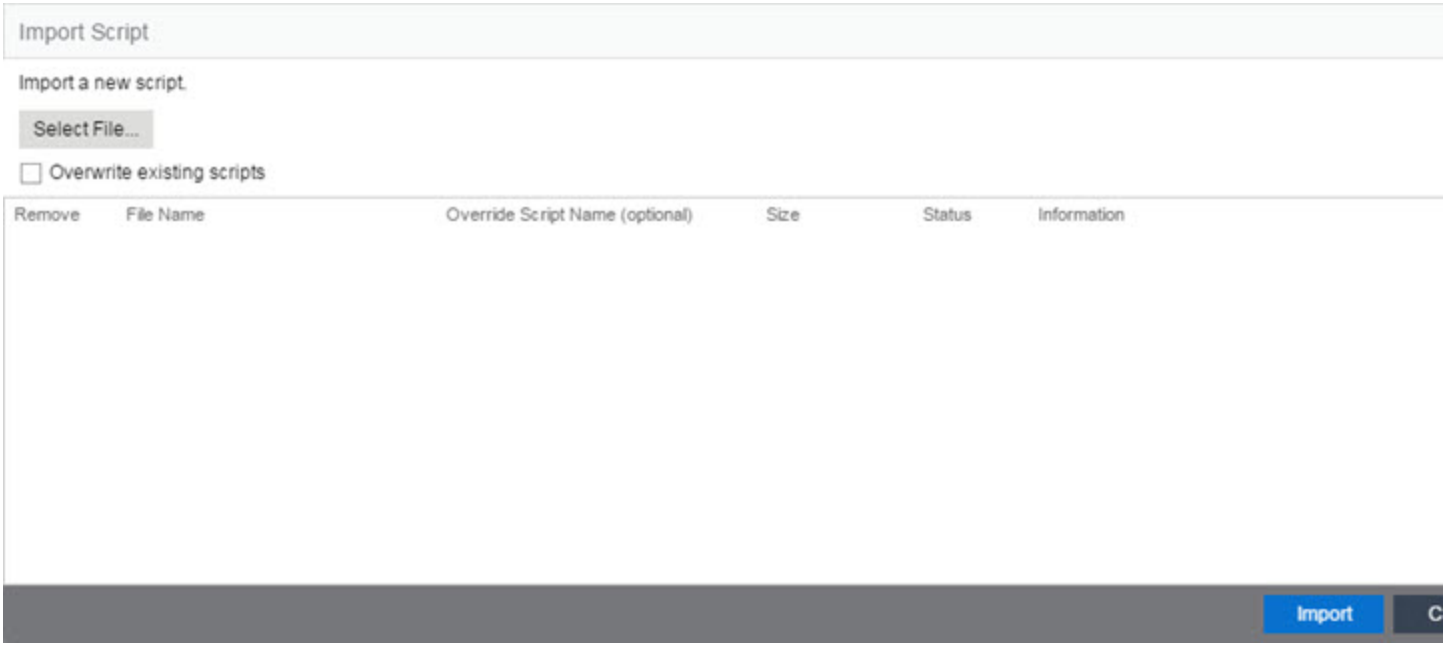
Script Results

Once a script is run, results are stored in the `~server~/appdata/scripting/tmp` folder. The folder in which script results are stored cannot be configured. An event is stored in the console.log file each time a script is executed that contains the location of the audit file. These audit logs reside in the tmp directory and remains 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 up to 1000 files. Once the number of files exceeds 1,000, the oldest 100 are deleted.

Importing Scripts into Extreme Management Center

Import XML-formatted scripts into Management Center. To import a script:

1. In the **Scripting** 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.

Exporting a Script

To export a script:

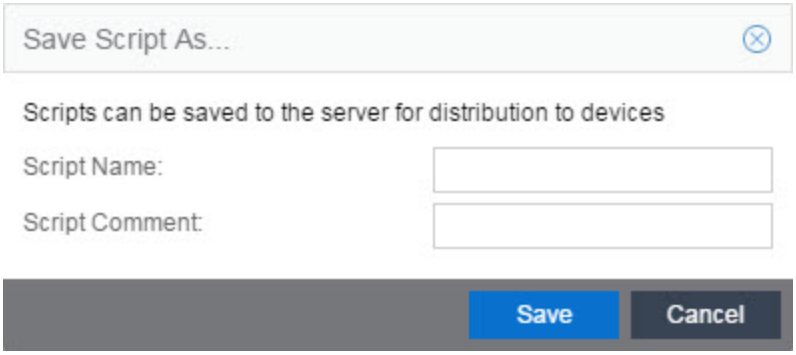
1. From the Scripting tab, select a script.
2. Click the Export button.

It is exported to your browser download directory. The script is saved in XML format.

Editing a Script

To edit a script:

1. In the **Scripting** tab, click **Scripts**.
2. In the script table, select the script you want to edit.
3. Click the **Edit** button. The script opens in the Edit Script window setting, from which you can edit the script or scripts.
4. Click **Save As**. The **Save Script As** dialog box appears.



5. Type a name for the script file in the **Script Name** box and, if desired, a comment about the script in the **Script Comment** box.
6. Click **Save**.

The edited script is saved as a new script with the **Script Name** you entered.

Deleting a Script

To delete a script:

1. In the **Scripting** tab, click **Scripts**.
2. In the script table, select one or more scripts you want to delete.
3. Click the **Delete** button.
4. Click **Yes** to confirm the script deletion.

Script Task Overview

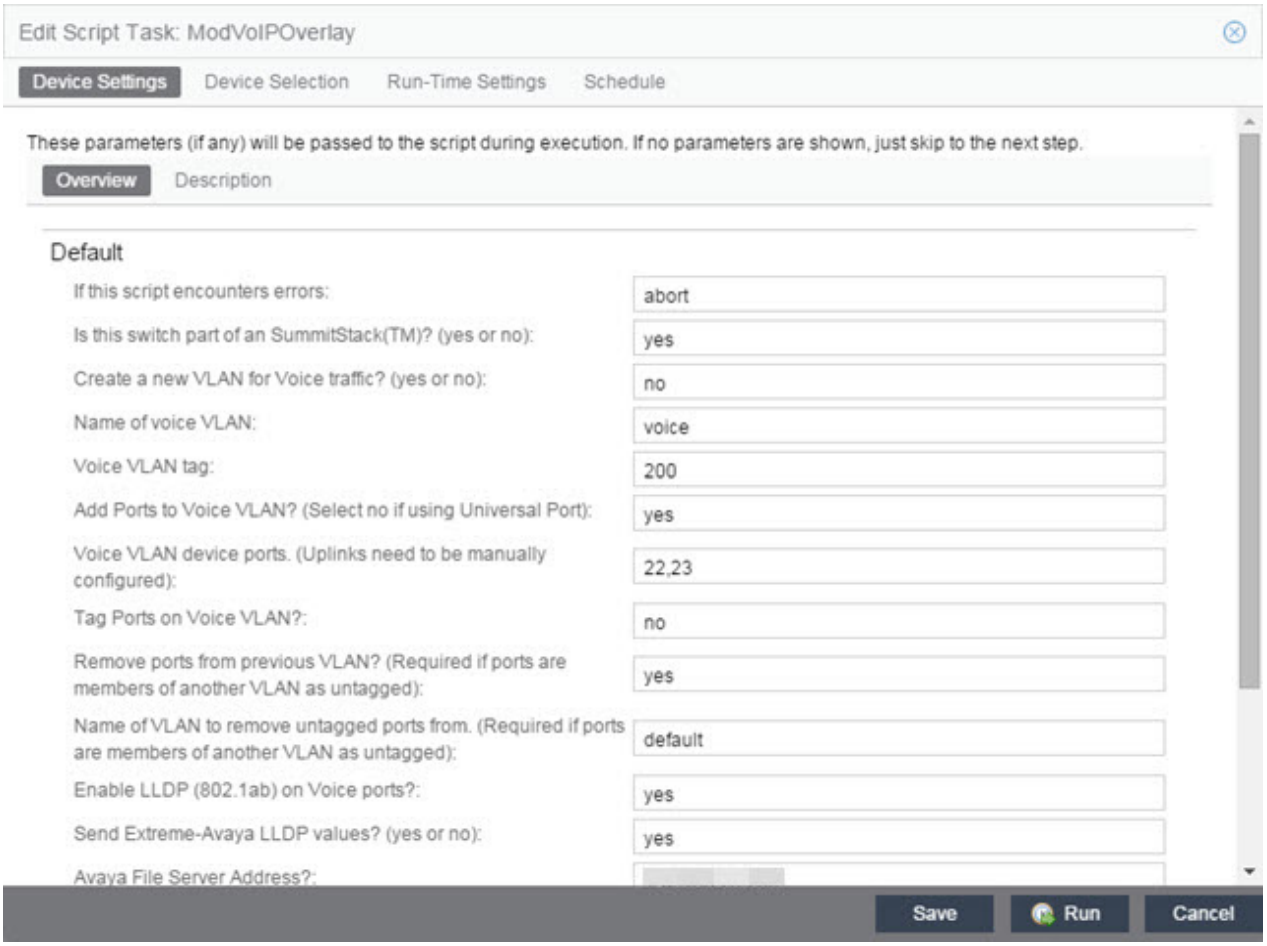
When you run a script, you can save it as a task that appears in the **Script Tasks** tab. This saves your device selections and run-time settings, and then allows you to manually run the script task at a later time or schedule it to run in the future either once, or on regular basis.

The **Script Tasks** tab allows you to change a script task's device selections and run-time settings, and specify a schedule for running it.

Creating Script Tasks

To create a script task, you need to:

1. Create a script. For additional information, see Creating a New Extreme Management Center 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. For additional information, see Running a Script.
3. Click the **Script Tasks** tab.
4. Double-click the script task or click the script task and click **Open**. The script dialog box appears (see the following figure).



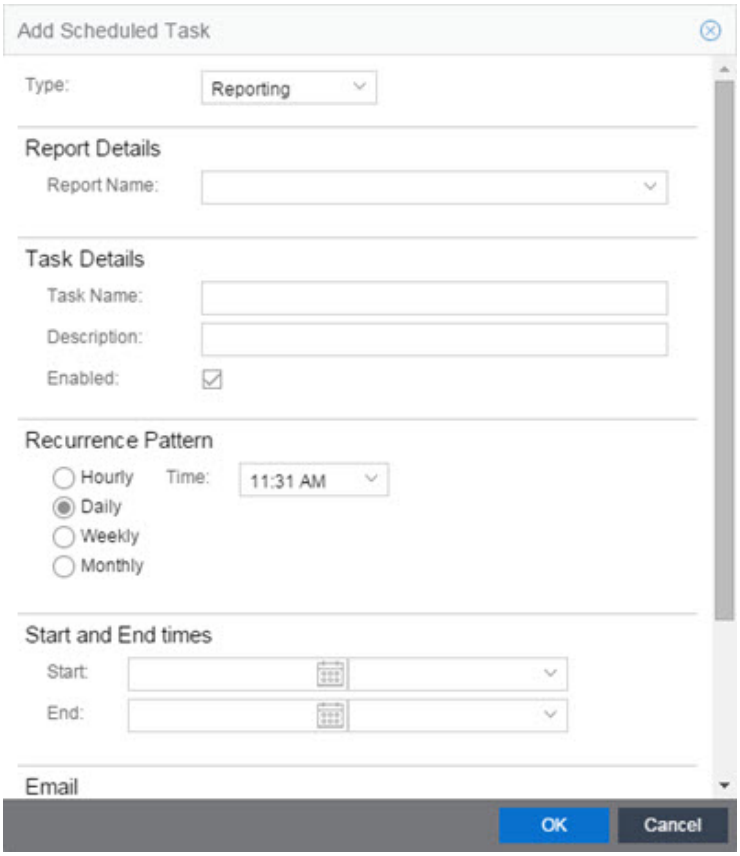
5. Add, remove, or reorder devices against which the script runs on the **Device Selection** tab, if necessary.

6. Change the run-time settings for the script on the **Run-Time Settings** tab, if necessary.
7. Click **Save** to save any changes.
8. Click **Run** to run the script task or **Cancel** to exit the script task.

The script task is created.

If you want to schedule the script task to run automatically:

9. Click on the **Scheduler** view.
10. Click the **Add** button. The Add Scheduled Task window opens, as shown in the following figure.



11. Select a Task Type:
    - **Reporting** — Sends a report via email automatically on a schedule you configure.
    - **Scripting Task** — Runs a script on a schedule you configure.

12. Select the report you want to send or the script task you want to run in the Report Details/Script Task Details drop-down menu.
13. Enter a Task Name and Description for the scheduled task in the Task Details section.
14. Select how often you want the scheduled task to run in the Recurrence Pattern section.
15. Select a start date indicating the date from which the scheduled task runs automatically and an end date indicating the date to which the scheduled task runs automatically.
16. Enter the scheduled task recipient's email address as well as the Subject and Body information you want to include in the email when the scheduled task is sent.
17. Click **OK**.

Deleting Script Tasks

If desired, delete script tasks you no longer need. To delete a script task:

1. From the **Administration** > **Scripting** tab, click the **Script Tasks** tab.
2. Select the task in the table.
3. Click the **Delete** button.
4. Remove any schedules configured (Scheduled = Recurring or One-time) with the script task by clicking the **Scheduler** tab, selecting the associated schedule, and clicking **Delete**.

Extreme Management Center Script Reference

This section contains reference information for Management Center scripts. It contains the following topics:

- Metadata Tags
- Management Center-Specific Scripting Constructs
- Tcl Support in Management Center Scripts
- Entering Special Characters
- Line Continuation Character
- Case Sensitivity in Management Center Scripts
- Reserved Words in Management Center Scripts

- ExtremeXOS CLI Scripting Commands Supported in Management Center Scripts
- Management Center-Specific System Variables

A 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 a 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 a 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. Comment on each line in the description. 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. If this is the last section of the metadata, ending with a `#@MetaDataEnd` tag, then the `#@SectionEnd` tag is not required. 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 device-specific or global (uses the same value for all devices). 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 (shows the parameter input field as a text field in the Overview tab).

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 all values by command 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 Management Center:

- Specifying the wait time between commands.
- Printing system variables.
- Configuring a carriage return prompt response.
- Synchronizing the device with 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 <

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
```

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

```
download image 10.22.22.22 t.txt <cr> //cancel download
```

Synchronizing the Device with Extreme Management Center

The PerformSync command manually initiates a synchronization for specified 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, Management Center moves on to the next command in the script without waiting for the synchronization to complete.

Examples

```
PerformSync -scope VPLS
```

Saving the Configuration on the Device Automatically

The run time settings for the script may include the option to issue the save command in the background after the script runs successfully on the device.

Printing a String to the Output File

Example

```
# Write Device IP address to file ECHO "device ip is
$deviceIP"
```

NOTE: The Tcl puts and ECHO commands have the same function. However, the ECHO command is not case-sensitive, while the puts command is case-sensitive.

Tcl Support in Extreme Management Center Scripts

The following Tcl commands are supported in 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 a Management Center script, use the backslash character (\ ) as the Escape character if you need to enter special characters, such as quotation marks (“ ”), colon (:), or 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 a Management Center script.

Line Continuation Character

The line continuation character is not supported in Management Center scripts. Place each command statement on a single line.

Case Sensitivity in Extreme Management Center Scripts

The commands and constructs in a 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 Management Center documentation.

Example (Usage of the 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 cannot be used as variable names in a Management Center script. They are reserved by Management Center.

- Names of system variables (see Management Center-Specific System Variables)
- Names of Management Center command extensions (see Management Center-Specific Scripting Constructs)
- Names of ExtremeXOS CLI commands
- Names of Tcl functions

In addition, do not use a period (.) within a variable name. Instead, use an underscore (_).

ExtremeXOS CLI Scripting Commands Supported in Extreme Management Center Scripts

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 Management Center Scripts for a list of supported Tcl commands.

Switch Compatibility

Devices running ExtremeXOS 11.6 and higher support this command.

```
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 $UPPERCASE ("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 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 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 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 hostname of the Management Center server.

$serverName
The hostname of the Management Center server.

$serverPort
The port number used by the 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 date on the Management Center server.

$vendor

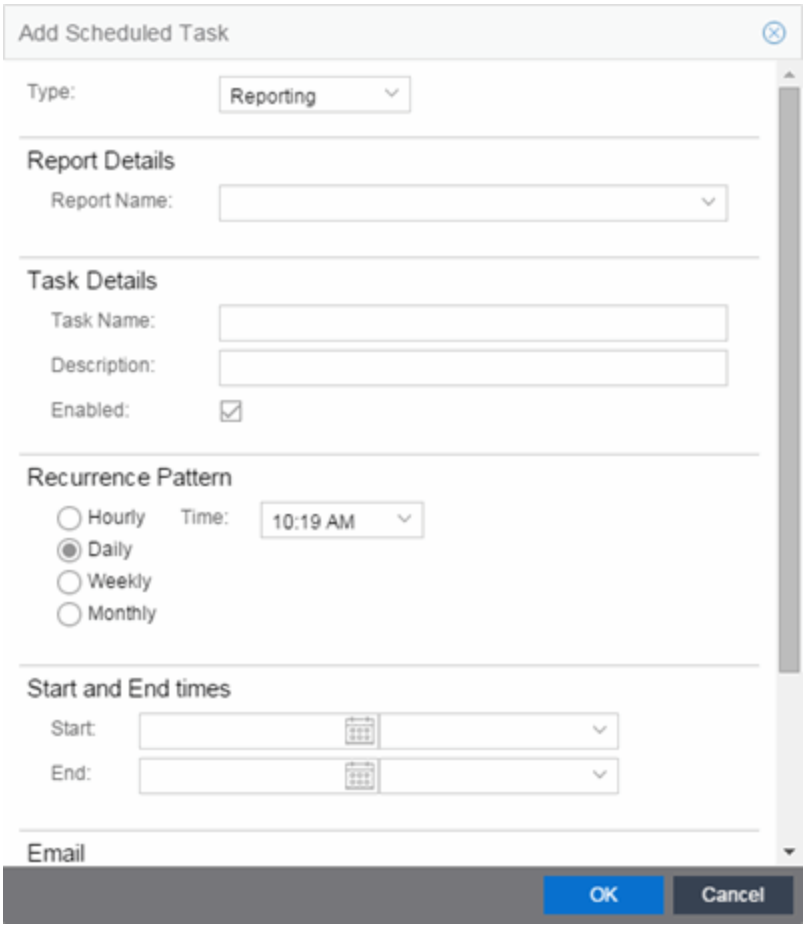
Vendor name of the device; for example, Extreme.

How to Schedule a Task

The Extreme Management Center Scheduler provides the ability to schedule automatic generation of a subset of available reports in PDF format. The reports are then emailed to a specified recipient. Report generation can be scheduled to occur on an hourly, daily, weekly, or monthly basis.

Access the Scheduler from the Administration tab.

1. Launch Management Center. In the **Administration** tab, select the **Scheduler** sub-tab.
2. Click the **Add** button. The Add Scheduled Task window opens.



3. Use the **Report Name** drop-down menu to select the report you want to generate. Depending on the type of report selected, you may need to make other selections such as specifying the source engine or controller.

4. Edit the task name and description, if desired.
5. Use the **Enabled** checkbox to enable or disable the task. A disabled task is not performed.
6. 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.
7. If desired, specify a start and end date and time for the task.
8. Enter the email address or list of email addresses (separated by semicolons) where you want the generated PDF reports sent.
9. Set your SMTP Email Server options in the Suite-Wide options.
    a. Click the **SMTP** button in the **Scheduler** tab.
    The SMTP E-Mail Server Options window opens.
    b. Define your outgoing email server, the sender's address for your email notifications, and the password.
10. Edit the subject line and enter body text for the email, if desired.
11. Click **OK**. The task appears in the Scheduled Task table.

    Use the toolbar buttons to edit, copy, or delete the task. Click the **Run** button to run the scheduled task immediately, if desired.

Related Information

For information on related topics:

- Administration

Web-Based FlexViews

Web-based FlexViews provide a convenient way for Operations people to view FlexView data without requiring access to Console. These views are accessible from Extreme Management Center Devices and do not require the installation of any software (including Management Center) other than the browser itself.

To launch a web-based 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 web-based FlexView, you must be a member of an authorization group that is assigned the OneView > FlexView > OneView FlexView Read/Write Access capability. For more information on authorization capabilities, see the Help topic, "How to Configure User Access to Extreme Management Center Applications," located in Management Center Suite-Wide Tools > Authorization Device Access.

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 web-based 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 Web-Based FlexViews

Use the following steps to launch and open a web-based FlexView from the Network tab. The maximum number of FlexViews you can open at one time is 10.

1. Launch Management Center and click on Network > Devices.
2. Select one or more devices in the Devices list. The maximum number of devices you can select for a FlexView is ten.

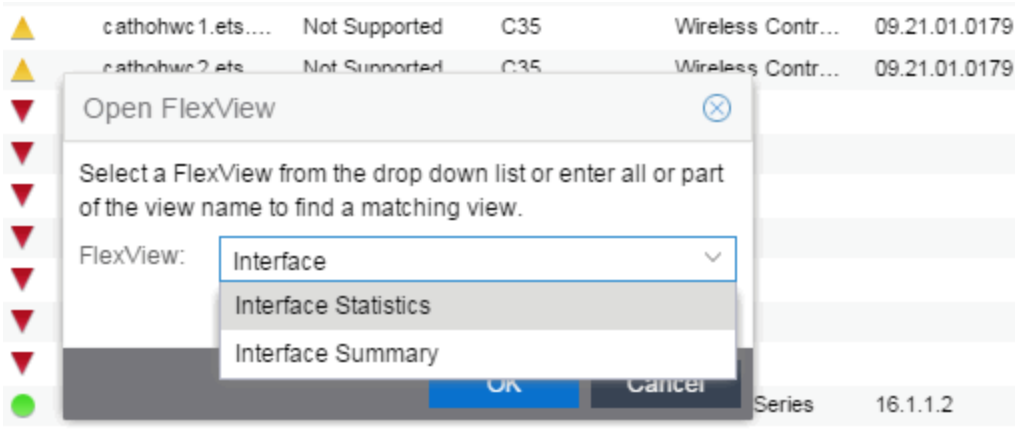
NOTE: When you select multiple devices, a web-based FlexView may take additional time to populate with data, depending on the number of rows displayed in the particular view. Because of this, we recommend that, for interface-based FlexViews, you select five devices or fewer.

---

3. Click the gear menu and select Choose FlexView from the menu. You can also click on the device Name link 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 in Console is listed for selection, including standard FlexViews and custom FlexViews you create.



   The FlexView opens in a new browser tab.

Using Web-Based FlexViews

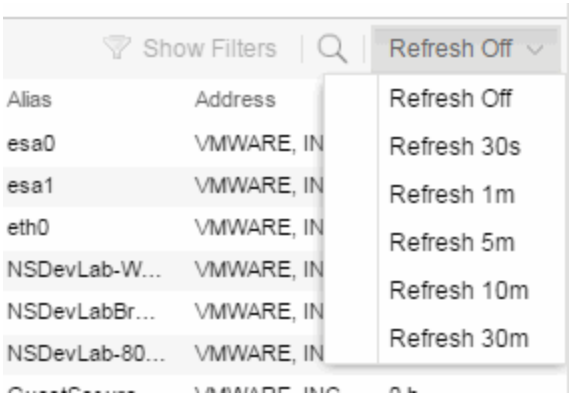
Web-based FlexViews let you manipulate the table data in several ways to customize the view for your own needs:

- 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 web-based 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.

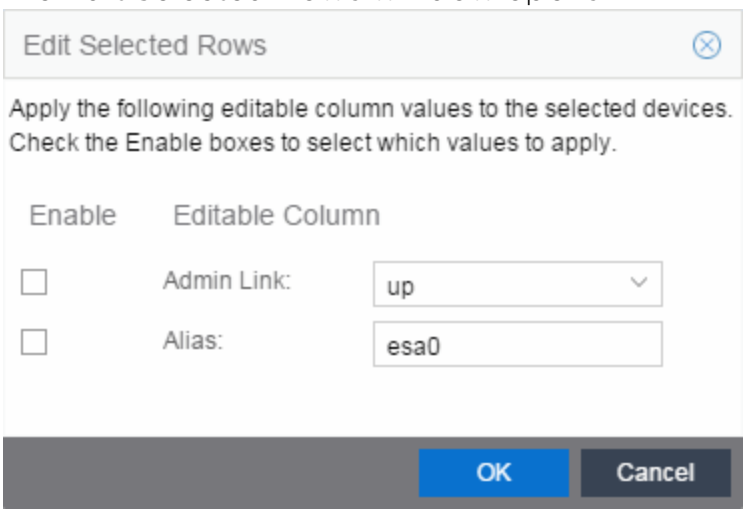


Editing Writable Values

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. Check the writeable objects you are changing and enter the appropriate values as needed.
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 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 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 Management Center Server and Wireless Controllers to communicate: SSH: 22 SNMP: 161, 162 Langley: 20506